

Staff Guide to Subject Access Requests

Context

Under data protection legislation any individual (sometimes referred to as the 'Data Subject') may request a copy of their personal information as held by the University or any of its wholly owned campus companies. Such requests are known as a 'Subject Access Request' or 'SAR' for short.

The purpose of this guide is to explain the context to such requests and to provide guidance for staff. A request can be made verbally or in writing and there is no prescribed text or form in which to make it. It is therefore essential that all staff recognise when a request is made and understand both their own and DCU's obligations when dealing with one. The University's Data Protection Unit (DPU) manages all SARs on behalf of the University and should be informed immediately on receipt of a SAR.

What can be requested?

All individuals have the right to obtain a copy of their personal data held by DCU in what is technically referred to as a 'Relevant Filing System'. To come within the scope of a SAR the personal data must have been collected by DCU with the intention of transferring it to a relevant filing system (i.e. an organised or indexed collection of records e.g. paper or electronic files, databases, CCTV recordings, audio recordings, emails). This definition therefore excludes personal data held in an informal medium (e.g. yellow sticky notes, rough writing pads etc.) as it was not created with the intention of filing to a relevant filing system. However, if handwritten notes referencing an individual in any way are maintained or indexed in an organised manner then the individual is entitled to a copy of his/her personal data contained in those notes.

On foot of an SAR, and under the legislation, individuals (also referred to as 'Data Subjects'), are entitled:

- (a) to be informed as to whether or not DCU processes their personal data;
- (b) to a copy of their personal data;

Note: however, this does not necessarily mean a copy of the actual record. For example if an individual's name is included on an email, or on a paper document from HR authorizing pay deductions along with the details of other members of staff, then they are entitled to be told about it but they are not entitled to a copy of that email or other document as personal data relating to other individuals may also be included. To give the individual the record would be a breach of the data protection rights of the other individuals also included on the record. An option in this case is to give the individual a copy of the email or document but only after ensuring that the names and personal details of other individuals have been redacted. Alternatively, the personal

Staff Guide to Subject Access Requests

data specific to the individual could be extracted from the record(s) and collated into a separate Word document which will then be given to them on foot of the SAR.

- (c) to be informed of the purposes of the processing of their data;
- (d) the categories of Personal Data concerned or processed;
- (e) the recipients, or categories of recipient, to whom the Personal Data has been or will be disclosed;
- (f) where possible, the envisaged period for which the Personal Data will be stored, or if not possible, the criteria used to determine that period;
- (g) the existence of the 'Rights of Rectification, Restriction, Erasure and Objection';
- (h) the right to lodge a complaint with the Irish Data Protection Commissioner;
- (i) where the Personal Data is not being collected directly from the Data Subject, any available information as to its source (e.g. the relevant Data Sharing Agreement);

and
- (j) the existence of automated decision-making (if applicable).

How is a Subject Access Request made?

A SAR can be made either verbally or in writing (both are legitimate) to any member of the University's staff. While the DPU's preference is for the request to be made in writing an individual is not obliged to do so and a verbal request is equally valid.

The DPU's preferred / recommended approach for making a request is:

- Apply to the DPU in writing.

The Data Subject may do this by means of the standard application form which can be found on the University website or by phone enquiry.

- Provide any details which might be needed to help the DPU locate all the personal data that DCU may possess, (e.g., previous addresses, staff/student ID #, location of relevant records in DCU units etc.); &
- Provide two proofs of their identity.

Staff Guide to Subject Access Requests

What are our obligations when processing a request?

The obligations on the University and its staff upon receipt of a SAR are as follows:

- Members of staff must inform the DPU immediately upon receipt of a SAR and it will manage / process the request.
- The University is obliged to provide a copy of the personal data within **one calendar month** unless an extension for additional time has been invoked by the DPU;
- Provide the information in a form which will be clear to an ordinary person (e.g. any internal DCU codes or annotations must be explained);
- Ensure that the personal data provided relates only to the individual who made the request or someone acting on his or her behalf and with their authority (e.g. solicitor or barrister).

Note

- A) Staff should normally not provide any personal information by phone.
- B) If the University does not hold any personal data in a relevant filing system about the individual then they should be informed as soon as possible after receipt of the SAR. All members of staff of the University are obliged to co-operate with the DPU when processing SARs.

Guidance on Emails


A particularly common issue that often arises with SARs is how are emails to be treated. Some general some principles to be aware of are as follows.

- The fact that an individual is referenced in an email does not necessarily imply that the email in its entirety is also 'personal data'.
- To qualify as personal data at least one of the following elements must be present in the email (per an Article 29 Working Party opinion):
 - **Content Element** - The data in the email refers to or is about the individual. Normal and / or routine business emails sent to or by the individual are not relevant.
 - or
 - **Purpose Element** - The data in the email is used, or is likely to be used, to evaluate or treat the individual in a certain way or to influence the status or behaviour of the individual.
 - or
 - **Result Element** - The use of the data in the email is likely to have an impact on the individual's rights and interests.

Staff Guide to Subject Access Requests

- Individuals are only entitled to their own personal data so the personal data of others within an email must not be provided. The personal data of others must either be redacted in full or alternatively the individual can be given a summary of the personal data in the email about them by way of a Word document rather than the redacted email in which it appears.
- There is no entitlement to ‘records’ under data protection law. An individual is only entitled to a copy of their personal data and this is a key distinction between Data Protection and Freedom of Information legislation. The University is entitled to extract the personal data from the relevant email or record and provide it in a summarized format as noted in the bullet point above. The right to obtain personal data does not mean the right to obtain ‘all records’ containing the personal data.
- The University has the option to supply a list of the relevant points of personal data about an individual so long as the source record is also referenced where it has not been provided.
- If the personal data is held in a backup or archived format only then there is no requirement to search these locations for personal data in response to a SAR. An example would be the redundant email account of a former member of staff who has left the University.

Version Control

| | | | |
|--------------------------|-------------------------------|-------------------------|--|
| Document Name | SAR Staff Guide | |  <p>Ollscoil Chathair Bhaile Átha Cliath Dublin City University</p> |
| Owner | Data Protection Unit | | |
| Version Reference | Original Version – 4.0 | Reviewed Version | |
| Approved by | Risk & Compliance Officer | N/a | |
| Effective Date | August 24 th 2023 | N/a | |

End.

Appendix 1 - Additional Guidance from the Irish Data Protection Commissioner's website

Exceptions to the right of access to personal data

The restrictions upon the right of access fall into five groups:

- Section 5 of the Data Protection Act provides that the right of access does not apply in a number of cases, in order to strike a balance between the rights of the individual, on the one hand, and some important needs of civil society, on the other hand, such as the need to investigate crime effectively, and the need to protect the international relations of the State.
- The right of access to medical data and social workers' data is also restricted in some limited circumstances, to protect the individual from hearing anything about themselves which might cause serious harm to his or her physical or mental health or emotional well-being.
- The right of access to academic examination results is modified slightly.
- The right of access does not include a right to see personal data about another individual, without that other person's consent. This is necessary to protect the privacy rights of the other person. Where personal data consists of expressions of opinion about the data subject by another person, the data subject has a right to that expression of opinion except where that expression of opinion was given in confidence.
- The obligation to comply with an access request does not apply where it is impossible for the data controller to provide the data or where it involves a disproportionate effort in terms of the benefits derived from the personal data being provided. However care must be taken with claiming this exemption.

Access Requests relating to Personnel Records

The Data Protection Acts apply to data held in a "relevant filing system" (electronic or manual) and, as such personnel records will therefore normally come within the terms of the Acts. No issues should generally arise in respect of access requests made for most categories of personnel records. This section seeks to address access requests for data relating to:

- 1) discipline, grievance and dismissal
- 2) appraisal and performance reports
- 3) medical reports

1. Discipline, grievance and dismissal

In relation to creating and keeping records, HR staff should be conscious of the accuracy requirement and that data kept should be "adequate, relevant and not excessive". In the case of records relating to disciplinary, grievance or dismissal processes the right of access supports fair procedures and natural justice which provide that an individual be made aware of the case s/he has to answer.

Staff Guide to Subject Access Requests

The general rule is that an employee has a right of access to personal data relating to him/her in connection with discipline, grievance and dismissal procedures, even if the disciplinary procedure is on-going or the subject of legal proceedings such as an unfair dismissals claim. There are however some limitations and exemptions to this right which are provided in Sections 4 & 5 of the Acts. These limitations and exemptions include:

(i) Opinions given in confidence

Section 4(4A) provides that personal data containing expressions of opinion about the data subject may be given to the data subject without the permission of the person who expressed that opinion but this does not include opinions “given in confidence or on the understanding that it would be treated as confidential”. Where personal data consists of an expression of opinion about the data subject by another person, the data subject has a right to access that opinion except if that opinion was given in confidence. If the opinion was not given in confidence then the possible identification of the individual who gave it does not exempt it from the right of access.

An opinion given in confidence on the understanding that it will be kept confidential must satisfy a high threshold of confidentiality. Simply placing the word “confidential” at the top of a page will not automatically render the data confidential. The Data Commissioner will look at the data and its context and will need to be satisfied that the data would not otherwise have been given but for this understanding. Supervisors and managers will not normally be able to rely on the provision as it is an expected part of their role to give opinions on staff which they should be capable of standing over. On the other hand, a colleague who reports a matter relating to an individual in confidence to a supervisor could be expected to be protected by the confidentiality provision.

(ii) Professional legal privilege

The right of access does not apply to data - "in respect of which a claim of privilege could be maintained in proceedings in a court in relation to communications between a client and his/her professional legal advisers or between those advisers." (Section 5(g))

Accordingly, the subject access provisions in section 4 of the Acts do not apply to personal data where the circumstances are such that a claim of privilege could be maintained in court proceedings in relation to communications between a client and his professional legal advisers or between those advisers.

This is a limited exemption which only applies in connection with the provision of legal advice or in anticipation or furtherance of litigation.

(iii) Protecting the source of data

Section 4(1)(a)(iii)(II) provides that the source of the data does not have to be provided if to do so would be contrary to the public interest. This would apply in situations where revealing the source of the information would be a disincentive to others providing similar information in the future. Examples would be “whistleblowers” or the reporting of child abuse.

Staff Guide to Subject Access Requests

(iv) Investigation of an offence

If access would or potentially could prejudice a criminal investigation, access may be refused pursuant to section 5(1)(a) of the Acts. This provides that “this Act does not apply to personal data kept for the purpose of preventing, detecting or investigating offences...in any case in which the application of that section (viz. section 4) to the data would be likely to prejudice any of the matters aforesaid”.

(v) Other exemptions under Section 5

Section 5 also provides exemptions from access in other circumstances including:

- estimates of liability in respect of a compensation claim
- back-up data

Note: A Data Controller such as DCU is not obliged to search through backups, in either electronic or paper form, for data relating to an individual. An example of this are emails which now exist solely in backups maintained by ISS. However if a copy of the email is still on another staff member’s email account it will fall under the access request.

2. Appraisal, Performance Reports and References

The right of access applies to Appraisal and Performance Reports and the Commissioner considers that the confidentiality provision of section 4(4A)(b)(ii) cannot reasonably be applied to them.

In regard to references, it is often said that these are given in confidence. Notwithstanding this, the Commissioner considers generally that the right of access applies to them. There would need to be particular exceptional circumstances which would cause the Commissioner to be satisfied that the data would not otherwise have been given but for this understanding

3. Medical reports

The Data Protection (Access Modification) (Health) Regulations, 1989 (S.I. No. 82 of 1989) provide that health data relating to an individual should not be made available to that individual, in response to an access request, if that would be likely to cause serious harm to the physical or mental health of the data subject. A person who is not a health professional should not disclose health data to an individual without first consulting the individual’s own doctor or some other suitably qualified health professional.

Staff Guide to Subject Access Requests

An employee has a right of access to medical data held by the organisation's company doctor or medical officer, unless the "harm" exemption, detailed above, applies. Experience is that such situations are rare.

Organisations should have a procedure in place so that when HR data is requested, clarification is sought as to whether the request includes medical data. If medical data is being sought, HR should advise the Company Doctor/Medical Officer who should make the data available to the employee directly.

End.