General Data Protection Regulation ("the GDPR") Individuals Rights

Author	Head of Information Assurance and Governance
Approved by	
Approval date(s)	May 2018
Review date	May 2019
Version	1.0
Document type	Guide
Activity/Task	Information governance and security
Keywords	GDPR, DPA 2018
Confidentiality	PUBLIC

Version Control Table

Version Number	Purpose / Changes	Author	Date
1.0	First version.	C Milne	25 May 2018

Contents

Introduction

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

This guide explains these rights, the circumstances where these are/are not available and how to exercise these with the University.

1 The right to be informed

One of the principles of data protection legislation is transparency, with one of the data protection rights being the right to be informed. This means that organisations that collect/receive personal data must clearly and fully inform the individuals concerned, in writing, normally at the point when personal data is being collected, how their personal data will be used. 'Privacy information' is normally presented in a privacy notice. There are a few circumstances when organisations do not need to provide people with a privacy notice, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.

A privacy notice should:

- confirm the identity of the organisation that is responsible for making use of personal data in line with the data protection legislation, along with providing the contact details of who to approach with questions on how such data is managed;
- set out how personal data will be used and the legal basis underpinning that use;
- identify other organisations and/or individuals that personal data may be shared with (recipients);
- note when personal data may be transferred to a country outwith the European Economic Area and what protections will be put in place to safeguard those data;
- state how long personal data will be retained, or, where that is not possible, the criteria used to determine this;
- summarise the rights available to individuals under data protection legislation and explain how those rights can be exercised;
- advise on the right of complaint to the data protection regulator i.e. the UK Information Commissioner's Office ("the ICO");
- note where there are any statutory or contractual obligations to provide an organisation with personal data; and
- confirm where automatic decision-making takes place, including the provision of details of profiling and any consequences of such uses.

The privacy notices in use by the University are available from the University website, from: https://www.st-andrews.ac.uk/terms/data-protection/.

In some instances summary privacy notices will be made available at the point where personal data are collected from the University, either electronically e.g. when applying for a job, online or in paper as part of an application e.g. joining the Library as an external reader.

Privacy notices are all subject to periodic review and as such, you may wish to consult these from time to time. If significant changes are made to privacy notices then you will be advised, normally through articles in University newsletters such as 'In the Loop.'

2 The right of access

The right of access, commonly referred to as subject access or a subject access request, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why an organisation is using their personal data, and to understand if that use is lawful.

2.1 What information can you expect to receive?

Individuals have the right to obtain:

- confirmation that their personal data is being processed/used by the University;
- a copy of their personal data; and
- supplemental information, which includes many of the elements of a privacy notice e.g. details of how the personal data are used, the legal basis for making use of personal data and who data is shared with.

2.2 Subject access request form

A subject access request form is available from the University's website. While this form does not have used, completing it may help to process requests more promptly, ensuring that all of the necessary information to identify the requestor and the information they seek is provided.

2.3 How will personal data be provided?

Where request are made via email, then unless it is specified otherwise, responses will be made electronically in a '.pdf' file format. It may be necessary to encrypt files by applying a password; which helps to maintain the privacy and confidentiality of personal data.

GDPR encourages organisations to provide people with access to their own personal data via self-service facilities, of which there are several in the University for students and staff.

2.4 How long will it normally take for a response to be made?

The University must respond to requests within one month of receipt. The clock starts ticking the day after a request was received and stops on the corresponding calendar date in the following month. There are some variations to this, i.e. if the:

- following month is shorter (and there is no corresponding calendar date), the date for response will be up to the last day of the following month and
- corresponding date falls on a weekend or a public holiday, the response can be made until the next working day.

2.5 The circumstances in which the time to respond to a request can be extended

The time to respond can be extended by a further two months if the request is complex or where multiple requests have been made by the same individual. Where an extension is to be put in place, the University will let the individual know within one month of receiving their request and explain why the extension is necessary.

2.6 Requests made about others

The GDPR does not prevent an individual making a subject access request via a third party. This could be a solicitor acting on behalf of a client. In such cases, the University will need 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.

2.7 When a subject access request contains personal data about other people

The right of subject access only extends to an individual's own personal data. However, when responding to a subject access, on occasion a request may involve information that relates both to the individual making the request and to another individual(s). The Data Protection Act 2018 states that personal data of a third party should not be disclosed in response to a subject access request if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose personal data which includes information about the requestor and another individual the following factors are to be taken into account:

- the type of information that would be disclosed;
- any duty of confidentiality owed to the other individual;
- whether it is reasonable to seek the other person's consent or if the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

2.8 Can a subject access request be refused?

- Yes, where the request is fund to be manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. If a request is refused, then an explanation must be given.

3 The right to rectification

If personal data is inaccurate, out of date, or incomplete, individuals have the right to correction, update or completion of that data. Collectively this is referred to as the right to rectification. Rectification may involve filling the gaps i.e. to have to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve adding a supplementary statement to the incomplete data to highlight any inaccuracy or claim thereof.

This right only applies to an individual's own personal data; a person cannot seek the rectification of another person's information.

3.1 What is the definition of inaccurate personal data?

The Data Protection Act 2018 defines inaccurate personal data as:

- "*"inaccurate", in relation to personal data, means incorrect or misleading as to any matter of fact*."

This may mean that opinions cannot be disputed under this right. Guidance from the UK Information Commissioner notes that:

- "*Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified*."

3.2 When will the right to rectification not apply?

This right is not available when:

- The legal basis for processing the personal data is either -
  - Legal obligation; or
  - Public task.
- The Data Protection Act 2018 contains exemptions i.e. situations where this right is not available, these are:
  - public health reasons;
  - archiving in the public interest, scientific or historical research purposes or statistical purposes and erasure would seriously impair these objectives;
  - for the establishment, exercise or defence of legal claims; and
  - for journalistic, academic artistic or literary purposes.

3.3 Other circumstances where the right to rectification may not be available

If a request for rectification is found to be manifestly unfounded or excessive, taking into account whether the request is repetitive in nature, then it can be refused.

3.4 Refusing a request to rectification

If a request is refused then within one month of receipt of the request the University will confirm in writing the:

- reasons for refusal;
- right to make a complaint to the ICO; and
- ability to seek to enforce this right through a judicial remedy.

4 The right to erasure (right to be forgotten)

The right to be forgotten is set out in Article 17 of the GDPR, in certain circumstances people can ask for their personal data to be erased from the records held by organisations. However this is a qualified right; it is no absolute, and may only apply in certain circumstances.

4.1 When may the right to erasure apply?

- the personal data is no longer necessary for the purpose for which it was originally collected or processed for;
- consent was the lawful basis for processing personal data and that consent has been withdrawn. NB the University relies on consent to process personal data in very few circumstances;
- the University is relying on legitimate interests as a legal basis for processing personal data and an individual has exercised the right to object (Article 21 GDPR), and it has been determined that the University has no overriding legitimate grounds to refuse that request;
- personal data are being processed for direct marketing purposes e.g. a person's name and email address, and the individual objects to that processing;
- personal data have not been processed lawfully i.e. the University does not have an appropriate legal basis to for retaining (holding) or using the data e.g. contract was the legal basis for retaining and using personal data - the contract is no longer in force and the time period when a civil claim can be made (normally 5 years) has since passed; and
- there is legislation that requires that personal data are to be destroyed.

4.2 When does the right to erasure not apply?

The right will not apply, when it is necessary for an organisation to make use of personal data for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation e.g. tax legislation requires that certain financial records are kept for a number of years;
- for the performance of a task carried out in the public interest or in the exercise of official authority. NB the core missions of the University i.e. teaching, learning and research and other elements such as management of the institutions property and resources, maintaining a register of graduates (the General Council Register) are established as public tasks, through the authority provided in the Universities (Scotland) Acts;
- 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 established grounds where the right will not apply to personal data with the designation "special category", which includes information about a person's racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, physical and mental health or sex life or sexual orientation. These are:

- public health purposes that are in the public interest e.g. protecting against serious disease with the potential to cross boarders; and
- preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies 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 state registered health professional).

4.3 Other circumstances where the right to rectification may not be available

If a request for rectification is found to be manifestly unfounded or excessive, taking into account whether the request is repetitive in nature, then it can be refused.

4.4 Refusing a request to rectification

If a request is refused then within one month of receipt of the request the University will confirm in writing the:

- reasons for refusal;
- right to make a complaint to the ICO; and
- ability to seek to enforce this right through a judicial remedy.

5 The right to restrict processing

Where the use of personal data is in dispute e.g. there is a claim that personal data are inaccurate, the right to restrict processing may then apply. This means that an individual can limit the way that an organisation uses their personal data. This is an alternative to requesting the erasure of their data. If the right to restrict processing is available and applied, then the University can continue to retain/store personal data, however, no other use of the data can be made until such times as a restriction is lifted. In most cases a restriction will only apply for a limited time period.

5.1 When may the right to restrict apply?

- a person contests the accuracy of their personal data and the University then needs to verify the accuracy of that data;
- the data has been unlawfully processed i.e. there is no lawful basis available that can be applied to validate the University's use of that personal data, and the person concerned does not wish for their data to be erased and requests the right of restriction as an alternative;
- the University no longer needs the personal data, but an individual needs their data to be retained in order to establish, exercise or defend a legal claim e.g. this could apply to CCTV footage; or
- an individual has exercised their right to object (Article 21(1) GDPR) (see below) and the University is in the process of considering whether there are legitimate grounds that would allow for the right to object to be refused.

5.2 How would a restriction be applied to the use of personal data?

Restrictions may involve:

- temporarily moving the personal data to another system e.g. taking data from the student record system and placing this into an archive, from which the data may be returned to the live system after a restriction is lifted;
- making the data unavailable to users; or
- temporarily removing published data from a website.

5.3 What use of restricted data can be made?

The University can only retain/store personal data that is subject to a restriction, unless:

- consent has been given for specific use other than storage;
- the personal data are required for the establishment, exercise or defence of legal claims;
- it is necessary to use the personal data to protect the rights of another person (natural or legal); or
- there are reasons of important public interest.

5.4 When can a restriction be lifted?

Restrictions will normally be temporary when the accuracy of personal data are being contested, or when an objection to the use/processing of data has been made and an assessment of where the legitimate interest to further use may lay is being considered. Once decisions on either of those questions have been settled then a restriction can be lifted, however before doing so the University must inform the person concerned.

5.5 Circumstances where the right to restriction may not be available

If a request for restriction is found to be manifestly unfounded or excessive, taking into account whether the request is repetitive in nature, then it can be refused.

5.6 Refusing a request to restriction

If a request is refused then within one month of receipt the University will confirm in writing the:

- reasons for refusal;
- right to make a complaint to the ICO; and
- ability to seek to enforce this right through a judicial remedy.

6 The right to portability

Individuals have the right to get some of their personal data from an organisation in a way that is accessible and machine-readable, for example as a csv file. Associated with this, individuals also have the right to ask an organisation to transfer their personal data to another organisation. However, the right to portability:

- only applies to personal data which a person has directly given to the University in electronic form; and
- onward transfer will only be available where this is “technically feasible”.

6.1 When may the right to portability be available?

Requests can be made where:

- personal data have been made available to the University in electronic form under the legal basis of consent or contract; and
- the personal data are processed by automated means i.e. paper files/records are excluded from this right.

6.2 Circumstances where the right to portability may not be available

If a request for restriction is found to be manifestly unfounded or excessive, taking into account whether the request is repetitive in nature, then it can be refused.

6.3 Refusing a request to portability

If a request is refused then within one month of receipt the University will confirm in writing the:

- reasons for refusal;
- right to make a complaint to the ICO; and
- ability to seek to enforce this right through a judicial remedy.

7 The right to object

In some circumstances, individuals have the right to object to the processing if the University agrees to an objection, it must stop using the personal data for that purpose unless it can give strong and legitimate reasons to continue to make use of the data, despite the objections that were raised.

Individuals have an absolute right to object to an organisation using their personal data for direct marketing – in broad terms this means promoting an organisations aims and objectives and trying to sell things. Once such an objection is raised use of personal data for direct marketing purposes must stop.

7.1 When may the right to object be available?

Individuals can only object to their personal data being used by the University, where this is used for the legal basis of:

- a task carried out in the public interest;
- [the University's] legitimate interests;
- scientific or historical research, or statistical purposes, or
- direct marketing.

When raising an objection, an individual must give specific reasons why they are objecting to the processing of their personal data. These reasons should be based upon their particular situation.

7.2 Under what grounds could the objection to the use of personal data be refused?

Other than objection to direct marketing, which is an absolute right that must be acted upon, when raised, the University can refuse a request for objection where:

- it can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

7.3 Refusing a request to objection

If a request is refused then within one month of receipt the University will confirm in writing the:

- reasons for refusal;
- right to make a complaint to the ICO; and
- ability to seek to enforce this right through a judicial remedy.

8 Rights in relation to automated decision making and profiling.

Individuals have the right to object to automatic decision making and profiling. Presently the University does not have such processes in operation; should it do so then that will be made known in the relevant privacy notice(s).

9 How long will it normally take for a response to be made?

The University must respond to requests within one month of receipt. The clock starts ticking the day after a request was received and stops on the corresponding calendar date in the following month. There are some variations to this, if the:

- following month is shorter (and there is no corresponding calendar date), the date for response will be up to the last day of the following month and
- corresponding date falls on a weekend or a public holiday, the response can be made until the next working day.

10 Contacts/further information

Please contact dataprot@st-andrews.ac.uk if you have any questions or require more information about the rights available to you under GDPR.