Data Subjects Rights Regulation and Procedure

13/03/2024

Ref NO. DP003

Document owner and approver(s)	
Owner	The International Institute for Justice and the Rule of Law (IIJ)
Approver(s)	Mr. Steven Hill (Data Controller) Mr. Reinhard Uhrig (Acting Data Controller)

Introduction

This regulation ensures that the rights of data subjects are taken into consideration and adhered to appropriately when The International Institute for Justice and the Rule of Law, hereinafter referred to as “the IIJ”, 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 the IIJ, requesting information about the personal data that they reasonably believe the IIJ 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. The IIJ must include any information held by outsourced services in our responses to a Data Subject Access Request.

Scope

All personal data processed by the IIJ is within the scope of this regulation. 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 Administration and Data Protection Officer on dimechk@theiij.org without undue delay. This equally applies to any complaints that might be made about "the IIJ's handling of Data Subjects Rights Request. Employees shall forward or lodge a complaint by email on dimechk@theiij.org without undue delay

Data Subject Rights

The IIJ recognises that data subjects have the following rights:

- To be provided with 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.
- 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, the IIJ will ensure it ceases the processing without delay.
- To have their personal data provided in a readable format and portable to another organisation. The IIJ responds to such requests by providing the requested information in a generally readable file.
- To lodge a complaint with the Information and Data Protection Commissioner.
- To claim compensation from the data controller, data processor or the supervisory authority for any infringement of their rights.

The above-mentioned rights apply depending on the legal basis on which the IIJ processes the personal data. Each data subject request must be assessed to determine whether the right requested is applicable in each case.

The IIJ 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 IIJ Administration and Data Protection Officer (Karl Dimech) handles any complaints in accordance with the complaint's procedure.

Data Subject Rights Requests

1. Scope, Purpose, and Users

This procedure sets out the key features regarding handling or responding to data subject rights requests (hereinafter referred to as "DSRR") including requests for access to personal data made by data subjects, their representatives or other interested parties. This procedure will enable the IIJ to comply with legal obligations, provide better customer care, improve transparency, enable individuals to verify that information held about them is accurate, and increase the level of trust by being open with individuals about the information that is held about them. This procedure applies to employees that handle data subject rights requests.

A Data Subject Access Request (hereafter referred to as the "DSAR") is any request made by an individual or an individual's legal representative for information held by the IIJ about that individual. The DSAR provides the right for data subjects to see or view their own personal data as well as to request copies of the data.

A DSAR or other DSRR must be made in writing. In general, verbal requests for information held about an individual are not valid DSAR's. In the event a formal DSRR is made verbally to a staff member of the IIJ, the staff member is to direct the data subject to make his request in writing and further guidance should be sought from the Administration and Data Protection Officer who will consider and approve all DSRR applications.

A DSRR can be made via any of the following methods: email, post, website, or any other method. DSRR's made online must be treated like any other DSRR when they are received however, the IIJ will not provide personal information via social media channels.

2. The Rights of Access of a Data Subject

The rights to data subject access include the following:

- Know whether a data controller holds any personal data about them.
- Receive a description of the personal data held about them and a copy of the personal data undergoing processing *(if further copies are requested by the data subject, the data controller may charge a reasonable fee based on administrative costs).*
- Be informed of the purpose(s) for which that data is being processed, and from where it was received.
- Be informed regarding which categories of personal data are processed in his/her regard.
- Be informed whether the information is disclosed to third parties (if any), and if so, the identity of those recipients.
- Be provided with information as to the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
- Be informed of his/her right to request from the IIJ rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.
- Be informed of his/her right to lodge a complaint with the Information and Data Protection Commissioner (IDPC).

- Where personal data are not collected from the data subject, any available information as to their source, the data subject shall be provided with the following information:

    - the identity and the contact details of the IIJ as the data controller.
    - the purposes of the processing for which the personal data are intended as well as the legal basis for the processing.
    - the categories of personal data concerned.
    - the recipients or categories of recipients of the personal data, if any.

- The right of data portability. Data subjects can ask that their personal data be transferred to them or a third party in machine readable format (Word, PDF, etc.). However, such requests can only be fulfilled if the data in question is: 1) provided by the data subject to the IIJ, 2) is processed automatically and 3) is processed based on consent or fulfilment of a contract.

- If the data is being used to make automated decisions about the data subject, to be told what logic the system uses to make those decisions and to be able to request human intervention.

The IIJ must provide a response to data subjects requesting access to their data within one (1) month from receipt of the DSAR. The aforesaid timeframe may be extended by a further two (2) months if the DSAR is complex or if several DSAR's from the respective individual were received. In case the IIJ deems it necessary to extend the timeframe as outlined above, the data subject shall be informed regarding such decision and shall also be provided with an explanation as to why such extension is required.

3. Requirements for a valid DSRR

In order to be able to respond to the DSRR's in a timely manner, the data subject should:

- Submit his/her request in writing.

- Provide the IIJ with sufficient information to validate his/her identity (to ensure that the person requesting the information is the data subject or his/her authorized person).

Subject to the exemptions referred to in this document, the IIJ shall provide information to data subjects whose requests are in writing and are received from an individual whose identity can be validated by the IIJ.

However, the IIJ will not provide data where the resources required to identify and retrieve it would be excessively difficult or time-consuming. Requests are more likely to be successful where they are specific and targeted at particular information.

Factors that can assist in narrowing the scope of a search include identifying the likely holder of the information (e.g. by making reference to a specific department), the time period in which the information was generated or processed (the narrower the time frame, the more likely a request is to succeed) and being specific about the nature of the data sought.

4. DSRR Process

i. Request

Upon receipt of a DSRR, the Administration and Data Protection Officer will acknowledge the request. The data subject may be asked to provide additional information to better enable the IIJ to locate the relevant information.

ii. Identity verification

The Administration and Data Protection Officer shall check the identity of anyone making a DSRR to ensure information is only given to the person who is entitled to it. In the case of a DSAR if the identity of the person making the request has not already been provided, the person receiving the request will ask the person making the request to provide two forms of identification, one of which must be a photo identity and the other confirmation of address. If the DSRR is a query of a general nature which will not require the processing of personal data, then no further means of identification shall be requested from the data subject.

If the person making the request is not the data subject, written confirmation that the person making the request is authorized to act on behalf of the data subject is required, unless the person acting on behalf of the data subject is a legal professional.

iii. Information for DSRRs

Where the Administration and Data Protection Officer is reasonably satisfied with the information received, she/he will notify the person making the request that his/her DSRR will be responded to within one (1) month. The one (1) month time period begins from the date that any required documents are received. The person making the request will be informed by the Administration and Data Protection Officer in writing if there will be any deviation from the one (1) month timeframe due to other intervening events in line with clause 2 above.

iv. Review of Information

The Administration and Data Protection Officer will contact and ask the relevant unit(s) and/or department(s) for the required information as requested in the DSRR. This may also involve an initial meeting with the relevant unit(s) and/or department(s) to go through the request, if required. The unit(s) and/or department(s) which hold the information must return the required information by the deadline imposed by the Administration and Data Protection Officer and/or a further meeting is arranged with the unit(s) and/or department(s) to review the information. The Administration and Data Protection Officer will determine whether there is any information which may be subject to an exemption and/or if consent is required to be provided from a third party.

The Administration and Data Protection Officer must ensure that the information is reviewed/received by the imposed deadline to ensure the one (1) month timeframe is not breached.

v. Response to Access Requests

The Administration and Data Protection Officer will provide the finalized response together with the information retrieved from the unit(s) and/or department(s) and/or a statement that the IIJ does not hold the information requested, or that an exemption applies. The Administration and Data Protection Officer will ensure that a written response will be sent back to the person making the request. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the personal data shall be provided in a commonly used electronic form. The IIJ shall only provide information via channels that are secure. When hard copies of information are posted, they will be sealed securely and sent by recorded delivery.

In the case of other DSRRs the Administration and Data Protection Officer shall provide the data subject with a reply in writing to the request. In the event that the request is not aceded to the Administration and Data Protection Officer must inform the data subject of the reasons for the refusal of the request and of their right to file a complaint with the Information and Data Protection Commissioner should they disagree with such refusal.

vi. Archiving

After the response has been sent to the person making the request, the DSRR will be considered closed and archived by the Administration and Data Protection Officer.

5. Exemptions

An individual does not have the right to access information recorded about someone else, unless they are an authorized representative, or have parental responsibility.

The IIJ is not required to respond to requests for information unless it is provided with sufficient details to enable the location of the information to be identified, and to satisfy itself as to the identity of the data subject making the request.

In principle, the IIJ will not normally disclose the following types of information in response to a DSAR:

- Information about other people – a DSAR may cover information which relates to an individual or individuals other than the data subject. Access to such data will not be granted, unless the individuals involved consent to the disclosure of their data;

- Repeat requests – where a similar or identical request in relation to the same data subject has previously been complied with within a reasonable time period, and where there is no significant change in personal data held in relation to that data subject, any further request

made within a six (6) month period of the original request will be considered a repeat request, and the IIJ will not normally provide a further copy of the same data;

- Publicly available information – the IIJ is not required to provide copies of documents which are already in the public domain.

- Opinions given in confidence – the IIJ does not have to disclose personal data held in relation to a data subject that is in the form of an opinion given in confidence.

- Privileged documents – any privileged information held by the IIJ need not be disclosed in response to a DSAR. In general, privileged information includes any document which is confidential and is created for the purpose of obtaining or giving legal advice.

- If the information is kept only for the purpose of statistics or research, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved.

- Requests made for other, non-data protection purposes.

In the case of other DSRRs the IIJ may refuse requests where the processing of personal data is necessary:

(a) for compliance with a legal obligation;
(b) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or
(c) for the establishment, exercise or defence of legal claims
(d) for any other valid reason at law depending on the circumstances of the particluar DSRR.

Responsibilities

The overall responsibility for ensuring compliance with a DSRR rests with the Administration and Data Protection Officer.

If the IIJ is acting as a data controller towards the data subject making the request, then the DSRR will be addressed based on the provisions of this procedure.

If the IIJ is acting as a co-controller with another entity, the Administration and Data Protection Officer shall also forward the request to the appropriate joint-controller with whom the IIJ processes personal data of the data subject making the request.

Breach statement

Violations of this protocol by staff members will be thoroughly examined. As previously mentioned in this regulation any observed or reported breaches shall be forwarded to the IIJ Administration and Data Protection Officer on dimechk@theiij.org for further investigation.