

Last Revised: September 30, 2024

JOB PORTAL PRIVACY POLICY

1. INTRODUCTION

This Job Portal Privacy Policy (“**Policy**”) of **LOTTE Biologics USA, LLC**, a Delaware limited liability company (“**our,**” “**us,**” or “**we**”), applies to each individual from whom we receive personal information through our Job Portal (defined below) (“**you**” or “**your**”).

Your Click Consent. Our job application webpage displays a link to this Policy. By clicking the link, you provide your consent for us and our affiliates (including Greenhouse Software, Inc.) to receive, process, store, and use your personal information (including any sensitive personal information that you provide) in accordance with this Policy for our purposes of receiving, analyzing, and evaluating your job application (“**Click Consent**”).

This is an important document that describes how we collect, use, and disclose your personal information. We do not guarantee or warrant the security or protection of your personal information, and you assume the risk that an unauthorized party (e.g., a hacker or cyber attacker) might access, misuse, or destroy your personal information. Therefore, please carefully review this Policy, and ensure that you find it acceptable before using our Job Portal or providing your personal information to us.

In this Policy, we use certain terms that have specific meanings, such as “automated profiling,” “targeted advertising,” “deidentified,” “personal information,” “sell,” and “sensitive personal information.” For the full set of definitions, please see the end of this Policy at **Section 6.5**.

We may update this Policy from time to time. The date provided at the top of this Policy is the latest revision date of this Policy. To request a prior version of this Policy, please contact us using our contact information provided in **Section 3.10**.

2. OUR JOB PORTAL

The following is a list of the resources and property that we and our affiliates may use to collect your personal information, which may vary depending on the nature of your interactions with us and may not include all of the examples listed below (collectively, our “**Environment**”):

- the web portal that displays this Policy as well as any mobile version of such web portal accessible via mobile applications (collectively, our “**Job Portal**”).
- any of our emailing and messaging systems that enable you to communicate with us via emails, texts, or direct messages relating to our job postings.
- any of our phone systems and video conferencing systems that enable you to communicate with us via teleconference, video conference, or video session messaging relating to our job postings.

3. OUR NOTICES TO YOU

3.1 No Sale; No Sharing for Targeted Advertising. We do not sell your personal information, nor do we sell any of your sensitive personal information that we may collect. Furthermore, we do not distribute or provide your personal information (sensitive or otherwise) to any advertising network or other third party for purposes of targeted advertising. We do not want to receive personal information from anyone under 16 years of age. However, if we receive personal information from someone under 16 years of age, we will treat it as described in this Section.

3.2 Our Use of AI/Automated Processing Tool. You understand and agree that we and our affiliates may use a variety of tools and resources in our efforts to review and analyze job applications. One type of tool that we use involves automated profiling, artificial intelligence (AI) technology, or algorithm-based technology. We use this tool to process your job application information, including your personal information. The feedback from this tool is only one of several factors that we consider with respect to your job application. Our hiring decisions are based on a variety of factors that we evaluate in accordance with applicable law.

3.3 Categories of Personal Information That We Collect. The following is a list of the categories of your personal information that we may collect for our Application Processing Purposes, which may vary depending on the nature of your interactions with us and may not include all of the examples listed below:

- **Identifiers** – such as your real name, alias, postal address, telephone number, unique personal identifier, online identifier, username, email address, account name, social security number, driver’s license number, state identification card number, passport number, signature, social security number, or other similar identifiers.
- **Job Application Information** – such as education credentials, professional background, biographical information, employment history, and any other information that you decide to provide to us or submit through our Environment.
- **Browser/Device Information** – such as your Internet Protocol (IP) address, which we may use with essential cookies as described below.

3.4 Sensitive/Special Personal Information. Certain laws, such as the California Consumer Privacy Act, as amended (“CCPA”) and the GDPR (defined in **Section 5.1**) provide additional privacy protection for sensitive personal information or special personal information. The GDPR describes this special personal information as personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, or data concerning sex life or sexual orientation. We do not want any sensitive or special personal information and direct you not to provide it, but if you provide it anyway, and if these laws apply to you, then your Click Consent is your explicit permission for us and our affiliates to store and process this information for our Application Processing Purposes in accordance with applicable law.

3.5 Our Purposes for Collecting Your Personal Information. We may collect, use, or disclose your personal information for the following purposes (“**Application Processing Purposes**”):

- **Services** – performing services related to your job application, including analyzing your job application, reviewing the information that you provide to us, making our hiring decisions, and providing similar services on our behalf.
- **Quality & Safety** – undertaking activities to verify or maintain the quality or safety of a service or device that we own or use for receiving or processing job applications, or to improve, upgrade, or enhance the service or device.
- **Security** – helping to ensure security and integrity to the extent our use of your personal information is reasonably necessary and proportionate for these purposes.
- **Short-Term Use** – short-term, transient use, provided that your personal information is not disclosed to another third party and is not used to build a profile about you or otherwise alter your experience outside the current interaction with us.
- **Additional Necessary Purposes** – our operational purposes and the following additional purposes, provided that our use of your personal information is necessary and proportionate to achieve our Application Processing Purposes related to your job application:
 - **Auditing** – auditing for our compliance with applicable law.
 - **Debugging** – debugging to identify and repair errors that impair existing intended functionality.
 - **Internal Research** – undertaking internal research for technological development and demonstration.
 - **Marketing** – providing marketing services (other than targeted advertising) to you related to any career or job opportunities that we offer.
- **Complying with Law** – our purposes of: (a) complying with federal, state or local laws; (b) complying with civil, criminal or regulatory inquiries, investigations, search warrants, subpoenas, summons, orders, injunctions and mandates issued by courts, judicial authorities, law enforcement authorities or governmental authorities, including federal, state or local authorities; and (c) cooperating with such authorities.

3.6 How We Collect Your Personal Information

- **Methods.** We may use our Environment to collect your personal information through a variety of methods, such as the following:

- automatically pulling the IP address from your browser or device for use with essential cookies, as described below.
- receiving information you have provided to us via phone, text, email, electronic message, online form submission, or other communications.
- receiving information from third parties who have disclosed to us, the information you have made publicly available, such as photos, videos and content you have posted on publicly available social media platforms.
- communicating with you in person.

3.7 Sources of Your Personal Information. We may obtain your personal information from the following categories of sources:

- **You** – You may provide your personal information to us when you use our Environment.
- **Your Devices** – We may pull your IP address from your devices and browsers by placing essential cookies, as described below.
- **Our Affiliates** – On our behalf, our affiliates may collect and provide us with your personal information for our Application Processing Purposes.

3.8 Receivers of Your Personal Information. We may disclose your personal information to the following third parties:

- **Technology Suppliers** – our third-party affiliates, including Greenhouse Software, Inc., that provide, supply, deploy, host, or operate software-based tools, programs, servers, databases, web-based applications, online platforms, or software-as-a-service that are part of our Environment.
- **Contractors** – our third-party affiliates that provide, lease, or license products, services, data centers, or other facilities to us, such as customer support providers, payment processing consultants, order fulfillment contractors, product developers, event managers, information technology consultants, cyber security advisors, computer programmers, business advisors, auditors, accountants and attorneys.
- **Corporate Affiliates** – our third-party affiliates that control us, that we control, or that are under common control with us, such as our parents, subsidiaries and sister entities.
- **Legal Authorities** – legal authorities, such as courts, judicial authorities, law enforcement authorities or governmental authorities (including federal, state, or local authorities) in connection with any civil, criminal or regulatory inquiry, investigation, search warrant, subpoena, summons, order, injunction or mandate issued by any such legal authority.

3.9 How Long We Keep Your Personal Information. For each of the categories of personal information provided above, we may keep your personal information for a period lasting as long as is reasonably necessary for our purpose of collecting it or as otherwise required by applicable law. At the end of the period, we may permanently destroy, erase, delete, encrypt or disable access to your personal information in a manner designed to ensure that it cannot be reconstructed or read. You will not be able to recover such personal information later.

3.10 Consumer Privacy Rights. Some consumer privacy laws and personal data protection laws, as written, may not apply to job applicants and, therefore, may not provide you with some or any of the rights described in this Section below (“**Consumer Privacy Rights**”). Depending upon where you reside, applicable law may or may not provide you with the Consumer Privacy Rights. To the extent that applicable law does provide you with any of the Consumer Privacy Rights, we will comply with the applicable law.

- **Right to Know.** As described above, this Policy informs you of the categories of your personal information that we collect, our purposes for collecting or using it, whether we sell it or share it for targeted advertising, and the length of time that we retain it.
- **Right to Request Deletion.** You have the right (if granted to you, as a job applicant, by applicable law) to request that we delete your personal information that we have collected.
- **Right to Request Correction.** You have the right (if granted to you, as a job applicant, by applicable law) to request that we correct any inaccurate personal information about you that we maintain.
- **Right to Request Usage Details.** You have the right (if granted to you, as a job applicant, by applicable law) to request that we disclose the following to you: (a) confirmation as to whether or not we are collecting, using, storing, disclosing, analyzing deleting or modifying your personal information; (b) the categories of personal information that we have collected about you; (c) the categories of sources from which we have collected your personal information; (d) the business or commercial purpose for collecting your personal information and for any selling of it or sharing of it for targeted advertising; (e) the categories of third parties to whom we have disclosed your personal information; and (f) the specific pieces of personal information that we have collected about you, which may be requested in a portable, and to the extent technically feasible, readily usable format that enables you to transmit the personal information to another entity without hindrance.
- **Right to Request Details About Sales, Sharing or Disclosure.** You have the right (if granted to you, as a job applicant, by applicable law) to request that we disclose the following to you: (a) the categories of any of your personal information that we have sold or shared to third parties for targeted advertising; (b) the categories of any such third parties, itemized by category of your personal information; and (c) the categories of your personal information that we have disclosed to persons for an Application Processing Purpose, and the categories of those persons.

- **Right to Opt Out.** You have the right (if granted to you, as a job applicant, by applicable law) to, at any time: (a) direct any business that sells your personal information or shares it for targeted advertising, not to do so; (b) opt out of automated profile-based advertising; and (c) opt out of automated profiling, including automated profiling conducted in furtherance of decisions that produce legal or similarly significant effects concerning you.
- **Right to Limit Use and Disclosure of Sensitive Personal Information.** You have the right (if granted to you, as a job applicant, by applicable law) to, at any time, direct any business that collects your sensitive personal information to limit its use of your sensitive personal information to the extent authorized by regulations adopted pursuant to applicable law or only as necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, including the services that we perform for the Application Processing Purposes.
- **Right of Non-Discrimination.** You have the right (if granted to you, as a job applicant, by applicable law) to be free of any discrimination related to your exercise of any of your Consumer Privacy Rights.
- **Right and Method to Contact Us.** To submit a request or notice to us under this Section, you may send your request or notice by writing or emailing us at the following address:

LOTTE Biologics USA, LLC
 6000 Thompson Road
 East Syracuse, New York 13057
 Email Address: LBA_legal@lottebiologics.com

- **Right to Authorize an Agent.** You may authorize another person to provide us with your request or notice under this Section, and we will comply with such request or notice if we can verify that you have given such authority as described in **Section 3.11**.

3.11 Our Response Procedures

- **Verification.** For security purposes, before processing your request or notice under **Section 3.10**, we will take steps to determine whether the request is a verifiable request or whether the notice is verifiable. We are not obligated to provide information that you may request under this Section if we cannot verify, pursuant to applicable law, that the person making the request is the individual about whom we have collected information or is a person authorized by the individual to act on the individual's behalf.
- **Our Response.** If required by applicable law for job applicants, we will respond to your requests and notices within a reasonable timeframe and in accordance within the requirements, frequency and timing specified by applicable law. We may decline part or all of your requests or notices as permitted by applicable law, and we will inform you of the reason for the decline.

- **Decline of Requests.** We may decline to delete your personal information if it is reasonably necessary for us to maintain your personal information in order to: (a) complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by you, or reasonably anticipated by you within the context of our ongoing business relationship with you, or otherwise perform a contract between you and us; (b) help to ensure security and integrity to the extent the use of the your personal information is reasonably necessary and proportionate for those purposes; (c) debug to identify and repair errors that impair existing intended functionality; (d) exercise free speech, ensure the right of another consumer to exercise that your right of free speech, or exercise another right provided for by law; (e) engage in public or peer-reviewed scientific, historical, or statistical research that conforms or adheres to all other applicable ethics and privacy laws, when our deletion of the information is likely to render impossible or seriously impair the ability to complete such research, if you have provided informed consent; (f) enable solely internal uses that are reasonably aligned with the expectations of you based on your relationship with us and compatible with the context in which you provided the information; or (g) comply with a legal obligation or applicable law.
- **Frequency and Historical Period.** Pursuant to applicable law, we may not be required to provide you with the same type of information under this Section more than twice in a twelve (12) month period, and we may not be required to provide more than twelve (12) months of historical information.

4. COOKIES

4.1 Cookies. A cookie is a small data file that our websites store on the browser of your device, such as your computer or smartphone. Your browser, such as Chrome, Firefox, Edge or Safari, stores cookies in the memory of your device. Our web servers or the web servers of our affiliates may receive and use essential cookies, described below, when you return to our websites. You can learn more information about cookies at www.allaboutcookies.org.

4.2 Essential Cookies. In accordance with applicable law, we may use certain types of cookies (sometimes referred to as essential cookies or necessary cookies) without your prior consent to enable our Job Portal to work properly, securely and efficiently for Application Processing Purposes, including enabling our Job Portal to perform the functions described in this Section below. We use these types of cookies: (a) for the performance of a contract to which you are a party; (b) to take steps at your request before entering into a contract; or (c) as necessary for us to process your personal information for purposes of our legitimate interests. For example, we may use these types of cookies for the following purposes:

- To save pieces of information you have entered during online transactions at our Job Portal, such as items you have added to a submission webpage, as well as names, addresses, usernames, passwords and other text you have entered into our Job Portal.
- To verify whether you are logged in to an account on our Job Portal for authentication and security purposes.
- To operate with adequate security, speed, and electronic performance.

5. EUROPE

5.1 General Data Protection Regulation. In the event that our business activities bring us within the scope of the General Data Protection Regulation ((EU) 2016/679)) (the details of which may be found at https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en) (“GDPR”), we will comply with the GDPR as described below. In this **Section 5**, (a) the term “you” or “your” refers to an individual or data subject who is located in the European Economic Area, which includes member-countries of the European Union (“EEA”), or who is located the United Kingdom (UK) or Switzerland, (b) the term “personal information” means “personal data,” as defined in the GDPR or other applicable laws of the UK or Switzerland, and (c) we are considered the “data controller” under the GDPR or other applicable laws of the UK or Switzerland. If our business activities bring us within the scope of the GDPR, the information set forth in this **Section 5** and the other information in this Policy provides you with the notices required by the GDPR.

5.2 Legal Basis. In accordance with the GDPR, we may process your personal information under several cases, including any one of the following cases:

- You have given us your Click Consent to process your personal information for one or more specific purposes, including the Application Processing Purposes.
- It is necessary for us to process your personal information to comply with a legal obligation to which we are subject.
- It is necessary for us to process your personal information in order to protect vital interests of you or another person.
- It is necessary for us to process your personal information for purposes of our legitimate interests pursued by us or a third party (which includes our Application Processing Purposes), except where the interests are overridden by the interests or fundamental rights and freedoms of you that require protection of personal information, particularly if you are a child.

5.3 Supervisory Authority. If you have any concerns regarding our collection or processing of your personal information, you have the right to lodge a complaint with the supervisory authority established for your location in the EEA, the UK, or Switzerland.

5.4 International Transfers of Personal Information

- **Adequacy Decisions.** The GDPR restricts the transfer of personal information from countries of the EEA to other countries. Likewise, the data protection laws of the UK and Switzerland restrict the transfer of personal information from those countries. The European Commission, the UK, and Switzerland have issued or otherwise adopted adequacy decisions or regulations which allow for the transfer of personal information from the EEA, the UK, and Switzerland, respectively, to certain countries deemed to have adequate protection for personal information.

- **Appropriate Safeguards.** Standard contractual clauses (“SCCs”) are written commitments between parties that establish data protection safeguards. SCCs can be used as grounds for personal information transfers from the EEA to other countries. You can find the latest version of the approved SCCs, [here](#). The European Commission has approved the use of SCCs for personal information transfers from the UK and Switzerland to other countries.
- **Trans-Atlantic Data Privacy Framework.** The European Union and the United States reached an agreement that resulted in the Trans-Atlantic Data Privacy Framework, which includes the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) (collectively, the “DPF”). The DPF relates to the transfer of personal information from the EEA, UK (and Gibraltar), and Switzerland to the United States. The European Union has issued an adequacy decision, concluding that the United States ensures an adequate level of protection under the DPF. By self-certifying through the DPF, businesses and other entities may transfer personal information to the United States from the EEA, the UK, and Switzerland in accordance with the GDPR. To learn more about the DPF, please visit the [DPF website](#).
- **Our Approach to International Transfers.** Our Job Portal is accessible to anyone having Internet access throughout the world. An individual located in the EEA, the UK, or Switzerland could use our Job Portal to submit personal information, which will be transmitted to one or more of web servers of us or our affiliates. If our business activities bring us within the scope of the GDPR and any of these web servers are physically located in the United States or another country outside of the individual’s residence, the transfer of the personal information will comply with the GDPR on the basis of: (a) an adequacy decision in place that permits such transfer, as described above; (b) SCCs that we have put in place, as described above; or (c) self-certification under the DPF by us or our relevant affiliate, together with a data protection agreement in place between us and our affiliate to the extent required by the DPF.

6. MISCELLANEOUS

6.1 Deidentified Information. With respect to deidentified information derived from your personal information, we retain the right to collect, process, use, store, sell, share, disclose, and distribute the deidentified information in accordance with applicable law. If we exercise this right, we will maintain and use the deidentified information and not to attempt to reidentify it, except that we may reidentify the information only to determine whether our deidentification processes satisfy the requirements of applicable law.

6.2 Unsubscribing to Our Emails and Messages. Our Job Portal may enable you to subscribe to or sign up for our marketing communications, such as emails or text messages that provide our newsletters, updates, or marketing messages. Our Job Portal or the communications will enable you to unsubscribe to our emails and messages by changing a setting, clicking an unsubscribe link, texting “Stop,” or making another input. Even if you opt out or unsubscribe to receiving our

marketing communications, we may continue to send you non-marketing communications, such as communications for our Application Processing Purposes.

6.3 Transfer/Storage Outside of the United States. Unless prohibited by applicable law or contractual obligations that we owe to our affiliates, we may store your personal information in web servers located anywhere in the world, and we may transfer your personal information from one country (e.g., the United States) to any other country, where it may be stored and processed for the uses described in this Policy.

6.4 Law Enforcement and Legal Claims. Nothing in this Policy will prevent or restrict us from:

- complying with federal, state, or local laws or complying with a court order or subpoena to provide information.
- complying with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.
- cooperating with law enforcement agencies concerning conduct or activity that we, our affiliates or associates reasonably and in good faith believe may violate federal, state, or local law.
- cooperating with a government agency request for emergency access to your personal information if a natural person is at risk or in danger of death or serious physical injury provided that: (a) the request is approved by a high-ranking agency officer for emergency access to your personal information; (b) the request is based on the agency's good faith determination that it has a lawful basis to access the information on a nonemergency basis; and (c) the agency agrees to petition a court for an appropriate order within three days and to destroy the information if that order is not granted.
- exercising or defending legal claims.

6.5 Definitions. In this Policy, we use the words and phrases "including," "includes," "such as" and "e.g." in a non-limiting fashion, and the following terms (whether used in capitalized or lowercase form) will have the following meanings given to them:

"affiliates" means our third-party technology suppliers, contractors, corporate affiliates, service providers, processors, vendors, licensors, lessors, and other third parties with whom we have a business relationship.

"automated profiling" (referred to in some jurisdictions as "profiling") means any form of automated processing of personal information to evaluate, analyze, or predict personal aspects concerning any identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

"biometric information" means an individual's physiological, biological, or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes: (a) imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an

identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted; (b) keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information; and (c) information based on an individual's retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, which is used to identify the individual, excluding any item of such information that is not deemed biometric information according to specific exclusions set forth in applicable law.

“business” means a sole proprietorship, partnership, limited liability company, corporation, association, person other than a consumer, or other legal entity.

“consumer” (referred to in some jurisdictions as “data subject”) means a natural person.

“deidentified” (referred to in some jurisdictions as “pseudonymized”) means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, provided that the business that possesses the information satisfies the requirements of applicable law related to the use of deidentified information.

“personal information” (referred to in some jurisdictions as “personal data”) means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household, but personal information does not include: (a) publicly available information as defined or characterized by applicable law; (b) lawfully obtained, truthful information that is a matter of public concern; or (c) consumer information that is deidentified.

“security and integrity” means the ability of: (a) networks or information systems to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information; (b) businesses to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions and to help prosecute those responsible for those actions; and (c) businesses to ensure the physical safety of natural persons.

“sell,” “selling,” “sale,” or “sold” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration, excluding any of the foregoing activities that are not deemed to be a sale according to specific exclusions set forth in applicable law.

“sensitive personal information” means: (1) personal information that reveals: (a) a consumer's social security, driver's license, state identification card, or passport number; (b) a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (c) a consumer's precise geolocation, including any data that is derived from a device and that is used or intended to be used to locate the consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, except as prescribed by applicable law; (d) a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; (e) the contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication; or (f) a consumer's genetic data; (2) the processing of biometric

information for the purpose of uniquely identifying a consumer; (3) personal information collected and analyzed concerning a consumer's health; and (4) personal information collected and analyzed concerning a consumer's sex life or sexual orientation. Sensitive personal information that is "publicly available" (as described above) will not be considered sensitive personal information or personal information.

"targeted advertising" (referred to in some jurisdictions as "cross-context behavioral advertising") means the targeting of advertising to a consumer based on data that is derived from the consumer's behavior across distinctly-branded platforms (e.g., websites, applications, and other venues) beyond the business or distinctly-branded platform with which the consumer intentionally interacts. The definition of targeted advertising does not include advertising based on your activities within our Job Portal, nor does it include other advertising activities that are not deemed to be targeted advertising according to specific exclusions set forth in applicable law.

"verifiable request" means a request that is made by you, by you on behalf of your minor child, by a natural person or a person authorized by you to act on your behalf, or by a person who has power of attorney or is acting as a conservator for you, and that we can verify, using commercially reasonable methods, pursuant to applicable law.

End of Job Portal Privacy Policy

© 2024 LOTTE Biologics USA, LLC