DCI Consulting Group, Inc.

dciconsult.com

Data Privacy Administration Policy

Policy Published Date: April 15, 2026

1. Data Privacy Administration Policy

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

DCI is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) for any and all handling of personal data as described in this policy. Additionally, DCI has a requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements

1.1 EU-U.S. Data Privacy Framework

DCI complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. DCI has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the EU and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. DCI has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern.

To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF,DCI commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner’s Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF in the context of the employment relationship.

1.2 Consent

In the course of conducting DCI client services, DCI is classified as the “Data Processor” whereas the client is classified as the “Data Controller”. As such, it is the responsibility of the client to obtain consent from its’ employees prior to the transfer of personally identifiable information (PII). DCI assumes no liability should a data subject submit a complaint regarding DCI’s receipt of their data. All data is processed in accordance with the agreed-upon client contract.

1.3 Requests from Data Subjects

At DCI, data subjects are considered the employees of the client. All data subjects have the right to inquire about their data and its intended use. In all instances where such an inquiry is received by DCI, the main client point of contact is engaged for contractual purposes.

The following applies to data requests from data subjects. These rights extend to EU, United Kingdom (UK), and Swiss individuals.

1.3.1 Making a Request

Requests are made to the DPO. The role of the DPO is fulfilled by the Information Security & 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
  - P.O. Box 65780
  - Washington, DC 20035-5780

1.3.2 Types of Requests

The following types of data requests may be submitted:

1. Determine what type of data you have on me.
2. Correct the data that you have on me.
3. Erase the data that you have on me.
4. Transfer the data that you have on me to another place.
5. Limit the use and disclosure of data you have on me.

1.3.2.1 Responding to Requests: "What type of data do you have on me?"

The company performs the following:

- Upon receipt of 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 inform the type of data DCI possesses of the data subject.
- 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 by whom the data was collected and where the data is located.
  - Submits the data request to the client point of contact and 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.

1.3.2.2 Responding to Requests: "Correct the data you have on me."

The company performs 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 by whom the data was collected and where the data is located.
    - Submits the data request to the client point of contact and the appropriate team for corrective 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.

1.3.2.3 Responding to Requests: "Erase the data you have on me."

The company performs 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 by whom the data was collected and where the data is located.
    - Submits the data request to the client point of contact and the appropriate team for erasure action.
    - Verifies the data erasure occurred.
    - Notifies the requestor the data erasure occurred.
    - Updates the PII Data Request Log of the request and action taken.

1.3.2.4 Responding to Requests: "Transfer the data you have on me."

The company performs 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 by whom the data was collected and where the data is located.
    - Submits the data request to the client point of contact and the appropriate team for transfer action.
    - Obtains the data in a machine readable (CSV 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.

1.3.2.5 Responding to Requests: "Limit the use and disclosure of data you have on me."

The company performs 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 limit use and/or disclosure of 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 by whom the data was collected and where the data is located.
    - Submits the data request to the client point of contact and the appropriate team for limiting action.
    - Obtains the data in a machine readable (CSV 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.

1.4 PII Data Request Log

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

- Who requested
- What was requested
- Actions taken by DCI

1.4.1 Complaint Handling Process

The DPO oversees 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 appeal 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 reviews and responds in writing to a complaint within 15 business days of receiving the complaint. If additional time is required, the DPO notifies the Complainant of the delay and provides an estimate of when DCI will provide a substantive response.

DCI is obligated to arbitrate claims and follow the terms as set forth in Annex I of the DPF Principles, provided that an individual has invoked binding arbitration by delivering notice to DCI and following the procedures and subject to conditions set forth in Annex I of Principles.

1.5 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.

DCI performs annual due diligence on all vendors that support storing, processing, or transmission of data. Under no circumstances does DCI transmit, transfer, nor disclose data to any third party for any purpose.

If for any legitimate business justification, the transfer of personal information to a third party takes place acting as an agent on behalf of DCI, DCI remains liable if personal information is processed in a manner inconsistent with its intended use.