Procedure for GDPR subject rights requests

1 Basics

GDPR gives individuals a set of rights over their data:

Access to their data
Rectification
Erasure
Restriction in certain circumstances
Portability
Objection over the use of certain legal bases
Rights over automated decisions

Whatever a person asks you to do, some principles should always apply:

- Correspondence for each request must be kept together
- Every request will be allocated a reference number
- Every request will be logged onto the request database so that compliance with the timescales can be monitored
- Ask anyone making a request verbally or via social media to put their request in writing
- Any applicant who does not include proof of ID with their request should be asked to provide it

Consider having an application form on your website for individuals to use – this might allow you to encourage applicants to focus or target their requests, but it is also an opportunity for you to explain how the rights work and to give the applicants advice.

Proof of identity

If there is any doubt about the identity of the subject (and to meet the requirement to protecting the confidentiality of data under the sixth GDPR principle), ORGANISATION should obtain proof of ID. GDPR does not prescribe what proof of ID is required, so the ORGANISATION should request sufficient proof to establish the identity of the data subject but not an excessive level of proof. For example, sending information to an email address that you regularly use to communicate with the person may negate the need for an identity check where the data is not sensitive. Do not ask for original copies of ID.

Verbal requests

The GDPR does not specify that requests have to be made in writing – logically, this means that a request can be made verbally. A legitimate request for proof of ID will facilitate a written request in many cases.

2 Timescales

Once the proof of ID and proof of consent (where required and requested) have been provided, the clock starts ticking. You have one month to respond.

Request	Timescale
Request from the individual	**The same date in the next month following receipt of proof of ID and (where requested) clarity over what they are asking for**
Request from solicitors or others representing the subject	**The same date in the next month following receipt of consent & entitlement and (where requested) clarity over what they are asking for**
Requests from family for records of deceased – GDPR does not apply to these requests	**As soon as is reasonable after receipt of proof of status (e.g. executor or closest surviving relative)**

The timescale can be extended by up to two months if the request is complex, or if there are multiple requests from the same person. The reasons for extending the deadline should be clearly set out in the reply. The complexity must be caused by the request itself, rather than problems with the organisation's internal records management and systems. The applicant must be informed of any delay before the end of the first month and told when their request will be answered.

3 Fees

The default is that no fee can be charged for dealing with a request – this includes time take to locate information, take any requested action, redact irrelevant data or references to other individuals where necessary, scanning, printing and postage where relevant.

There are only two situations where a charge can be made

- If the request is manifestly unfounded
- If the request is manifestly excessive

In both cases, the decision to charge a fee should usually be based on the nature of the request – any decision to look at correspondence or activities outside the request itself should be clearly documented.

Examples of when it may be legitimate to charge a fee

Manifestly unfounded	**Manifestly excessive**
The applicant has asked for the same thing before and received it or a legitimate refusal	The request explicitly includes back-ups or other data sources that are not live
The request involves a complex, detailed search and there is no evidence that they have a relationship with the organisation	The request covers a large amount of data and the applicant refuses to limit the scope
There is evidence that the applicant has made the request to waste time or distract the resources of the organisation from another matter	

4 General Procedure

- If information is held (or likely to be held) in more than one department, consider asking applicant for further information
    - who have they have dealt with
    - what information do they want?
    - do they have any identifiers or reference numbers which may assist in the search?

- If not already been provided, ask applicant for proof of their identity –
    - a copy of driving licence OR
    - current passport OR
    - current utility bill (not a mobile phone or store card)
    - if the applicant cannot provide any of these, ask what other proofs of ID they can provide

- If the data is about a child, ask for:

    - copy of child's birth certificate OR
    - current child's passport
      AND
    - proof of parent's identity
    - if there is any doubt about whether the parent is entitled to information, request a copy of child benefit letter or payments to establish that the child is living with the parents

- If the data is about the child who does not live with the applicant parent, contact any professionals involved with the child with whom you have contact (e.g. health, social care) to consider whether there is any court order or other reason why supplying information is not in the child's interests. If no professional can be contacted, contact the parent with whom the child lives. The other parent does not have a veto, but the interests of the child are paramount.

- If the applicant is a solicitor, proofs of identity can be requested, but signed consent from the subject for the solicitor to make the request on their behalf must be provided.

- Once the above has been received, the request is valid, and the clock is ticking. Log the request and acknowledge it.

- When information is requested from colleagues, they should be given a maximum of 15 days to provide the information.

- NOMINATED ROLE (senior officer) will chase the request after 20 days to ensure that the data is supplied with enough time to consider the issues.

- Unedited copies of relevant documents should be provided to the DP LEAD from teams that hold the data – originals should be accepted only in exceptional circumstances. The transfer of original copies of data is an unnecessary security risk that should generally be avoided.

- If a child is likely to have capacity to make decisions, consideration should be given to whether the child may have rights to the information. A child who has capacity to understand the implications of their data may be entitled to have access to it – decisions should always be taken in the child's interests. If an adult does not have capacity, the decision should be referred to an appropriate professional, or a person who has power of attorney for the subject.

Exemptions

The DP LEAD should be consulted on whether an exemption applies, and whether it is necessary to remove data to protect some other interest or refuse a request.

5 Subject access issues

The applicant is entitled to receive:

- the data itself
- the purposes of the processing;
- the categories of personal data being processed;
- the recipients of data
- retention period of the data
- information about the subject's rights to request rectification, restriction or objection
- the right to lodge a complaint with a supervisory authority;
- any available information about the source of the personal data
- information about significant instances of automated decision-making, including profiling

Withholding information about third parties

Information about third parties – family members, friends or others - should be disclosed where it is fair and reasonable in all the circumstances to do so. For example, where the data would clearly be known to the subject, or is already be in the public domain, there is no need to edit the information out. Care should be taken to ensure that data is not private, and that disclosure will not put the third party at any risk. The names of professionals involved in the care of or decisions about the individual should not normally be removed.

Confidential information

If information about the person was provided in confidence (e.g. a complaint or as part of an investigation conducted in confidence), information can be withheld. The DP lead should decide whether the duty of confidence outweighs the person's subject access rights. They will consider whether to ask the third party's permission to disclose. Withheld information should be retained to make sure that it is possible to justify any refusal should there be any complaints.

Sending out information

- Information should be sent out by recorded delivery, and the envelope properly sealed.
- Copies of disclosed records, as well as any information withheld, should be retained with all correspondence relevant to the request.

The DP LEAD will record the reasons for any use of exemptions. The applicant does not need to be informed that exemptions have been used.

Teams should be advised that concerns about the harm caused by disclosure must be raised by an appropriate professional before supplying copies of the records. Unless concerns are raised, the DP LEAD will assume that disclosure should go ahead.

6 Restriction issues

If the restriction request is valid, a marker must be added to the relevant records stating that the information should not be accessed. **NOMINATED ROLE** should determine whether it is necessary to limit access to the personal data rather than simply add a marker

If request is to be refused, **NOMINATED ROLE** must document which exemption applies.

Important public interest
Need to protect the rights of another person
The establishment exercise or defence of legal claims
DP Act 2018 Exemption

7 Right to be forgotten issues

A person has a right to request that data is erased.

NOMINATED ROLE is responsible for ensuring that data is erased, and evidence for the erasure must be retained. Evidence of erasure must be made available to the **Data Protection Officer / DP Lead** on request.

If request is to be refused, **NOMINATED ROLE** must document which exemption applies and retain evidence of the decision, or pass it to the **Data Protection Officer / DP Lead**.

Freedom of expression
Legal obligation, public interest task, official authority
Public health / public interest
Archiving, scientific or historical research purposes or statistical purposes
Establishment, exercise or defence of legal claims
DP Act 2018 Exemption

8 Portability issues

NOMINATED ROLE is responsible for extracting portable data.

It will be disclosed to the applicant using secure email or other secure file transfer methods.

The data subject has the right to request that the portable personal data is transmitted directly from one controller to another, where this is technically feasible. A refusal to transfer the data should be documented by **NOMINATED ROLE**

9 Objection issues

A person has a right to object to processing where the legal basis is public interest task or official authority, or legitimate interests.

NOMINATED ROLE should consider such objections, taking into account the original basis for the decision (including the balancing exercise carried out for legitimate interests). They should consider any particular issued raised by the applicant about why the processing should cease. If refusing the request, the **NOMINATED ROLE** be able to demonstrate why the processing is necessary despite the objection in relation to the person concerned.

NOMINATED ROLE must document any decision to override the objection of the individual, including the reasons why the importance / significance of the processing is deemed to override the objection request.

10 Automated issues

A person should not be subject to a wholly automated decision except in certain limited circumstances – where the decision is necessary for a contract, where it is authorised by law, or where explicit consent has been obtained.

Where a person objects to a wholly automated decision, NOMINATED ROLE must ensure that that the decision is made by an officer and the individual is allowed to make representations and have access to information about how the decision is made.

Where this will not be provided, the reasons should be documented by the DP LEAD.

11 TRANSFER ISSUES

Where a person successfully requests rectification, restriction or erasure, and their request should be transferred to any other data controller to which the data in question has been disclosed. The reasons for any refusal to do so (impossible or disproportionate effort) should be clearly documented.

12 Complaints and challenges

- If the applicant has legitimate cause to complain that information is missing from the response, or is held and should have been included, this should be provided as soon as possible, unless an exemption has been used.

- Any inaccuracy that the individual identifies in the information that has been supplied should be corrected or amended as soon as possible. Original records should not be altered to obscure the original information

- Applicants should be advised to use ORGANISATION's complaints procedure if they are not satisfied.