



Policy: Subject Access Request Policy
Ref: P43

Introduction

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing. Z2K (Zacchaeus 2000 Trust) must comply with the requirements of the General Data Protection Regulations (GDPR) and we must be able to demonstrate compliance to the Information Commissioner's Office (ICO).

Upon receipt of a request for information, our internal policy is as follows:

Responsibility

Tanya Sutton is responsible for the handling of Subject Access Requests (SAR). The duties of Tanya Sutton include but are not limited to:

- Log the receipt and fulfilment of all requests received from a data subject / requester to see his or her personal information.
- Acknowledge the SAR.
- Verify the identity of any person making a SAR.
- Verify whether we are the controller of the data subject's personal data or just a processor. If just a processor, then will inform the data subject and refer them to the actual controller. This needs to be recorded in writing.
- Where applicable, decide if a request is excessive, unfounded or repetitive and communicate this to the requestor.
- Decide if an exemption applies.
- If a SAR is submitted in electronic form, any information should preferably be provided by electronic means as well. In the case of HR related requests, data will be provided on an encrypted USB storage device.

Oral or written requests

While Z2K does prefer that a data subject submits the *Data Subject Access Form*, requests can be made in writing, electronically or verbally.

If a member of staff is in any doubt if a certain situation has given rise to a SAR, contact Tanya Sutton by email producing full details of the incident. Staff should do this without delay and certainly within two business days.

Where a member of staff receives a subject access request, they must email the relevant information to Tanya Sutton without delay and certainly within two business days.

How do we verify the requestor's identity?

The requestor must supply valid evidence to prove their identity. We may verify the requestor's identity or by requesting forms of identification. We may accept requests from third parties on behalf of the data subject so long as it is accompanied by signed authority from the data subject and positive forms of identification from both the data subject and the third party.

We accept the following example forms of identification:

- Current Passport
- UK diving license
- Financial Statement issued by bank, building society or credit card company
- Utility bill for supply of gas, electricity, water or telephone (landline)

How to process the request

Our aim is to determine what information the requestor is asking for. *The Data Subject Access Request form* has a field allowing the data subject to identify specific data required. If the request is not clear, or where we process a large quantity of information about an individual, the GDPR permits us to ask the individual to specify the information the request relates to. Where this applies, we will proceed with a request for additional information.

We must verify whether we process the data requested. If we do not process any such data, we must inform the data subject accordingly.

We must respond to the data subject within 30 days of receiving the request as valid. This is a requirement under the GDPR.

Any employee who received a request from Tanya Sutton to locate and supply information relating to a SAR, must make a full exhaustive search of the records which they are responsible for or own. This may include, but is not limited to, emails (including archived emails and those that have been deleted but are still recoverable), Word documents, spreadsheets, databases, systems, removable media (for example, memory sticks), recordings, paper records in relevant filing systems.

Tanya Sutton should check whether the data requested also involves data on other data subjects and make sure this data is redacted before the requested data is supplied to the requestor; if data cannot be redacted, ensure that other data subjects have consented to the supply of their data as part of the SAR.

All the information that has been requested must be provided unless an exemption can be applied (see below). Information must be supplied in an intelligible form where we explain acronyms, codes or complex terms.

No charge to comply with the request (with exceptions)

We will provide a copy of the information free of charge, as per the GDPR rules. However, we may charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

We may also charge a reasonable fee to comply with requests for further copies of the same information. We understand that this does not mean that we can charge for all subsequent access requests.

Where applicable, Tanya Sutton will determine the 'reasonable fee' that must be based on our administrative cost of providing the information.

Excessive, manifestly unfounded or repetitive requests

Where requests are manifestly unfounded, excessive and repetitive, we may refuse to act on the request or charge a reasonable administration fee. Tanya Sutton will make a decision on this.

Tanya Sutton must provide information on our decision to the requestor in writing within 30 days and must state how she reached her decision.

Complex requests

As stated, we have to respond to a SAR within 30 days. If more time is needed to respond to complex requests, an extension of another two months is permissible, provided this is communicated to the data subject in a timely manner within 30 days.

Where we decide not to take action on the request of the data subject, we need to inform the data subject of this decision without delay and at the latest within 30 days of receipt of the request.

Our response to the requestor

After processing the SAR, our response to the requestor should include:

- The categories of personal data concerned;
- If relevant, the recipients, or categories of recipients, to whom personal data has been or will be disclosed, in particular third party recipients (e.g. Department for Works and Pensions, Her Majesty's Courts and Tribunals Services), including any appropriate safeguards for transfer of data;
- A copy of the relevant section of our file retention policy that relates to that data showing the period for which personal data will be stored.
- The existence of the right to request rectification 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 ICO;
- If the data has been collected from a third party: the source of such data.

How to handle exemptions?

If a member of staff believes that we have a valid business reason for an exemption, please inform Tanya Sutton without delay by email.

Exempt information must be redacted from the released documents with an explanation of why that information is being withheld.

Complaints

Where a requestor is not satisfied with a response to a SAR, we must manage this as a complaint. We must advise the requestor that if they remain unhappy with the outcome they may complain to the Information Commissioner's Office or take legal action against us.

Breach statement

Breaches of this policy by members of staff will be investigated and may result in disciplinary action. Serious breaches of policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against the relevant staff member.

Monitoring & Review

Date created: August 2020

Date reviewed: September 2020

Date of next review: November 2021

Responsible for Review: Office Manager & CEO