Pindrop Security
EU/UK/Swiss – US Data Protection Framework Statement

Effective: March 27, 2025

Pindrop Security, Inc. (**Pindrop**) complies with the EU-U.S. Data Privacy Framework (**EU-U.S. DPF**), the UK Extension to the EU-U.S. DPF (**UK Extension**), and the Swiss-U.S. Data Privacy Framework (**Swiss-U.S. DPF**) (together, the **Data Privacy Framework** or **DPF**) as set forth by the U.S. Department of Commerce.

Pindrop 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. Pindrop also 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. We refer to the EU-U.S. DPF Principles and the Swiss-U.S. DPF Principles as the **DPF Principles**.

The nature and scope of the personal data Pindrop receives in reliance on the DPF Principles are described in Section 1 (Scope of this DPF Statement and Purposes of Personal Data Processing) below.

If there is any conflict between the terms in this DPF Statement and the DPF Principles, the DPF Principles shall govern.

Visit https://www.dataprivacyframework.gov/ to learn more about the Data Privacy Framework program and to see our certification.

1. Scope of this DPF Statement and Purposes of Personal Data Processing

Pindrop Security, Inc., together with its subsidiaries operating in the United Kingdom (Pindrop Security UK Ltd.) and France (Pindrop Security SAS), provides authentication and anti-fraud solutions to our business customers in connection with their dealings with their own clients and prospective clients (**users**). Where we are acting as a processor to our customers, our customer's privacy notice and/or their agreement with the user will dictate the scope and manner of processing.

When our customers purchase one of these solutions, they may provide us with the personal data of customer users and ask us to process that data at the customer's direction, as a processor on behalf of our customer. This personal data may include a telephone number, and it may include data elements extracted from the audio portion of calls placed with the customer's service center by a user.

Our solutions use this information to help authenticate and/or verify users according to our customers' specifications and to inform fraud risk analyses generated by our products and services when our customers confirm that certain information was involved in actual or suspected fraud.

Where the user is calling one of our customers in the EU, UK or Switzerland, the user's telephone number may be transferred to Pindrop Security, Inc., our U.S. based entity, in reliance on the DPF Principles.

2. Pindrop's Adherence to the DPF Principles

Pindrop has certified that it adheres to the DPF Principles: Notice, Choice, Accountability for onward transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability with respect to telephone numbers received from the EU, UK, or Switzerland in reliance on the DPF.

Notice

Pindrop acts as a processor of the telephone numbers that are transferred to us in the U.S. by, or on behalf of, one of our customers in the EU, UK or Switzerland. Our customer is responsible for providing appropriate notice to its users and ensuring it is collecting the telephone number in reliance on an appropriate legal basis.

We also provide information in this DPF Statement about the telephone numbers transferred in reliance on the DPF Principles and the purposes of processing those numbers on behalf of our customers.

In addition, Pindrop provides in our GDPR Privacy notice available here (https://www.pindrop.com/privacy/gdpr-privacy-notice) and in our Pindrop Solutions notice available here (https://www.pindrop.com/pindrop-solutions) more general information about the types of personal data we collect, purposes of processing, sharing of personal data with third

parties, the rights data subjects have for limiting the use and disclosure of their personal data, and how to contact us about our personal data practices.

Choice

Pindrop acts as a processor of the telephone numbers that are transferred to us in the U.S. by, or on behalf of, one of our customers in the EU, UK or Switzerland. Our customer is responsible for providing certain choices to its users about the use of their personal data. Pindrop will assist our customers with their response to individuals who wish to exercise their choices regarding their personal data

Accountability for Onward Transfer

From time to time, it will be necessary to share the telephone numbers covered by this DPF Statement with Pindrop group entities. Pindrop may also appoint third-party agents (service providers that process personal data under our instructions) to assist us in providing information, solutions or services to our customers. Pindrop may share user telephone numbers with these related entities and third-party service providers to perform services that these parties have been engaged by Pindrop to perform on Pindrop's customer's behalf, subject to appropriate contractual restrictions and security measures, or if we believe it is reasonably necessary to prevent harm or loss, or we believe that the disclosure will further an investigation of suspected or actual illegal activities.

Pindrop will remain responsible for the processing of telephone numbers it receives under the DPF and subsequently transfers to a third party acting as an agent, unless we are able to prove that neither we, nor our third-party service providers, are responsible for the event giving rise to damage.

If Pindrop transfers personal data covered by this DPF Statement to a third party acting as a controller, the transfer will be consistent with any notice provided to the relevant users and any consent they have given (where applicable), and only if the third party has provided contractual assurances that it will (i) process the personal data for limited and specified purposes consistent with any consent provided, (ii) provide at least the same level of protection as is required by the DPF Principles and notify us if it makes a determination that it cannot do so; and (iii) cease processing the personal data or take other reasonable and appropriate steps to remediate if it cannot provide the level of protection required by the DPF Principles. If Pindrop has knowledge that a third party acting as a controller is processing the telephone numbers transferred reliant on the DPF in a way that is contrary to the DPF Principles, Pindrop will take reasonable steps to prevent or stop such processing.

Pindrop may be required to disclose telephone numbers covered by this DPF Statement in response to lawful requests by public authorities, which may include complying with national security or law enforcement requirements.

Security

We have implemented commercially reasonable precautions designed to protect personal data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. Please be aware that no data security measures can guarantee 100% security. Our policies and controls permit only authorized employees, who are trained in the proper handling of personal data, to have access to that data. Pindrop conducts periodic reviews of employee compliance with these policies. Employees who violate our security and privacy policies may be subject to disciplinary procedures.

Data Integrity and Purpose Limitation

Pindrop retains personal data covered by this DPF Statement as instructed by its customers acting as controllers. Personal data may also be retained for a period of time necessary to comply with state, local, federal regulations, or country specific regulations and requirements, and in accordance with Pindrop's Records and Information Management Policy.

Pindrop will not use the telephone numbers covered by this DPF Statement in a manner that is incompatible with the purpose for which they were originally collected, except as required or permitted by applicable law.

Access

When Pindrop receives the telephone numbers covered by this DPF Statement, Pindrop acts as a processor for its customers and our customers are responsible for providing users with access to the telephone numbers, and the right to correct, amend or delete those numbers where it is inaccurate or where they have been processed in violation of the DPF Principles, as appropriate. Users should direct their questions to the appropriate Pindrop customer. If a user is unable to contact the appropriate customer, or does not obtain a response from the customer, Pindrop will provide reasonable assistance in forwarding the user's request to the customer.

Recourse, Enforcement and Liability

Pindrop is subject to the investigatory and enforcement powers of the US Federal Trade Commission (FTC), which has jurisdiction over Pindrop's compliance with this DPF Statement and the DPF Principles.

In compliance with the DPF Principles, Pindrop commits to resolve DPF Principles-related complaints about our collection or use of your personal data covered by this DPF Statement, that is, your telephone number used to contact our customer in the EU, UK or Switzerland.

Users who have inquiries or complaints regarding our handling of the telephone numbers received in reliance on the DPF should first contact Pindrop at legal@pindrop.com

In compliance with the DPF Principles, Pindrop commits to refer unresolved complaints concerning our handling of telephone numbers received in reliance on the DPF to JAMS, an independent, alternative dispute resolution provider based in the U.S. Information about JAMS dispute resolution is available at the following address: https://www.jamsadr.com/DPF-Dispute-Resolution. Pindrop will cooperate with JAMS to resolve DPF related complaints. Accordingly, if you have contacted us at privacy@pindrop.com but 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://www.jamsadr.com/file-a-dpf-claim to file a complaint. The services of JAMS are provided at no cost to you.

If your DPF complaint cannot be resolved through the above channels, you may be entitled, under certain conditions, to invoke binding arbitration for certain residual claims not resolved by other redress mechanisms. See https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf for further information.

Pindrop agrees to periodically review and verify its compliance with the DPF Principles, and to remedy any issues arising out of failure to comply with the DPF Principles. Pindrop understands that if it fails to provide an annual self-certification to the U.S. Department of Commerce, Pindrop will be removed from the Department's list of DPF participants.

3. Contact Information

If you have any questions in relation to this DPF Statement or you wish to exercise any of your rights, please contact us at:

privacy@pindrop.com

You may also contact us at:

Pindrop Security, Inc.
1115 Howell Mill Road, Suite 700
Atlanta, GA 30318

Or by phone at: +1(404) 721-3767

4. Changes to this DPF Statement

Any changes or updates we may make to this DPF Statement will be posted on this page in advance. Please check back frequently to see any updates or changes made to this DPF Statement.