Data Subject Rights Procedure

Scope

All personal data processed by Instinctif Partners is within the scope of this procedure.

Individuals have the right to:

- confirmation that you are processing their data;
- access to their personal data;
- have personal data rectified if it is inaccurate or completed if it is incomplete;
- be forgotten and can request the erasure of personal data;
- block or restrict the processing of their personal data;
- object to the processing of their personal data in certain circumstances.

Responsibilities

The Compliance Committee are responsible for the application and effective working of this procedure.

Timeline

The following timeline applies to all procedures stated in this document.

An individual can make a request for rectification verbally or in writing. You must verify the identity of the person making the request using "reasonable means".

You should respond to a request without delay and at least within one month of receipt. You should calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

A calendar month ends on the corresponding date of the next month (e.g. 2 January to 2 February), unless that date does not exist in which case it is the last day of the next month (e.g. 31 January to 28 February).

If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond (e.g. you receive a request on 30 March and the time limit starts from the next day (31 March). As there is no equivalent date in April, you have until 30 April to respond. However, if 30 April falls on a weekend, or is a public holiday, you will have until the end of the next working day to respond).

This means that the legal deadline will vary from 28 days to 31 days depending on the month. For practical purposes, the Compliance Committee have adopted a 28-day period to ensure compliance is always within a calendar month.

You can extend this period by a further two months for complex or numerous requests (in which case you must inform the individual and explain the delay). It is good practice to make a note on the record showing that it is under dispute and why.

1. Subject access request

Overview

Subject access provides a right to see the information contained in personal data, rather than a right to see the documents that include that information.

Individuals can request information verbally or in writing. You must provide a copy of the information free of charge. However, you can charge a 'reasonable fee' when a request is:

- manifestly unfounded or excessive, particularly if it is repetitive, unless you refuse to respond; or
- for further copies of the same information (that's previously been provided). This does not mean that you can charge for all subsequent access requests.

You must base the fee on the administrative cost of providing the information.

Further information can be found here - https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/

Process

1. The data subject specifies a specific set of data held by the organisation on their subject access request (SAR). The data subject can request all data held on them.

2. The organisation records the date that the identification checks were conducted, and the specification of the data sought. This is recorded in the SAR register held by the Compliance Committee (CC).
    a. The organisation provides the requested information to the data subject within 28 days from this recorded date.

3. The SAR application is immediately processed by the CC, who will ensure that the requested data is collected within the specified time frame in (2a) above. Collection entails:
    a. Collecting the data specified by the data subject, or
    b. Searching all databases and all relevant filing systems (manual files) in the organisation, including all backup and archive files, and all email folders and archives. The CC maintains a data register detailing the location of all stored information.

4. If any of the requested data is being held or processed under one of the following exemptions, it does not have to be provided:
    - National security
    - Crime and taxation

- Health
- Education
- Social Work
- Regulatory activity
- Journalism, literature and art
- Research history, and statistics
- Publicly available information
- Corporate finance
- Examination marks
- Examinations scripts
- Domestic processing
- Confidential references
- Judicial appointments, honours and dignities
- Crown of ministerial appointments
- Management forecasts
- Negotiations
- Legal advice and proceedings
- Self-incrimination
- Human fertilization and embryology
- Adoption records
- Special educational needs
- Parental records and reports

5. The CC reviews all documents that have been provided to identify whether any third parties are present in it, and either removes the identifying third party information from the documentation or obtains written consent from the third party for their identity to be revealed. Note:
    a. The Act says you do not have to comply with the request if to do so would mean disclosing information about another individual who can be identified from that information, except where:
        i. the other individual has consented to the disclosure; or
        ii. it is reasonable in all the circumstances to comply with the request without that individual's consent.

6. The organisation provides a copy of the information in a permanent form, unless the individual agrees otherwise or doing so would be impossible or involve disproportionate effort.

2. Right to rectification and data quality

Overview

Individuals have the right to have personal data rectified if it is inaccurate or completed if it is incomplete.

You must verify the identity of the person making the request, using "reasonable means". If you have shared the personal data with other organisations (for example other controllers or processors) you must inform them of the rectification where possible.

You should regularly review the information you process or store to identify when you need to take action, e.g. correct inaccurate records. Records management policies, with rules for creating and keeping records (including emails) can help.

Conducting regular data quality reviews of systems and manual records you hold will help to ensure the information continues to be adequate for the purposes you are processing for.

You should also ensure that you complete regular data quality checks to provide assurances on the accuracy of the data being inputted by your staff.

If you identify any data accuracy issues, you should communicate lessons learned to staff through ongoing awareness campaigns and internal training.

Process

1. The data subject submits a request to rectify their personal data, either verbally or in writing.

2. The organisation records the date that the identification checks were conducted, and the scope of the rectification. This is recorded in the Subject Data Rectification register held by the Compliance Committee (CC).
    a. The organisation provides confirmation of rectification to the data subject data subject within 28 days from this recorded date.

3. The request is immediately processed by the CC, who will ensure that the data is rectified within the specified time frame in (2a) above.

4. The organisation confirms to the data subject that the data has been rectified.

3. Right to erasure including retention and disposal

Individuals have the right to be forgotten and can request the erasure of personal data when:

- it is no longer necessary for the purpose you originally collected/ processed it for;
- the individual withdraws consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- it was unlawfully processed (i.e. otherwise in breach of the GDPR);
- it has to be erased in order to comply with a legal obligation; or

- it is processed for information society services to a child.

You can refuse to comply with a request for erasure if you are processing the personal data for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- to perform a public interest task or exercise official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- to exercise or defence of legal claims;
- for public health purposes in the public interest; or
- for processing that is necessary for the purposes of preventive or occupational medicine, if you are processing the data by or under the supervision of a health professional.

A written retention policy or schedule will remind you when to dispose of various categories of data, and help you plan for its secure disposal.

You should regularly review your retention schedule to make sure it continues to meet business and statutory requirements and agree any amendments with managers and incorporate them into the new schedule.

You should designate responsibility for retention and disposal to an appropriate person.

Process

1. The data subject submits a request to erase their personal data, either verbally or in writing.

2. The organisation records the date that the identification checks were conducted, and the scope of the erasure. This is recorded in the Subject Data Erasure register held by the Compliance Committee (CC).
    a. The organisation provides confirmation of erasure to the data subject data subject within 28 days from this recorded date.

3. The request is immediately processed by the CC, who will ensure that the data is erased within the specified time frame in (2a) unless there is reason to refuse.

4. The organisation confirms to the data subject that the data has been erased or reasons for continued retention.

4. Right to restrict processing

Individuals have a right to block or restrict the processing of their personal data.

When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in the future. As a matter of good practice, you should consider restricting the processing of personal data if:

- an individual contest the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.
- an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your businesses legitimate grounds override those of the individual.
- processing is unlawful, and the individual opposes erasure and requests restriction instead.
- you no longer need the personal data, but the individual requires the data to be retained to allow them to establish, exercise or defend a legal claim.

You may need to review procedures to ensure you are able to determine if you need to restrict the processing of personal data.

If you have disclosed the personal data to other organisations (controllers or processors), you must inform them about the restriction, unless it is impossible or involves disproportionate effort to do so.

You must inform individuals when you decide to lift a restriction on processing.

Process

1. The data subject submits a request to restrict processing their personal data, either verbally or in writing.

2. The organisation records the date that the identification checks were conducted, and the scope of the restriction. This is recorded in the Subject Data Restricted Processing register held by the Compliance Committee (CC).
    a. The organisation provides confirmation of restriction to the data subject data subject within 28 days from this recorded date.

3. The request is immediately processed by the CC, who will ensure that the data is restricted within the specified time frame in (2a) unless there is reason to refuse.

4. The organisation confirms to the data subject that the data has been restricted or reasons for continued processing.

5. Right to object

Individuals have a right to object to the processing of their personal data in certain circumstances. Whether it applies depends on your purposes for processing and your lawful basis for processing. You must inform individuals of their right to object “at the point of first

communication" and present it separately from other information on rights clearly laid out in your privacy notice. Individuals can object verbally or in writing.

If the right to object does apply, it is not always absolute. Whether it is an absolute right depends on your purposes for processing the data.

Individuals have an absolute right to object to any processing (including profiling) undertaken for the purposes of direct marketing.

You must stop processing for direct marketing as soon as you receive an objection. There are no exemptions or grounds to refuse.

Individuals can object, on 'grounds relating to his or her particular situation' to processing (including profiling) based on:

- your legitimate interests;
- the performance of a task in the public interest; or
- exercise of official authority.

In these circumstances the right to object is not absolute. You must stop processing the personal data unless:

- you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

If you are processing personal data for the purposes of scientific/historical research purposes or statistical purposes the right to object is more restricted and does not apply if the processing is necessary for the performance of a task carried out for reasons of public interest.

Process

1. The data subject submits a right to object, either verbally or in writing.

2. The organisation records the date that the identification checks were conducted, and the scope of the objection. This is recorded in the Subject Data Objection register held by the Compliance Committee (CC).
    a. The organisation provides confirmation of objection to the data subject data subject within 28 days from this recorded date.

3. The request is immediately processed by the CC, who will ensure that the request is processed within the specified time frame in (2a) unless there is legal basis to refuse.

4. The organisation confirms to the data subject that their personal data will no longer be processed, or any legal basis for refusing the request.

Document Owner and Approval

The Compliance Committee is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the GDPR.