DATA PROCESSING AGREEMENT

This Data Processing Agreement (hereinafter: the “**DPA**”) is made between:

1. **The “Customer” or the “Controller”**

2. Lempire SAS a company incorporated under the laws of France with its registered office 128 rue la Boétie, 75008, Paris, (hereinafter: the “**Provider**” or the “**Processor**”),

Each a “Party” and together “the Parties”.

WHEREAS

1. The Customer and the Provider have entered into an agreement for the provision of the services “Automated (cold) E-mailing and sales automation” (hereinafter: the “**Services**”).
2. When supplying the Services, the Provider will process information including Personal Data contained in content hosted or otherwise managed on the Customer’s behalf.
3. The parties agree to enter into this DPA in order to confirm the data protection provisions relating to their relationship and so as to meet the requirements of the Data Protection Laws and Regulations in relation to the protection of Personal Data.

1. Definitions and interpretation

1.1. In addition to terms defined elsewhere in this DPA, the following definitions apply throughout this DPA unless the contrary intention appears:

Controller The entity which alone or jointly with others determines the purposes and means of the Processing of Personal Data.

Data Protection Laws and Regulations All laws and regulations, including laws and regulations of the European Union and their member states, applicable to the Processing of Personal Data under the DPA, such as but not limited to the GDPR and the laws and regulations implementing the latter within the member states of the European Union, as well as the French Data Protection Act

GDPR Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Data Subject An identified or identifiable natural person, the latter being one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

DPA This Data Processing Agreement entered into between the Customer (Controller) and the Provider (Processor), that is binding on Provider with regards to Customer and sets out, among others, the subject-matter of the Processing of Personal Data.

European Union The member states of the European Union and, if and when the GDPR is incorporated within the EEA Agreement, the member states of the European Free Trade Association.

Personal Data Any information relating to a Data Subject.

Personal Data Breach A breach of security leading to the accidental or unlawful destruction loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Processing Any operation or set of operations which is performed upon Personal Data or sets of Personal Data, whether or not by automated means such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor The entity which Processes Personal Data on behalf of the Controller.

Service Agreement The agreement entered into between the Controller (as the client) and the Processor (as the service provider)

Sub-Processor Any entity appointed by or on behalf of Processor to Process Personal Data on behalf of Controller.

2. PURPOSE OF DPA

2.1. The purpose of this DPA concerns the Processing of Personal Data to allow the performance of the Services.

2.2. The Parties hereby explicitly determine the Provider to be the Processor and the Customer to be the Controller for the Processing of Personal Data.

2.3. As part of their contractual relations, the Parties shall undertake to comply with the applicable Data Protection Laws and Regulations and, in particular the GDPR.

3. DESCRIPTION OF THE PROCESSING

3.1. The Processing of Personal Data by Provider, on behalf of Customer, comprises of performance of the following Services :

3.1.1. “Automated (cold) E-mailing” services (Sending cold emails with automated follow up process);

3.1.2. Prospection on professional social networks and by phone.

3.2. When providing the Services, the Provider shall carry out the following processing activities:

3.2.1. Collecting and storing Personal Data with the sole purpose of completing the Services.

3.2.2. The Provider shall process the types of Personal Data as described in Annex 1– Description of the Processing.

3.2.3. The categories of Data Subjects as involved in the Processing of Personal Data by Provider are contained in Annex 1.

3.2.4. Both, Provider and Customer shall Process Personal Data in accordance with the requirements of the applicable Data Protections Laws and Regulations and this DPA.

4. Instructions

4.1. The Provider shall undertake to process Personal Data only on behalf of, and in accordance with documented instructions from the Customer, including with regards to the possible transfers of Personal Data to a third country or to an international organization outside of the European Union, unless the Provider is required to do so by Union law or applicable Member state law. In such a case, the Provider shall inform the Customer about the legal requirements before the Processing of Personal Data, unless the applicable law prohibits this notification based on important grounds of public interest.

4.2. The instructions of the Customer to the Provider, for the Processing of Personal Data, shall comply with all applicable Data Protection Laws and Regulations.

4.3. The Customer hereby instructs the Provider to process Personal Data for the following purposes:

4.3.1. Processing as follows from the DPA.

4.3.2. Processing to comply with any further reasonable explicit written instructions of the Customer.

4.4. The Provider shall immediately inform the Customer if, in its opinion, an instruction infringes the GDPR or other applicable Data Protection Laws and Regulations.

5. OBLIGATIONS AND RIGHTS OF THE PROVIDER

5.1. The Provider shall undertake, considering the nature of the Processing, to assist the Customer, insofar as this is possible, for the fulfillment of the Customer's obligation to respond to requests for exercising the Data Subject's rights: right of access, to rectification, erasure and to object, right to restriction of processing, right to data portability, right not to be subject to an automated individual decision (including profiling). Where requests are made directly to the Provider, the Provider shall send such requests to the Customer as soon as possible.

5.2. The Provider shall ensure that its personnel authorized to process the Personal Data hereunder:

5.2.1. have committed themselves to confidentiality thereof or are under an appropriate statutory obligation of confidentiality.

5.2.2. Receive the appropriate Personal Data protection training.

5.3. Provider shall guarantee the confidentiality of Personal Data processed and ensure that access to Personal Data is limited to its authorized personnel.

5.4. The Provider undertakes to assist the Customer and to respond without undue delay to any request for information sent by the Customer, whether in the context of a request for the exercise of their rights by data subjects, a privacy impact assessment, prior consultation of the supervisory authority, or a request made by a supervisory authority or the Customer's data protection officer.

5.5. The Provider shall make available to the Customer, at the Customer's request, all information and documents necessary to demonstrate compliance with its obligations and allow for audits. The Customer may carry out audits once a year, at its own expense to verify the Provider's compliance with the obligations set forth in this article. The Customer will inform the Provider of the audit at least two (2) weeks before. The Provider may refuse the identity of the auditor if it belongs to a competing company. The audit shall be conducted during work hours and with the least possible disturbance for the Provider’s activity. The audit shall not threaten (i) technical and organizational security measures implemented by the Provider, (ii) security and confidentiality of data of the Provider’s other customers, (iii) the proper functioning and organization of the Provider. When possible, Parties will agree beforehand on the scope of the audit. The audit report will be sent to the Provider as so to submit comments, which will be attached to the final version of the audit report. Each audit report will be considered confidential information.

6. OBLIGATIONS AND RIGHTS OF THE CUSTOMER

6.1. The Customer undertakes to:

6.1.1. Ensure the performance of the rights of the Data Subjects as stated in the Data Protection Laws and Regulations;

6.1.2. Provide the Provider with the personal data mentioned in Appendix 1, except any improper, disproportionate or unnecessary personal data, and except any “particular” personal data within the meaning of the Applicable regulation, except if the processing activities justify it. In this case, the Client will have to document these justifications and to take all measures, notably of prior information, to collect appropriate consent and appropriate security measures, appropriate for such particular data;

6.1.3. Document, in writing, any instruction bearing on the Processing of Personal Data by the Provider;

6.1.4. Collect under its liability, lawfully, fairly and in a transparent manner the personal data provided to the Provider, for the performance of its services, and in particular, to ensure the lawfulness of processing and the information due to data subjects;

6.1.5. Maintain a record of processing activities carried out and more generally, comply with the principles of the Applicable regulation;

6.2. The Customer is responsible for the accuracy and legality of the Personal Data as described in Appendix 1 and the means by which it acquires the Personal Data.

6.3. The Customer shall comply, before and throughout the Processing, with the terms of this DPA and all the applicable Data Protection laws and Regulations.

6.4. The Customer shall implement appropriate technical and organizational procedures to protect the Personal Data.

7. SECURITY

7.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Provider undertakes to implement the appropriate technical and organizational measures to protect the security, confidentiality and integrity of personal data.

7.2. To this end, the Provider undertakes to implement the security measures included in Annex 2 – Security Measures.

7.3. Upon request, the Provider shall assist the Customer in ensuring compliance with the obligations pursuant to articles 32 to 36 GDPR, taking into account the nature of Processing and the information available to the Provider.

8. PERSONAL DATA BREACHES

The Provider shall notify the Customer of any personal data breach relating to the processing operations covered by this Agreement, without undue delay after becoming aware of it and to provide the Customer with all relevant information and documentation relating to such personal data breach.

The notification shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

9. SUB-PROCESSORS

9.1. The Customer hereby grants its general written authorisation to the Provider to appoint Sub-Processors for the purpose of performing the Services and the DPA. The list of Sub-Processors is set out in the Annex I. If the Customer connects to an external provider within the tool by the use of external API, or when ordering to external providers within the tool, the Customer will be informed about the Sub-Processors.

9.2. When and insofar the Customer has agreed to the appointment of a Sub-Processors, the Provider shall enter into a written agreement with such Sub-Processor imposing at least the same obligations for the Sub-Processors as those in this DPA for the Provider.

9.3. If during the duration of the Service Agreement, the Provider intends to replace an existing Sub-Processor and/or to commission additional Sub-Processors, the Provider shall inform the Customer in writing or per email of any intended changes concerning the addition or replacement of Sub-Processors as listed. This information must clearly indicate which processing activities are being subcontracted out, the name and contact details of the Sub-Processor and the dates of the subcontract. The Customer has a maximum time frame of 20 (twenty) days from the date on which it receives said information to submit its legitimate and justifiable objections thereto with registered letter upon receipt with immediate effect. Such subcontracting is only possible where the Customer has not objected thereto within the agreed timeframe.

In the event of Client's continuing objections, the Parties shall meet in good faith and use their best efforts to discuss a resolution. The Provider may choose to (i) not hire the Sub-Processor or (ii) take the corrective action requested by the Client in connection with the objections before hiring the Sub-Processor. If neither option is reasonably possible, and if the Provider cannot for legitimate reasons hire another processor for the intended processing, either Party may terminate this Agreement upon a thirty (30) days' notice.

9.4. The Sub-Processor is obliged to comply with the obligations hereunder on behalf of and on instructions from the Customer. It is the initial Provider's responsibility to ensure that the Sub-Processor provides the same sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing meets the requirements of the GDPR. Where the Sub-Processor fails to fulfill its data protection obligations, the Provider remains fully liable with regard to the Customer for the Sub-Processor's performance of its obligations.

10. TRANSFER OF PERSONAL DATA OUTSIDE THE EUROPEAN UNION

The Provider is authorized to transfer personal data processed as part of this Agreement to countries located outside the European Union, if appropriate safeguards have been implemented as defined under Chapter V of GDPR.

11. RE-USE OF DATA BY THE PROVIDER

The Customer hereby authorizes the Service Provider to process the personal data collected in the context of the services (in particular, the data contained in the

prospecting emails sent by the Customer) for the purpose of improving the services of the Service Provider.
The Service Provider shall act as a data controller within the meaning of the applicable Regulations and undertake to comply with the legal provisions on Data Protection in the context of the aforementioned processing.

12. DATA PROTECTION OFFICER

The Provider has appointed a Data Protection Officer. The Controller can contact the Data Protection Officer via email at privacy@lemlist.com.

13. DURATION AND FATE OF PERSONAL DATA

13.1. The present DPA shall come into effect and remain valid for the term of the Service Agreement, and shall be effective for an additional period after the expiry of the Service Agreement as long as necessary to duly fulfill the obligations relating to the personal data processing outstanding after the expiry of the Service Agreement (or for a longer period if it is provided for in applicable legal acts).

13.2. At the termination of the Service Agreement, the Provider shall, at the discretion of Customer, destroy or return all Personal Data received from the Customer on the basis of the Service Agreement and the present DPA. The Provider shall ensure that its Sub-Processors would also destroy or return the received personal data. Together with said return, all existing copies in the Provider's information systems must be destroyed. Once destroyed, the Provider must demonstrate, in writing, that this destruction has taken place.

13.3. The Provider shall be entitled to keep the Personal Data received from the Customer to the extent they are necessary for compliance with the requirements of the applicable legal acts, also ensuring the protection and confidentiality of all such Personal Data, or for the purpose of archiving.

14. WARRANTIES AND LIABILITY

14.1. The Parties acknowledge and agree that the liability caps set forth in the Service Agreement between the Parties in connection with processing carried out by the Provider, shall apply to the Provider’s compliance with the terms of this DPA and Applicable Regulation.

14.2. The Provider will not be held liable for any claim brought by a Data Subject arising from any action or omission by the Provider, to the extent that such action or omission resulted directly from the Customer’s instructions.

15. GOVERNING LAW AND COMPETENT JURISDICTION

15.1. This DPA shall be subject to French law.

15.2. In the event of a dispute between the Parties relating to the formation, interpretation or performance of this DPA, exclusive jurisdiction is given to the courts within the jurisdiction of the Court of Appeal of Paris notwithstanding plurality of defendants, even for emergency proceedings or conservatory proceedings by way of summary proceedings.

16. MISCELLANEOUS

16.1. Should a provision of this DPA be invalid or become invalid then, to the extent possible, the legal effect of the other provisions shall be unaffected. A valid provision is deemed to have been agreed which comes closest to what the parties intended and shall replace the invalid provision.

16.2. In the event of any discrepancies between the terms of this DPA and other arrangements made between the Parties, including the Service Agreement, the terms of this DPA shall prevail.

Annex 1 – Description of the Processing.

Annex 2 – Security Measures.

IN WITNESS WHEREOF, the Parties authorized signatories have duly executed this Data Processing Agreement including its appendices:

Provider	**Customer**
Signature:	Signature:
Name of signatory:	Name of signatory:
Position:	Position:
Date:	Date:

Annex I –Description of the Processing

A. Type of Personal Data processed:

The Processing of Personal Data includes the following data types/categories (List/Description of the Data Categories)

✓ Personal Master Data (Key Personal Data, e.g. account id)

✓ Contact Data (e.g. Name, E-Mail, Phone Number)

✓ Professional Data (e.g. title, position, etc.)

✓ Disclosed Information (from third parties, e.g. from Public Directories)

✓ IP Address

B. Categories of Data Subjects:

Customer's Employees, Prospects, opportunities & customers.

C. List of Sub-Processors

Some of the Service's features and integrations require the use of additional Sub-Processors. Some Sub-Processors will apply as a default, and some Sub-Processors will apply only if and when activated. In either case, the controller may choose not to use the Applicable Service provided by these Sub-Processors. The name of the Provider is usually displayed right next to the feature. When the Controller is connecting their own external tools or using an external provider, it should rely on their own DPA.

Authorized subsequent subcontractors	Outsourced processing activities	Country	Appropriate safeguards in place for data transfers outside the EU
OVH	Data hosting	France	N/A
Scaleway	Data Backup	France	N/A
CloudFlare	Data Backup	USA	Adequacy decision (DPF) and SCCs
CleverCloud	Elastic Search	France	N/A
Intercom	Customer Support	USA (data hosted in EU)	DPA with SCCs

OpenAI, L.L.C. (optional)	AI function (controller can use their own API key)	USA	DPA with SCCs - data minimized before sending, user decides which data is sent to the LLM, no conservation or reuse by the provider
Anthropic AI (optional)	AI function (controller can use their own API key)	USA	DPA with SCCs - data minimized before sending, user decides which data is sent to the LLM, no conservation or reuse by the provider
Google Gemini (optional)	AI function (controller can use their own API key)	USA	DPA with SCCs - data minimized before sending, user decides which data is sent to the LLM, no conservation or reuse by the provider
Perplexity AI (optional)	AI function (controller can use their own API key)	USA	DPA with SCCs - data minimized before sending, user decides which data is sent to the LLM, no conservation or reuse by the provider
ElevenLabs (optional)	AI Voice cloning	USA	DPA with SCCs - the voice record is deleted by the Provider minutes after the cloning, no re-use

Annex II – Security Measures

The Provider will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data as updated from time to time, and accessible via https://trust.lemlist.com/ or otherwise made reasonably available by the Provider.

The Provider has been certified SOC2 Type II.

All treated information is protected in transit using the HTTPS protocol.

All servers are located in the EU in order to be fully GDPR compliant.

All the backups are encrypted using AES 256. In order to ensure a high availability of our service, we track everything with Prometheus, Grafana and Loki with alert monitoring that contacts the development team in case of failure. A history of the service status can be found on https://status.lempire.com/.

In order to always keep the highest level of security, the Provider has developed a set of policies in regard to its Security Policies:

Human Resources

Employee Handbook / Code of Conduct : Organizational values and behavioral standards are communicated to all personnel through an Employee Handbook, which outlines the company's policy regarding Standards of Conduct and Code of Business Ethics.

Security Awareness Training : Security awareness training is provided to new employees, and to all employees on a recurring annual basis, to promote strong security practices for the whole company.

Human Resources Policy : The company has a Human Resources Policy that outlines the requirements and responsibilities of the Human Resources department.

Board of Directors : A Board of Directors exercises independent oversight of the company's strategic direction, operational performance, and internal control.

Security Officer : Management and the Board of Directors consider requirements relevant to security, availability, processing integrity, and confidentiality. These considerations are documented in the company's Information Security Policy, which specifically delegates the overall responsibility of security to the Security Officer.

Organizational Structure : The company has an appropriate organizational structure based on functional departments, with an executive leader heading each department.

Confidentiality Agreement : All employees and contractors must sign a confidentiality agreement with the company prior to gaining access to any sensitive information.

Termination Process : Termination checklists are executed upon separation with an employee or contractor to ensure asset return, and prompt and complete access revocation.

Employee Performance Reviews : The company has established a formal review process that includes semi-annual employee self-reviews and immediate manager reviews. Reviews include performance assessments, goal setting, and an evaluation of resources required for the next review period.

Disciplinary Process : Material violations of the company's Acceptable Use Policy, Code of Conduct, and Information Security policies and procedures applicable to each employee subjects the individual to disciplinary action that could include termination.

Job Descriptions : Roles and responsibilities of company employees are communicated through documented job descriptions.

Board Oversight : The company leadership conducts formal reviews of the company's internal performance results with the Board of Directors.

Access Control

Administrative Access : Administrative access privileges for sensitive systems are only granted to a restricted, small set of personnel, with a clearly defined business need to maintain and administer those systems.

Customer Confidential Systems Access Review : A review of users with access to Customer Confidential systems is performed periodically to ensure that access is restricted to appropriate personnel.

Single Sign-On (SSO) : The company leverages SSO authentication for sensitive systems, wherever available.

Requesting and Approving Access : Access to systems is requested by filing an internal access request ticket specifying the need for the access. Access is approved by the respective manager and granted by administrators based on a least-privilege principle.

Password Management Tool : All users with privileged access to sensitive systems are required to use a password management solution.

Role-Based Access Control : Defined permission roles are utilized to assign and segregate access privileges to data and systems.

Multi-Factor Authentication (MFA) : Access to sensitive systems requires multi-factor authentication.

Password Configurations : Password configuration settings are managed in compliance with the company's Password Policy.

Least-Privilege Access : Access to sensitive systems and resources is granted based on the principle of least privilege.

Monitoring

Centralized Logging : Applications and system logs are pushed to a central logging repository where possible. Access control to the central repository is enforced based on the Access Control policy. Logs are retained in compliance with applicable legal, regulatory, customer, and operational requirements.

Security Event Logging : Security tools are deployed and system components are configured to monitor for security-related events.

Security Event Review : Security events are triaged and reviewed for unauthorized and malicious activity. High priority findings are treated as potential security incidents.

Business Operations

Disaster Recovery Testing : A disaster recovery test with predefined RTO goals is performed annually, assuming a full outage of our primary cloud region.

Change Management Workflow : The Change Management documentation outlines the internal workflow for propagating application and infrastructure code changes to the production environment, including tracking, testing, reviewing and approving.

Status Page : The company has a Status Page that provides information about the company's status, including outages, incidents, and other relevant information.

Terms of Use : The company's Terms of Use are available online to visitors and customers, and outline the requirements and commitments of both parties relative to security and confidentiality.

Corrective Actions : Control owners take corrective actions when issues and nonconformities with their controls are identified.

Control Reviews : Management periodically reviews control activities to reaffirm each control's relevance, and updates the set of controls as necessary.

Documentation Site : The company maintains a customer-accessible technical documentation site containing high-level overviews and detailed information about the company's products and services, including security-oriented articles and guides.

Security Incident - Tracking : Incidents are recorded and tracked, and all applicable evidence and documentation is reviewed in post-mortem meetings.

Risk Register : The company maintains a Cumulative Risk Register storing control deficiencies identified as part of ongoing system reviews, and reviews the register as part of the company's regular Risk Assessment process.

Support Channel : External users are provided with a support channel for reporting systems failures, incidents, concerns, and other complaints to appropriate personnel.

Release Notifications : The company communicates system changes to its users and customers through an established channel and procedure.

Fraud Risk : The company assesses the potential for fraud from internal or external stakeholders as part of its Risk Assessment process.

Control Selection : The company designs and implements controls to mitigate risks identified during the risk assessment process.

Trust Center : The company has a Trust Center that provides information about the company's security practices, policies, and procedures.

Legal Proof of Company Registration : The company holds an official legal document confirming its registration in the relevant jurisdiction.

Production Deployment Access : The ability to deploy application changes to production environments is restricted to authorized personnel.

Change Management Tooling : Change Management procedures are expressed, as much as possible, in appropriate configuration of Continuous Integrations / Continuous Deployment tools, in order to minimize human error and increase auditability of the changes.

Master Services Agreement : The company's Master Services Agreement with its customers communicates the responsibilities of both parties relative to internal controls impacting Security, Availability, Processing Integrity and Confidentiality.

Security Incident Management Program : The Security Incident Management Program outlines the requirements and process for declaring and responding to security incidents, including the roles and responsibilities, and the internal and external communication necessary to take the issue to resolution.

Backup Storage : Backups are encrypted, stored in geographically independent regions, and have equivalent access control to the original system.

SDLC - Separation of Environments : The company maintains separate production and non-production environments.

Business Continuity / Disaster Recovery Program : The company maintains a Business Continuity Policy and Plan which outlines the requirements and a process to recover from prolonged disruptions of business operations.

Technology Control : Control activities over the technology infrastructure and technology access control are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.

Privacy Policy : The company's Privacy Policy is available online to visitors and customers, and outlines the receipt, sharing, use, and disposal of visitor and subscriber data.

Backup Plan : Customer data is automatically backed up according to a backup configuration scheduled described in the Backup Policy.

Policy Management : The company develops and maintains formal policies that govern information security within the company. The policies are formally reviewed and approved at least once a year, and are communicated to all employees.

Cyber Insurance : The company has cyber insurance to mitigate the risk of financial impact from security incidents.

Risk Management : The company maintains a risk management program to identify, prioritize, and mitigate risk to acceptable levels.

Agile Process : The company's software development process includes frequent team meetings which facilitate the communication and evaluation of objectives between team members. These touch points include Scrum meetings, sprint planning, and sprint retrospective meetings.

Internal Support Channel : Employees have access to an internal support channel that can be used to report incidents, concerns, and complaints.

Asset Management

Workstations - OS : The company monitors the IT infrastructure devices for compliance with the Asset Management Policy and checks for requirements such as hard drive encryption, user authentication requirements, and security patching.

Architecture Diagram : The company has an architecture diagram that shows the physical and logical network topology, including all systems, connections, and security controls.

Inventory : The company maintains an inventory of IT infrastructure devices.

Acceptable Use : The Acceptable Use Policy outlines the acceptable use of computer equipment and systems at the company.

System Inventory : The company maintains an inventory of all information systems, services, and assets, and classifies them based on the data they store. Inventory is reviewed as part of an annual Risk Assessment.

Application Security

Encryption Documentation : The company maintains documented guidance on the selection and configuration of appropriate cryptographic methods.

Static Code Analysis : A static code analysis tool is configured to scan the source code for vulnerabilities.

Source Control : The company uses a version control system to manage source code and documentation, and to implement and run change management functions. The version control software is only accessible by authorized personnel.

Cloud Security

Vulnerability Scanning : Vulnerability scanning tools are utilized to proactively identify CVEs across OS and applications, and issues found are resolved promptly based on severity.

TLS Certificates and Endpoints : TLS usage is evaluated on a quarterly basis using tools such as ssllabs and any grades lower than A are promptly corrected.

Penetration Testing : Third-party vendors are used to perform penetration tests against the production system on an annual basis. Identified Critical and High issues are promptly resolved and the rest are prioritized as appropriate.

Infrastructure as Code : All infrastructure is managed as code and follows the standard code review process including approvals and automated testing.

Firewalls : Firewalls are configured to restrict network traffic to the minimum required for the system to function.

Host Hardening : The company maintains a host hardening policy for VMs and containers that describes the baseline security standard for hosts. The policy is expressed as code and playbooks, and all new hosts are built using it.

Patch Management : OS patches and docker image updates are applied at least weekly.

Data

File Systems Encryption : File systems for databases and other sensitive data storage require at least block level encryption.

Data Retention : Retention periods for customer data are specified in the company's Data Retention Procedure and adhere to compliance, regulatory, contractual, and organizational requirements.

Data Classification : All company and customer data is classified as per the data classification policy.

Data in Transit Encryption : Data in transit over the public Internet is encrypted with industry-standard algorithms.

File Store Encryption : Third-party cloud filestores such as S3 and GCS are configured with a minimum server-side encryption using the vendor's key.

Cryptography

Data Store Encryption : Data stores are configured to enable encryption at rest.

Data Classification

Data Disposal : Customer data is securely disposed of after its retention period passes, and any retained data is sanitized and anonymized.

Third Party Management

Inventory and Classification : The company maintains an inventory of its vendors and classification of the data they store or process.

Vendor Monitoring : Vendors are evaluated on a periodic basis, by reviewing their audit reports or other means, in order to track and determine the impact of any changes in their security posture.

Vendor Risk Assessment : As part of the risk management process, vendors storing data classified as Customer Sensitive undergo due diligence and risk assessment.