



TOPRA Subject access request (SAR) policy

Policy Number: 013

Date of issue: 8 May 2018

Last review: 8 May 2018

Introduction and Purpose

To be compliant with GDPR, TOPRA has a policy and procedure for dealing with subject access requests (SAR). Any living person can make a subject access request.

An individual is entitled to be:

- told whether any of their personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the personal data; and
- given details of the source of the data (where this is available)

An individual may request amendment of their personal information if it is inaccurate or incomplete

An individual may request the deletion of the information, if:

- The personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- The individual withdraws consent.
- The individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation. An individual can also request information about the reasoning behind any automated decisions taken about him or her, or an assessment of their performance (except where this information is a trade secret).

In preparing this policy due note has been taken of the information in the Subject Access Code of Practice issued by the ICO, which should be consulted for detailed guidance when responding to a SAR.

What is 'personal' data?

For information to be 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 organisation's possession).

Personal data can be in any form: database records, images, emails, paper records etc.

Who can make requests?

Members, staff members, customers of any kind and stakeholders can make a SAR. TOPRA can take reasonable steps to verify the identity of someone making a request.

An individual cannot make a request to see another individual's data unless they can show they have written authority from the individual (examples include recruitment consultants, solicitors).

How are requests for access made?

Requests MUST be made in writing, either by letter, fax or by email or even via social media unless there are good reasons (ie disability) for this to be impossible.

There is no specific form and TOPRA cannot stipulate the format of the request.

TOPRA will not respond to requests by using social media and will either respond by email or by letter.

TOPRA is not obliged to respond to oral requests. Anyone who appears to be making an oral SAR should be asked to submit it in writing to the Data Protection Officer.

TOPRA will make brief guidance available on the web site which will include:

- where the request should be sent to;
- any fee and the options for payment;
- the information that the requester will need to provide to confirm their identity;
- the one –month period for responding to the request; and
- details of a point of contact for any questions.

Is there a fee?

TOPRA will not charge a fee for dealing with a single SAR. However, if an individual makes multiple requests it is possible to charge a fee which will be discussed with the individual prior to responding to the request. TOPRA reserves the right to charge fees for requests if this is permitted in specific legislation.

What must TOPRA provide?

Subject access provides a right for the requester to see their own personal data, rather than a right to see copies of documents that contain their personal data.

What are the time frames?

TOPRA will acknowledge a request for SAR within 24 hours of receipt. The legal maximum is one calendar month, but TOPRA should approach any request as part of its good service to members and respond as soon as possible.

Who deals with requests?

A request can come into anyone in TOPRA and so all staff must be aware of this policy and be able to recognise a SAR. All SARs must be passed immediately to the persons responsible for Data Protection, namely the Data Controller (Executive Director) and Data Protection Officer (Head of Membership) who will acknowledge the request, designate a staff member to collate the data and decide who will reply. Staff members must not respond directly without following the process outlined below.

Process

- An SAR is identified by a member of staff
- It is passed to the DPO **immediately** (cc the Executive Director in case the DPO is absent)
- The DPO logs the request, date received and date by which a response must be made (one month)
- The DPO acknowledges the request within 24 hours of receipt and, if required, takes steps to validate the identity of the requester
- The DPO informs the Executive Director and Operations Director and all will meet within **three working days of receipt** to discuss the request and decide how it might be met (where the information is stored, who will retrieve it and who will be responsible for collating the information) and the **target date** for making the response, which should be as soon as possible and no more than 30 days from the date of receipt of the SAR. The team will take note of the guidance from the DPO in planning the response.
- If clarifications or context are needed to fulfil the request correctly the DPO will ask for them and a response will not be made until clarifications are received.
- The requested data will be collected and reviewed to ensure it does not disclose personal data about other people.
- The response is prepared by the person responsible and signed off by at least one other of the DPO, ED or Director of Operations
- The response is sent and the DPO logs the date.

Follow up

The requester will be asked to acknowledge the response and to confirm that the information received is satisfactory.

If the personal data has been shared with a third party (eg University) any agreed amendments to the data must be shared with that third party.

If the requester has further questions, requests amendment of the information held or deletion of the information, this will be acknowledged by the DPO and the DPO, Director of Operations and/or the Executive Director will discuss the response. A response will be made within one month, explaining what has been done. TOPRA will take into account relevant ICO guidance when deciding its response.

If the requester is not satisfied with the response they may make a formal complaint to the Board of TOPRA via the Executive Director.

If the Board upholds the action of the TOPRA staff, then the requester may take the matter further with the relevant legal authorities.