INTERCEPT DATA PRIVACY FRAMEWORK POLICY

Scope

This Data Privacy Framework Policy (the "Policy") sets forth the privacy principles that Intercept Pharmaceuticals, Inc. and its subsidiaries (collectively, “Intercept”) follow with respect to Personal Data received from the European Economic Area (“EEA”), Switzerland and the United Kingdom (“UK”).

Intercept has certified that it adheres to the EU-US Data Privacy Framework, UK Extension to the EU-US DPF, and the Swiss-U.S. Data Privacy Framework (collectively, “the DPF”) and the Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability, as set forth by the US Department of Commerce. To learn more about the DPF program, and to view our certification page, please visit https://www.dataprivacyframework.gov/s/.

This Policy applies to the processing of Personal Data that Intercept receives in the United States concerning individuals who reside in the EEA, Switzerland and the UK. This Policy does not cover data from which individual persons cannot be identified.

Intercept employees who handle Personal Data from the EEA, Switzerland or the UK are required to comply with the principles stated in this Policy.

Information Collected

Intercept may collect Personal Data about healthcare professionals, including clinical investigators and their staff; Intercept suppliers, contractors, and their personnel; and Intercept’s current, prospective and former employees. Information collected includes curriculum vitae data, business contact information and other non-sensitive information.

Sensitive information may be collected in certain instances, including from patients or potential patients, with the consent of the individual or where required by applicable law. In some instances, prospective patients or their family members may choose to provide Personal Data to Intercept via our websites in order to request information.

Purposes of Processing

Intercept processes Personal Data to facilitate the development and commercialization of its products and for its business purposes. Personal Data may be used for purposes of clinical research, business development, marketing and sales, regulatory affairs, procurement, human resources management, and other Intercept business activities.

Intercept transfers personal data to third-party processors providing a variety of services, including, but not limited to, clinical trial operations, payroll, systems hosting, and sales and marketing activities.

Onward Transfers to Third Parties

Intercept will take measures to obtain assurances from third-party service providers that process Personal Data on Intercept’s behalf that they will process such information in a manner consistent

with Intercept policies and DPF Principles. Intercept remains responsible under the DPF Principles if third-party service providers that Intercept engages to process Personal Data on its behalf do so in a manner inconsistent with the DPF Principles, except where Intercept is not responsible for the event giving rise to the damage. Intercept will take measures to only disclose Personal Data that is necessary for the third parties to provide the agreed upon services to Intercept. Where Intercept has knowledge that a third-party business partner is using or disclosing Personal Data in a manner contrary to Intercept's privacy policies or DPF Principles, Intercept will take reasonable steps to prevent or stop the use or disclosure.

Intercept may be required to disclose Personal Data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Access

Upon request, and as required by DPF Principles and applicable law, Intercept will provide individuals with reasonable access to Personal Data about them. Intercept will also take reasonable steps to allow individuals to review Personal Data for the purposes of correcting, amending or deleting such information in instances where Personal Data is demonstrated to be incomplete or inaccurate.

Individuals can contact Intercept at privacyprotection@interceptpharma.com in order to request access or to make inquiries regarding limiting the use and disclosure of Personal Data about them.

Dispute Resolution

Intercept is subject to the investigatory and enforcement powers of the US Federal Trade Commission ("the FTC").

Any questions or concerns regarding the use or disclosure of Personal Data should be directed to the Intercept addresses provided below. Intercept will investigate and attempt to resolve complaints and disputes regarding use and disclosure of Personal Data by reference to DPF Principles.

In addition, Intercept has agreed to participate in the following independent dispute resolution procedure in the investigation and resolution of complaints to resolve disputes pursuant to the DPF Principles:

- JAMS
  Information about how to file a complaint with the JAMS DPF program can be found at:
  https://www.jamsadr.com/eu-us-data-privacy-framework

With regard to Personal Data of Intercept employees in the EU, Switzerland or the UK, Intercept agrees to cooperate with competent EU supervisory authorities (Data Protection Authorities), the Swiss Federal Data Protection and Information Commissioner (FDPIC) or the UK Information Commissioner's Office.

An individual may invoke binding arbitration, at his or her own cost, subject to procedures set forth by the EU-US DPF.

Changes to this Policy

This Policy may be amended from time to time, consistent with the requirements of the DPF Principles. Intercept will provide appropriate notice about such amendments.

Contact Information

Intercept Pharmaceuticals, Inc.
Legal Affairs Department
305 Madison Avenue
Morristown, NJ 07960

e-mail: privacyprotection@interceptpharma.com

Updated as of October 2023