Olivelabs.AI

Data Subject Requests Manual

Version 1.0

PURPOSE

This Data Subject Requests Manual (‘Manual’) establishes an effective, accountable, and transparent framework for ensuring compliance with the requirements regarding data subject rights under the General Data Protection Regulation (GDPR)/ California Consumer Privacy Act (CCPA).

SCOPE AND APPLICABILITY

The Manual applies across all entities or subsidiaries owned, controlled, or operated by Olivelabs.AI (herein referred to as organization) and to all personnel, including temporary or contract employees, that handle Personal Data on behalf of the organization.

DEFINITION

- Controller shall mean the party responsible for determining the purposes and means of processing the Personal Data;
- Data Subject means a natural person whose Personal Data is processed by a controller or processor;
- A Data Subject Request (‘DSR’) is a request made by a Data Subject to exercise any or all of the rights mentioned under para 5.1 below.
- Personal Data has the meaning given to it in GDPR/CCPA and shall include any information relating to an identified or identifiable natural person.
- Processor shall mean the party who processes Personal Data on behalf of Controller;
- Processing includes any operation performed on Personal Data, whether or not by automated means, including collection, use, recording, etc.
- Supervisory Authority shall have the meaning assigned to it under the GDPR/CCPA ;

ROLES AND RESPONSIBILITIES

The Privacy Officer is responsible for ensuring compliance with related legislation requirements regarding handling DSR at the organization.

All functions/staff that handle Personal Data are responsible for processing it in compliance with the relevant privacy policies and procedures.

REQUIREMENTS

GDPR/CCPA provides certain rights to Data Subjects regarding processing their Personal Data. Individuals can request that we exercise these rights as part of our relationship with them.

Under the GDPR/CCPA, organizations must respond to such requests within one month. Failure to do so would amount to non-compliance with GDPR/CCPA and could lead to risks, including administrative fines.

The manual describes enabling individuals to exercise their data subject rights. Key considerations are as follows:

1. All staff must be aware of their responsibilities to provide information when receiving data subject access requests. When a DSR is received, it should immediately be reported to the info@olivelabs.ai Data Protection Officer to log and track each request.
2. The preferred mode of making a DSR would be as per para 10 below, without limitation to other media.
3. The statutory response time is one month.

PROCEDURE

When a DSR is received from an individual, it should immediately be reported to the Data Protection Officer at info@olivelabs.ai, who will log and track each request. If you are asked to provide information, you will need to consider the following before deciding how to respond:

Under GDPR/CCPA, individuals have the following rights:

- To be informed of the processing of their Personal Data;
- To access their own data;
- To rectification;
- To erasure (Right to be Forgotten);
- To restrict of the processing,
- To data portability;
- To object;
- To object to automated decision-making.

DSR can be raised as per the process mentioned below:

The type of access you must provide, and the fee you are allowed to charge may vary depending on how the records are held.

Suppose a request has already been complied with, and an identical or similar request is received from the same individual. The second request can be charged a fee unless a reasonable interval

has elapsed.

Requests should include the entire organization, date of birth, and address of the person seeking access to their information. To comply with the GDPR/CCPA, information relating to an individual must only be disclosed to them or someone with their written authority to receive it.

Before processing a request, the requestor's identity must be verified. Examples of suitable documentation include:

- valid passport
- valid identity card
- valid driving license
- birth certificate and other proof of address, e.g., an organization's utility bill.

No fee can be charged for providing information in response to a data subject access request unless it is 'manifestly unfounded or excessive,' mainly because it is repetitive. Alternatively, we may refuse the request on appropriate grounds.

SUBJECT ACCESS REQUESTS MADE BY A REPRESENTATIVE OR THIRD PARTY

Anyone with full mental capacity can authorize a representative/third party to help them make a data subject request. Before disclosing any information, the organization must be satisfied that the third party has the authority to request on behalf of the requestor and that the appropriate authorization to act on their behalf is included.

COMPLAINTS

Suppose a Data Subject is dissatisfied with how we handled their subject access request. In that case, they should be advised to exercise their right to complain against us with the relevant Supervisory Authority.

PROCESSING DSR

Where business units within an organization process a large quantity of information about a Data Subject, they should request the Data Protection Officer to ask such an individual to provide more specifics on the Personal Data sought.

The GDPR/CCPA does not include an exemption for requests that relate to large amounts of data, but we may consider whether the request is manifestly unfounded or excessive.

If a decision is made to refuse a DSR, we must explain why the request is being refused within one month. In addition, we must inform the individual requesting their right to complain to the relevant Supervisory Authority.

Considering the administrative costs of providing the information, a reasonable fee may only be applied where requests are deemed manifestly unfounded or excessive, mainly because they are repetitive. Should the decision be taken to charge a fee, this must be communicated to the individual making the request.

The onus is on the officials in business areas handling the DSR to identify the relevant Personal Data and where the data is held. In doing so, these officials must have regard to the following:

Consider all electronic and manual filing systems and any third-party data processors who may also hold relevant Personal Data.

Personal Data may be structured or unstructured and stored in electronic and paper-based filing systems. Every effort should be made to identify and supply data held on an individual.

Retrieve all relevant data and prepare for action as per the DSR. For example, in case of a request to access, a copy of retrieved Personal Data would be made available to the Data Subject concerned after redacting the Personal Data of other individuals.

The business unit official prepares a schedule listing the data provided and a breakdown of any data refused or redacted, which will accompany the data provided to the individual. The schedule should also provide information on

- The purposes for processing the data.
- The categories of Personal Data concerned.
- Others outside the function/department to whom the data has been or will be disclosed.
- Whether the data has been or will be transferred outside the organization.
- The period for which the data will be stored or the criteria used to determine retention periods.
- Whether the individual has been subject to automated decision-making.
- Information must be provided in an “intelligible and easily accessible form” so individuals can view and understand their data.

The schedule and the data should be returned to the Data Protection Officer for a response within the required time frame. The letter should mention the Data Subject’s right to complain to the Supervisory Authority and the rights mentioned under Section 6 above. If the request is made electronically, the reply should be provided in a commonly used electronic form unless otherwise requested by the data subject. The data to be supplied will need to be redacted and scanned.

The organization should not retain the data as this is merely generating more copies of existing Personal Data. If a copy is made, it may be retained for a short period, a maximum of one month, in case material goes astray in the post.

MODE OF RAISING A DATA SUBJECT REQUEST

Data subjects should email their DSRs to the Data Protection Officer at info@olivelabs.ai.

We must respond to them in the same way within one month. Due to the complexity or number of DSRs involved, we may extend this period by two months, but we must inform the concerned individual of this within the first month.

One may request information by phone, but verifying identity is very difficult. If we can confirm the identity, we must provide the information requested orally (by phone). This is feasible for small volumes of information, such as confirmation of processing or requests for minimal Personal Data requests. However, it would be a disproportionate effort to provide copies of Personal Data orally in response to a DSR except where the volume of data is low. However, we recognize that visually impaired individuals may have no other means of making a DSR, where they should be provided access through other compatible means and media.

It is not necessary to make a DSR via a solicitor; however, it is an individual's right to do so should they so wish.

We prefer to complete the DSR form and email it to the Data Protection Officer to make your request. Please be as specific as possible so that we can direct your DSR to the appropriate area(s).

The data subject can contact our Data Protection Officer by sending an email at

info@olivelabs.ai

PROVING YOUR IDENTITY

We must protect personal data, but it can only be disclosed under a valid request. The organization must be satisfied that the individual making the DSR is the Data Subject of the Personal Data requested. We, therefore, need to verify the identity of the requestor. We need to collect one of the following forms of identity:

A copy of a photo identity with an address, such as a passport or driving license. The organization shall not retain these documents once we have verified the identity. Please do not collect original documents or

A copy of a photo identity without an address and a copy of a document containing proof of address, e.g., a recent utility bill or a letter from a public service body. The organization shall not retain these documents once we have verified the identity. Please do not collect original documents.

The identity of current staff and contractors can be verified with relevant teams, e.g., the human resources team.

If the Data Subject does not have any of the identity documents above, please direct such an individual to contact the Data Protection Officer at info@olivelabs.ai .

ENFORCEMENT

The violation of the procedure above or any provisions thereof by an employee shall invite disciplinary actions.

Any personnel found to have violated the Manual may be subject to disciplinary actions, including termination of employment and applicable penalties.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Oct 8 2025	Initial Release	Scrut Team	Ashish Sharma	Rukmini