



INCYTE PRIVACY NOTICE INCYTE BUSINESS CONTACTS UNITED KINGDOM

We use this Privacy Notice to tell you what personal data we collect from you when you interact with us in the course of business, when visiting Incyte facilities, when fulfilling contract or consulting (individual service provider) roles, or as employees of our business partners. For more information about the collection of your personal data, please contact privacy@incyte.com. For information about how your personal data is treated under the European Union's General Data Protection Regulation (GDPR) when it is transferred into the European Union (EU), please see the EU specific Privacy Notice.

When we collect your personal data:

- We take or require appropriate technical, physical, and organisational measures (such as multifactor password authentication, encryption, access restriction, etc.) to protect your personal data from misuse or unauthorized alteration, loss, or access;
- We collect and use your personal data only for the purpose(s) for which we collect it;
- We only collect the personal data that we need; and
- We keep your personal data up to date and ensure that it is accurate.

This Privacy Notice is effective July 15, 2021.

What personal data do we collect and use and why?

We collect and use the following personal data:

1. Building Visitors

- Contact Information: Your name; email address, and telephone numbers, signature;
- Your job title and employer (if applicable to your visit)
- A standard photo of you for access purposes (if required);
- Records of surveillance cameras, if applicable and as per local legislation; and
- Your fingerprints in order when you access an Incyte building with this capability, if applicable and as per local legislation.
- We collect and use this personal data directly from you or during the course of your visit, our systems, to the extent necessary for the pursuit of Incyte's legitimate interests to manage business operations and for the security of its property, reputation, customers, employees, and third parties.
- We keep and use your information for as long as necessary for the administration of our relationship and for history of our interactions, but longer than three years after your visit.

2. Contractors/Non-HCP Consultants

- **During Your Work for Incyte**
 - Contact Information: Your name; professional email address, professional email address and telephone number, and personal email address and telephone number (as applicable);



- Payment and/or bank details (for those with direct contracts with Incyte).
- Job/position: Contract title and description; Incyte contracting entity name; branch/unit/department; Job location; status and type of contract (full time/part time); actual hours worked for Incyte, start and termination dates, hourly rate, and employer/agency;
- Meetings attended; recordings of those meetings (in compliance with image and voice rights); and materials presented or used;
- Department specific, corporate, and compliance trainings attended and related certificates;
- Department specific, corporate, and compliance policies and procedures read;
- Video or photographs of you in a larger group of employees and contractors as part of corporate projects and company activities such as an annual yearbook or company event;
- IT System identifiers: System-ID; LAN –ID; system-passwords; software- or other licenses; and device identifiers for devices provided by Incyte;
- Log details internal databases and drives;
- Emails and email content created by or received by you where such emails contain your personal data;
- Instant messages created by or received by you where such messages contain your personal data;
- Records of electronic content created by or accessed by you using Incyte systems and Incyte-owned devices;
- Monitoring records of general activity in systems including downloads to USB and uploads to cloud storage services to prevent loss of and unauthorized access to data;
- A standard photo of you for access card purposes;
- Records of surveillance cameras, if applicable and as per local legislation;
- Your fingerprints in order when you access an Incyte building with this capability, if applicable and as per local legislation; and
 - Use of your access card to Incyte premises.
- We collect and use this personal data directly from you, your employer, or in our systems during the course of your work for Incyte, to the extent necessary for the pursuit of Incyte’s legitimate interests to manage business operations and for the security of its property, reputation, customers, employees, and third parties. If you are under contract directly with Incyte, we collect and use the personal data provided by you (1) in performance of a contract with Incyte; and (2) for legal proceedings, investigations, and questions from competent authorities relating to our contract with you.
- We keep and use your information for as long as necessary for the administration of our relationship but for history of our interactions, no longer than three years after the last contact with you. In some of the areas you may support during your contracted work for Incyte, your personal data may be legally required to be kept for longer than three years in which case your personal data will be kept for that required time period instead.
- **When You Give Your Consent**
 - From time to time we may ask for your consent to collect certain personal data from you. You will receive more detailed information on what we want your consent to collect and what it will be used for at that time. In cases where we explicitly rely on your consent or where we mark the provision of data as optional you are not obliged to provide us with the data and in not doing so, your contracted role with Incyte will not be placed in jeopardy.

3. Third-Party/Vendor/Business Partner Employees

- Contact Information: first name; last name; professional address; professional e-mail address;



- professional telephone numbers;
- Job title and description and employer;
- Information specific to our professional interactions such as meetings, meeting notes, and audio or visual recordings;
- System Identifiers: System-ID; LAN –ID; system-passwords; software- or other licenses; and device identifiers for any devices provided to you by Incyte;
- Log details of internal databases and drives for access provided to you by Incyte;
- Emails and email content sent to you from Incyte or sent by you to Incyte where such emails contain your personal data;
- Instant messages sent to Incyte by you where such messages contain your personal data;
- Records of electronic content created by or accessed by you (if accessed) using Incyte systems and Incyte-owned devices;
- Monitoring records of general activity in Incyte systems (if accessed) including downloads to USB and uploads to cloud storage services to prevent loss of and unauthorized access to data;
- We collect and use this personal data directly from you, your employer, or in our systems during the course of your interactions with Incyte, to the extent necessary for the pursuit of Incyte’s legitimate interests to manage business operations and for the security of its property, reputation, customers, employees, and third parties.
- We keep and use your information for as long as necessary for the administration of our relationship but for history of our interactions, no longer than three years after the last contact with you. In some of the areas you may support during your interactions with Incyte, your personal data may be legally required to be kept for longer than three years in which case your personal data will be kept for that required time period instead.

Do you need to provide us with your personal data?

You are not obliged to provide us with your personal data, however you will not be able to take part in any of the activities listed above if you do not do so.

Who do we share your personal data with?

Your personal data is shared by Incyte with:

- Other companies in the worldwide Incyte Group, wherever located (a list of all Incyte companies is available under: <http://www.incyte.com/contact-us/headquarters.aspx>);
- Third party consultants, service providers, partner companies contracted by or on behalf of Incyte or its affiliates, wherever located;
- Healthcare professional boards, authorities, wherever located;
- Government agencies, regulators, or public authorities, but only when they require us to. In some



instances, these government agencies may make your personal data public in accordance with applicable laws or guidelines;

- Publically online as part of mandatory or voluntary transparency disclosures; and
- Where required by institutional policy or government entity, to your employer.

Where is your personal data used or stored?

We transfer your personal data outside of the United Kingdom. Your personal data is transferred:

1. To the European Union, Switzerland, and Japan: The European Union, Switzerland, and Japan are considered as providing adequate data protection standards.
2. To countries where data protection standards have not been determined to be adequate by the United Kingdom: these countries include the United States, India, and China. In these cases we will ensure that any recipients of your personal data are bound by contract to UK data protection standards.

What are your rights?

You have a number of rights that apply to our use of your personal data. The availability of some of these rights depends upon our lawful basis for processing your personal data and your rights may also be subject to certain conditions and restrictions. You may have the right:

- to obtain access to your personal data together with information about how and on what basis that personal data is processed;
- to rectify inaccurate personal data (including the right to have incomplete personal data completed);
- to erase your personal data in limited circumstances where it is no longer necessary in relation to the purposes for which it was collected or processed or where you object to or withdraw your consent. This right may also apply where the processing was unlawful;
- to restrict processing of your personal data where:
 - the accuracy of the personal data is contested;
 - the processing is unlawful but you object to the erasure of the personal data;
 - we no longer require the personal data for the purposes for which it was collected, but it is required for the establishment, exercise, or defense of a legal claim; or
 - you have objected to the processing.
- to challenge processing which we have justified on the basis of a legitimate interest;
- to object to the processing of your personal data;
- to object to decisions which are based solely on automated processing (to the extent that these are taken);
- to withdraw your consent for processing where the legal basis relied on is consent;
- to obtain a portable copy of your personal data, or to have a copy transferred to a third party controller in certain circumstances;



- to obtain more information as to safeguards under which your personal data is transferred outside of the UK (if relevant); or
- to lodge a complaint with the data protection/supervisory authority noted below.

We may ask you for additional information to confirm your identity and for security purposes before processing your request.

Who can you contact regarding your rights?

Data Controller: The entity that determines why and how your personal data is processed is called a Controller. The Controller for the processing of your personal data is the Incyte organisation or affiliate listed below, depending on our relationship with you.

- **Building Visitors:** the Incyte affiliate that you visit.
- **Contractors/Non-HCP Consultants:** the Incyte affiliate who you or your employer have a contract with.
- **Third-Party/Vendor/Business Partner Employees:** the Incyte affiliate who you work with.

A list of all Incyte companies is available under: <http://www.incyte.com/contact-us/headquarters.aspx> .

Data Protection Officer Incyte: privacy@incyte.com

Data Protection Authority/Supervisory Authority: The Data Protection Authority/Supervisory Authority for the processing of your personal data is the Information Commissioner's Office (ICO), <https://ico.org.uk>, or the Data Protection Authority/Supervisory Authority located in the EU country where your personal data is processed. More information about how to contact these authorities can be found here: https://edpb.europa.eu/about-edpb/board/members_en.