

# Data Privacy Framework Notice

Ironclad 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. Ironclad 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. Ironclad 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 DPF program, and to view our certifications, please visit <https://www.dataprivacyframework.gov/>.

Ironclad is subject to the investigatory and enforcement powers of the Federal Trade Commission in the case of any failure to comply with the DPF.

Ironclad is responsible for the processing of personal data we receive under the DPF. See Ironclad's [Privacy Policy](#) for information on what data we process, the purpose for which we process the data, and the third parties who may receive the data. When we receive personal data under the DPF and then transfer it to a third-party acting as our agent on our behalf, we may have certain responsibility under the DPF if both (a) the agent processes the personal data in a manner inconsistent with the DPF and (b) we are responsible for the event giving rise to the damage. Ironclad complies with the DPF Principles for all onward transfers of personal data from the EU, UK, and Switzerland, including onward transfer liability provisions.

If you are an EEA, UK, or Swiss citizen you may be able to exercise certain choices under the DPF regarding how some of your personal data is used and disclosed, and may access, correct or delete certain personal data. For more information on how to exercise these choices, please contact us using the information in the "Contact Us" section of Ironclad's [Privacy Policy](#). Because Ironclad often acts as its customers' "processor" within the meaning of the EEA, UK, and Swiss laws, we often must refer such requests to our customers to handle, consistent with such laws and the DPF Principles.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Ironclad commits to refer unresolved complaints concerning their handling of personal 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 to JAMS, an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgement 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://www.jamsadr.com/DPF-Dispute-Resolution> for more information or to file a complaint. The services of JAMS are provided at no cost to you. In certain conditions, if your DPF complaint has not been resolved following the JAMS procedure above and taking certain other steps, you may be able to invoke binding arbitration through a DPF panel, in accordance with the DPF at <https://www.dataprivacyframework.gov/framework-article/ANNEX-I-introduction>.

## Digital Services Act

The Digital Services Act ("DSA") went into effect in February 2024. If you are an EU resident, please see the following DSA disclosures.

Ironclad's [Terms of Service](#) explain the restrictions on the use of Ironclad's platform and how Ironclad monitors and enforces those restrictions. Users of Ironclad's platform may reach out to [privacy@ironcladhq.com](mailto:privacy@ironcladhq.com) if the user believes any content on the platform is

illegal.

Communications regarding the DSA should be directed to Ironclad's privacy team ([privacy@ironcladhq.com](mailto:privacy@ironcladhq.com)).

## Export Control & Economic Sanctions

In order to comply with US export control and economic sanctions laws and regulations, Ironclad does not support user access to Ironclad's application from the following countries: Cuba, Iran, North Korea, Ukraine, and Syria. More information about US export control and economic sanctions laws and regulations can be found at:

[US Department of Commerce's Bureau of Industry and Security](#)

[US Treasury Department's Office of Foreign Assets Control](#)

## Cybersecurity and Firewall Factors

Access to Ironclad's platform has also been restricted in Russia to address latency issues caused by a high volume of spam-related traffic. We will whitelist IP addresses in Russia so that they can access the application upon request.

Though Ironclad has not blocked access to our platform in China, the platform generally cannot be accessed due to government firewalls.