

Visterra Privacy Policy

Effective Date : September 1, 2026

Visterra, Inc. (“Visterra,” “we,” “us,” or “our”) recognizes and respects the privacy rights of individuals regarding their personal data. This policy describes how we collect, use, share and secure your personal data and choices and rights you may have regarding your data. This policy applies to personal data that we collect through our websites and from other sources.

While this policy applies to all individuals about whom we collect personal data, certain parts of this policy apply only to residents of California. See [“California Privacy Rights”](#) below for more information. If you have any questions about this policy or your personal data we collect, please contact us as described under [“How to Contact Us”](#) at the end of this policy.

You may download a printable copy of this Policy (PDF): [here](#).

Table of Contents

A. How Do We Get Your Personal Data?	G. How We Respond to Opt-out Preference Signals
B. What Types of Personal Data Do We Collect?	H. Children's Privacy
C. How Do We Use Your Personal Data?	I. Links to Other Sites
D. Who Do We Share Your Personal Data With?	J. Privacy Policy Updates
E. How Do We Protect Your Personal Data?	K. California Privacy Rights
F. Cookies and Web Beacons	M. How to Contact Us

A. HOW DO WE GET YOUR PERSONAL DATA?

Directly from you. You may give us personal data through our websites or through other direct interactions with us, for example, when you:

- contact us by email, phone or mail, either using the addresses or numbers posted on our website or when you contact our employees directly;
- enter in a business transaction with us to provide goods or services; or
- apply for employment with us or when you become an employee

Automatically from your use of our website. As you use our website or intranet, we may automatically collect data about your equipment, browsing patterns and use of our website. We collect this personal data by using cookies, and other similar technologies. See [“Cookies and Web Beacons”](#) below for more information.

From third parties or publicly available sources. We may receive personal data about you from various third parties and public sources, such as:

- online analytics providers such as Google Analytics and search information providers;
- recruiters, staffing agencies and employment background search firms;
- government, industry and professional directories; and
- clinical sites, investigators, research organizations and other vendors involved in clinical research in which you enroll and/or participate.

B. WHAT TYPES OF PERSONAL DATA DO WE COLLECT?

In the past twelve months, we may have collected the following types of personal data:

- **Personal Identifiers** such as first name, maiden name, last name, username or similar identifier, marital status, title, date of birth, and social security number.

- **Contact Data** such as billing address, delivery address, email address, telephone numbers and home address.
- **Financial Data** such as bank account, credit card, and payroll data.
- **Transaction Data** such as details about payments to and from you.
- **Internet or other similar network activity**, such as your internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our website or intranet, and information about how you interact with our website.
- **Professional and employment-related data** such as completed job applications and resumes.
- **Sensitive Personal Information** such as social security number, health information, genetics, and/or biometric data.

C. HOW DO WE USE YOUR PERSONAL DATA?

We may use your personal data to:

- fulfill your requests and answer your questions;
- process employment applications;
- manage your employment with us, including payroll and benefits enrollment;
- perform contractual obligations and enforce contractual rights under agreements with you;
- improve our websites and intranet (for more information, see [“Cookies and Web Beacons”](#) below);
- conduct clinical trials of the investigational products we are developing; and
- comply with legal and regulatory requirements, including those related to clinical trial adverse events and patient safety.

We do not use your personal data for marketing purposes, and we do not sell or share your personal data with other companies or organizations.

D. TO WHOM MAY WE DISCLOSE YOUR PERSONAL DATA?

Depending on the specific use(s) set forth above, we may disclose your personal data with the following groups and individuals:

- **Affiliates:** our parent company, Otsuka Pharmaceutical Company Ltd., and our other affiliated companies.
- **Service providers and other business partners:** Service providers and other third parties with whom we engage to provide services or products on our behalf (e.g., IT system administrative service companies, data storage companies, data analytics companies, contract research organizations that conduct clinical trials, travel planning companies, payroll and benefits service providers, banks and other payment facilitators, employment background check providers) or with whom we collaborate or work together to research and develop products and services (e.g., other biotechnology and pharmaceutical companies and academic research institutions).

We do not allow our service providers or other third-party business partners to use your personal data for their own purposes and only permit them to access and use your personal data for specified purposes and in accordance with our instructions.

- **Professional advisers:** advisors (e.g., lawyers, bankers, auditors and insurers) who provide us with consultancy, banking, legal, compliance, insurance and accounting, and payroll services.
- **Government authorities:** the U.S. Internal Revenue Service, the U.S. Food and Drug Administration, and other federal and state government agencies, regulators, and authorities.
- **Acquirors and successors:** third parties to whom we may seek to sell, transfer, or merge parts of our business or our assets, such as through a merger, consolidation, acquisition, reorganization, bankruptcy or dissolution.

E. HOW DO WE PROTECT YOUR PERSONAL DATA?

We have appropriate security measures in place to help prevent your personal data from being lost and protect it from unauthorized access, use, alteration, and disclosure. We limit access to your personal data to our employees, agents, contractors and other third parties who have a business need to know your data. They are required to process your personal data only in accordance with our instructions and, except in the case of government authorities, are subject to confidentiality obligations.

We have appropriate procedures in place to help address any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

No measures or procedures can ensure that your personal data is always and completely secure, and accordingly, we cannot guarantee the security of your personal data.

F. COOKIES AND WEB BEACONS

Cookies are small data files that are automatically stored on your computer or device when you visit our website. Cookies are used to track the pages of the websites you have visited and do not include or retain any information that will directly identify you such as your name, address or any financial information. We may use cookies to enable you to use certain website features, store your preferences, recognize you when you return to our website, and help us understand how our websites and intranet are performing and being used. Third-party analytics services, like Google Analytics, use their own cookies to collect and analyze browsing history and behavior, and make that analysis available to website owners like us.

Most internet browsers automatically accept cookies, but if you do not wish to have cookies stored on your computer or device, you can set your browser preferences to refuse them or to alert you when cookies are being sent.

To disable cookies, please consult your browser's "help" section for instructions. If you choose to decline cookies, you may not be able to fully experience the features of our website. To find out more about cookies, including how to see what cookies have been set and how to manage and

delete them, visit www.aboutcookies.org or www.allaboutcookies.org. To opt out of being tracked by Google Analytics across all websites, visit <http://tools.google.com/dlpage/gaoptout>.

Web beacons are small strings of code that are placed in a web page or in an email message. They are sometimes called “clear GIFs” (Graphics Interchange Format), “GIF tags”, “action tags”, or “pixel tags”. Web beacons are most often used in conjunction with cookies to track activity on our website. For example, when you visit our website, web beacons can notify us of what pages you visited. Since web beacons are used in combination with cookies if you disable cookies, the web beacons will only detect an anonymous website visit. When used in an email, web beacons enable us to know whether you have received the email.

Please note that linked third-party websites may also use cookies. We cannot control the use of cookies by these third-party websites. For example, when you link from this site to a third-party website, that website may have the ability to recognize that you have come from our site by using cookies. If you have any questions about how third-party websites use cookies, you should contact such third parties directly.

G. HOW WE RESPOND TO OPT-OUT SIGNALS

An opt-out preference signal is a signal sent by a platform, technology, or mechanism that communicates a consumer's choice to opt out of the selling or sharing of their personal information. We do not sell or share your personal information, so we do not currently monitor opt-out preference signals. We do not respond to 'do-not-track' signals.

H. CHILDREN’S PRIVACY

While in some instances we may collect personal data about children with the consent of a parent or guardian, such as clinical trial-related activities, we do not otherwise knowingly solicit or collect data from children. If a parent or guardian becomes aware that his or her child has provided us with personal data without the parent’s or guardian’s consent, he or she should contact us as described under [“How to Contact Us”](#) below. We will take reasonable steps to delete such data from our records.

I. LINKS TO OTHER SITES

For your convenience and information, we may provide links on our websites and intranet to other third-party websites that we do not operate or control. By providing these links, we are not endorsing the content, owner or operator of those sites. When you visit other websites by clicking on a link, this policy no longer applies, and your use of that site is subject to that site's privacy policies.

J. PRIVACY POLICY UPDATES

We may update this policy from time to time. If we make any changes, the updated policy will be posted with a revised "Effective Date." You should check this policy periodically for changes.

K. CALIFORNIA PRIVACY RIGHTS

The California Consumer Privacy Act of 2018 ("CCPA"), modified by the California Privacy Rights Act of 2020 ("CPRA"), provides California residents with specific privacy rights, subject to certain limitations and exceptions, regarding their personal information. All terms defined in the CCPA/CPRA have the same meaning when used in this section of this policy.

As may be required under applicable local law, the chart below lists the third parties to whom we may disclose categories of personal information and the reason for doing so.

Category of personal information	Categories of third parties to whom we may disclose personal information for a business purpose
Identifiers	• Related entities • Service providers • Government entities
Protected Classifications	• Related entities • Service providers • Government entities

Internet and other similar network activity	• Related entities • Service providers • Government entities
Professional or employment-related information	• Related entities • Service providers • Government entities
Sensitive personal information	• Related entities • Service providers • Government entities

We do not “sell” or “share” your personal information as defined under applicable local law. We do not use or disclose your sensitive personal information for purposes other than permitted under applicable law.

California residents have the right to:

- Request information about what personal information we have collected, used and disclosed during the prior 12 months, including categories of personal information, categories of sources of personal information, business purposes for collecting and using personal information and categories of third parties with whom we shared such information.
- Request a copy of the personal information we have collected about them.
- Request correction of any of their personal information that is inaccurate. Request that we limit the use and disclosure of your sensitive personal information to that which is necessary to perform the services or provide the goods reasonably expected by an average consumer.
- Request deletion of their personal information (subject to certain exceptions).
- Not be discriminated against for exercising their privacy rights under the CCPA/CPRA.

To submit a request to exercise your rights, you may contact us by email at privacy@visterrainc.com or by calling us toll-free at 1-877-4-VISTERRA (1-877-484-7837).

Before we act on a request to correct, delete, or provide a copy of personal information we have collected, if any, we will verify your identity by asking you to provide certain personal information. This information may include a description of your relationship with Visterra, your first and last name, email address, telephone number and postal address or other personal information that will allow us to verify your identity. You may submit a request through an authorized agent, in which case, we will require your agent to provide us with your written authorization confirming its authority to make the request on your behalf.

The CCPA/CPRA does not apply to personal information we collect in all circumstances. For example, it does not apply to personal information we collect in connection with conducting clinical trials or certain information governed by HIPAA (the Health Insurance Portability and Accountability Act of 1996). Also, we are not required to delete personal information in certain circumstances. We will notify you if we deny a request. We will not discriminate against you for exercising your rights under the CCPA/CPRA.

Data Retention

We aim to retain Personal Data, including Sensitive Personal Information, for only as long as reasonably necessary to fulfil the purposes described in this Notice or for the purposes of meeting legal, regulatory, accounting, or reporting requirements.

To determine the appropriate retention period, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure, the purposes for which we process it, and applicable legal requirements. For example, personal data related to our clinical trials is retained in accordance with FDA and other regulatory requirements, which may be for a period of several years after a trial is complete.

HOW TO CONTACT US

Visterra, Inc.

Attn: Legal – Privacy

275 2nd Avenue

Waltham, MA 02451

United States

privacy@visterrainc.com

1-877-4-Visterra