



DATA PRIVACY FRAMEWORK STATEMENT

October 30, 2023 | Version 2

Overview

As set forth in Abacus' Global Code of Conduct: "We respect the confidentiality and privacy of our clients, our people and others with whom we do business."

Abacus Information Technology, LLC d/b/a Abacus Group, LLC and GoVanguard NJ LLC (doing business as Gotham Security). (together "Abacus") complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), 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. Abacus 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 European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Abacus 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 Data Privacy Framework Policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. Abacus U.S. is subject to investigatory and enforcement powers of the U.S. Federal Trade Commission.

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

We previously certified with the requirements of the EU-US Privacy Shield Framework in relation to our processing of personal data.

This Data Privacy Framework Policy applies to personal information within the scope of Abacus' Data Privacy Framework certification, which covers the following categories of information:

- Personal information regarding current, former and prospective partners, principals and employees for the purposes of operating and managing Abacus, performing human resource administration and maintaining contact with individuals.
- Personal information regarding current, former and prospective clients and their personnel or others for the purposes of delivering Abacus services, maintaining ongoing relationships and performing business development activities.
- Personal information regarding our third parties (e.g., vendors, service providers, etc.) and their personnel for the purposes of managing and administering Abacus' business relationships with such third parties.
- Additionally, Abacus may, from time to time, collect personal information from the general public in order to answer inquiries or provide information requested.

- Collected personal data may include: contact information, name, work email address, work mailing address, work telephone number, title, and company name.

For the purposes of this Data Privacy Framework Policy, “personal information” means information that is about, or pertains to a specific individual and can be linked either directly or indirectly to that individual. In addition, certain personal information covered by Abacus’ Data Privacy Framework certification may be subject to more specific privacy policies of Abacus, which are also consistent with the requirements of the Principles, and in the case of any conflict between these policies and the Principles, the Principles will control.

For example:

- Certain Abacus websites maintain their own privacy policies that apply to personal information collected via those sites. These policies may be accessed through those websites.
- Personal information obtained from or relating to clients or former clients is further subject to the terms of any specific privacy notice provided to the client, any contractual arrangements with the client and applicable laws and professional standards.

Individual Notice and Choice

We collect and process personal information from certain individuals and for the purposes described in this Data Privacy Framework Policy. Personal information covered by this Data Privacy Framework Policy is collected and processed only as permitted by the Principles.

Notice to individuals regarding the personal information collected from them and how that information is used may be provided through this Data Privacy Framework Policy, other Abacus website notices, or other direct forms of communication with appropriate parties, such as contracts or agreements.

Disclosures & Accountability for Onward Transfers

Consistent with the Principles, Abacus may transfer personal information to third parties, including transfers from one country to another. We will only disclose an individual’s non-public personal information to third parties under one or more of the following conditions:

- The disclosure is to a third party providing services to Abacus, or to the individual, in connection with the operation of our business, and is consistent with the purpose for which the personal information was collected for example, we use an external data centre, cloud services and third party procurement companies..
- We maintain written contracts with these third parties and require that these third parties provide at least the same level of privacy protection and security as required by the Principles, and require that the third party notify Abacus if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles.

- Abacus will take reasonable and appropriate steps to stop and remediate unauthorized processing. To the extent provided by the Principles, Abacus remains responsible and liable under the Principles if a third-party that it engages to process personal information on its behalf does so in a manner inconsistent with the Principles, unless Abacus proves that it is not responsible for the matter giving rise to the damage.
- With the individual's permission to make the disclosure;
- Where required to the extent necessary to meet a legal obligation to which Abacus is subject, including a lawful request by public authorities and national security or law enforcement obligations and applicable law, rule, order, or regulation.
- Where reasonably necessary for compliance or regulatory purposes, or for the establishment of legal claims.

Individuals' rights and choice

Individuals whose personal information is covered by this Data Privacy Framework Policy have the right to access the personal information that Abacus maintains about them as specified in the Principles.

Individuals may contact us to limit the use and disclosure of their personal data. Individuals may also contact us to correct, amend or delete such personal information if it is inaccurate or has been processed in violation of the Principles. Requests for access, correction, amendment or deletion should be sent to: privacy@abacusgroupllc.com.

Abacus will consider all such requests and provide our response within a reasonable period (and in any event within one month of your request unless we tell you we are entitled to a longer period under applicable law). Please note, however, that certain personal data may be exempt from such requests in certain circumstances, for example if we need to keep using the information to comply with our own legal obligations or to establish, exercise or defend legal claims.

Individuals have a right to ask us to restrict the way that we process their personal information in certain specific circumstances. As such they can choose to opt out of whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individual. Any such opt-out requests should be sent to privacy@abacusgroupllc.com

Security

Abacus takes appropriate measures to protect personal information in its possession to ensure a level of security appropriate to the risk of loss, misuse, unauthorized access, disclosure, alteration, and destruction. These measures take into account the nature of the personal information and the risks involved in its processing, as well as best practices in the industry for security and data protection.

Data Integrity and Purpose Limitation

Abacus collects and processes personal information only to the extent that it is compatible with the purposes for which it was collected or subsequently authorized by the data subject. Abacus

does not retain personal information after it no longer serves the purposes for which it was collected or subsequently authorized. Abacus takes reasonable steps to ensure that personal information is accurate, complete, current, and reliable for its intended use.

Non-HR Data Recourse, Enforcement, and Liability

In compliance with the Principles, Abacus commits to resolve Principles-related complaints about our collection and use of your personal information. EU, UK and Swiss individuals with inquiries or complaints regarding our handling of personal data received in reliance on the EU-U.S. DPF and the Swiss-U.S. DPF should first contact Abacus at: privacy@abacugroupllc.com. Abacus has a policy of responding to individuals within forty-five (45) days of an inquiry or complaint.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Abacus commits to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and Swiss-U.S. DPF to the International Centre for Dispute Resolution/American Arbitration Association (ICDR/AAA) <https://www.icdr.org/dpf>, an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit https://go.adr.org/dpf_irm.html for more information or to file a complaint. The services of the ICDR/AAA are provided at no cost to you.

If your complaint is not resolved by us or by the ICDR/AAA, you may, under certain conditions, have the option to invoke binding arbitration under the Principles. For further information, please see the Data Privacy Framework website (<https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf>).

Renewal and Verification

Abacus will renew its EU-U.S. DPF and Swiss-U.S. DPF certifications annually, unless it subsequently determines that it no longer needs such certification or if it employs a different adequacy mechanism.

Prior to the re-certification, Abacus will conduct an in-house verification to ensure that its attestations and assertions about its treatment of Individual Customer and Personnel Personal Data are accurate and that the company has appropriately implemented these practices. Specifically, as part of the verification process, Abacus will undertake the following:

- Review this Data Privacy Framework Policy and its publicly posted website privacy policy to ensure that these policies accurately describe the practices regarding the collection of Individual Customer Personal Data
- Ensure that the publicly posted privacy policy informs Individual Customers of Abacus' participation in the EU-U.S. DPF and Swiss-U.S. DPF programs and where to obtain a copy of additional information (e.g., a copy of this Policy)
- Ensure that this Policy continues to comply with the Data Privacy Framework Principles
- Confirm that Individual Customers are made aware of the process for addressing complaints and any independent dispute resolution process (Abacus may do so through its publicly posted website, Individual Customer contract, or both)

- Review its processes and procedures for training Employees about Abacus' participation in the Data Privacy Framework programs and the appropriate handling of Individual's Personal Data

Abacus will prepare an internal verification statement on an annual basis.

Modifications

Abacus may update this Policy at any time by publishing an updated version here. We will not update this Data Privacy Framework Policy in contravention to the Principles so long as we remain certified to the Data Privacy Framework.