ÚDARÁS UCHTÁLA na hÉIREANN
THE ADOPTION AUTHORITY of IRELAND

Data Subject Rights Policy

Version	Approved by	Approved Date	Revision Date
1.0	Board	28 November 2018	June 2019

Table of Contents

1. Introduction

This policy sets out the procedures to be followed in the Adoption Authority of Ireland when handling and responding to requests for Subject Access Rights under GDPR made by the data subjects, their representatives or other interested parties.

This policy explains the rights of individuals with respect to their personal data and clarifies what the Authority must do to comply with its duties as a data controller.

This Subject Access Rights covered in the policy are:

- The Right to be Informed
- Subject Access Requests (Article 15)
- Requests for Data Erasure also referred to as the Right to be Forgotten (Articles 17 & 19)
- Requests for Data Rectification (Article 16)
- Requests for Restriction of Processing (Articles 18 & 19)
- Data Portability (Article 20)

Policy Scope

This policy sets out the procedures to be followed by the Authority to ensure it complies with its obligations under Articles 15, 16, 17, 18, 19 and 20 of the GDPR.

For information to be deemed personal data, it must *relate to* a living individual and allow that individual to be *identified* from it, either on its own or along with other information likely to come into the Authority's possession.

Requests may be received from employees or from any other individual that the Authority has had dealings with and about whom the Authority holds data. This includes information held both electronically and manually and includes personal information recorded within electronic systems, spreadsheets, databases, paper files and photographs.

Definitions

The following definitions of terms used in this policy are provided to ensure clarity to the reader.

The **"Data Controller"** is the natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the *purposes and means* of the processing of personal data.

"**Filing system"** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

“Personal Data” is 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.

“Processing” is defined as any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Subject Access Request” - subject access request (SAR) is simply a written request made by or on behalf of an individual for the information about them, which is held by the Authority.

“Recipient” - means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

2. Subject Access Requests under the GDPR (Art15)

Requests made under Art 15 must be made in writing - this may be by letter or email. GDPR allows for the use of social media, such as Facebook or Twitter, however the Authority is not on any social media platform so the references to social media platforms to not apply.

Where the applicant is not able to make the request in person they may nominate someone to act on their behalf.

The applicant must provide proof of their identity and provide sufficient information to allow the Authority locate the record or information requested.

Where a representative is acting on behalf of the applicant the representative must provide proof of their own identity and proof that they have the right of access to the other person's personal information.

There is no fee involved for a Subject Access Request, except where the request is deemed manifestly unfounded or excessive.

All Subject Access Requests received must be forwarded to the Data Protection Officer in the first instance.

All requests must be responded to by the Authority within 30 days of receipt of the request.

Responses to Subject Access Requests must be sent by a secure methodology.

Recording Subject Access Requests

All requests received will be logged in the Subject Access Request Register detailing:

- Date received;
- Date response due (within 30 days unless complex);
- Applicant's details;
- Information requested;
- Exemptions applied in respect of information not to be disclosed, where applicable;
- Details of decisions to disclose information without the data subjects consent, where applicable;
- Details of information to be disclosed and the format in which it was supplied;
- When and how information was supplied to the applicant, for example, in paper copy and postal method used to send the information. Where information is to be posted to the applicant Registered Post will be used unless the applicant requests otherwise.

Exceptions to Subject Access Requests

The scope of the obligations and rights provided for in the following Articles may be restricted by way of a legislative measure:

- 12 to 22 (Rights of the Data Subject)
- Article 34 (Communication of a personal data breach to the data subject)
- Article 5 (Principles relating to processing of personal data) in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22.

Article 23, sets out an exhaustive list of requirements which must be met to lawfully impose a restriction. The Article also confirms that any measure used to restrict the rights of a data subject must be of limited scope and applied in a strictly necessary, proportionate and specific manner. such restrictions should respect the essence of the fundamental rights and freedoms and be a necessary and proportionate measure in a democratic society to safeguard:

- National Security;
- Defence;
- Public Security;
- The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
- Other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;
- The protection of judicial independence and judicial proceedings;
- The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- A monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority;
- The protection of the data subject or the rights and freedoms of others;
- The enforcement of civil law claims.

In particular, any legislative measure shall contain specific provisions at least, where relevant, as to:

- The purposes of the processing or categories of processing;
- The categories of personal data;
- The scope of the restrictions introduced;
- The safeguards to prevent abuse or unlawful access or transfer;
- The specification of the controller or categories of controllers;

- The storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
- The risks to the rights and freedoms of data subjects; and
- The right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

Rights of access by the data subject

The data subject shall have the right to obtain from the Authority confirmation as to whether or not personal data concerning him or her are being processed. Where that is the case the data subject shall have the right to access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller Subject Access Request or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with the Data Protection Commission;
- where the personal data are not collected from the data subject, any available information as to their source;
- where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 25 relating to the transfer.

The Authority shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

The right to obtain a copy referred to above shall not adversely affect the rights and freedoms of others.

Exemptions to Subject Access Requests

Under the current data protection legislation, the exemptions are extremely narrow and only apply in very limited circumstances. The following exemptions may be available:

- An opinion given in confidence (this would not apply to manager comments on a staff member);
- Third party data within the data (this data should just be redacted, and the rest supplied);
- Multiple requests from the same person (the organisation can wait a reasonable interval before having to respond to the exact same data access request);
- Data relating to the investigation of a criminal offence (where it would prejudice the investigation);
- Where legal professional privilege applies to the data (for example communications between the organisation and its legal advisors for the purposes of obtaining legal advice);
- Certain health data (where its disclosure is likely to cause serious mental or physical harm to the person);
- A disproportionate effort would be involved (this is an extremely high threshold to reach).

Requests made about or on behalf of other individuals

A third party, for example a solicitor, may make a valid Subject Access Request on behalf of an individual. However, where a request is made by a third party on behalf of another living individual, appropriate and adequate proof of that individuals' consent or evidence of a legal right to act on behalf of that must be provided by the third party, for example Power of Attorney.

Where the Authority thinks that an individual may not understand what information would be disclosed to a third party who has made a Subject Access Request on their behalf, the Authority 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.

Data Subject Access Requests Procedure

The Authority must act on a request for Subject Access Request from a data subject unless they are unable to establish their identity.

The procedure for responding to Data Subject Access Requests is set out below and expanded on in Table 1. The specifics of each step will vary depending on the request and the systems where the data is held.

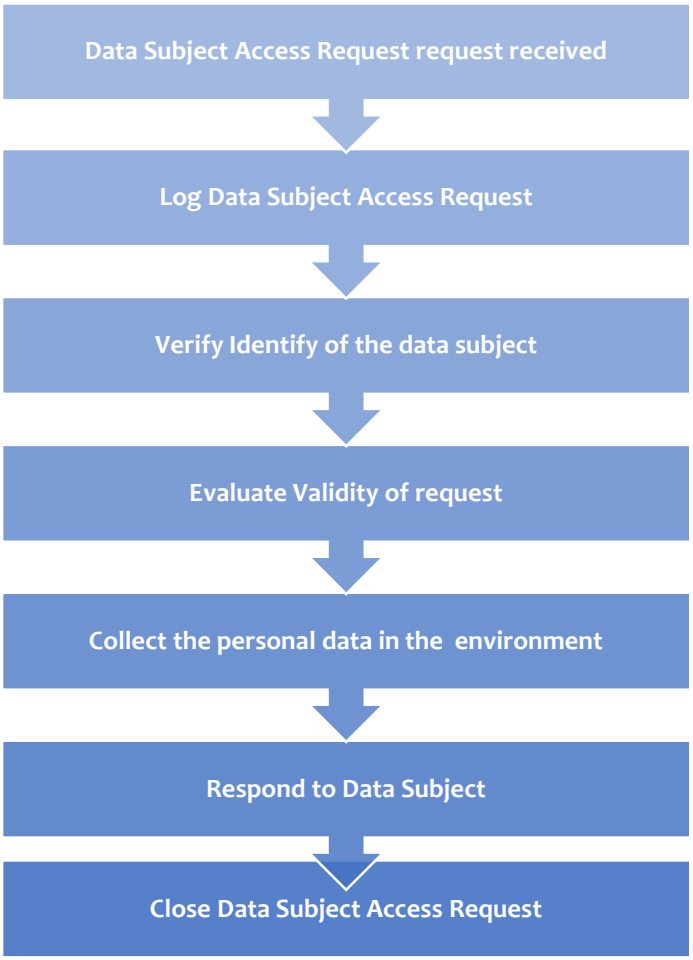


Table 1

Step	Description
Data Subject Access Request received	The Data Subject submits a Subject Access Request via email or website or by letter using the Subject Access Request Form. The Request is sent to the Data Protection Officer.
Log Data Subject Access Request.	The Data Protection Officer logs the Request in the Data Subject Access Request Register and the date of the request is recorded.
Verify Identity of the data subject	The identity of the data subject is confirmed by production of passport, drivers licence etc. If necessary additional information may be requested to confirm identity. If the identity of the data subject cannot be confirmed the request can be rejected and the reason for this communicated to the data subject.
Evaluate Validity of request	Data Protection Officer will establish if the Authority holds the data requested.
Locate the personal data	Data Protection Officer will work with unit managers to locate the relevant information.
Compile requested Personal Data	Unit managers will compile the personal data as requested. The Data Protection Officer will establish what information is to be released. In instances where information is not to be released the legal basis for any such exception or exemption will be established.
Respond to Data Subject	The response will be sent to the data subject. The data subject will be advised of their right to appeal any decision made with respect to the data released or not released as appropriate.

Close Data Subject Access request	The response to the request is logged in the Data Subject Request Register. The request will remain open until such time as the date for appeal has passed, or in the case of an ongoing appeal, until such time as the appeal process is concluded. The date of closure will be entered onto the Register. Documents provided as identification for the request will be destroyed.

ÚDARÁS UCHTÁLA na hÉIREANN
THE ADOPTION AUTHORITY of IRELAND

Data Protection
Subject Access Request (SAR)
Application Form

Request for access to Personal Data under the General Data Protection Regulation (GDPR) and Data Protection Acts 1988-2018.

Notes:

1. **In order to respond to your request for personal data, you will need to provide us with adequate Proof of Identity:**

    a. a copy of photographic ID (passport/drivers licence/ Public services card) and
    b. a copy of a recent Utility Bill or Government letter.

2. **Where a request is manifestly unfounded, excessive, of a repetitive nature or where more than one copy of the data is sought, a fee may apply.**

3. **You may contact our Data Protection Officer to assist you in the completion of this Form.**

Data Retention

We will only keep a copy of these documents provided to prove your identity until your subject access request has been fully processed and issued to you and all relevant review or appeal procedure timelines have expired.

Please complete **all parts** of this Form **in full**

Part 1 – Details of Data Subject (Your Details)

Contact Details *(in block capitals)*:

Name: _____

Surname: _____

Address: _____

_____

_____

Eircode: _____

Contact Phone Number: _____

E-mail Address (where applicable): _____

Part 2 – Details of Request

Help Us to Help You

To assist us in locating the data you are requesting, please include as many specific details as possible in relation to your interactions with us in the past (for example please state the area(s) of the Authority you have corresponded with/the types of applications you may have made, etc).

_____

_____

_____

_____

Please tell us the relevant period of time or timelines involved for which you are seeking the personal data (for example *01 January 2018 – 31 December 2018).*

_____

_____

_____

Please provide us with any reference numbers relating to your contact with us in the past (for example file reference numbers, previous correspondence references, etc.).

_____

_____

_____

_____

_____

Please provide us with any other specific details that you feel are relevant in assisting us in locating your personal data. By providing us with as much detail as possible in relation to your access request, we will be able to assist you more efficiently.

_____

_____

_____

_____

_____

_____

PART 4 DECLARATION

I declare that all the details I have provided in this Form are true and complete to the best of my knowledge.

Signature of Requester: _____

Date: _____

Please return the completed Form by post to:

Data Protection Officer
The Adoption Authority of Ireland
Shelbourne House
Shelbourne Road
Ballsbridge
Dublin 4 D04 R6F6

Or by e-mail to:

dataprotection@aai.gov.ie

Further information on Data Protection:

- The website of the Data Protection Commissioner – www.dataprotection.ie

PART 5 CHECKLIST

Please remember to check that you have:

1. Completed the Subject Access (SAR) Request form in full - YES/NO
2. Signed and dated the Declaration above - YES/NO
3. Provided us with sufficient details to locate your personal data - YES/NO
4. Provided adequate Proof of Identity - YES/NO

Privacy Statement

The Adoption Authority of Ireland will treat all information and personal data that you provide as confidential, in accordance with the General Data Protection Regulation and Data Protection legislation.

3. Right to Rectification under the GDPR (Art 16)

Under Article 16 of the GDPR where a data subject believes their data is inaccurate they have the right to request that it be corrected. Where they believe their data is incomplete they have the right to have their personal data completed based on information they provide.

The Authority must respond to such a request where necessary and take steps to validate the information provided by the Data Subject to ensure that it is accurate before amending it.

If the Authority has to rectify personal data the Authority must also notify any one to whom it has disclosed such data, unless this would be impossible or involve disproportionate effort.

Requests for rectification of data must be submitted in writing to the Data Protection Officer, proof of identification must accompany the request.

Log and record all Requests for Rectification

All requests received will be logged in the Subject Access Request Register detailing:

- Date received;
- Applicant's details;
- Details of rectification requested;
- Details of response to requestor confirming action taken.

4. Right to restriction of Processing (Art18)

Under Article 18 of the GDPR individuals have a right to 'block' or suppress processing of their personal data.

When is the restriction applicable?

The Authority will be required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing of the data should be restricted until the accuracy of the personal data has been verified;
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and the Authority are considering whether its legitimate grounds override those of the individual;
- When processing is unlawful, and the individual opposes erasure and requests restriction instead;

- If the Authority no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If the Authority has disclosed the personal data in question to others, the Authority must contact each recipient and inform them of the restriction on the processing of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, the Authority must also inform the individuals about these recipients.

What is meant by restriction?

Under GDPR If personal data is 'restricted', then the Authority may only store the data. It may not further process the data unless:

- The individual consents; or
- The processing is necessary for establishment of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important (Union or Member State) public interest.

If the data have been disclosed to others, then the controller must notify those recipients about the restricted processing (unless this is impossible or involves disproportionate effort).

The Authority can retain just enough information about the individual to ensure that the restriction is respected in future.

5. Right to Erasure under the GDPR (Art17)

Data Subjects have the right under Article 17 of the GDPR to have their data 'erased' in certain specific situations. This is commonly referred to as 'the right to be forgotten'. The Authority must respond to such a request without undue delay and in any event within one month, although this can be extended in difficult circumstances.

When does the Right to Erasure apply?

- When data are no longer necessary for the purpose for which they were collected or processed.
- If the individual withdraws consent to processing (and if there is no other justification for processing).
- To processing based on legitimate interests - if the individual objects and the controller cannot demonstrate that there are overriding legitimate grounds for the processing.

- When the data are otherwise unlawfully processed (for example in some way which is otherwise in breach of the GDPR).
- If the data have to be erased to comply with Union or Member State law which applies to the controller.
- When the data was relevant to the data subject as a child. (T*his is a reference to data which was obtained from the subject when he or she was a child as opposed to information about them as a child).*

If the Authority has to erase personal data the Authority must also notify any third parties to whom it has disclosed such data, unless this would be impossible or involve disproportionate effort.

Exceptions to this Regulatory Requirement

This obligation does not apply if processing of the data is necessary;

- for the exercise of the right of freedom of expression and information;
- for compliance with a Union or Member State legal obligation;
- **for performance of a public interest task or exercise of official authority;**
- for public health reasons;
- **for archival, research or statistical purposes (if any relevant conditions for this type of processing are met);** or
- for the establishment, exercise or defence of legal claims.

The Authority can refuse to comply with the request to erasure when one of the exceptions above as set out in Art 17.2 of the GDPR applies.

Erasure Request Procedure

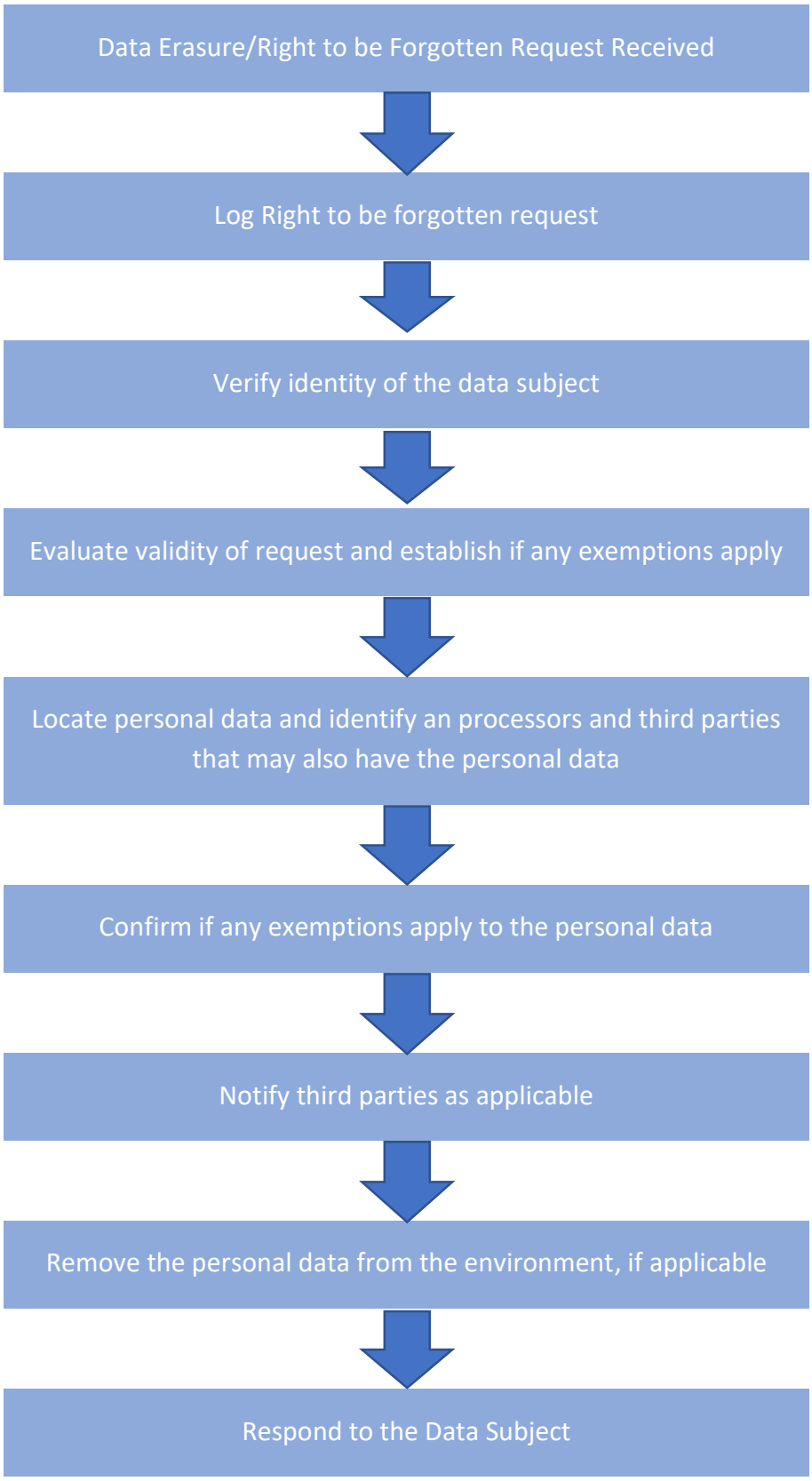
The Authority must act on a request for erasure from a data subject unless they are unable to establish their identity.

Under Article 12.3 of the GDPR, The Authority has 30 days to provide information on the action the organisation will decide to take on a legitimate erasure request. This timeframe can be extended up to 60 days depending on the complexity of the request.

If it decided to refuse a request, the Authority must inform the data subject within 30 days stating the reason(s) and informing the data subject of their right to complain to the supervisory authority, the Data Protection Commission.

The procedure for processing requests for erasure is set out below and expanded on in Table 1. The specifics of each step will vary depending on the request and the systems where the data is held.

Table 2 provides information on categories of data held in the Authority where an exemption to the right of erasure might apply.



Close the Request

Table 1

Step	Description
Data Erasure request received	The Data Subject submits a Request for Erasure/Right to be Forgotten via email or website or by letter. The Request is sent to the Data Protection Officer.
Log Data Erasure Request	The Data Protection Officer logs the Request in the Data Subject Access Request Register and the date of the request recorded.
Verify Identify of the data subject	The identity of the data subject is confirmed by production of passport, drivers licence etc. If necessary additional information may be requested to confirm identity. If the identity of the data subject cannot be confirmed the request can be rejected and the reason for this communicated to the data subject.
Evaluate Validity of request or if an exception applies	The DPO will examine the request to establish whether any of the exceptions apply to the data and if the request is to be approved or denied. Article 17 (3) of the GDPR

<table>
<tr><td rowspan="2">Confirm if any exemptions apply to the personal data</td><td colspan="2">Most commonly the Authority will rely on Article 17 (b)
- for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or
- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.</td></tr>
<tr><td>If an exemption applies a proper notice explaining the exception must be sent to the data subject within 30 days. The letter must also inform them they have the right to file a complaint to the Data Protection Commission where they feel the request has been processed unlawfully or unfairly.</td><td>If no exemption applies go to next step.</td></tr>
<tr><td>Locate the personal data</td><td colspan="2">Data Protection Officer will work with unit managers to locate all the relevant information.</td></tr>
<tr><td>Identify all processors and third parties that may also</td><td colspan="2">Where it is established that the right of erasure applies the DPO will notify all identified third parties that have access</td></tr>
</table>

have the personal data and Notify Third parties	to the personal data to completely remove the data from their environments and confirm erasure
Remove the personal data from your environment.	Where it is established that the right of erasure applies. Remove the personal data from your environment. There may be circumstances where erasing personal data from digital and physical backups is not required: If the Authority can easily delete individual subject data from backups without undue hardship, they will be required to fulfil erasure requests
Respond to Data Subject	Respond to the data subject to confirm data erasure from your environment and all associated third parties. The Authority has 30 days to respond to data subject erasure requests, and this could be extended depending on the excessiveness, repetitiveness, and complexity of the request.
Close Data Erasure Request	The fact that the request has been responded to is logged in the Data Subject Request Register together with the date of closure.

Data made available in the Public Domain

If the Authority has made personal data public, and where it is obliged to erase the data, the Authority must also inform other controllers who are processing the data that the data subject has requested erasure of those data.

The obligation is to take reasonable steps and account must be taken of available technology and the cost of implementation.

Table 2 Schedule of categories of personal data which may come under the Exemptions

No	Processing activity	Basis for Exception from Erasure
1	Employee data	Art 17 (3) (e) for the establishment, exercise or defence of legal claims although certain records may sometimes be deleted if they do not relate directly to the employment contract.
2	Adoption Records	Art 17 (3) (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
3	Register of Intercountry Adoptions	Art 17 (3) (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
4	Gender Recognition Register of intercountry Adoption;	Art 17 (3) (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
5	Relevant Non-Guardian Register	Art 17 (3) (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

6. Right to Data Portability under the GDPR (Art 20)

Data Subjects have the right under Article 20 of the GDPR to have their personal data ported to them or a new provider in a readable format if the data in question was: 1) provided by the data subject to the controller (interpreted broadly); and 2) is processed based on consent or fulfilment of a contract

The Authority must respond to such a request without undue delay and in any event within one month, although this can be extended in difficult circumstances.

The subject access right provided under the GDPR already gives individuals the right to require their data to be provided in a commonly used electronic form but Data portability goes beyond this and requires the controller to provide information in a structured, commonly used and machine-readable form so that it may be transferred by the data subject to another data controller where it is technically feasible to do so.

When does the Right of Data Portability Apply and to what data?

The right to data portability only applies:

- to personal data an individual has provided to a controller; and
- where the processing is based on the individual's consent or for the performance of a contract.

Formats for Personal Data Portability

While the GDPR does not require any specific technical standard for data returned in response to a data portability request, the data provided must be "in a structured, commonly used and machine-readable format" to make the data interoperable. A format that can only be read subject to costly licensing constraints would be considered inadequate.

Working Party29 (WP29) notes that data controllers are responsible for securely transmitting data to requesting data subjects, but those security measures may not be obstructive or require additional costs to data subjects. WP29 also recommends that controllers make data subjects aware of steps they can take to secure their information upon receipt, and further suggests the best practice of recommending appropriate formats and encryption measures.

In anticipation of data requests too big to download directly, WP29 advises data controllers to consider alternate means of providing data, such as through physical media or through direct transmission to another data controller where technically feasible.