

5. Data Privacy Administration Policy

The data privacy administration policy establishes the administrative processes to administer the data privacy and protection practices, henceforth called, “privacy policy”. This policy is aligned with the European Union’s General Data Protection Regulation (GDPR) and the California Consumer Privacy Act.

5.1 Consent

Given the nature of client data used in the course of DCI business operations, it is the responsibility of the client to obtain consent from its’ employees prior to the transfer of such data. DCI assumes no liability should a data subject submit a complaint regarding DCI’s receipt of their data.

5.2 Employee Personal Data Review

Employees may request copies of their PII to determine its accuracy. Upon reviewing the PII data, an employee may request editing or modifying elements of the data.

- Request for data review or modification will be made to the Business Operations Department.
 - Jerilyn Whitmer, VP of Business Operations
 - jwhitmer@dciconsult.com
 - (202) 280-2178

5.3 Requests from Data Subjects

The following guidelines apply to data requests from data subjects.

5.3.1 Making a Request

Requests are made to the Data Privacy Officer (DPO). The role of the DPO is fulfilled by the IS & Compliance Manager, Cristina Maldonado. The contact information for the DPO is:

- Cristina Maldonado
 - cmaldonado@dciconsult.com
 - (202) 794-7168
- Mailing Address:
 - Cristina Maldonado
 - Data Privacy Officer
 - 1920 I St., N.W.,
 - Washington, DC 20006

5.3.2 Types of Requests

The following types of data requests may be submitted:

- Determine what type of data you have on me
- Correct the data that you have on me
- Erase the data that you have on me
- Transfer the data that you have on me to another place

5.3.3 Responding to Requests: “What type of data do you have on me?”

The company will provide the following:

- Upon receipt for a request for data, the Data Privacy Office has fifteen (15) business days to furnish the information.
- If the request is made by email, the response may be via email.
- If the request is made by written/mail request, the response will be by mail.
- The DPO determines if the data is client or DCI data.
- If the data is supplied to DCI by a client, the DPO:
 - Notifies the client DPO or client point of contact of the request to correct data.
- Notify the requestor that the request was forwarded to the client for action.
- Update the PII Data Request Log of the request and action taken.
- If the data was collected by DCI, the DPO:
 - Determines where the data is located.
 - Submits the data request to the appropriate team to gather the data for sending to the requestor.
 - Upon receiving the data from the team, the DPO sends a list of the requestor’s data to the requestor.
 - Updates the PII Data Request Log of the request and action taken.
- The DPO updates the PII Data Request Log.

5.3.4 Responding to Requests: “Correct the data you have on me.”

The company provides the following:

- The DPO determines if the data is client or DCI data.
- If the data is supplied to DCI by a client, the DPO:
 - Notifies the client DPO or client point of contact of the request to correct data.
 - Notifies the requestor that the request was forwarded to the client for action.
 - Updates the PII Data Request Log of the request and action taken.
- If the data was collected by DCI, the DPO:
 - Determines where the data is located.
 - Submits the data request to the appropriate team for correction action.
 - Verifies that the data correction occurred.
 - Notifies the requestor that the data correction occurred.
 - Updates the PII Data Request Log of the request and action taken.

5.3.5 Responding to Requests: “Erase the data you have on me.”

The company provides the following:

- The DPO determines if the data is client or DCI data.
- If the data is supplied to DCI by a client, the DPO:
 - Notifies the client DPO or client point of contact of the request to erase data.
 - Notifies the requestor that the request was forwarded to the client for action.
 - Update the PII Data Request Log of the request and action taken.

- If the data was collected by DCI, the DPO:
 - Determines where the data is located.
 - Submits the data request to the appropriate team for erasure action.
 - Verifies that the data erasure occurred.
 - Notifies the requestor that the data erasure occurred.
 - Updates the PII Data Request Log of the request and action taken.

5.3.6 Responding to Requests: “Transfer the data you have on me.”

The company will provide the following:

- The DPO determines if the data is client or DCI data.
- If the data is supplied to DCI by a client, the DPO:
 - Notifies the client DPO or client point of contact of the request to transfer data.
 - Notifies the requestor that the request was forwarded to the client for action.
 - Updates the PII Data Request Log of the request and action taken.
- If the data was collected by DCI, the DPO:
 - Determines where the data is located.
 - Submits the data request to the appropriate team for transfer action.
 - Obtains the data in a machine readable (CVS or Excel) from the team.
 - Sends the data to the controller in accordance with the client request.
 - Updates the PII Data Request Log of the request and action taken.

5.3.7 PII Data Request Log

A PII Data Request Log is maintained on all actions generated by request from data subjects. The PII Data Request Log records:

- Who requested
- What was requested
- Actions taken by DCI
- When action was completed

Requests will be maintained and retained for six (6) years.

5.3.8 Complaint Handling Process

The DPO provides oversight to the Complaints Handling Process. Data subjects have the right to complain to DCI related to the processing of their personal data, the handling of the data subject’s request, and the data subject’s appeals on how complaints have been handled.

Complaints regarding how personal data has been processed are submitted to DCI’s DPO using the contact information above. The DCI DPO will review and respond in writing to a complaint within 15 working days of receiving the complaint. If additional time is required DCI will notify the Complainant of the delay and will provide an estimate of when DCI will provide a substantive response.

5.4 Data Protection Vendor Agreements

DCI requires that all vendor agreements document adherence to strong data protection practices to ensure that appropriate controls are in place to protect the company’s data and supporting infrastructure.

5.6. Data Protection Administration Schedule

The company establishes and monitors all policy activities.

| Task | Occurrence | Performed By |
|---|----------------------|-------------------------|
| Prepare process for HR to receive and distribute PII request to DPO | Immediate | Marketing Manager, DPO |
| Act on Data Request for any PII | As needed | DPO |
| Act on Data Request to correct PII | As needed | DPO |
| Act on Data Request to erase PII | As needed | DPO |
| Act on Data Request to Transfer PII | As needed | DPO |
| Establish PII Data Request Log | Immediate | DPO |
| Establish data protection agreements with suppliers | Immediate, As needed | DPO |
| Review Policy | Annually | IS & Compliance Manager |