

ALL4 GLOBAL HR PRIVACY NOTICE

FEBRUARY 2025



Last Updated: February 17, 2025

This Notice is issued on behalf of **ALL4, LLC** (including ALL4, LLC **entities, subsidiaries, and affiliates**) and applies to:

Individuals located in the European Economic Area (EEA), the United Kingdom (UK), Switzerland, and/or Individuals employed or engaged by a subsidiary or affiliate of ALL4 in the United States or Europe who are:

- Current or former employees
- Applicants for any position (permanent, temporary, contractor, or contingent worker)
- Contractors or contingent workers
- Dependents or beneficiaries of employees or former employees

We may change this notice at any time and will notify you of any significant changes to it before they take effect.

- 1.0 Introduction: Who We Are and Our Commitment
- 2.0 What Personal Data We Collect and How We Collect It
 - 2.1 How We Collect Personal Data
 - 2.2 Exclusions
- 3.0 Legal Bases and Purposes for Processing Your Data
 - 3.1 Special Categories of Personal Data
- 4.0 Automated Decisions and Monitoring
- 5.0 Who We Share Your Data With
- 6.0 International Transfers
- 7.0 How We Keep Your Data Safe
- 8.0 How Long We Keep Your Data
- 9.0 Your Rights
- 10.0 Complaints and Contact Details
- 11.0 Commitment to Accuracy

1. INTRODUCTION: WHO WE ARE AND OUR COMMITMENT

ALL4 LLC (ALL4) takes data privacy and security seriously. We have implemented policies and procedures to protect your personal data whenever we process it. ALL4 is the data controller (or “business” under U.S. law) for the personal data described in this Notice. This Notice covers ALL4 and the following legal entities of ALL4:

- ALL4 LLC
- LARAGON MARKETING E INNOVACION, S.L. (Subsidiary)
- Laragon Sustainability Solutions Mexico SA (Subsidiary)
- ALL4 NC, P.C. (Affiliate)
- WVS Engineering, P.C. (Affiliate)

2. WHAT PERSONAL DATA WE COLLECT AND HOW WE COLLECT IT

Personal data or personal information is defined here as information relating to an identifiable individual. It does not include de-identified or aggregated data. Table 2-1 shows the primary categories of personal data ALL4 collects, where permitted by local law:

Table 2-1
Personal Data Categories

Data Category	Examples
Contact and Identifying Information	Name (including previous), address, personal phone, personal email, date of birth, gender, nationality, government-issued identifiers (e.g., Social Security Number), emergency contacts, marital status, dependents, photos/videos.
Financial Data	Bank account details, payroll records, tax information, company credit card details, expense information.
Employment Records	Salary, leaves of absence, benefits, start/end dates, workplace location, job titles, work history, performance reviews, disciplinary or grievance

	information, training records, Paid Time Off (PTO) records, compensation history, professional memberships.
Marketing Information	Photos and video footage from ALL4 events, media release consents.
Candidates and New Hire Data	Driver's license, passport or other legal identification copies, right-to-work documents, references, credit/criminal/education background checks where permitted, proof of address, curriculum vitae (CV), resume, cover letter details.
Business Contact Details	Business phone, business email.
Technical Data	IP address, login data, browser type, geolocation when using company systems, device location.
Usage Data	Information about your use of ALL4's systems (file/app usage, websites visited), closed-circuit television (CCTV) footage, building access logs.
Electronic Communications	Business-related email content, telecommunications (e.g., recorded calls if part of service delivery), complaints or requests raised by the employee.
Special Categories	Racial or ethnic origin, union membership, biometric data, health data, or criminal conviction data (processed only when legally permitted).
Other Personal Data	Health information (medical reports, reasons for absence), assessments, training results, complaints.

2.1 HOW WE COLLECT PERSONAL DATA

We collect data in several ways including:

- **Directly from you** (e.g., during onboarding or through self-service Human Resources (HR) portals).
- **From third parties**, such as:
 - Former employers or references
 - Employment/recruiting agencies
 - Credit/background check providers
 - Public authorities or public sources
 - Insurance agencies or benefits providers
- **From your managers or colleagues**

- **Through your interactions** with ALL4 systems (e.g., IT logs) or premises (e.g., security badges, CCTV)

If you choose not to provide the requested information, we may be unable to meet certain employment obligations (e.g., payroll, benefits, tax, or health and safety).

2.1.1 Personal Data About Children Under 18

We do not knowingly collect data about minors under the age of 18 except when listed as a dependent or emergency contact for employees. If we discover that we have collected such data without appropriate consent, we will remove it as required by law.

2.2 EXCLUSIONS

This Notice does not cover:

- De-identified or aggregated information (no longer identifying an individual)
- Health or medical information covered by the Health Insurance Portability and Accountability Act (HIPAA), the Confidentiality of Medical Information Act (CMIA), or similar U.S. laws.
- Financial data governed by the Gramm-Leach-Bliley Act (GLBA).

For personal data collected outside of the employment context (e.g., from customers or website visitors), see our [ALL4 Global Privacy Notice](#).

3. LEGAL BASES AND PURPOSES FOR PROCESSING YOUR DATA

We only process personal data when we have a valid reason including:

General Data Protection Regulation (GDPR) Lawful Bases:

- **Contract:** To fulfill contractual obligations with you.



- Legitimate Interest: Pursuing our business interests in ways not overridden by your fundamental rights/freedoms.
- Legal Obligation: Complying with applicable laws.
- Consent: Where you have given explicit permission (withdrawable at any time).
- Vital / Public Interest: Rare cases where processing is necessary to protect vital interests or serve the public interest.

California Consumer Privacy Act / California Privacy Rights Act (CCPA/CPRA) Business Purposes:

- Security, fraud prevention, internal operations, HR management, fulfilling legal obligations, etc.

Where both GDPR and CCPA/CPRA apply, we align our processing with the most stringent requirements. Examples are provided in the following table.

Table 3-1

Purpose/Activity	GDPR Lawful Basis	CCPA/CPRA Business Purpose
Payroll and Benefits	Contract, Legal Obligation	Business Purpose (Payroll/HR Administration)
Recruitment and Onboarding	Contract, Legitimate Interest (or Consent)	Business Purpose (HR Administration)
Background Checks (Where Lawful)	Legitimate Interest, Legal Obligation, Consent	Business Purpose (Security/Fraud Prevention)
IT and Facility Security (CCTV, Log Data)	Legitimate Interest, Legal Obligation	Business Purpose (Security)
Performance Management, Disciplinary Action	Contract, Legitimate Interest	Business Purpose (HR Administration)
Marketing/Public Relations (Use of Images)	Legitimate Interest, Consent	Business Purpose (Marketing/Promotion)

3.1 SPECIAL CATEGORIES OF PERSONAL DATA

Some data (e.g., health, biometric, race/ethnic origin, or criminal records) may receive extra protection under GDPR and CCPA/CPRA as sensitive personal information. We only process such data if:

- You have explicitly consented; or
- It is necessary for employment (e.g., occupational health, workplace accommodations); or
- It is required by law or for legal claims; or
- It is in the material public interest (where local law permits).

Access to sensitive data is limited to personnel with a strict need to know.

4. AUTOMATED DECISIONS AND MONITORING

We do not make decisions that legally or significantly affect you based solely on automated processing. Where automated tools or analytics are used (e.g., for initial background screenings), human review is included before any final decision.

We also monitor usage of ALL4 systems, premises, and facilities to ensure policy compliance, IT security, and efficient operations. Such monitoring may include:

- **Software logs:** Websites visited, email headers/content (as permitted by law)
- **Physical security:** CCTV footage, badge access logs
- **Cybersecurity:** IT and network security

5. WHO WE SHARE YOUR DATA WITH

We share personal data only where lawful, necessary, and subject to confidentiality/security obligations. Recipients include:

- **ALL4 subsidiaries and affiliates**
- **HR service providers** (payroll, benefits, recruitment tracking, background screening)
- **Security providers** IT/network security, building security
- **Enterprise IT service providers** (cloud hosting, collaboration tools, Enterprise Resource Planning (ERP) travel/expense platforms)
- **Government authorities** (e.g., tax agencies) where legally required
- **Credit/fraud protection, risk management agencies** if needed to prevent or detect crime
- **Professional advisers** legal counsel, auditors
- **Customers/clients** if necessary for service delivery (e.g., call recordings)
- **Potential buyers/partners** in a merger/acquisition under appropriate confidentiality agreements

We do not sell your personal data. Any transfers to third parties are governed by appropriate measures (e.g., contractual clauses).

5.1 ONWARD TRANSFER LIABILITY

Under applicable data protection laws and the Data Privacy Framework (DPF), ALL4 remains liable if a third-party processor processes your personal data in a manner inconsistent with those laws or DPF Principles unless we can demonstrate that we are not responsible for the event that gave rise to any unauthorized or improper processing.

6. INTERNATIONAL TRANSFERS

ALL4 may transfer personal data outside the European Economic Area (EEA), United Kingdom, or Switzerland. Some countries have been deemed by the European Commission or the UK government to provide an adequate level of data protection. Where no adequacy decision exists, ALL4 uses appropriate safeguards (e.g., Standard Contractual Clauses or Binding Corporate Rules) to ensure your data remains protected.

We typically transfer data to, among others, the United States, Spain, Ireland, Mexico, or the UK.

ALL4 complies with the EU-U.S. DPF where applicable, ensuring appropriate protection for personal data transferred from Europe to the United States.

7. HOW WE KEEP YOUR DATA SAFE

We apply physical, administrative, and technical measures to protect personal data from accidental loss, misuse, unauthorized access, alteration, or disclosure. Access to personal data is limited to those who have a business need and are bound by confidentiality obligations.

If a suspected breach occurs, we will follow our internal protocols and notify you and/or regulators where legally required.

8. HOW LONG WE KEEP YOUR DATA

We retain personal data as long as it is needed for the purpose for which it was collected or to comply with legal, contractual, accounting, or reporting requirements. We consider:

- The volume, nature, and sensitivity of the data;
- Potential risk of harm from unauthorized use or disclosure;
- The reasons we process the data and whether those purposes can be achieved by other means;
- Legal or regulatory recordkeeping requirements.

In general, we keep your data for the duration of your employment or application process; this may include our need to satisfy a legal, regulatory, accounting, or reporting requirement.

9. YOUR RIGHTS

Depending on your jurisdiction (e.g., EEA, UK, Switzerland, California), you may have one or more of the following rights regarding your personal data:

- **Access:** Request a copy of the personal data we hold.
- **Correction:** Have inaccurate or incomplete data corrected.
- **Erasure** (“Right to be forgotten”): Request deletion where no lawful basis for continued processing exists.
- **Objection:** Object to processing based on our legitimate interests or for direct marketing.
- **Restriction:** Ask us to pause processing in certain scenarios (e.g., pending accuracy checks).
- **Data Portability:** Receive data in a readily usable format (where processing is based on consent or contract).
- **Withdraw Consent:** Revoke consent at any time where we rely on it.
- **Automated Decision-Making:** You are not to be subject to decisions with significant effect made solely by automated means.



9.1 CALIFORNIA RESIDENTS (CCPA/CPRA)

California employees have similar rights, including the right to access, delete, correct, limit certain uses of sensitive personal information, and opt out of the sale/sharing of personal data per CCPA/CPRA. Please note ALL4 does not sell personal data.

9.2 EXERCISING YOUR RIGHTS

To exercise any of these rights, please contact our Data Protection Officer via the email or phone number provided in Section **Error! Reference source not found..** We may ask for proof of identity and/or additional information to confirm the request's validity. We will strive to respond promptly within one month.

10. COMPLAINTS AND CONTACT DETAILS

10.1 CONTACT US

If you have any questions, concerns, or wish to make a complaint about how ALL4 handles your personal data, please contact the Data Protection Officer.

Data Protection Officer

Email: dpo@all4inc.com

Phone: +1 610-933-5246

Postal Address:

ALL4
Attn: Data Protection Officer
2393 Kimberton Road
P.O. Box 299
Kimberton, PA 19442
USA

10.2 DISPUTE RESOLUTION

We will investigate and respond within applicable legal timeframes. If you believe we have not resolved your issue, you may contact:

- Your local Data Protection Authority in the EEA/UK/Switzerland.
 - https://edpb.europa.eu/about-edpb/board/members_en
 - <https://ico.org.uk/global/contact-us/>
- The Federal Trade Commission for privacy complaints under the EU-U.S. DPF.
- The California Attorney General or California Privacy Protection Agency for CCPA/CPRA complaints.

10.2.1 VeraSafe Data Privacy Framework Dispute Resolution

Where a privacy complaint or dispute cannot be resolved through ALL4's internal processes, we have agreed to participate in the VeraSafe Data Privacy Framework Dispute Resolution Procedure. Subject to the terms of the VeraSafe Data Privacy Framework Dispute Resolution Procedure, VeraSafe will provide appropriate recourse free of charge. To file a complaint with VeraSafe and participate in the VeraSafe Data Privacy Framework Dispute Resolution Procedure, please submit the required information here:

<https://www.verasafe.com/public-resources/dispute-resolution/submit-dispute/>

10.2.2 Binding Arbitration

If your concern remains unresolved after participating in the above procedures, you may have the option of engaging in binding arbitration under the Data Privacy Framework's "Recourse, Enforcement, and Liability" Principle.

11. COMMITMENT TO ACCURACY

ALL4 may change this notice at any time and will always post the latest version of the policy on our website.



This Notice is not contractual and does not form part of any employment or service agreement.

ALL4 HR Privacy Notice

Last Updated: February 17, 2025