Privacy Policy

SCOPE

This Privacy Policy applies to personal information processed by Krystal Biotech, Inc. and its subsidiaries ("**Krystal**," "**we**," "**us**," and "**our**") in the course of our business, as collected on our website (the "**Site**") (regardless of where you visit it from) and via other related online or offline offerings (collectively, the "**Services**").

This Privacy Policy covers our use of "personal information." When we say "personal information," we mean information that relates to you individually or that can be used to identify you as an individual. Personal information does not include data that has been de-identified or aggregated such that you can no longer be identified.

Because we offer our Services on a global basis we have chosen to use the European Union (GDPR) model, often considered as the strictest model for user transparency, as the format for this Privacy Policy. Consequently, based on the location from which you access our Site, you may not necessarily understand the meaning of some of the terms used in this Privacy Policy; we therefore refer you to our Glossary of terms at the end of this Privacy Policy to help you make better sense of this document
This Privacy Policy is provided in a layered format so you can click through to the specific areas set out below. [Alternatively you can download a pdf version of the policy here [LINK]].

Table of contents

I. IMPORTANT INFORMATION AND WHO WE ARE

Purpose of this Privacy Policy

This Privacy Policy aims to give you information on how Krystal collects and processes your personal information through your use of this Site, including any information you may provide through this Site when you access and use our Services, when you contact us using our Contact Us form, or when you apply to one of our available positions.

It is important that you read this Privacy Policy together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you so that you are fully aware of how and why we are using your information. This Privacy Policy supplements the other notices and is not intended to override them.

Controller

Krystal is made up of different legal entities, details of which can be found here. This Privacy Policy is issued on behalf of the Krystal Group so when we mention "Krystal", "we", "us" or "our" in this Privacy Policy, we are referring to the relevant company in the Krystal Group responsible for processing your information. Krystal Biotech, Inc. is the controller and responsible for this Site.

II. WHAT PERSONAL INFORMATION WE COLLECT

When you use our Services, communicate with us or apply for a position, we may collect the following kinds of information:

- Identification data (full name, date of birth, social security number, pseudonymized or de-identified ID number)
- Contact data (phone number, email address, postal address, etc.)
- Connection data (IP address, user settings, IMEI, MAC address, cookie identifiers, pages you visit, items you interact with on our services, etc.)
- Professional data (CV, work experience, current position, etc.)
- Financial data (compensation, tax ID number, bank account details, social security/health insurance details, etc.)

- Location data (geolocation, travels destinations, attendance to events, etc.)
- In very limited cases, Special categories of personal data (race/ethnicity, gender, criminal record, etc.)
- Any information you provide us with directly when interacting with us through emails, comments, blogs, social media pages, etc.

If you apply for a position at Krystal, some of this information may be verified using external sources, such as training institutions, your former employers, and government agencies. Your authorization will systematically be requested beforehand.

Where we need to collect personal information by law, or under the terms of a contract we have with you, and you fail to provide that information when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with our Services). In this case, we may have to cancel a Service you have with us but we will notify you if this is the case at the time.

III. HOW IS YOUR INFORMATION COLLECTED

We use different methods to collect data from and about you including through:

Direct interactions. You may give us your Identification, Contact and Financial Data by filling in forms or by corresponding with us by mail, phone, email or otherwise. This includes personal information you provide when you:

- Subscribe to our Services;
- request marketing to be sent to you;
- apply for one of our available positions; or
- give us some feedback.

Automated technologies or interactions. As you interact with our Website, we may automatically collect Connection Data about your equipment, browsing actions and patterns. We collect this personal information by using cookies, [server logs] and other similar technologies. Please see our cookie section below for further details.

Third parties. We may receive personal information about you from various third parties as set out below:

Connection Data from the following parties:

- analytics providers [such as Google based in the United States]

IV. HOW WE USE YOUR INFORMATION

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with you.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal obligation.

Click here [LINK TO GLOSSARY, LAWFUL BASIS] to find out more about the types of lawful basis that we will rely on to process your personal information.

Generally, we do not rely on consent as a legal basis for processing your personal information although we will get your consent before sending third party direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us.

We have set out below, in a table format, a description of all the ways we plan to use your personal information, and which of the legal bases under the GDPR we rely on to do so. For our users based in the EU, Switzerland, or the UK, we have also identified what our legitimate interests are where appropriate.

Purpose/Activity	Categories of personal information	Legal basis	Retention period
Process information requests sent through contact form or emails	• Identification data • Contact data • Connection data	Legitimate business interests to answer your request	Active database: 1 year Archives: 10 years
Provide access to the services on our website	• Connection data • Location data	Contractual necessity	Active database: until you stop using our services Archives: 1 year
Monitor activity on our website	• Connection data • Location data	Legitimate business interests to update and improve our	Active database: 13 months Archives: None

		website according to usage statistics	
Manage recruitment operations	• Identification data • Contact data • Professional data • Financial data • Location data	At your initiative: Contractual necessity At our initiative: Legitimate business interests to offer employment opportunities to talented individuals	Active database: for the duration of the recruitment process Archives: 2 years if you consent to it
Manage background checks	• Identification data • Contact data • Professional data • Financial data • Location data • Special categories of personal data	Standard categories: Legitimate business interests to verify the information you provide is accurate Special categories: our rights and obligations in the field of employment law	Active database: for the duration of the recruitment process Archives: Only discrepancies are kept for 5 years if you are recruited. Otherwise, the data is erased.
Marketing our products and services	• Identification data • Professional data	Legitimate business interests to communicate about our products	Active database: 3 years Archives: 10 years
Complying with requests from public authorities	• Identification data • Contact data	Legal obligation	Active database: for the duration of the request

			Archives: 10 years
Monitoring the development of expanded access programs	• Identification data • Special categories of personal data	Legal obligation	Active database: for the duration of the program Archives: 10 years or less if required under local legislation
Management of pre-litigation and litigation	• Identification data • Contact data • Connection data • Professional data • Financial data • Location data • Special categories of personal data	Legitimate business interests to mediate take any necessary measure for the establishment, exercise or defence of legal claims	Active database: for the duration of the litigation Archives: 10 years
Management of contracts to which you are a party	• Identification data • Contact data • Professional data • Financial data	Contractual necessity	Active database: for the duration of the contract Archives: 10 years after the term of the contract

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

V. HOW WE DISCLOSE YOUR INFORMATION.

A. We Use Service Providers.

We may share any personal information we collect about you with our third-party service providers. The types of service providers to whom we entrust personal information include service providers for: (i) the provision of the Services; (ii) the provision of information, products, and other services you have requested; (iii) marketing and advertising; (iv) payment processing; (v) customer service activities; and (vi) the provision of IT and related services.

B. Affiliates.

We may share personal information with our affiliated companies.

C. Business Partners.

If you consented to it, we may provide personal information about you to business partners to provide you with a product or service you have requested. We may also provide personal information to business partners with whom we jointly offer products or services.

D. Disclosures to Protect Us or Others.

We may access, preserve, and disclose your personal information to public authorities and/or attorneys if we believe doing so is required or appropriate to: (i) comply with law enforcement or national security requests and legal process, such as a court order or subpoena; (ii) protect your, our or others' rights, property, or safety; (iii) to collect amounts owed to us; (iv) when we believe disclosure is necessary or appropriate to prevent financial loss or in connection with an investigation or prosecution of suspected or actual illegal activity; or (v) if we, in good faith, believe that disclosure is otherwise necessary or advisable.

E. Merger, Sale, or Other Asset Transfers.

If we are involved in a merger, acquisition, financing due diligence, reorganization, bankruptcy, receivership, purchase or sale of assets, or transition of service to another provider, then your information may be sold or transferred as part of such a transaction as permitted by law and/or contract.

F. Transfers of information outside of Europe

We share your personal information within the Krystal Group. If you are in the European Economic Area (the EU, Iceland, Lichtenstein or Norway), the United Kingdom, or Switzerland, please note that this will involve transferring your personal information to countries offering a different level of protection than the one provided in your country of residence, notably the United States.

Many of our external third parties are based outside the EEA, the UK and Switzerland, so their processing of your personal information will also involve a transfer of information outside the EEA, the UK and Switzerland.

If you are based in the EEA, the UK or Switzerland, please note that whenever we transfer your personal information out of the EEA, the UK, or Switzerland, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

· We will only transfer your personal information to countries that have been deemed to provide an adequate level of protection for personal information by the European Commission and the Swiss FADP. For further details, see European Commission: *Adequacy of the protection of protection of personal data in non-EU countries* and *Recognition by Switzerland of States that guarantee an adequate level of data protection.*

· Where we transfer your personal information within our company or where we use certain service providers, we may use specific contracts approved for use in the UK or by the European Commission (as applicable) which give personal information the same protection it has in Europe, namely the UK International Data Transfer Agreement or the UK International Data Transfer Addendum to the European Commission's standard contractual clauses for international data transfers, or the EU Commission's standard contractual clauses (as applicable). For further details, see *European Commission: Model contracts for the transfer of personal data to third countries* and *UK Information Commissioner's Office: International data transfer agreement and guidance*

· Where we use service providers based in the U.S., we may transfer your personal information to them if they are part of the EU-U.S. and/or Swiss-U.S. Data Privacy Framework, which frameworks require them to provide similar protection to personal information shared between Europe and the U.S. For further details, see *Data Privacy Framework* .

Please contact us at *privacy@krystalbio.com* if you want further information on the specific mechanism used by us when transferring your personal information out of Switzerland, the UK, or the EEA.

VI. YOUR CHOICES

A. Your Privacy Rights

In accordance with applicable law, you may have the right to:

- (i) request confirmation of whether we are processing your personal information and obtain access to a copy of it;
- (ii) receive an electronic copy of personal information that you have provided to us, or ask us to send that information to another company (the “right of data portability”);
- (iii) restrict our uses of your personal information;
- (iv) object or opt-out to certain uses of your personal information;
- (v) withdraw your consent to our use of your personal information at any time;
- (vi) seek correction or amendment of inaccurate, untrue, incomplete, or improperly processed personal information; and
- (vii) request erasure of personal information held about you by Krystal, subject to certain exceptions prescribed by law.
- (viii) if you are based in the EEA, the UK, or Switzerland, lodge a complaint with your local data protection authority

U.S Residents: Your State Privacy Rights

California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, and Virginia provide (now or in the future) their state residents with rights to:

- Confirm whether we process their personal information.
- Access and delete certain personal information.
- Correct inaccuracies in their personal information, taking into account the information's nature processing purpose (excluding Iowa and Utah).
- Data portability.
- Opt-out of personal data processing for:
  - targeted advertising (excluding Iowa);
  - sales; or

    - profiling in furtherance of decisions that produce legal or similarly significant effects (excluding Iowa and Utah).
- Either limit (opt-out of) or require consent to process sensitive personal information.

The exact scope of these rights may vary by state. If you would like to exercise any of these rights, please contact us as set forth in the "Contact Us" section, below. We will process such requests in accordance with applicable laws. To protect your privacy, Krystal may take steps to verify your identity before fulfilling your request.

To appeal a decision regarding a consumer rights request, please send us an email at privacy@krystalbio.com, specifying the nature of your rights affected by the decision and your arguments in support of the appeal, and include a copy of the decision, along with any supporting documentation, and the best phone number and email address to reach you back on. We will get back to you without undue delay from the receipt of your appeal email.

Nevada provides its residents with a limited right to opt-out of certain personal information sales. Residents who wish to exercise this sale opt-out rights may submit a request to privacy@krystalbio.com. However, please know we do not currently sell data triggering that statute's opt-out requirements.

B. Email Communications

You may object to the reception of further promotional emails from us using the "unsubscribe" link found at the bottom of each email. Note that you will continue to receive transaction-related emails regarding products or Services you have requested. We may also send you certain non-promotional communications regarding us and our Services, and you will not be able to opt out of those communications (e.g., communications regarding the Services or updates to this Privacy Policy).

C. Access Analysis Tools and Personalized Advertising.

You may withdraw your consent to certain cookies and similar access analysis tools as described in section IX of this Policy.

VII. SECURITY OF YOUR INFORMATION

We take steps to ensure that your information is treated securely and in accordance with this Privacy Policy. Unfortunately, the Internet cannot be guaranteed to be 100% secure, and we cannot ensure or warrant the security of

any information you provide to us. To the fullest extent permitted by applicable law, we do not accept liability for unintentional disclosure.

By using the Services or providing personal information to us, you agree that we may communicate with you electronically regarding security, privacy, and administrative issues relating to your use of the Services. If we learn of a security system's breach, we may attempt to notify you electronically by sending a notice through the Services or by sending an e-mail to you.

The Services may contain links to other websites/applications and other websites/applications may reference or link to our Services. These third-party services are not controlled by us. We encourage our users to read the privacy policies of each website and application with which they interact. We do not endorse, screen or approve, and are not responsible for the privacy practices or content of such other websites or applications. Visiting these other websites or applications is at your own risk.

VIII. CHILDREN'S INFORMATION

The Services are not directed to children under 13 (or other age as required by local law), and we do not knowingly collect personal information from children. If you learn that your child has provided us with personal information without your consent, you may contact us as set forth below. If we learn that we have collected any child's personal information in violation of applicable law, we will promptly take steps to delete such information.

IX. COOKIES, WEB BEACONS, AND OTHER ANALYSIS TOOLS

We, as well as third parties that provide content, advertising, or other functionality on the Services, may use cookies, pixel tags, local storage, and other technologies to automatically collect information through the Services.

A. What types of analysis tools we may use

- **Cookies.** Cookies are small text files placed in visitors' device browsers to store their preferences. Most browsers allow you to block and delete cookies. However, if you do that, the Services may not work properly.
- **Pixel Tags/Web Beacons.** A pixel tag (also known as a web beacon) is a piece of code embedded on the Services that collects information about users' engagement. The use of a pixel allows us to record, for example, that

a user has visited a particular web page or clicked on a particular advertisement. We may also include web beacons in e-mails to understand whether messages have been opened, acted on, or forwarded.

Our uses of cookies and similar access analysis tools fall into the following general categories:

- **Operationally Necessary.** This includes Technologies that allow you access to our Services that are required to identify irregular behavior, prevent fraudulent activity and improve security or that allow you to make use of our functions;
- **Performance Related.** We may use Technologies to assess the performance of our Services, including as part of our analytic practices to help us understand how our visitors use the Services;
- **Functionality Related.** We may use Technologies that allow us to offer you enhanced functionality when accessing or using our Services. This may include identifying you when you sign into our Services and keeping track of your specified preferences or past pages viewed;
- **Advertising or Targeting Related.** We may use first-party or third-party Technologies to develop and deliver content, including ads relevant to your interests, on our Services or on third-party sites.

B. What analysis tools we currently use

To identify which analysis tools we currently use, you can click on the “cookie settings” link at the bottom of each page. The details of the which tools are used can be found in the “cookie details” link for each section.

C. How to manage your cookies

The deposit of cookies based on your consent is optional. Your consent is requested through the banner that appears when you first browse the site. You can choose to accept the deposit of cookies for all the purposes listed, refuse them or customize your choice. You may withdraw your consent at any time by going to the [Cookie Settings] page at the bottom of each page of the site.

You also have the choice to set your browser to accept or reject all cookies, to delete cookies periodically, or to see when a cookie is issued, how long it remains valid, and what it contains, and to refuse to store it on your hard drive. This can be done using the instructions of your internet browser provider.

Please note that cookie-based opt-outs are not effective on mobile applications. However, you may opt-out of personalized advertisements on some mobile applications by following the instructions for Android and iOS.

The online advertising industry also provides websites from which you may opt-out of receiving targeted ads from advertisers that participate in self-regulatory programs. You can access these, and also learn more about targeted advertising and consumer choice and privacy, at www.networkadvertising.org/managing/opt_out.asp and www.aboutads.info/choices/.

Do Not Track ("**DNT**") is a privacy preference that users can set in certain web browsers. Please note that we do not respond to or honor DNT signals or similar mechanisms transmitted by web browsers.

X. CHANGES TO OUR PRIVACY POLICY AND YOUR DUTY TO INFORM US OF CHANGES

We may revise this Privacy Policy from time to time in our sole discretion. If there are any material changes to this Privacy Policy, we will notify you as required by applicable law. You understand and agree that you will be deemed to have accepted the updated Privacy Policy if you continue to use the Services after the new Privacy Policy takes effect.

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your relationship with us.

XI. HOW TO CONTACT US

If you have any questions about our privacy practices or this Privacy Policy, please contact our DPO at privacy@krystalbio.com, or at

Krystal Biotech, Inc.

2100 Wharton Street, Suite 701
Pittsburgh, Pennsylvania 15203
United States

If you are based in the European Union, in Switzerland or in the United Kingdom please note that you also have the right to make a complaint at any time to your national supervisory authority for data protection issues. We would, however, appreciate the chance to deal with your concerns before you approach your national regulator so please contact us in the first instance.

XII. GLOSSARY

LAWFUL BASES

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal information for our legitimate interests. We do not use your personal information 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). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

Performance of Contract means processing your information where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Comply with a legal obligation means processing your personal information where it is necessary for compliance with a legal obligation that we are subject to.

Consent means processing your personal information where you have signified your agreement by a statement of clear opt-in to processing for a specific purpose. Consent will only be valid if it is a freely given, specific, informed and unambiguous indication of what you want. You can withdraw your consent at any time by contacting us.

YOUR RIGHTS IN RELATION TO YOUR PERSONAL INFORMATION

You have the right to:

Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

Request correction of personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected, though we may need to verify the accuracy of the new information you provide to us.

Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal information to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal information for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request restriction of processing of your personal information. This enables you to ask us to suspend the processing of your personal information in the following scenarios:

- If you want us to establish the information's accuracy.

- Where our use of the information is unlawful but you do not want us to erase it.

- Where you need us to hold the information even if we no longer require it as you need it to establish, exercise or defend legal claims.

- You have objected to our use of your information but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer of your personal information to you or to a third party. We will provide to you, or a third party you have chosen, your personal information in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

Withdraw consent at any time where we are relying on consent to process your personal information. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain services to you. We will advise you if this is the case at the time you withdraw your consent.