ALL4 Data Privacy Notice

March 2025

INFO@ALL4INC.COM
610.933.5246
WWW.ALL4INC.COM

STRATEGY WITH SOLUTION.
PARTNERSHIP WITH A PURPOSE.

ALL4 Data Privacy Framework Privacy Notice

Effective Date: March 17, 2025

1. INTRODUCTION AND SCOPE

ALL4 LLC (ALL4, we, us, our) is committed to safeguarding personal data entrusted to us by our employees, clients, prospective employees, prospective clients, and business partners.

This Privacy Notice (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)

This Privacy Notice ("Notice") explains:

- **What personal data we collect**
- **Why we collect it**
- **How we use it**
- **With whom we share it**
- **Your rights regarding how we process personal data.**

This Notice incorporates requirements from the **EU-U.S. Data Privacy Framework ("EU-U.S. DPF")**, the **UK Extension to the EU-U.S. DPF**, the **Swiss-U.S. Data Privacy Framework ("Swiss-U.S. DPF")**, the **General Data Protection Regulation ("GDPR")**, and the **California Consumer Privacy Act ("CCPA") / California Privacy Rights Act ("CPRA")**. In the event of any conflict between this Notice and the Data Privacy Framework Principles, the **DPF Principles** will prevail.

2. DATA WE COLLECT AND WHY

The following table provides an overview of the categories and types of data we collect, the purpose(s) of processing that data, the lawful basis under the General Data Protection Regulation (GDPR), and the typical retention period or criteria:

Data Categories

Data Category	Identifier Examples	Purpose(s)	Lawful Basis Under GDPR	Retention Period
Website/Email Contacts	Name (including previous name), address, personal phone, personal address, personal email address, IP address, login data, browser type, geolocation when using company systems, device location.	To respond to inquiries or complaints; send marketing communications (if consented); analyze and improve our services.	Consent (marketing); Legitimate Interest; Contractual Necessity (inquiries)	Until consent is withdrawn or as required by law.
Client Representatives	First and last name, business telephone number(s), business email address(es)	To provide contracted services; manage billing and client relationships; correspond with client contacts.	Contractual Necessity	Duration of the contract plus any applicable statutory limitations.
Social Network Contacts	Name (including previous name), address, personal phone, personal email	To engage with our online community;	Consent (interacting	As long as you follow or interact with

	address, photos and video footage from ALL4 events, media release consents.	respond to direct messages and comments.	on social platforms)	ALL4; user-managed via social networks.
Job Applicants	References, education, media searches, sanction list searches, medical report or questionnaire to the extent permitted under local law, other information included in a resume, or cover letter or as part of the application process.	For recruitment and selection; to evaluate candidacy.	Pre-Contractual Steps	During the selection process or for up to one year, unless otherwise required by law.
Employees/ Contractors	Driver's license, passport or other ID copies, right-to-work documents, references, credit, criminal/education background checks where permitted, proof of address, CV or cover letter details.	For HR administration; payroll, benefits, and performance management.	Contractual Necessity Legal Obligation (payroll, taxes)	Typically for the duration of employment and statutory record-keeping periods.

If we process additional personal data for specific projects or services, we will provide relevant information at the time of collection (e.g., via a project-specific notice or data processing agreement).

3. DISCLAIMERS AND IMPORTANT NOTES

The following disclaimers and important notes apply.

3.1 THIRD-PARTY DATA

If you choose to provide us with personal data about others, you must inform them and obtain consent where required by law. We disclaim liability for any failure to do so.

3.2 CHILDREN'S DATA

We do not knowingly collect or process personal data from individuals under 18 years old. If you are under 18, do not provide personal data.

3.3 ELECTRONIC COMMUNICATIONS

We may use email or similar methods to address your inquiries or to send you information (including commercial information) if permitted by law or if you have consented.

3.4 ACCURACY AND LIABILITY

We take steps to safeguard your data, but we rely on you to provide accurate, lawful information, especially regarding third parties or minors.

4. SHARING PERSONAL DATA (ONWARD TRANSFER)

4.1 SERVICE PROVIDERS

We share personal data with service providers who process it on our behalf to deliver services or support our operations. Such third parties include those:

- Providing IT systems and infrastructure
- Managing our IT systems and infrastructure
- Providing customer support

4.1.1 Cross-Border Transfers and Confidentiality

Some of these service providers may be located outside the United States, including in countries that may not provide the same level of data protection as your home jurisdiction. In such cases, we will:

1. Obtain your explicit consent (where legally required) before transferring your personal data; or
2. Require contractual safeguards, ensuring they maintain at least the same level of confidentiality and data protection as we do. For transfers from the European Economic Area (EEA), Switzerland, or the United Kingdom, we may rely on recognized mechanisms (e.g., Standard Contractual Clauses, Data Privacy Framework certification).

4.1.2 Other Disclosure of Your Personally Identifiable Information

We may disclose your Personally Identifiable Information (PII) to the extent required by law or if we have a good-faith belief that such disclosure is necessary to comply with official investigations or legal proceedings initiated by governmental and/or law enforcement officials or private parties, including but not limited to: in response to subpoenas, search warrants, or court orders; or if we sell or transfer all or a portion of our company's business interests, assets, or both, or in connection with a corporate merger, consolidation, restructuring, or other company change; or to our subsidiaries or affiliates only if necessary for business and operational purposes as described in the section above.

We reserve the right to use, transfer, sell, and share aggregated, anonymous data. This data does not include any personally identifiable information (PII) about our employees, clients, prospective employees, prospective clients, business partners, or users. We may use this aggregated information for any legal business purpose, such as analyzing usage trends or identifying compatible advertisers, sponsors, clients, and customers.

If we must disclose your PII in order to comply with official investigations or legal proceedings initiated by governmental and/or law enforcement officials, we may not be able to ensure that such recipients of your PII will maintain the privacy or security of your PII.

4.1.3 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.

4.2 BUSINESS TRANSFERS

In the event of a merger, acquisition, or other corporate reorganization, personal data may be transferred to the acquiring or surviving entity, subject to confidentiality obligations and applicable data protection laws.

4.3 AGGREGATED DATA

We may use or share aggregated, anonymized data for lawful purposes such as analytics or marketing. This data does not identify individual users or employees.

5. INTERNATIONAL DATA TRANSFERS

ALL4 is headquartered in the United States. Personal data may be transferred from the EEA, Switzerland, or the UK to the U.S. under one of the following mechanisms:

- EU-U.S. DPF
- UK Extension to the EU-U.S. DPF
- Swiss-U.S. DPF

We have certified our adherence to these Framework Principles. To learn more about the Data Privacy Framework Program, and to view ALL4's certification, please visit:

- Data Privacy Framework Program

- DPF Participant Search

Where required, we may also rely on Standard Contractual Clauses (SCC) or other legally recognized transfer mechanisms for cross-border data transfers.

6. SECURITY MEASURES

We employ appropriate technical (e.g., encryption, access controls) and organizational (e.g., policies, training) security measures to safeguard personal data from unauthorized access, theft, or loss. These measures are regularly reviewed and updated in line with industry standards and the sensitivity of the data processed.

7. DISPUTE RESOLUTION AND ENFORCEMENT

7.1 INTERNAL COMPLAINTS

If you believe we have mishandled your personal data or infringed upon your rights, please **Contact Us**. We will investigate and attempt to resolve your concerns.

7.2 VERASAFE PRIVACY PROGRAM

ALL4 is a member of the VeraSafe Privacy Program. With respect to personal data processed in the scope of this Notice, VeraSafe has assessed ALL4's data governance and security for compliance with the VeraSafe Privacy Program Certification Criteria. These criteria require a high standard of privacy, addressing:

- Notice
- Onward Transfer
- Choice
- Access
- Data Security

- Data Quality
- Recourse and Enforcement

For more information about the VeraSafe Privacy Program, please visit VeraSafe's Website.

7.3 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/

7.4 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.

7.5 REGULATORY OVERSIGHT

ALL4 is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC). For HR data of EU/UK/Swiss employees, we also cooperate with the relevant Data Protection Authorities (EU DPAs, UK ICO, Swiss FDPIC).

8. YOUR RIGHTS

Depending on your jurisdiction and applicable laws such as\, GDPR in the EU/UK and the California Consumer Privacy Act / California Privacy Rights Act in California, you may have the following rights regarding your personal data:

- **Right to Access**: Request information about personal data we hold.
- **Right to Rectify**: Correct or update inaccurate or incomplete data.
- **Right to Delete (Erasure)**: Request deletion of data as permitted by law.
- **Right to Restrict Processing**: In certain circumstances, limit how we use your data.
- **Right to Object**: Object to certain data processing (e.g., direct marketing).
- **Right to Data Portability**: Request a copy of your data in a structured, machine-readable format.
- **Right to Withdraw Consent**: Where processing is based on consent.

Additional Rights for California Residents (CCPA/CPRA)

- **Right to Know**: About the categories of personal information we collect, use, and disclose.
- **Right to Delete**: Request deletion of your personal information, subject to legal exceptions.
- **Right to Opt-Out of Sale or Sharing**: If applicable, request that we do not sell or share your personal information.
- **Right to Non-Discrimination**: We will not discriminate against you for exercising these rights.

To exercise any of these rights, please **Contact Us**. We may require additional information to verify your identity before proceeding with your request.

9. DATA RETENTION

We retain personal data as long as needed to fulfill the purposes described in this Notice, comply with legal obligations, or meet legitimate business needs. This may include:

- **Legal Obligations** such as litigation holds and regulatory investigations.
- **Regulatory Requirements,** industry- or sector- specific.
- **Business Needs** for historical reference or future services.

Emails or documents containing personal data may be stored longer than typical retention periods to ensure traceability and continuity of services.

10. COOKIE NOTICE

We use cookies and similar technologies on our website too:

- Analyze usage patterns
- Personalize content and advertisements
- Provide social media features, where relevant

11. CHANGES TO THIS NOTICE

We may modify this Notice to reflect changes in our data practices or regulatory obligations. Any material changes will be posted here with an updated Effective Date at the top. We encourage you to review this Notice regularly.

12. CONTACT US

If you have questions about this Notice, want to exercise any of your rights, or wish to file a complaint, please contact us:

Email: DPO@all4inc.com

Phone: +1 610-933-5246

Postal Address:
ALL4
Attn: Data Privacy Officer
2393 Kimberton Road
P.O. Box 299

Kimberton, PA 19442

USA

We will respond in accordance with applicable laws. Please allow up to four weeks for a response.

13. GLOSSARY

- **Personal Data / Personal Information / PII**: Any information that identifies or can be used to identify an individual.
- **Controller**: The entity that determines the purposes and means of processing personal data.
- **Processor**: The entity that processes personal data on behalf of the controller.
- **EEA**: European Economic Area (EU Member States plus Iceland, Liechtenstein, and Norway).
- **DPF**: Data Privacy Framework (EU-U.S., Swiss-U.S., UK Extension).
- **GDPR**: General Data Protection Regulation (EU law governing data protection).
- **CCPA/CPRA**: California Consumer Privacy Act / California Privacy Rights Act, which govern the handling of personal information of California residents.