

Privacy Notices

for the fulfilment of information obligations



Content

Privacy Information for Business Partners	2
Privacy information for Online Events	4
Privacy information for Job Applicants	6

The LICOR Group develops and markets high-precision measurement, analysis and imaging systems for environmental and climate research, as well as for biomedical and biotechnological research. We respect your privacy and are committed to protecting your personal information. This Privacy Notice explains how we collect, use, disclose, retain and protect personal information relating to our customers, suppliers, distributors, service providers, prospective customers and other business partners. This notice is intended to provide transparency in accordance with applicable United States federal and state privacy laws, including the Nebraska Data Privacy Act (NDPA), the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), and other applicable state privacy laws.

The rights described below apply to the extent provided by the laws applicable to the individual and the processing activity concerned.

1. Responsible for data processing

The data controller within the meaning of data protection law is: LI-COR Biotech LLC, 4647 Superior Street, Lincoln, NE 68504, USA

2. Contact data of the data protection officer

You can contact our Data Protection Officer at the addresses provided above, or by email at privacy@licorbio.com.

3. Purposes and legal bases of data processing

We collect and use personal information for legitimate business purposes, including:

- We collect and use personal information for legitimate business purposes, including:
- Identifying and communicating with customers, suppliers and other business partners.
- Preparing quotations, negotiating contracts and processing orders.
- Delivering products and providing services.
- Managing customer accounts and business relationships.
- Providing technical assistance, maintenance, warranty services and customer support.
- Managing suppliers, distributors and service providers.
- Processing invoices, payments, accounting records and financial transactions.
- Organizing training courses, product demonstrations, webinars and other business events.
- Providing information about our products, services and business activities.
- Conducting permitted marketing, customer satisfaction surveys and market research.
- Improving our products, services, business processes and customer experience.
- Maintaining the security, availability and integrity of our IT systems.
- Detecting and preventing fraud, misuse, unauthorized access and other security incidents.
- Complying with applicable legal, regulatory, tax, accounting and export control obligations.
- Establishing, exercising or defending legal claims.

4. Categories of Personal Information

Depending on the nature of our business relationship, we may collect and process the following categories of personal information:

- Identification and business information: First name, last name, title, employer, department, professional role and business affiliation.
- Contact information: Business address, postal address, telephone number, email address and other business contact details.
- Commercial information: Products and services purchased or requested, quotations, orders, contracts, transaction history, warranty information and customer support records.
- Financial and payment information: Billing details, payment information, transaction records and information required for accounting and financial administration.
- Communications: Correspondence, inquiries, complaints, feedback and other information exchanged during our business relationship.
- Technical and device information: Product registration information, device identifiers, technical support records, service logs and information required for product maintenance or troubleshooting.
- Internet and electronic network activity: IP addresses, website usage information, online interactions and information collected through cookies or similar technologies, where applicable.
- Marketing and preference information: Product interests, communication preferences, event participation, survey responses and marketing interaction history.
- Other information: Personal information reasonably necessary for establishing, managing or performing our business relationship.

We generally do not require sensitive personal information for ordinary business relationships. Where such information is necessary, we apply additional safeguards and comply with applicable legal requirements.

5. Sources of Personal Information

We may obtain personal information:

- We may obtain personal information:
- Directly from you, including through inquiries, orders, contracts, correspondence and other interactions.
- From your employer or the organization you represent.
- From other companies within the LI-COR Group.
- From distributors, sales representatives and other business partners.
- From publicly available sources, including company websites, professional directories and business networking platforms.

- From service providers and other third parties where permitted by applicable law.
- Automatically through our websites, business applications and electronic communications, where applicable.

We may also use personal information for other compatible purposes or purposes disclosed to you at the time of collection.

Where applicable law requires consent or provides a right to opt out of particular processing activities, we will comply with those requirements.

6. Disclosure of Personal Information

We may disclose personal information to the following categories of recipients where reasonably necessary:

- LI-COR Group companies: For centralized administration, customer relationship management, sales, technical support, accounting, information technology and other internal business functions.
- Service providers and contractors: Including providers of IT infrastructure, cloud services, CRM systems, ERP systems, payment processing, communications, cybersecurity, data backup and technical support.
- Distributors and commercial partners: Where necessary to process orders, provide products or services, or support customers.
- Logistics and shipping providers: For product delivery and related services.
- Professional advisers: Including auditors, accountants, legal advisers and insurance providers.
- Public authorities and regulatory bodies: Where disclosure is required or permitted by applicable law.
- Parties involved in corporate transactions: Where necessary in connection with a merger, acquisition, restructuring or sale of business assets, subject to applicable safeguards.

We require service providers processing personal information on our behalf to implement appropriate safeguards and use the information only for authorized purposes, subject to applicable contractual and legal requirements.

7. Sale, Sharing and Targeted Advertising

Under certain United States state privacy laws, the terms "sale," "sharing" and "targeted advertising" have specific legal meanings that may extend beyond the conventional understanding of selling personal information for money.

Where applicable law provides a right to opt out of such activities, we will provide an appropriate mechanism for exercising that right.

We will not discriminate against individuals for exercising their legally protected privacy rights.

8. Retention of Personal Information

We retain personal information only for as long as reasonably necessary to fulfill the purposes described in this Privacy Notice, unless a longer retention period is required or permitted by applicable law.

Retention periods depend on the nature of the information, the business relationship and applicable legal obligations.

In particular, we may retain personal information for:

- The duration of the business relationship and any necessary follow-up activities.
- Applicable accounting, tax and financial reporting requirements.
- Product warranty, maintenance and customer support obligations.
- Compliance with contractual and regulatory requirements.
- Establishing, exercising or defending legal claims.
- Maintaining the security and integrity of our systems.

Where applicable, records may be retained in accordance with requirements under United States federal and state tax, accounting and commercial laws. Once personal information is no longer required, we will delete, anonymize or otherwise securely dispose of it in accordance with our retention policies and applicable legal requirements.

9. Data Security

We implement reasonable administrative, technical and physical safeguards designed to protect personal information against unauthorized access, disclosure, alteration, loss or destruction. These measures may include:

- Access controls and role-based permissions.
- Authentication and authorization mechanisms.
- Encryption of data where appropriate.
- Network and endpoint security.
- Monitoring and logging of relevant system activities.
- Backup and recovery procedures.
- Employee confidentiality obligations and security awareness training.
- Security incident management procedures.
- Appropriate contractual safeguards for service providers.

No security measure can guarantee absolute protection. We regularly review our security practices and adapt them to identified risks.

10. International Transfers of Personal Information

International Transfers of Personal Information

As an international business, the LI-COR Group may process and exchange personal information across different countries, including the United States, the United Kingdom, Switzerland and member states of the European Union. Personal information may be transferred to other LI-COR Group companies or authorized service providers where necessary for the purposes described in this Privacy Notice.

Where personal information is transferred from a jurisdiction that imposes specific restrictions on international transfers, we implement appropriate safeguards as required by the applicable law.

These safeguards may include:

- Applicable adequacy decisions.
- Standard Contractual Clauses approved by the European Commission.

- The United Kingdom International Data Transfer Agreement or UK Addendum, where applicable.
- Participation in an applicable and valid data transfer certification framework.
- Other legally recognized transfer mechanisms.

Further information about applicable international transfer safeguards may be requested using the contact details provided above.

11. Your Privacy Rights

Depending on your state of residence and the applicable privacy law, you may have some or all of the following rights:

- Right to access: Request confirmation of whether we process your personal information and obtain access to information covered by applicable law.
- Right to correction: Request correction of inaccurate personal information.
- Right to deletion: Request deletion of personal information, subject to applicable legal exceptions.
- Right to data portability: Obtain certain personal information in a portable and readily usable format, where required by law.
- Right to opt out: Opt out of certain processing activities, including the sale of personal information, targeted advertising or qualifying profiling activities, where applicable.
- Right to withdraw consent: Withdraw consent where processing is based on consent and applicable law provides this right.
- Right to appeal: Appeal a refusal to act on a privacy request where the applicable state privacy law provides an appeal mechanism.
- Right to non-discrimination: Exercise applicable privacy rights without unlawful discrimination or retaliation.

Some of these rights may not apply to personal information collected or processed exclusively in a commercial or employment context, depending on the relevant state law.

12. Exercising Your Privacy Rights

To exercise your applicable privacy rights, please contact the following mail address: privacy@licorbio.com

We may request additional information that is reasonably necessary to verify your identity and process your request.

We will respond within the time limits required by the applicable law. Where permitted, we may extend the response period and will notify you accordingly.

If we deny your request, we will explain the reasons required by law and provide information about available appeal procedures.

13. Additional Privacy Information for Residents of Certain U.S. States

Certain U.S. states provide additional privacy rights to their residents. These may include California, Colorado, Connecticut, Nebraska, Texas, Virginia, Oregon, New Jersey, Maryland, Minnesota and other states with applicable comprehensive privacy legislation.

The availability and scope of these rights depend on the applicable law, including its business applicability thresholds, definitions, exemptions and permitted exceptions.

13.1. California Residents

Where the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), applies, California residents may have additional rights, including:

- The right to know the categories and specific pieces of personal information collected, subject to applicable limitations.
- The right to request deletion of personal information.
- The right to correct inaccurate personal information.
- The right to opt out of the sale or sharing of personal information.
- The right to limit certain uses and disclosures of sensitive personal information, where applicable.
- The right not to be discriminated against for exercising CCPA rights.

The categories of personal information described in Section 4 may correspond to categories defined under the CCPA, including identifiers, commercial information, internet or electronic network activity information, professional information and other applicable categories.

13.2. Residents of Other U.S. States

Residents of other states with applicable comprehensive privacy laws may exercise the rights granted by those laws.

These may include rights to access, correct or delete personal information, obtain portable copies, opt out of certain processing activities and appeal decisions on privacy requests.

Certain state laws exclude personal information processed exclusively in a business-to-business or employment context.

We will evaluate and respond to requests in accordance with the law applicable to the individual and the relevant processing activity.

14. Direct Marketing Communications

We may use business contact information to provide information about our products, services, events, training opportunities and other relevant business activities.

Commercial electronic communications are sent in accordance with applicable laws, including the U.S. CAN-SPAM Act.

Marketing emails include an appropriate method to opt out of future commercial communications.

You may unsubscribe at any time using the unsubscribe link provided in our marketing emails or by contacting us at privacy@licorbio.com.

We will process opt-out requests in accordance with applicable legal requirements.

Please note that opting out of marketing communications does not prevent us from sending necessary transactional, contractual or service-related communications.

15. Automated Decision-Making and Profiling

We may use automated tools to support certain business processes, including customer relationship management, sales analysis and service improvement.

Where applicable law grants rights relating to such processing, we will provide the required information and mechanisms to exercise those rights.

16. Obligation to Provide Personal Information

During a business relationship, certain personal information may be necessary to:

- Establish and maintain contact.
- Prepare and perform contractual obligations.
- Process orders and payments.
- Provide products, services and technical support.
- Comply with applicable legal obligations.

If the required information is not provided, we may be unable to establish or continue the relevant business relationship or provide the requested products or services.

Information requested for optional purposes, such as certain marketing activities, is generally voluntary.

17. Privacy Regulatory Authorities

Privacy and consumer protection requirements in the United States are enforced by various federal and state authorities. Depending on the applicable law, these may include:

- Federal Trade Commission (FTC), United States
Website: <https://www.ftc.gov>
- Nebraska Attorney General, Office of the Attorney General, Lincoln, Nebraska
Website: <https://ago.nebraska.gov>
- California Privacy Protection Agency (CPPA), California, United States
Website: <https://cppa.ca.gov>

Individuals may submit complaints to the competent regulatory authority where permitted by applicable law.

The authority responsible for a particular matter depends on the applicable law and the nature of the complaint.

18. Updating of this data protection information

This privacy notice regarding our data processing may change from time to time. We will publish any changes on our website. We will provide you with previous versions on request.

Thank you for your interest in our webinars, online meetings and other virtual events (collectively referred to as "online events").

Through our online events, we aim to provide valuable information about our products, services, technologies and current industry topics.

In connection with your registration and participation, we collect and process personal information. This Privacy Notice explains how we collect, use, disclose, retain and protect your personal information, as well as the privacy rights available to you under applicable United States federal and state laws, including the Nebraska Data Privacy Act (NDPA), the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), and other applicable state privacy laws.

1. Responsible for data processing

The data controller within the meaning of data protection law is:

LI-COR Environmental LLC, 4647 Superior Street, Lincoln, NE 68504, USA

2. Contact data of the data protection officer

You can contact our Data Protection Officer at the addresses provided above, or by email at privacy@licorbio.com.

3. Purposes of data processing

We process your personal data for the following purposes:

- **Conducting and organizing online events:** We process the personal data you provide for the purpose of registration, conducting, and following up on the online event. This includes:
 - First and last name
 - Company
 - Job title / Position
 - Email address
 - Phone number (if provided)
 - Registration details
 - Participation information
 - Time and duration of participation
 - Technical connection data

The information is used to organize and conduct the online event, communicate with participants, provide event materials and respond to inquiries.

Processing is carried out for legitimate business purposes and, where applicable, in connection with providing the services requested by participants.

- **Conducted via Microsoft Teams:** We use Microsoft Teams to conduct our online events. The provider is Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland. When using Microsoft Teams, the following data is processed:
 - Participant data
 - Device and connection information
 - Audio and video data
 - Chat messages
 - Screen sharing
 - Usage data

This information is processed to provide the technical functionality necessary for conducting online events.

For more information on data processing by Microsoft, please visit:

<https://privacy.microsoft.com/de-de/privacystatement>

- **Transcription of online events:** For quality assurance, documentation, and the continuous improvement of our offerings, online events may be transcribed automatically or manually. For this, we use the Granola transcription software (<https://www.granola.ai>). In particular, the following may be processed:
 - Presentations by speakers,
 - Questions from participants,
 - Contributions to the discussion,
 - Chat messages,
 - Other content exchanged during the online event.

The transcripts will be deleted as soon as they are no longer needed for the stated purposes and will be used for the following internal purposes:

- for follow-up on online events,
- to answer participant questions,
- for quality assurance,
- to optimize future events,
- to create training and informational materials.

Transcripts will be deleted when they are no longer required for these purposes, subject to applicable retention obligations.

Participants will be informed about transcription practices as required by applicable law.

Where consent is required for the recording or transcription of communications, we will obtain the necessary consent before activating the relevant functionality.

- **Recording of Online Events:** Individual online events may be recorded following prior notice. The recording is used for:
 - making the content available to participants,
 - documenting technical content,
 - internal training,
 - quality assurance,
 - and the reuse of online event content.

Participants can join the event by turning off their camera and microphone, so they do not appear in the recording. The recording may include the following data:

- Audio contributions,
- Video contributions,
- Screen shares,

- Chat messages,
- Questions and comments from participants.

Participants will be informed when an event is recorded.

Where required under applicable federal or state law, including state communication privacy and recording consent laws, we will obtain the necessary consent before recording.

Participants who do not wish to appear in a recording may generally keep their cameras and microphones disabled. However, this does not necessarily prevent the recording of their names, chat messages, questions or other contributions.

Where recording or transcription is a condition of participation, this will be communicated before the event.

- **Use of Camera and Microphone:** The use of a camera and microphone during the online event is voluntary.

Participants may choose to:

- Keep their camera disabled
- Mute their microphone
- Submit questions through chat or email, where available

Participants who activate their camera or microphone during a recorded event should be aware that their audio and video contributions may be included in the recording.

Where applicable law requires express consent for recording or transcription, merely activating a camera or microphone will not be treated as a substitute for obtaining legally required consent.

- **Storage in the CRM system:** We use Salesforce CRM to manage our relationships with customers and prospects. The provider is: Salesforce Ireland Limited, Salesforce Tower, 60 R801 North Dock, Dublin 1, Ireland.

Any transfers to the United States are made in accordance with the EU-U.S. Data Privacy Framework or the EU Standard Contractual Clauses.

The following information may be stored in the CRM system:

- Contact information
- Company information
- Online event participation
- Communication history
- Interests in products and services
- Sales activities
- Newsletter preferences

This information is used to maintain relationships with customers and prospects, document business contacts and follow up on online participation. For more information, please visit

<https://www.salesforce.com/company/legal/privacy/>

- **Contact from our sales team:** Following the online event, our sales team may contact you in accordance with legal requirements. The purpose of this contact is:

- to answer any open questions,
- to provide additional information,
- to present relevant products and services,
- to assist prospective customers,
- to initiate or strengthen a business relationship.

Such communications will be carried out in accordance with applicable federal and state laws.

- **Newsletters and Information:** After the online event, participants may receive information on the following topics:

- Products and services,
- Technical information,
- Online-Events,
- Webinars,
- Training courses,
- Company news.

Commercial email communications are subject to applicable requirements, including the U.S. CAN-SPAM Act.

Where consent is required by applicable law, we will obtain it before sending the relevant communications.

Recipients may unsubscribe from marketing emails at any time using the unsubscribe mechanism provided in those messages.

- **Sale, Sharing and Targeted Advertising:** Certain U.S. state privacy laws define the sale or sharing of personal information broadly and may regulate the use of personal information for targeted advertising. Where applicable, participants may have the right to opt out of these activities,

4. Categories of personal data

You must provide the information required for registration and participation to attend the online event. Without this information, participation is not possible. The following data may be processed in connection with online event registration and participation:

- First and last name
- Company and Position / Role
- Contact data (E-Mail address, phone number, login credentials)
- Participation information
- Audio and video data
- Chat messages, questions and comments
- Screen sharing
- Technical connection data (IP address, device information)
- Usage logs
- Communication history
- Interests in products and services
- Marketing preferences

We generally do not require sensitive personal information to participate in online events.

Participants should avoid disclosing sensitive personal information during presentations, chats or discussions unless necessary and appropriate. Certain audio, video or other information may qualify as sensitive personal information under applicable state privacy laws depending on its content and use.

Information necessary for registration and participation must be provided to attend the online event. Other information, such as a telephone number or the use of a camera, may be optional.

5. Data recipients

Your data may be transferred to the following recipients in particular:

- Internal LI-COR departments
- Sales and marketing teams
- Other LI-COR Group companies
- IT and cloud service providers
- Microsoft, for online event functionality
- Salesforce, for customer relationship management
- Granola, for transcription services
- Other technical service providers necessary for organizing and conducting online events

Personal information may also be disclosed to professional advisers or public authorities where required or permitted by applicable law.

We require service providers processing personal information on our behalf to implement appropriate safeguards and process the information only for authorized purposes, subject to applicable contractual and legal requirements.

6. International Transfers of Personal Information

As an international business, the LI-COR Group may process personal information in the United States and other countries.

In connection with the use of Microsoft Teams, Salesforce, Granola and other business applications, personal information may be transferred to or accessed from countries outside the United States.

Where personal information originates from the European Union, the United Kingdom, Switzerland or another jurisdiction imposing restrictions on international data transfers, appropriate transfer mechanisms will be implemented where required.

Depending on the circumstances, these may include:

- Applicable adequacy decisions
- Standard Contractual Clauses approved by the European Commission
- The UK International Data Transfer Agreement or UK Addendum
- Participation in an applicable and valid data transfer certification framework
- Other legally recognized safeguards

Further information about applicable international transfer safeguards may be requested using the contact details provided above.

7. Retention period

We retain personal information only for as long as reasonably necessary to fulfill the purposes described in this Privacy Notice, unless a longer retention period is required or permitted by applicable law. The retention period depends on:

- Conducting and following up on the online event
- Maintaining relationships with customers and prospective customers
- Responding to participant inquiries
- Quality assurance and documentation
- Applicable legal and regulatory requirements
- Legitimate business needs
- Existing contractual relationships

Recordings and transcripts will be retained only for as long as necessary for their stated purposes and will subsequently be deleted or anonymized, unless further retention is legally required or permitted.

8. Your Privacy Rights

Depending on your state of residence and the applicable privacy law, you may have some or all of the following rights:

- Right to access: Request confirmation of whether we process your personal information and obtain access to information covered by applicable law.
- Right to correction: Request correction of inaccurate personal information.
- Right to deletion: Request deletion of personal information, subject to applicable legal exceptions.
- Right to data portability: Obtain certain personal information in a portable and readily usable format, where required by law.
- Right to opt out: Opt out of certain processing activities, including the sale of personal information, targeted advertising or qualifying profiling activities, where applicable.
- Right to withdraw consent: Withdraw consent where processing is based on consent and applicable law provides this right.
- Right to appeal: Appeal a refusal to act on a privacy request where the applicable state privacy law provides an appeal mechanism.
- Right to non-discrimination: Exercise applicable privacy rights without unlawful discrimination or retaliation.

Some of these rights may not apply to personal information collected or processed exclusively in a commercial or employment context, depending on the relevant state law.

9. Exercising Your Privacy Rights

To exercise your applicable privacy rights, please contact the following mail address: privacy@licorbio.com

We may request additional information reasonably necessary to verify your identity and process your request.

We will respond within the time limits required by the applicable law. Where permitted, we may extend the response period and will notify you accordingly.

If we deny your request, we will explain the reason where required by law and provide information about available appeal procedures.

10. Additional Privacy Information for Residents of Certain U.S. States

Certain U.S. states provide additional privacy rights to their residents.

These may include California, Colorado, Connecticut, Nebraska, Texas, Virginia, Oregon, New Jersey, Maryland, Minnesota and other states with applicable comprehensive privacy legislation.

The availability and scope of these rights depend on the applicable law, including its business applicability thresholds, definitions, exemptions and permitted exceptions.

10.1. California Residents

Where the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), applies, California residents may have additional rights, including:

- The right to know the categories and specific pieces of personal information collected, subject to applicable limitations.
- The right to request deletion of personal information.
- The right to correct inaccurate personal information.
- The right to opt out of the sale or sharing of personal information.
- The right to limit certain uses and disclosures of sensitive personal information, where applicable.
- The right not to be discriminated against for exercising CCPA rights.

The categories of personal information described in Section 4 may correspond to categories defined under the CCPA, including identifiers, commercial information, internet or electronic network activity information, professional information and other applicable categories.

10.2. Residents of Other U.S. States

Residents of other states with applicable comprehensive privacy laws may exercise the rights granted by those laws.

These may include rights to access, correct or delete personal information, obtain portable copies, opt out of certain processing activities and appeal decisions on privacy requests.

Certain state laws exclude personal information processed exclusively in a business-to-business or employment context.

We will evaluate and respond to requests in accordance with the law applicable to the individual and the relevant processing activity.

11. Direct Marketing Communications

We may use business contact information to provide information about our products, services, events, training opportunities and other relevant business activities.

Commercial electronic communications are sent in accordance with applicable laws, including the U.S. CAN-SPAM Act.

Marketing emails include an appropriate method to opt out of future commercial communications.

You may unsubscribe at any time using the unsubscribe link provided in our marketing emails or by contacting us at privacy@licorbio.com.

We will process opt-out requests in accordance with applicable legal requirements.

Please note that opting out of marketing communications does not prevent us from sending necessary transactional, contractual or service-related communications.

12. Objection to Direct Marketing

You may request that we stop sending you direct marketing communications at any time. You can do so by:

- Using the unsubscribe link in our marketing emails.
- Contacting us at privacy@licorbio.com.

We will honor opt-out requests in accordance with applicable legal requirements, including the CAN-SPAM Act.

Opting out of marketing communications will not prevent us from sending necessary transactional or service-related communications, including information about an online event for which you have registered.

Where applicable state privacy laws provide additional rights to opt out of targeted advertising or the sale or sharing of personal information, we will provide the required mechanisms.

13. Privacy Regulatory Authorities

Privacy and consumer protection requirements in the United States are enforced by various federal and state authorities. Depending on the applicable law, these may include:

- Federal Trade Commission (FTC), United States
Website: <https://www.ftc.gov>
- Nebraska Attorney General, Office of the Attorney General, Lincoln, Nebraska
Website: <https://ago.nebraska.gov>
- California Privacy Protection Agency (CPPA), California, United States
Website: <https://cppa.ca.gov>

Individuals may submit complaints to the competent regulatory authority where permitted by applicable law.

The authority responsible for a particular matter depends on the applicable law and the nature of the complaint.

14. The data protection supervisory authority responsible for us

This privacy notice regarding our data processing may change from time to time. We will publish any changes on our website. We will provide you with previous versions on request.

We are pleased that you are interested in joining LI-COR and have applied or are considering applying for a position with our company. We respect your privacy and are committed to protecting your personal information throughout the recruitment and selection process.

This Privacy Notice explains how we collect, use, disclose, retain and protect personal information relating to job applicants and prospective employees, as well as the privacy rights available under applicable United States federal and state laws.

These laws may include the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), the Fair Credit Reporting Act (FCRA), the Americans with Disabilities Act (ADA), the Genetic Information Nondiscrimination Act (GINA), and other applicable employment and privacy laws.

The availability of specific privacy rights depends on the applicable law and the circumstances of the processing.

1. Responsible for data processing

The data controller within the meaning of data protection law is:

LI-COR Environmental LLC, 4647 Superior Street, Lincoln, NE 68504, USA

2. Contact data of the data protection officer

You can contact our Data Protection Officer at the addresses provided above, or by email at privacy@licorbio.com.

3. Purposes and legal bases of data processing

We process personal information provided in connection with your application to assess your suitability for the position, conduct the recruitment process and determine whether to establish an employment relationship.

Depending on the circumstances, we may process the following categories of personal information:

- Identification and contact information: First name, last name, address, email address, telephone number and other contact details.
- Application information: Cover letters, application forms, references, CVs, and other documents submitted during the application process.
- Professional information: Education, qualifications, certifications, employment history, professional experience, skills and training records.
- Recruitment information: Interview notes, assessment results, communication history, recruitment status and evaluations relating to your suitability for the position.
- Professional online information: Information available through professional networking platforms, company websites or other publicly accessible professional sources.
- Background verification information: Information obtained through reference checks, employment verification or background screening, where permitted by applicable law.
- Employment eligibility information: Information necessary to verify eligibility to work in the United States, including information required for employment authorization verification.
- Compensation information: Salary expectations and other information relevant to employment negotiations, subject to applicable state and local restrictions.
- Technical information: Information generated when using our recruitment systems, including IP addresses, login information and system activity records, where applicable.
- Other information: Additional personal information reasonably necessary for the recruitment process or compliance with applicable legal obligations.

We process this information for the following purposes:

- Reviewing and evaluating applications.
- Assessing qualifications, professional experience and suitability for available positions.
- Communicating with applicants.
- Organizing and conducting interviews and assessments.
- Verifying information provided during the application process.
- Conducting reference checks and legally permitted background screening.
- Determining compensation and employment conditions.
- Preparing employment offers and employment agreements.
- Verifying employment eligibility.
- Complying with applicable employment, immigration, tax and other legal requirements.
- Maintaining the security and integrity of recruitment systems.
- Preventing fraud and protecting our legitimate business interests.
- Establishing, exercising or defending legal claims.

4. Information Obtained from Third Parties

Where necessary and permitted by applicable law, we may obtain information about applicants from third parties. Such sources may include:

- Former employers.
- Professional references.
- Recruitment agencies.
- Educational institutions.
- Professional networking platforms, such as LinkedIn.
- Publicly available professional information.
- Background screening providers.

We will comply with applicable legal requirements when obtaining and using information from third parties.

Where background checks are conducted through a consumer reporting agency, we will comply with applicable requirements under the Fair Credit Reporting Act (FCRA), including separate disclosures, authorization and applicable pre-adverse and adverse action procedures.

We will not request or use information that is prohibited under applicable federal, state or local employment laws.

5. Processing of Sensitive Personal Information

Certain recruitment activities may involve sensitive personal information, including information relating to disabilities, medical conditions or other protected characteristics.

Such information will only be collected and processed where permitted or required by applicable law, in particular:

- Medical information will be handled in accordance with the Americans with Disabilities Act (ADA) and other applicable laws.
- Genetic information will be handled in accordance with the Genetic Information Nondiscrimination Act (GINA).
- Information relating to protected characteristics will not be used for unlawful discriminatory purposes.
- Medical and accommodation-related information will be subject to appropriate confidentiality and access restrictions.

Where applicants voluntarily provide information for equal employment opportunity monitoring or other legally permitted purposes, that information will be handled separately where required and will not be used to make unlawful employment decisions.

6. Automated Decision-Making and Profiling

We may use recruitment software and automated tools to support administrative activities, application management and candidate evaluation. Where automated tools are used, we will comply with applicable federal, state and local requirements concerning transparency, discrimination prevention, accessibility and automated employment decision-making.

Where required by applicable law, we will provide additional information, notices or opportunities to exercise relevant rights.

7. Duration of storage and retention periods

We retain applicants' personal information only for as long as reasonably necessary for the recruitment process and applicable legal, regulatory and business purposes.

Retention periods depend on the outcome of the application, the type of information and applicable federal, state and local requirements.

7.1. Unsuccessful Applications

Where an application is unsuccessful, we may retain relevant application records for a limited period to:

- Document the recruitment process.
- Comply with applicable employment recordkeeping requirements.
- Respond to inquiries or complaints.
- Establish, exercise or defend legal claims.

Applicable federal employment laws may require employers to retain certain recruitment and personnel records for specified minimum periods. Longer retention may be necessary in connection with pending complaints, investigations or legal proceedings.

7.2. Applicant Talent Pool

Where permitted by applicable law, we may retain information about unsuccessful applicants for consideration for future vacancies.

Applicants will be informed about this practice and, where required, asked for their consent.

Applicants may request removal from the talent pool, subject to applicable legal retention obligations.

7.3. Unsuccessful Applications

Where an applicant accepts an employment offer, relevant application information may be transferred to the employee's personnel record.

Such information will subsequently be retained in accordance with applicable employment, payroll, tax, immigration and other recordkeeping requirements.

Different retention periods may apply to different categories of employee records.

Personal information will be deleted, anonymized or otherwise securely disposed of when it is no longer required, subject to applicable legal obligations.

8. Data recipients

We use recruitment and human resources systems to manage applications and the selection process. Personal information may be disclosed to the following categories of recipients where necessary:

- Human Resources: To receive, review and manage applications.
- Hiring managers and relevant departments: To assess qualifications and suitability for available positions.
- LI-COR Group companies: Where necessary for centralized recruitment, HR administration or consideration for positions within the Group, subject to applicable law.
- Recruitment agencies: Where external recruitment services are used.
- IT and recruitment software providers: For application management, hosting, system maintenance and technical support.
- Background screening providers: Where legally permitted and necessary for the recruitment process.
- Professional advisers: Including legal advisers and other authorized service providers.
- Public authorities: Where disclosure is required or permitted by applicable law.

We use specialized recruitment software to support our application process. Applications are generally reviewed by Human Resources and, where appropriate, forwarded to the hiring managers responsible for the relevant position.

Access to applicant information is restricted to personnel and authorized service providers who require the information for legitimate recruitment or related business purposes.

We require service providers processing applicant information on our behalf to implement appropriate safeguards and comply with applicable contractual and legal obligations.

9. International Transfers of Personal Information

As part of an international corporate group, LI-COR may process applicant information in the United States and other countries where LI-COR Group companies or authorized service providers operate. Applicant information may be transferred internationally where necessary for:

- Centralized recruitment and HR administration.
- Assessment of applications for positions within the LI-COR Group.
- IT infrastructure and recruitment system administration.
- Technical support and maintenance.
- Compliance with applicable legal and regulatory requirements.

Where personal information originates from a jurisdiction that imposes specific restrictions on international data transfers, appropriate safeguards will be implemented as required by applicable law.

Depending on the circumstances, these safeguards may include:

- Applicable adequacy decisions.
- Standard Contractual Clauses approved by the European Commission.
- The UK International Data Transfer Agreement or UK Addendum.
- Participation in an applicable and valid data transfer certification framework.
- Other legally recognized safeguards.

Further information about applicable international transfer safeguards may be requested using the contact details provided above.

10. Obligation to provide data

To participate in the recruitment process, applicants must provide certain personal information necessary to evaluate their qualifications and suitability for the position.

This may include identification information, contact details, professional qualifications, employment history and other information relevant to the application.

If the required information is not provided, we may be unable to evaluate the application or continue the recruitment process.

Certain information may also be required by law, particularly where employment eligibility verification or other legal obligations apply.

Providing additional information that is not necessary for the recruitment process is generally voluntary.

Applicants are not required to disclose information that employers are prohibited from requesting under applicable employment laws.

11. Automated decision making

We may use digital recruitment and applicant management systems to organize, review and process applications. These systems may support administrative tasks such as:

- Managing incoming applications.
- Organizing applicant information.
- Scheduling interviews.
- Tracking recruitment progress.
- Supporting candidate assessments.

Where automated decision-making or AI-supported recruitment tools are used, we will comply with applicable legal requirements, including requirements relating to discrimination prevention, transparency, accessibility and applicant rights.

Where applicable law provides specific rights concerning automated employment decisions, we will provide the required information and procedures.

12. Location of data processing

Applicant information may be processed on LI-COR's internal IT infrastructure and through authorized cloud-based recruitment and HR systems.

Processing may take place in the United States and, where necessary, in other countries in which LI-COR Group companies or authorized service providers operate.

We implement appropriate administrative, technical and physical safeguards designed to protect applicant information against unauthorized access, disclosure, alteration, loss or destruction.

These safeguards may include access controls, authentication mechanisms, encryption, logging, confidentiality obligations and appropriate contractual requirements for service providers.

13. Your Privacy Rights

Depending on your state of residence and the applicable privacy law, you may have some or all of the following rights:

- Right to access: Request confirmation of whether we process your personal information and obtain access to information covered by applicable law.
- Right to correction: Request correction of inaccurate personal information.
- Right to deletion: Request deletion of personal information, subject to applicable legal exceptions.
- Right to data portability: Obtain certain personal information in a portable and readily usable format, where required by law.
- Right to opt out: Opt out of certain processing activities, including the sale of personal information, targeted advertising or qualifying profiling activities, where applicable.
- Right to withdraw consent: Withdraw consent where processing is based on consent and applicable law provides this right.
- Right to appeal: Appeal a refusal to act on a privacy request where the applicable state privacy law provides an appeal mechanism.
- Right to non-discrimination: Exercise applicable privacy rights without unlawful discrimination or retaliation.

Some of these rights may not apply to personal information collected or processed exclusively in a commercial or employment context, depending on the relevant state law.

14. Exercising Your Privacy Rights

To exercise your applicable privacy rights, please contact the following mail address: privacy@licorbio.com

We may request additional information reasonably necessary to verify your identity and process your request.

We will respond within the time limits required by the applicable law. Where permitted, we may extend the response period and will notify you accordingly.

If we deny your request, we will explain the reasons required by law and provide information about available appeal procedures.

15. Additional Privacy Information for Residents of Certain U.S. States

Certain U.S. states provide additional privacy rights to their residents.

These may include California, Colorado, Connecticut, Nebraska, Texas, Virginia, Oregon, New Jersey, Maryland, Minnesota and other states with applicable comprehensive privacy legislation.

The availability and scope of these rights depend on the applicable law, including its business applicability thresholds, definitions, exemptions and permitted exceptions.

14.1. California Residents

Where the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), applies, California residents may have additional rights, including:

- The right to know the categories and specific pieces of personal information collected, subject to applicable limitations.
- The right to request deletion of personal information.
- The right to correct inaccurate personal information.
- The right to opt out of the sale or sharing of personal information.
- The right to limit certain uses and disclosures of sensitive personal information, where applicable.
- The right not to be discriminated against for exercising CCPA rights.

The categories of personal information described in Section 4 may correspond to categories defined under the CCPA, including identifiers, commercial information, internet or electronic network activity information, professional information and other applicable categories.

14.2. Residents of Other U.S. States

Residents of other states with applicable comprehensive privacy laws may exercise the rights granted by those laws.

These may include rights to access, correct or delete personal information, obtain portable copies, opt out of certain processing activities and appeal decisions on privacy requests.

Certain state laws exclude personal information processed exclusively in a business-to-business or employment context.

We will evaluate and respond to requests in accordance with the law applicable to the individual and the relevant processing activity.

16. Direct Marketing Communications

We may use business contact information to provide information about our products, services, events, training opportunities and other relevant business activities.

Commercial electronic communications are sent in accordance with applicable laws, including the U.S. CAN-SPAM Act.

Marketing emails include an appropriate method to opt out of future commercial communications.

You may unsubscribe at any time using the unsubscribe link provided in our marketing emails or by contacting us at privacy@licorbio.com.

We will process opt-out requests in accordance with applicable legal requirements.

Please note that opting out of marketing communications does not prevent us from sending necessary transactional, contractual or service-related communications.

15. Privacy Regulatory Authorities

Privacy and consumer protection requirements in the United States are enforced by various federal and state authorities. Depending on the applicable law, these may include:

- Federal Trade Commission (FTC), United States
Website: <https://www.ftc.gov>
- Nebraska Attorney General, Office of the Attorney General, Lincoln, Nebraska
Website: <https://ago.nebraska.gov>
- California Privacy Protection Agency (CPPA), California, United States
Website: <https://cppa.ca.gov>

Individuals may submit complaints to the competent regulatory authority where permitted by applicable law.

The authority responsible for a particular matter depends on the applicable law and the nature of the complaint.

17. Updating of this data protection information

This privacy notice regarding our data processing may change from time to time. We will publish any changes on our website. We will provide you with previous versions on request.