Subject Access Requests ("SAR") Checklist

Inform data subjects of their right to access data and provide an easily accessible mechanism through which such a request can be submitted (e.g. a dedicated email address).

Make sure a SAR policy is in place within the council and that internal procedures on handling of SARs are accurate and complied with. Include, among other elements, provisions on:

Responsibilities (who, what)

Timing

Changes to data

Handling requests for rectification, erasure or restriction of processing.

Ensure personal data is easily accessible at all times in order to ensure a timely response to SARs and that personal data on specific data subjects can be easily filtered.

Where possible, implement standards to respond to SARs, including a standard response.

1. Upon receipt of a SAR

Verify whether you are controller of the data subject's personal data. If you are not a controller, but merely a processor, inform the data subject and refer them to the actual controller.

Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.

Verify the access request; is it sufficiently substantiated? Is it clear to the data controller what personal data is requested? If not: request additional information.

Verify whether requests are unfounded or excessive (in particular because of their repetitive character); if so, you may refuse to act on the request or charge a reasonable fee.

Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR.

Verify whether you process the data requested. If you do not process any data, inform the data subject accordingly. At all times make sure the internal SAR policy is followed and progress can be monitored.

Ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted.

Verify whether the data requested also involves data on other data subjects and make sure this data is filtered before the requested data is supplied to the data subject; if data cannot be filtered, ensure that other data subjects have consented to the supply of their data as part of the SAR.

Responding to a SAR

Respond to a SAR within one month after receipt of the request:

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 the first month;

If the council cannot provide the information requested, it should inform the data subject on this decision without delay and at the latest within one month of receipt of the request.

If a SAR is submitted in electronic form, any personal data should preferably be provided by electronic means as well.

If data on the data subject is processed, make sure to include as a minimum the following information in the SAR response:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules[1] or EU model clauses[2];
- where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
- 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 Information Commissioners Office ("ICO");
- if the data has not been collected from the data subject: the source of such data;
- the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Provide a copy of the personal data undergoing processing.

Adopted May 2018

[1] "Binding Corporate Rules" is a global data protection policy covering the international transfer pf personal data out of the European Union. It requires approval of a data protection regulator in the European Union. In most cases this will be the relevant regulator where an organisations head quarters is located. In the UK, the relevant regulator is the Information Commissioner's Office.

[2] "EU model clauses" are clauses approved by the European Union which govern the international transfer of personal data. The clauses can be between two data controllers or a data controller and a data processor.