

# Policy: Data Subjects Rights Policy

Updated April 2018

## Introduction

This policy ensures that the rights of data subjects are taken into consideration and adhered to appropriately when Transform processes personal data. Included amongst the rights of a data subject is the right to submit a Data Subject Access Request. A Data Subject Access Request is a request sent by (or on behalf of) a data subject to Transform, requesting information about the personal data that they reasonably believe Transform to be processing about them. The data subject can request information from either the data controller or the data processor; this depends on who they perceive to be processing their personal data. With regard to any outsourced services, Transform must include any information held by outsourced services in our responses to a Data Subject Access Request.

## Scope

All personal data processed by Transform is within the scope of this policy. GDPR regulations state that the reason for allowing data subjects to access their personal data is so that they are aware of, and can verify, the lawfulness of the data processing.

## Roles and responsibilities

All employees are responsible for ensuring that any Data Subject Rights Requests (including Data Subject Access Requests) are passed to the related Information Asset Owner and the Information Risk Officer without delay. This equally applies to any complaints that might be made about Transform's handling of a Data Subjects Rights Request.

## Policy

Transform will ensure that the contact details of our Information Control Officer are published on our website, clearly under the 'contact us' section.

Transform will ensure we have clear guidelines on our website page to enable data subjects to lodge a Data Subject Rights Request or complaint.

Transform will ensure we clearly provide data subjects with our Privacy Policy by publishing it on our website, clearly under the 'contact us' section and relative to the Data Subjects Rights and complaints form submission.

Transform recognises that data subjects have the following rights:

- To be provided with any and all information held about them, within one month, and free of charge (known as the Data Subject Access Request or DSAR)

- To have their personal data erased, within one month and free of charge (known as the Data Subject Erasure Request or DSER)
- To have incorrect or incomplete information rectified, within one month and free of charge (known as the Data Subject Request for Rectification or DSRR). When the request had been completed, the data subject to be informed in writing.
- To have any or all processing of their personal data restricted - the processing is to be suspended until the processing in question has been resolved.
- To object to specific forms of processing, such as marketing, automated decision making and profiling. When such an objection is received from the data subject, Transform will ensure it and ceases the processing without delay.
- To have their personal data provided in a readable format and portable to another organisation. Transform responds to such requests by providing the requested information in a generally readable csv file (standard Microsoft format) or a pdf.
- To lodge a complaint with the supervisory authorities.
- To claim compensation from the data controller, data processor or the supervisory authority for any infringement of their rights.

Transform also recognises that data subjects can complain about:

- How their personal data has been processed
- How their request for access to data has been handled
- How their complaint had been handled
- Appeal against any decisions made following a complaint

The Information Risk Officer handles any complaints in accordance with the complaints procedure.

The lawful basis for processing personal data affects which rights are available to the data subjects, as indicated in the table below:

| Lawful basis for processing | Right to erasure  | Right to portability | Right to object                    | Right to rectification |
|-----------------------------|---|----------------------|------------------------------------|------------------------|
| <b>Consent</b>              | Yes   | Yes                  | No (but right to withdraw consent) | Yes                    |
| <b>Contract</b>             | No (if current or < 6 Years)<br>Yes (if > 6 years after expiry) | Yes                  | No                                 | Yes                    |
| <b>Legal obligation</b>     | No  | No                   | No                                 | Yes                    |
| <b>Vital Interest</b>       | No  | No                   | Yes                                | Yes                    |
| <b>Public Task</b>          | No  | No                   | Yes                                | Yes                    |
| <b>Legitimate Interest</b>  | Yes   | No                   | Yes                                | Yes                    |

## Data Subject Access Process

- The Data Subject Access Request (which includes submission of a Data Subject Access Request Form) must be submitted in writing. This can be either by the traditional letter or email.
- If the data subject is unable to provide a written DSAR request for any reason (e.g. disability) an alternative mode for submitting the DSAR can be considered in exceptional situations.
- Transform's DSAR Form needs to be completed in full by the data subject. Should the DSAR come from a Transform client, Transform staff may offer to assist the client to complete the DSAR form where appropriate.
- Transform must verify the identity of anybody submitting a DSAR. Identity can be verified by providing at least two of the following:
  - Date of birth that can be matched to their records
  - An address that can be matched to their records
  - An account number that can be matched to their records
  - A copy of a recent utility bill
  - Copy of a recent bank or building society statement
  - A copy of a valid passport
  - A copy of a valid driving licence
- The data subject is entitled to submit a DSAR via a third party. (e.g. solicitor or parent/guardian acting on their behalf). However in these circumstances, Transform must confirm that the third party making the request is entitled to act on behalf of the data subject.
- Along with the confirmation as to processing of personal data, the data subject can also request:
  - Purpose of the data processing
  - The recipients, or categories of recipients, to whom their personal data has been disclosed
  - The envisaged period of retention and the criteria used to determine this period.
- When personal data is transferred to a third country, the data subject has the right to be informed of the appropriate safeguards relating to the transfer.
- The data subject may request all the information held about them specifically because they want to know the scale and extend of it. In this situation Transform shall identify and supply all personal information from all locations (Pyramid, emails, paper documents, voice recording, photographs, CCTV images, etc)
- When Transform is assembling the information required to satisfy a Data Subject Access Request, we should be scrupulously careful to redact any information about other persons (i.e. persons other than the data subject) or information that is confidential / non-sharable.
- Transform shall respond to a Data Subject Access Request within 30 days of receipt of a fully completed and signed Data Subject Access Request form.
- Transform shall be scrupulously careful to send the information to the correct postal address or email address. If we were to accidentally send to the wrong address this would constitute a data breach.
- Transform is required to a copy of all the information provided to the data subject in our response, as sometimes we may be asked supply further copies, or may be asked to provide evidence of compliance during an audit or investigation by the supervisory authority.

## Exceptions

There are some exceptions to GDPR requirements which state that the Data Subject Access Request can be refused, or a fee charged to action them, where the request from the data subject is:

- Manifestly unfounded
- Or excessive
- Or of a repetitive character

Transform can refuse to disclose CCTV footage if it will put a criminal investigation at risk. Transform should be able to demonstrate one of the above reasons for refusing a DSAR or for charging a fee to either the data subject or the supervisory authority.

## Compliance monitoring

On a periodic basis, the Data Protection Officer shall monitor all Data Subject Rights requests submitted to Transform to ensure that they are being conducted in compliance with the rights of data subjects and in compliance with the policy

A current version of this policy is available to all employees.

**Reviewed:** April 2018

**Review due by:** April 2021