Contrast Security, Inc.
Data Privacy Framework Privacy Policy

Contrast Security, Inc. ("Contrast") complies with the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework, and the UK Extension to the EU-U.S. Data Privacy Framework (collectively, the "DPF") as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Data transferred to the United States from the European Union ("EU"), Switzerland, and the United Kingdom ("UK"), respectively. Contrast has certified to the Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles when processing Personal Data regarding individuals who reside in the EU and the UK, and to the Swiss-U.S. Data Privacy Framework Principles when processing Personal Data regarding individuals who reside in Switzerland (collectively, the "DPF Principles"). For purposes of this Data Privacy Framework Privacy Policy ("Policy"), "Personal Data" means any information received by Contrast from the EU, Switzerland, or the UK recorded in any form, which relates to a natural person who is identified in, or identifiable based on, the Personal Data received. More information about the DPF, as well as Contrast's certification to the DPF, are available at www.dataprivacyframework.gov. If there is any conflict between the terms in this Policy and the DPF Principles, the DPF Principles shall govern.

Contrast's Collection and Use of Personal Data as a Service Provider to Its Customers

At its customer's request and on its behalf, Contrast may process Personal Data about EU and Swiss residents. The information collected may include, for example, business contact information (name, email, phone number, company address, etc.); Internet Protocol (IP) address and IP range; domain name(s); web application URL(s); vulnerability and attack data (HTTP request data and a series of method invocations); summary information about what libraries and classes are loaded by each application; sitemap information (including URLs, but not parameters); and software architecture information about back-end components and connections depending on the service or product provided. Contrast may also process Personal Data of EU and Swiss residents obtained through marketing activities, including business card information (name, company name, company email, company phone number), badge scanning at events, and through other various activities e.g., webinars and blog posts. Contrast receives this Personal Data in order to provide the services, to support the customer in the use of Contrast's products and services, and in furtherance of Contrast's continued operations. When Contrast processes this Personal Data on behalf of a customer, it does so only for the purpose of providing services in accordance with its customer's instructions.

Contrast's Disclosure of Personal Data

Contrast may disclose Personal Data of EU and Swiss residents, subject to written agreement, to authorized third-party service providers who assist Contrast in providing services to its customers. These third-party service providers may, for example, perform tasks on Contrast's behalf, including customer support, providing a customer relations

management database, and provision of email services. Upon notice, Contrast will act promptly to stop and remediate unauthorized processing of Personal Data by a recipient.

Contrast is accountable for Personal Data that it receives in the United States under the DPF and subsequently transfers to a third party as described in the DPF Principles. In particular, Contrast remains liable under the DPF Principles if third-party service providers that it engages to process Personal Data on its behalf do so in a manner inconsistent with the DPF Principles, unless Contrast is not responsible for the event giving rise to the damages.

Contrast may be required to disclose, and may disclose, Personal Data in response to lawful requests by public authorities, including for the purpose of meeting national security or law enforcement requirements.

Choices for Limiting the Use and Disclosure of Personal Data

Contrast relies on its customers to provide EU and Swiss residents with respect to whom the Customer requests a background report with clear, conspicuous, and readily available mechanisms to opt out from: (a) the disclosure of their Personal Data to a non-agent third party; and (b) the use of their Personal Data for purpose(s) that are materially different from the purpose(s) for which the Personal Data was originally collected or subsequently authorized by the individual. Contrast will follow its customers' instructions regarding the choices made by individuals.

Contrast does not review data processing notices provided by customers to EU and Swiss residents, or authorizations to the customer from EU and Swiss residents who are the subject of a background check requested by a customer to determine whether the notices or authorizations are in compliance with, or conflict with, applicable law or any policy or notice published by the customer. Contrast's customers are responsible for providing notices and authorizations that comply with their policies and applicable laws.

If, and to the extent, Contrast collects sensitive Personal Data (e.g., Personal Data which specifies (i) medical or health conditions, (ii) race or ethnic origin(s), (iii) political opinions, (iv) religious or philosophical beliefs, (v) trade union membership, (vi) sex life or sexual orientation, and/or (vii) other expressly delineated types of information by Privacy Shield Principles), Contrast obtains (directly or through Contrast's customer) affirmative express consent, i.e., opt-in, from the relevant EU or Swiss resident, with certain exceptions permitted by the DPF Principles, before such information is to be (i) disclosed to a third party, or (ii) used for a purpose other than those for which the sensitive Personal Data was originally collected or subsequently authorized by the EU or Swiss resident.

EU and Swiss residents who wish to exercise their Personal Data choices, including their choice to limit the use or disclosure of their Personal Data, as described in this Policy should submit their requests to privacy@contrastsecurity.com.

Individuals' Right to Access and Correct Their Personal Data

When Contrast receives Personal Data, it does so on its customer's behalf. Because Contrast acts as a data processor for Contrast's customers, it may be necessary for Contrast to direct an individual to Contrast's customer to provide the requested access.

Upon request and subject to the limitations and restrictions established by the DPF Principles, Contrast will, in cooperation with the relevant customer, grant EU and Swiss residents access to their Personal Data and will permit them to correct, amend or delete Personal Data that is inaccurate or incomplete or that is being processed in violation of the DPF Principles. Contrast is not responsible for errors that exist within third-party record sources. EU and Swiss residents who wish to exercise these rights can do so by contacting privacy@contrastsecurity.com. For security purposes, Contrast may require verification of the requester's identity before providing access to Personal Data.

Recourse, Enforcement and Liability

In compliance with the DPF Principles, Contrast commits to resolve complaints about its processing of the Personal Data of EU and Swiss residents in accordance with the DPF Principles. Any EU or Swiss resident who has a complaint regarding this Policy and/or Contrast's processing of his/her Personal Data should first submit the complaint to privacy@contrastsecurity.com. Contrast will promptly investigate, and attempt to resolve, such complaints in accordance with this Policy and the DPF Principles.

Contrast has further committed to refer unresolved privacy complaints under the DPF Principles to an independent recourse mechanism. Any individual who is not satisfied with Contrast's internal resolution of a complaint may seek redress with the Privacy Trust DPF Service if they reside in the EU and with the Swiss Federal Data Protection and Information Commissioner if they reside in Switzerland. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit https://www.jamsadr.com/eu-us-data-privacy-framework for more information and to file a complaint at no cost to you. In certain circumstances, the DPF provides the right to invoke binding arbitration to resolve complaints not resolved by other means, as described in Annex I to the DPF Principles.

The Federal Trade Commission has jurisdiction over Contrast's compliance with the DPF. Contrast is subject to the investigatory and enforcement powers of the Federal Trade Commission.

For More Information

EU and Swiss residents with questions about how Contrast processes Personal Data should first contact Contrast's customer on whose behalf Contrast collected that collected the Personal Data. When necessary, Contrast can be contacted at: privacy@contrastsecurity.com.