

## 1.0 PRIVACY AND YOUR PERSONAL DATA

We are delighted to have you as part of the Intercept Pharmaceuticals, Inc. (“Intercept”) team. As part of the employee enrollment process and in connection with your employment as a member of Intercept, you may be asked to provide, and Intercept may process, certain Personal Data. We respect your privacy and place great importance on maintaining the security of Personal Data.

As part of our commitment to your privacy, we would like to keep you informed of how we use the Personal Data you provide to us.

**Please read this notice carefully.**

## 2.0 PURPOSES OF PROCESSING

Intercept processes certain Personal Data about its employees for purposes of personnel management, career development, information technology support and administration in connection with the employment relationship and employment benefits, the administration of post-employment benefits, as well as to comply with Intercept’s legal, administrative and corporate obligations. Examples of specific activities that may require processing of your Personal Data include:

- compensation, payroll, and benefit planning and administration, including equity grants
- candidate attraction, assessment, selection and onboarding
- talent management, including objective performance management and succession planning
- business travel
- expense management (e.g., corporate card and expense administration)
- administration of employee participation in activities and programs (e.g., wellness activities)
- staffing (e.g., headcount planning, termination,)
- budget planning and administration
- internal investigations and other compliance activities, including assessing employee adherence to Intercept policies and procedures
- managing access to, use of, and security of Intercept systems, facilities and property - including third party premises such as serviced offices (which may, in some instances, include video monitoring in which case further information about such video monitoring will be provided in accordance with applicable law)
- employee education and training

<b>Document #:</b>	Policy-EU-0003	<b>Revision #:</b>	04	<b>Effective Date:</b>	07 May 2023
--------------------	----------------	--------------------	----	------------------------	-------------

- legal proceedings and government investigations, including preservation of Personal Data, when required
- compliance with statutory, regulatory and other legal duties

In the event that processing will occur for reasons outside of those detailed in this Notice, additional notice of that processing will be provided.


### 3.0 LEGAL BASES FOR PROCESSING

The legal bases Intercept relies on when processing employee data are described in the table below.

<b>Processing purpose</b>	<b>Legal basis</b>
To meet contractual obligations	Processing is necessary to meet our obligations of your employment contract with Intercept or to take steps that you request prior to entering into the contract.
To effectively run our business, including for purposes of planning, fraud prevention and safety	These processing activities constitute our legitimate interests. We balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).
To comply with law	Processing is necessary to comply with our legal obligations
With your consent	Processing is based on your consent. Where we rely on your consent you have the right to withdraw it anytime.

### 4.0 TYPES OF INFORMATION WE COLLECT

Examples of information that we may maintain regarding your employment include: name, address, date and place of birth, employment and educational history, academic & vocational attainments, hire date, vacations and benefits, complaints/grievances, bonuses, promotions, reviews and evaluations, work records, information related to health and welfare coverage, retirement plan, your national identification number, and equity plan details. Other types of information that we collect are listed below.

		<b>EU-US Data Privacy Framework (DPF) Policy</b>			
<b>Document #:</b>	Policy-EU-0003	<b>Revision #:</b>	04	<b>Effective Date:</b>	07 May 2023

- Sensitive Personal Data

Intercept may collect and process records of certain Personal Data (which may include, for example, marital status family status, health-related data, religious information or trade-union membership, criminal records) that may be considered “sensitive.” In the event that the collection and processing of sensitive information is necessary, you will receive a separate notice and request for your consent, if required.

- Tax and Finance Personal Data

Intercept may maintain records of certain Personal Data that requires special handling, including, for example, social security and other national identification numbers, bank account and financial information, and driver’s license and government-issued identification card numbers. We will only collect this type of Personal Data when required to do so by labor, tax, social security, or other laws, and/or when reasonably necessary in connection with your employment or Intercept’s business.

- Information on National Origin


Intercept strives to promote a work environment that is open and supportive to people of all backgrounds. Personal Data relating to national origin will be processed by Intercept only for the purpose of determining eligibility and/or requirements to work in the country in which a position is located and/or for anonymous monitoring purposes, to comply with applicable laws.

We collect Personal Data from you but may also collect it from other sources. You will be notified, as required, if we collect the Personal Data from other sources.

## 5.0 USE OF INTERCEPT RESOURCES

Intercept employees are required to read and comply with all applicable Intercept policies, including the applicable Intercept’s Employee Handbook and the Operations Policies set forth therein relating to the use of the Intercept’s equipment, systems and technical resources.

In order to manage information technology-related expenses and maximize system efficiency, Intercept may collect, process and transfer to third-party vendors, information about how its resources are used by employees. For example, Intercept collects and processes information on employee use of its information technology systems (e.g., intranet, internet, email) and telecommunications systems. By gathering this information, Intercept is able to improve and maintain its information technology and telecommunications systems.

		<b>EU-US Data Privacy Framework (DPF) Policy</b>			
<b>Document #:</b>	Policy-EU-0003	<b>Revision #:</b>	04	<b>Effective Date:</b>	07 May 2023

**6.0 NATURE OF DATA PROVISION**

Providing your personal data is essential to comply with the obligations deriving from the employment contract and from the applicable laws. Failure to provide your personal data may therefore result in an inability to commence and/or continue the employment relationship.

**7.0 HOW WE STORE YOUR INFORMATION**

The Personal Data you provide to us may be held and stored electronically and/or in hard copy. Intercept takes reasonable and appropriate security measures consistent with current industry practices to protect your Personal Data.

Intercept employees and authorized third parties (as discussed in the next section) that have access to your Personal Data are bound by strict confidentiality obligations and are required to treat your Personal Data in accordance with legal requirements. In addition, only Intercept employees and authorized third parties who have a legitimate business or legal purpose in accessing and processing your information will be permitted access.


Your Personal Data is only stored for as long as required for the purposes for which it was collected or as required by applicable law.

**8.0 TRANSFER OF INFORMATION TO THIRD-PARTY VENDORS**

When appropriate to support Intercept’s management and administration, Personal Data held by Intercept may be communicated to, disclosed to, transferred to, or processed by authorized third parties, specifically, third-party vendors. For example, Intercept may contract with third parties to assist it in identifying activities that do not comply with Intercept policies, may harm Intercept’s market position or financial integrity, or that may otherwise violate regulatory requirements to which Intercept is subject.

When reasonably necessary in connection with your employment or the business of Intercept, Intercept may transfer or disclose Personal Data to vendors outside of the country in which it was collected (for example, Personal Data may be transferred to the United States or other countries outside of the United Kingdom (“UK”)).

Some non-EU/EEA countries may not afford the same level of protection as in the UK. Intercept will therefore put appropriate legal safeguards in place, as required by applicable law. Intercept is certified to the UK Extension to the EU-US Data Privacy Framework (“DPF”), with respect to certain categories of personal data of UK resident data subjects processed on behalf of and transferred to Intercept in the United States. You can find further information about our commitment to comply with the DPF here.

		EU-US Data Privacy Framework (DPF) Policy			
<b>Document #:</b>	Policy-EU-0003	<b>Revision #:</b>	04	<b>Effective Date:</b>	07 May 2023

## 9.0 YOUR RIGHTS

We want to make sure your Personal Data is accurate and processed in accordance with your rights. You may ask us to take the following actions in relation to your personal data that we process:

- **Access.** Provide you with information about our processing of your personal data and give you access to your data.
- **Correct.** Update or correct inaccuracies in your personal data.
- **Delete.** Delete your personal data.
- **Transfer.** Transfer a machine-readable copy of your personal data to you or a third party of your choice.
- **Restrict.** Restrict the processing of your personal data.
- **Object.** Object to our reliance on our legitimate interests as the basis of our processing of your personal data that impacts your rights.

You also have the right to lodge a complaint to the data protection agency of the country in which you reside.

In compliance with the DPF Principles, we commit to resolve complaints about our collection or use of your Personal Data. UK individuals with inquiries or complaints regarding our DPF policy should first contact Intercept by emailing [privacyprotection@interceptpharma.com](mailto:privacyprotection@interceptpharma.com).

In compliance with the UK Extension to the EU-U.S. DPF, Intercept commits to cooperate and comply respectively with the advice of the UK Information Commissioner’s Office (ICO) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the UK Extension to the EU-U.S. DPF in the context of the employment relationship.

If you decide that you would like to exercise one of your rights, please contact a representative of Intercept’s International HR department or email your request to [privacyprotection@interceptpharma.com](mailto:privacyprotection@interceptpharma.com). You may also contact our Data Protection Officer by emailing [privacyprotection@interceptpharma.com](mailto:privacyprotection@interceptpharma.com) with DATA PROTECTION OFFICER in the subject line to obtain further information regarding your rights or to file a complaint about data processing activities.