1. Introduction

Ardoise maintains the following practices in order to support compliance with applicable data protection and privacy laws, including the General Data Protection Regulation (GDPR). This policy outlines Ardoise's role and responsibilities as a data processor and, where applicable, as an independent controller when handling customer data, the guiding principles followed, and the measures implemented to safeguard personal data.

Ardoise is a European-based company, headquartered in 31, rue de Mogador 75009 Paris France, operating independently and providing advanced AI-powered learning and coaching solutions.

This policy applies to all data processed by Ardoise on behalf of its customers, including but not limited to user profiles, learning content, platform usage data, and associated metadata. The scope covers the entire data lifecycle: collection, storage, processing, sharing, and deletion.

Ardoise commits to the following principles:

- **Lawfulness, fairness, and transparency** – all processing activities are conducted under a clear legal basis, communicated transparently to customers.
- **Purpose limitation** – data is processed solely for the purposes of delivering agreed services.
- **Data minimization** – only the minimum necessary personal data is collected.
- **Accuracy** – ensuring customer data is kept up to date.
- **Storage limitation** – retaining data only for as long as necessary.
- **Integrity and confidentiality** – protecting data with appropriate security measures, both organizational and technical.
- **Accountability** – maintaining records, assessments, and reporting obligations to demonstrate compliance.

This Data Processing Addendum (“DPA”) supplements and forms an integral part of the Agreement between Ardoise and the Customer and applies solely to the extent Ardoise Processes Customer Data on behalf of the Customer in the course of providing the Services. Capitalised terms used herein but not defined shall have the meaning given to them in the Agreement.

This DPA forms part of the Agreement and creates binding data protection obligations between the Parties to the extent Ardoise Processes Customer Personal Data on behalf of the Customer. It operates in accordance with the terms of the Agreement. The Customer's execution of the Agreement shall be deemed to constitute execution of this DPA and, where applicable, of the Standard Contractual Clauses incorporated by reference under Section 10.6.

© 2026 Ardoise. All rights reserved.

2. Definitions

For the purposes of this Policy, the following terms have the meanings set out below:

- **Customer Data**
  Any data, including personal data, provided by the Customer to Ardoise, or generated by the Customer's use of Ardoise's services, that is processed by Ardoise solely on behalf of the Customer. Customer Data remains the property of the Customer at all times.
- **Personal Data**
  Any information relating to an identified or identifiable natural person (the "Data Subject"), including but not limited to names, email addresses, contact details, usage data, and other identifiers as defined by the GDPR and relevant laws.
- **Special Categories of Personal Data**
  Data within Article 9 GDPR: health, genetic, or biometric data; racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; and data concerning sex life or sexual orientation.
- **Sensitive / Restricted Data**
  Other high-risk data requiring heightened protection, including government identifiers (social security, passport, driver's licence), payment card and financial data, account credentials, and children's data.

- **Processing**
  Any operation or set of operations performed on Customer Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, alignment, restriction, erasure, or destruction.
- **Controller vs. Processor**
  - **Controller**: the natural or legal person (the Customer) which determines the purposes and means of processing personal data.
  - **Processor**: Ardoise, which processes personal data on behalf of the Customer, following documented instructions and subject to contractual obligations.
- **Sub-Processor**
  Any third-party service provider engaged by Ardoise to process Customer Data on its behalf, such as hosting providers, storage solutions, or analytics vendors.
  Sub-processors are subject to contractual, technical, and organizational safeguards to ensure compliance with this policy.
- **Data Subject**
  An identified or identifiable natural person whose personal data is processed, such as end users, employees, or learners engaging with the Ardoise platform.
- **Large Language Models (LLMs) and AI Processing**
  In certain services, Customer Data may be processed through AI models, including Large Language Models (LLMs), for the purpose of enabling personalized learning, adaptive coaching, or content generation.

© 2026 Ardoise. All rights reserved.

    - Customer Data is not used to train or fine-tune public LLMs.
    - Data is processed in controlled, isolated environments, ensuring confidentiality and compliance.
    - Ardoise may use anonymized or aggregated data to improve the performance of its systems, but such data cannot be traced back to an individual Data Subject.
- **EU Data Protection Law and AI Regulations**
  Are all data protection and privacy laws applicable in the EEA and Switzerland, including (i) the General Data Protection Regulation (EU) 2016/679 ("GDPR"), (ii) the e-Privacy Directive 2002/58/EC and its national transpositions, (iii) Regulation (EU) 2024/1689 establishing harmonized rules on artificial intelligence ("AI Act"), as well as (iv) any applicable national legislation supplementing or replacing the foregoing.

- **Non-EU Data Protection Laws**
  Refers to all other data protection and privacy laws and regulations applicable to the processing of Personal Data under this DPA, including without limitation: the UK Data Protection Act 2018 and UK GDPR; the Japan Act on the Protection of Personal Information; the California Consumer Privacy Act and California Privacy Rights Act ("CCPA"); the Virginia, Colorado, Utah and Connecticut state privacy laws; Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"); Brazil's Lei Geral de Proteção de Dados ("LGPD"); Australia's Privacy Act 1988 (Cth); the Swiss Federal Act on Data Protection ("FADP"); the Personal Information Protection Law of the People's Republic of China ("PIPL"); and any other analogous privacy legislation in force from time to time.
- **Data Protection Laws**
  Refers to all applicable laws and regulations relating to the processing of Personal Data and privacy that may exist in the relevant jurisdictions, including, where applicable, EU Data Protection Law and Non-EU Data Protection Laws.
- **Standard Contractual Clauses**
  Refers to the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021

3. Roles & Responsibilities

The protection of Customer Data requires clearly defined responsibilities between Ardoise, the Customer, and authorised Sub-Processors. Ardoise operates under a dual-role model, acting as both a Processor and a Controller, depending on the nature of the data and processing activities.

© 2026 Ardoise. All rights reserved.

3.1 Customer (Data Controller)

The Customer is the Data Controller with respect to data it provides to Ardoise for onboarding and service delivery. The Customer is responsible for:

- Determining the purposes and lawful basis for processing Customer-provided data (e.g., onboarding users, assigning roles, managing teams).
- Ensuring that personal data provided to Ardoise is accurate, lawful, and collected in compliance with data protection laws.
- Informing data subjects about the transfer of their Personal Data to Ardoise.
- Responding to Data Subject requests related to Customer-provided data, with Ardoise's assistance where necessary.

Customer shall not provide Ardoise with any *Special Categories of Personal Data* or *Sensitive / Restricted Data* unless explicitly agreed in writing. Ardoise assumes no liability for any such data provided in breach of this prohibition. Ardoise shall promptly notify the Customer if, in its opinion, an instruction infringes Data Protection Law, and may refuse to comply with such instruction without being in breach of this DPA.

3.2 Ardoise (Processor Role)

Ardoise acts as the Processor when handling Customer-provided data, such as user identifiers, team assignments, or organizational role information. In this role, Ardoise is responsible for:

- Processing Customer Data strictly in accordance with the Customer's documented instructions.
- Implementing appropriate technical and organizational measures to protect Customer Data.
- Assisting the Customer in fulfilling obligations related to Data Subject rights, security, and compliance.
- Notifying the Customer without undue delay of any personal data breach involving Customer Data.

3.3 Ardoise (Controller Role)

Ardoise also acts as an independent Controller for data it collects directly from end-users during onboarding and throughout platform use. This includes information provided by users to personalize recommendations, configure preferences, or enhance the learning experience.

In this role, Ardoise is responsible for:

- Determining the purposes and means of processing user-provided data (e.g., tailoring content, generating personalized AI-driven recommendations).
- Providing end-users with a clear Privacy Notice explaining the data collected, its purposes, and their rights.

© 2026 Ardoise. All rights reserved.

- Enabling Data Subjects to exercise their rights directly with Ardoise (access, correction, erasure, objection).
- Ensuring that data collected for personalization is not repurposed for unrelated activities, such as training public LLMs.
- Where aggregated or anonymized data is used to improve Ardoise's platform features, ensuring that no individual can be re-identified.

3.4 Sub-Processors

- Ardoise may engage carefully selected third parties ("Sub-Processors") to support service provision (e.g., cloud hosting, storage, AI infrastructure).
- Sub-Processors are contractually bound to data protection obligations no less protective than those imposed on Ardoise.
- Ardoise maintains a list of authorized Sub-Processors and will notify Customers of any intended additions or replacements, and provide an opportunity to object, in accordance with the notice period and objection procedure set out in Section 6.3.

3.5 Data Protection Officer (DPO)

Ardoise has appointed a Data Protection Officer (DPO) responsible for:

- Monitoring compliance with GDPR and other applicable data protection laws.
- Advising on Data Protection Impact Assessments (DPIAs), particularly where AI and LLMs are involved.
- Acting as a point of contact for Customers, Data Subjects, and supervisory authorities.
- Providing internal guidance and training on data protection obligations.
- The DPO can be reached at: dpo@ardoise.ai

3.6 Responsibility Matrix – Data Protection & Processing

Activity / Obligation	Customer (Controller)	Ardoise (Processor)	Ardoise (Controller – personalization/AI)	Sub-Processors	Ardoise DPO
Defining lawful basis for processing	**A/R**	I	**A/R**	I	C
Providing onboarding user data (roles,	**A/R**	R	I	I	I

© 2026 Ardoise. All rights reserved. Data Processing & Protection Policy – Version 1.3 (Last updated: 01 July 2026)

This document describes Ardoise's Data Processing & Protection practices. It is provided for transparency and customer assurance.
Where referenced in a Data Processing Agreement (DPA) or contract, this Policy shall form part of the binding agreement between Ardoise and the Customer.

teams, identifiers)					
Collecting personalization data directly from users	I	I	**A/R**	I	C
Processing Customer-provided data for service delivery	A	**R**	I	R (under Ardoise)	C
Processing user-provided data for personalization & AI recommendations	I	I	**A/R**	R (if infra/AI tools used)	C
Ensuring data minimization & accuracy	A/R	R	A/R	R (tech scope)	C
Providing privacy notice to users	A	I	**A/R**	I	C
Data Subject Access Requests (DSARs)	**A/R** (for Customer data)	R (assist)	**A/R** (for personalization data)	I	C
Breach detection & notification	A	**R** (for Customer data)	**A/R** (for AI/personalization data)	R (must notify Ardoise)	C
Retention & deletion of data	A	**R** (on instruction)	**A/R** (for AI/personalization data)	R (per contract)	C
Use of anonymized/aggregated data for service improvement	I	I	**A/R**	R (if infra tools used)	C
Appointing Sub-Processors	I	**A/R**	I	R	C
Audit & compliance monitoring	C	**A/R**	R	R (provide reports)	C
Data Protection Impact Assessments (DPIAs)	A (when required for Customer processing)	C	**A/R** (for personalization & AI)	C	C

© 2026 Ardoise. All rights reserved.

This document describes Ardoise's Data Processing & Protection practices. It is provided for transparency and customer assurance.
Where referenced in a Data Processing Agreement (DPA) or contract, this Policy shall form part of the binding agreement between Ardoise and the Customer.

Liaison with Supervisory Authorities	C	C	C	I	**A/R**

Legend

- **R – Responsible**
  The party that performs the activity or task. They are directly in charge of execution.
- **A – Accountable**
  The party that is ultimately answerable for the activity. They ensure the task is completed and delegate responsibilities if needed. Where accountability is split by Ardoise's dual role or by data category, the matrix may show a separate 'A' for each such split.
- **C – Consulted**
  The party that provides input, expertise, or guidance before or during the activity. Communication is two-way.
- **I – Informed**
  The party that must be kept updated on progress or outcomes. Communication is one-way.

4. Data Processing Activities

Ardoise processes Customer Data and user-provided data in order to deliver its learning and coaching services. The scope of data processing depends on whether Ardoise acts as a Processor (on behalf of the Customer) or as a Controller (for personalization and AI-driven functionality).

4.1 Categories of Data Processed

- Customer-Provided Data (Ardoise in Processor role)
  - User identifiers (e.g., name, email, organizational role, team assignment)
  - Access credentials and account configuration
  - Organizational context (team/department structure)
  - Customer-managed preferences and permissions
- User-Provided Data (Ardoise in Controller role)
  - Onboarding information (skills, goals, learning preferences)
  - Responses to self-assessments, surveys, or coaching inputs
  - Personalization data (e.g., preferred communication style, learning format)
  - Usage patterns and interaction history with Ardoise services
- System-Generated Data (Ardoise in hybrid role)

© 2026 Ardoise. All rights reserved.

- Logs, analytics, and metadata related to platform usage
- AI model outputs and recommendation data
- Aggregated and anonymized data for service performance and improvement

4.2 Purposes of Processing

- As Processor (on behalf of Customer):
  - Onboarding and account setup for Customer's users
  - Managing user roles, teams, and organizational hierarchy
  - Delivering learning modules, coaching sessions, and collaboration features
  - Providing support and service maintenance
  - Ensuring system security and fraud prevention
- As Controller (for Ardoise's own legitimate business purposes):
  - Personalizing the user's learning and coaching experience
  - Generating AI-driven recommendations and adaptive pathways
  - Enhancing service quality through usage analytics and aggregated insights
  - Improving the performance of AI models (using anonymized or aggregated data)
  - Complying with Ardoise's own legal and regulatory obligations (e.g., security logging)

4.3 Legal Basis for Processing

- For Processor activities, Ardoise processes Customer Data on the lawful basis or bases determined by the Customer as controller, in accordance with the Customer's documented instructions. The Customer is responsible for ensuring a valid lawful basis for such processing.
- For its own processing as a controller, Ardoise relies on the lawful basis appropriate to each activity: performance of its contract with the user, to deliver the personalized coaching and learning the user has come to receive; its legitimate interests in service optimization, AI-driven personalization and aggregated, anonymized analytics, balanced against users' rights and subject to their right to object; and compliance with legal obligations, such as security and incident logging. Where Ardoise offers optional personalization features beyond core service delivery, personal data for those features is processed only on the basis of the user's freely given, specific and withdrawable consent, and only where such features are enabled for the relevant deployment.

4.4 Data Flows

1. Collection

© 2026 Ardoise. All rights reserved.

- Customer provides user onboarding information.
- Ardoise collects additional user data directly during onboarding or platform use.

2. Storage
    - Data is stored in secure, access-controlled environments, encrypted both at rest and in transit.
3. Processing
    - Customer-provided data is processed strictly according to Customer instructions.
    - User-provided personalization data is processed by Ardoise to tailor services and AI recommendations.
4. Sharing
    - Limited to authorized Sub-Processors (e.g., hosting, storage, AI model infrastructure) under strict contractual obligations.
    - No Customer Data is shared with external parties for independent use.
5. Deletion
    - Customer Data is deleted or returned at the end of the contract, in line with Customer instructions (unless otherwise legally required).
    - User-provided personalization data is retained only as long as necessary for service delivery and deleted upon account closure or user request.

4.5 Data Inventory Table

Data Category	Source	Purpose of Processing	Ardoise Role	Legal Basis	Retention Period
User identifiers (name, email, role, team)	Customer	Onboarding, account creation, role/team assignment	**Processor**	As determined by Customer as Controller; processed under Customer's documented instructions.	For duration of Customer contract; deleted or returned upon termination
Organizational context (team/department info)	Customer	Role-based access, reporting, collaboration features	**Processor**	As determined by Customer as Controller; processed under Customer's documented instructions.	For duration of Customer contract

© 2026 Ardoise. All rights reserved.

Login credentials, account configuration	Customer / User	Authentication, secure access to platform	**Processor**	As determined by Customer as Controller; processed under Customer's documented instructions.	Active account duration; deleted at offboarding
Onboarding details (skills, goals, preferences)	User (direct input)	Personalization of learning/coaching	**Controller**	Contract performance; Consent (optional fields)	Until account closure or user request
Self-assessments, surveys, coaching responses	User (direct input)	Adaptive learning, AI-driven personalization	**Controller**	Contract performance	Until account closure or user request
Usage patterns, activity logs, interaction history	System-generated	Service optimization, fraud prevention, support	**Processor (Customer reporting)** / **Controller (aggregated analytics)**	Controller: legitimate interests (service optimization, fraud prevention, security). Processor: as determined by Customer as Controller, where logs are surfaced to the Customer for reporting.	Logs: up to 12 months; analytics: anonymized/aggregated indefinitely
AI model outputs (recommendations, generated content)	System-generated from Customer/User data	Delivering personalized coaching and recommendations	**Processor (where based on Customer data)** / **Controller (where based on user-provided data)**	Controller: contract performance with the user (outputs from user-provided data). Processor: as determined by Customer as Controller (outputs from Customer-provided data).	Stored temporarily for delivery; anonymized outputs may be retained for service optimization

© 2026 Ardoise. All rights reserved.

This document describes Ardoise's Data Processing & Protection practices. It is provided for transparency and customer assurance.
Where referenced in a Data Processing Agreement (DPA) or contract, this Policy shall form part of the binding agreement between Ardoise and the Customer.

Aggregated / anonymized data	Derived from all sources	Service improvement, AI model refinement, usage analytics	**Controller**	Legitimate interests	Retained as long as data remains anonymized (non-identifiable)
Security and technical logs	System-generated	Security monitoring, incident detection, regulatory compliance	**Processor** (for Customer ops) / **Controller** (for Ardoise's own compliance)	Controller: legitimate interests (network and information security, Recital 49 GDPR), and legal obligation where retention or reporting is required by law. Processor: as determined by Customer as Controller for Customer-directed operational logging.	Retained up to 12 months

5. Data Protection Principles in Practice

Ardoise is committed to applying the core principles of data protection in all of its processing activities. These principles, derived from GDPR and other international standards, guide how Customer Data and user-provided information are handled throughout their lifecycle.

5.1 Lawfulness, Fairness, and Transparency

- All data processing is conducted on a valid legal basis (contract, consent, or legitimate interests).
- Privacy notices are provided to both Customers and end-users, clearly explaining what data is collected, why, and how it is used.
- No hidden or unauthorized uses of data are permitted.

© 2026 Ardoise. All rights reserved.

5.2 Purpose Limitation

- Customer Data is processed solely for the purposes defined in the Customer contract.
- User-provided data (e.g., personalization inputs) is used exclusively for tailoring recommendations and enhancing the learning experience.
- Data is never repurposed for unrelated activities (e.g., no sale of data, no training of external/public LLMs).

5.3 Data Minimization

- Only the data strictly necessary to provide services is collected.
- Personalization data collected directly from users is optional and limited in scope.
- Data intake workflows enforce minimisation by design, and regular reviews are conducted to ensure that unnecessary or outdated data is not retained.

5.4 Accuracy

- Customers are responsible for ensuring that the user information they provide (e.g., team assignments, roles) is accurate, up to date, and collected lawfully.
- Ardoise provides mechanisms for users to update user-provided personal details and preferences directly within the platform.
- Corrections are applied promptly across all systems where the data is stored.

5.5 Storage Limitation

- Data is retained only for as long as necessary to fulfill contractual or service delivery purposes.
- At contract termination, Customer Data is securely deleted or returned in accordance with Customer instructions.
- User-provided personalization data is deleted when accounts are closed or upon user request.
- Aggregated or anonymized data may be retained indefinitely, as it does not identify individuals.

5.6 Integrity and Confidentiality (Security)

- All personal data is encrypted at rest and in transit (AES-256, TLS 1.2+).
- Access is restricted using role-based access control (RBAC) and multi-factor authentication (MFA).
- Security measures include firewalls, intrusion detection/prevention systems, DDoS protection, and continuous monitoring.

© 2026 Ardoise. All rights reserved.

- Ardoise performs regular penetration testing, vulnerability scanning, and supplier/service reviews.
- Sub-Processors are contractually required to meet equivalent security standards.

5.7 Accountability

- Ardoise maintains detailed records of processing activities, including AI-related processing, in compliance with GDPR Article 30.
- Regular internal audits and external reviews are performed to assess compliance.
- Staff receive regular training on data protection, security, and responsible AI use.
- The Data Protection Officer oversees compliance and provides guidance on new or high-risk processing activities.

5.8 Responsible Use of AI and LLMs

- Ardoise sends limited Customer Personal Data to the AI Sub-Processors listed in Section 6.1 solely for inference, and only where the relevant AI feature is enabled for the Customer. Such data is not used by Ardoise or its AI Sub-Processors to train public foundation models, except where expressly agreed in writing.
- Customer Data is not shared with or exposed to external/public LLM providers without explicit Customer agreement.
- AI personalization uses only the data necessary for the specific coaching or learning task.
- Ardoise applies safeguards (e.g., anonymization, filtering) to prevent unintended retention or disclosure of personal data in AI workflows.
- Ardoise maintains a documented assessment of its AI-enabled features under Regulation (EU) 2024/1689. Its coaching and personalization functions are designed to assist and support human-led learning, rather than to replace human judgment, and do not on their own produce legal or similarly significant effects on natural persons. Ardoise monitors the classification of education- and vocational-training systems under Annex III, and where its features fall within that Annex it will implement any applicable high-risk obligations within the Regulation's timelines.
- Where end-users interact directly with Ardoise's AI-driven coaching or conversational features, they are clearly informed they are interacting with an AI system, and AI-generated content is identified as such, in accordance with Article 50 of Regulation (EU) 2024/1689 within the applicable timelines.
- Ardoise's AI Act classification depends on the configured use case. Customers shall not use the Services for admission, grading, employment or promotion decisions, or other legally or similarly significant assessment of individuals, unless expressly agreed and separately assessed in writing.

© 2026 Ardoise. All rights reserved.

6. Sub-Processors

Ardoise relies on carefully selected third-party service providers (“Sub-Processors”) to deliver its services. These Sub-Processors process Customer Data only as necessary to support Ardoise’s platform and are contractually bound to implement appropriate technical and organizational measures for data protection in accordance with Article 28(4) GDPR.

Ardoise maintains oversight of all Sub-Processors and ensures that they provide guarantees consistent with applicable data protection regulations (including GDPR). Customers will be notified of any intended changes to the list of Sub-Processors and may object where permitted by contract.

6.1 Current Sub-Processors

Sub-Processor	Service Provided	Location / Data Centers	Data Categories Processed
Azure OpenAI (Microsoft)	AI model inference (enterprise LLM deployment)	EU (France)	User-provided personalization data (inputs for AI responses); pseudonymized context
Amazon Web Services (AWS)	Primary hosting and storage infrastructure	EU (Paris, Frankfurt, Ireland)	Customer Data, user identifiers, content, usage logs
Cloudflare	CDN, DDoS protection, edge security	Global (with EU data residency options)	Network metadata, usage logs
OpenAI	AI model inference for coaching/personalization	US (with EU SCCs)	User-provided personalization data (inputs for AI responses); pseudonymized context
Google Gemini	AI model inference for coaching/personalization	US/EU (with SCCs)	User-provided personalization data (inputs for AI responses); pseudonymized context

© 2026 Ardoise. All rights reserved.

Anthropic Claude	AI model inference for coaching/personalization	US (with SCCs)	User-provided personalization data (inputs for AI responses); pseudonymized context
SCORM Cloud (Rustici Software)	eLearning content delivery & SCORM compliance	US (with SCCs)	Learning content, course completion data, usage logs
Brevo (formerly Sendinblue)	Transactional and marketing email services	EU (France / Germany)	User identifiers (email), notification content, communication preferences
OVH	Hosting and Storage Infrastructure	EU (Paris, Bordeaux)	Customer Data, user identifiers, content, usage logs

6.2 Sub-Processor Safeguards

- All Sub-Processors are subject to Data Processing Agreements (DPAs) with Ardoise that require GDPR-level protection as well as compliance with the applicable obligations under Regulation (EU) 2024/1689 establishing harmonized rules on artificial intelligence (the “AI Act”), where the processing or services provided fall within its scope.
- For transfers outside the EU/EEA, Standard Contractual Clauses (SCCs) or other recognized safeguards are in place.
- Ardoise conducts due diligence prior to onboarding Sub-Processors and monitors compliance regularly.

6.3 Customer Rights

- Customers may request the most up-to-date list of Sub-Processors at any time.
- Customers will receive at least 30 days’ prior written notice of any intended Sub-Processor changes and may object in writing within that window if they have reasonable data protection concerns in accordance with GDPR Article 28(2).
- Where permitted by contract, Customers may object to the engagement of a new Sub-Processor if they have legitimate concerns regarding data protection.

Where Customer has authorised the engagement of Sub-Processors pursuant to the Agreement, such authorisation shall apply to the Sub-Processors listed in section 6.1.

© 2026 Ardoise. All rights reserved. Data Processing & Protection Policy – Version 1.3 (Last updated: 01 July 2026)

This document describes Ardoise’s Data Processing & Protection practices. It is provided for transparency and customer assurance.
Where referenced in a Data Processing Agreement (DPA) or contract, this Policy shall form part of the binding agreement between Ardoise and the Customer.

7. Security Measures

Ardoise applies a combination of organizational, technical, and physical measures to protect Customer Data and user-provided information against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. These measures are designed in accordance with industry best practices, GDPR Article 32, and cloud security standards (e.g., ISO 27001, SOC 2).

7.1 Organizational Measures

- Policies and Governance – Ardoise maintains internal security and privacy policies reviewed at least annually.
- Confidentiality Agreements – All employees, contractors, and service providers handling Customer Data are bound by confidentiality obligations.
- Access Control – Role-based access control (RBAC) ensures that employees only access data necessary for their role. Privileged access is strictly limited and reviewed regularly.
- Training and Awareness – Regular training for staff on data protection, secure development, AI ethics, cyber-security, and incident response.
- Background Checks – Conducted in accordance with local laws for personnel with access to production systems.

7.2 Technical Measures

- Encryption in Transit and at Rest – TLS 1.2+ for data in transit; AES-256 or equivalent for stored data.
- Key Management – Cryptographic keys are managed securely with rotation policies.
- Authentication & MFA – Multi-Factor Authentication (MFA) is required for administrative access.
- Network Security – Use of firewalls, intrusion detection/prevention systems (IDS/IPS), DDoS protection (via Cloudflare).
- Monitoring & Logging – Continuous monitoring of infrastructure; logs retained for security analysis and compliance for incident forensics.
- Vulnerability Management – Regular patching, security scans, and penetration testing.
- Data Segregation – Logical separation of Customer Data to prevent unauthorized cross-access.

© 2026 Ardoise. All rights reserved.

7.3 Physical Measures

- Data Center Security – Hosting is provided via AWS, Azure and OVH, which implement ISO 27001, SOC 1/2/3, and other recognized security certifications.
- Restricted Access Controls – Physical access to data centers is restricted, logged, and monitored.
- Redundancy – Infrastructure is designed with redundancy and failover to ensure availability.
- Disaster Recovery – Data backups are encrypted and stored in geographically redundant locations. These locations include AWS (Paris/Frankfurt/Ireland), Microsoft Azure (Netherlands/France), or OVHcloud (France and Germany datacentres).

7.4 AI and LLM-Specific Safeguards

- Controlled AI Environments – All interactions with LLMs (OpenAI, Claude, Gemini, Azure OpenAI) are routed through secure, contractually-governed APIs.
- No Training on Customer Data – Customer Data is never used to train public LLMs. Data sent to LLMs is for inference only.
- Data Minimization for AI – Only the minimum necessary input is shared with AI models to generate outputs.
- Pseudonymization & Minimization – Inputs are minimized to the data necessary for the task, and direct identifiers are removed or reduced where not required to deliver the requested output.
- Isolation – Input/output prompts are processed in **logically separated tenant environments**, and testing and production environments remain segregated.

7.5 Business Continuity and Resilience

- Backup & Recovery – Daily backups, encrypted and tested regularly for restoration in geographically redundant regions.
- High Availability – Services deployed in multi-zone cloud architecture to ensure resilience.
- Incident Response – Documented incident response plan including detection, escalation, notification, and remediation.

8. Data Subject Rights

Ardoise is committed to supporting the rights of individuals (“Data Subjects”) as required under the General Data Protection Regulation (GDPR) and other applicable privacy laws. These rights apply to both Customer Data (where Ardoise acts as a Processor) and user-provided data (where Ardoise acts as a Controller).

© 2026 Ardoise. All rights reserved.

8.1 Rights of Data Subjects

Data Subjects may exercise the following rights with respect to their personal data:

- Right of Access – to obtain confirmation as to whether personal data is being processed, and access to that data.
- Right to Rectification – to have inaccurate or incomplete personal data corrected.
- Right to Erasure (“Right to be Forgotten”) – to request deletion of personal data, subject to contractual or legal obligations.
- Right to Restrict Processing – to request limitation of processing under certain conditions.
- Right to Data Portability – to receive personal data in a structured, commonly used, and machine-readable format, and to transmit it to another controller.
- Right to Object – to object to processing based on legitimate interests, or to direct marketing activities.
- Right to Withdraw Consent – to withdraw previously given consent at any time, without affecting the lawfulness of prior processing.
- Rights related to Automated Decision-Making and Profiling – to request human intervention or contest automated decisions where applicable.

8.2 Responsibilities by Role

For Customer-Provided Data (Processor role):

- The Customer, as Controller, is responsible for handling Data Subject Rights requests.
- Ardoise will provide reasonable assistance to the Customer, in line with GDPR Article 28(3)(e), in fulfilling such requests, in accordance with contractual obligations.
- Examples: Access to employee records, correction of role/team assignments, deletion of Customer-managed accounts.

For User-Provided Data (Controller role):

- Ardoise is responsible for responding directly to Data Subject Rights requests related to personalization data, self-assessments, and other information collected directly from users.
- End-users may submit requests directly to Ardoise via the contact information provided in the Privacy Notice.
- Examples: Deletion of personalization preferences, correction of onboarding details, objection to use of data for AI recommendations.

© 2026 Ardoise. All rights reserved. Data Processing & Protection Policy – Version 1.3 (Last updated: 01 July 2026)

This document describes Ardoise’s Data Processing & Protection practices. It is provided for transparency and customer assurance.
Where referenced in a Data Processing Agreement (DPA) or contract, this Policy shall form part of the binding agreement between Ardoise and the Customer.

8.3 Process for Exercising Rights

- Requests can be submitted by Data Subjects either to the Customer (for Customer Data) or directly to Ardoise (for Ardoise-collected personalization data).
- Requests will be verified to confirm the identity of the requester before action is taken.
- Ardoise will respond to all valid requests within one month, extendable by two further months where necessary due to complexity or volume, in accordance with GDPR Article 12.
- Where Ardoise is a Processor, it will promptly forward any requests received directly from Data Subjects to the relevant Customer.
- All requests are logged by Ardoise for audit and accountability purposes. Where technically feasible, Ardoise provides tools or APIs to enable Customers to carry out DSAR actions directly.

8.4 Limitations

- Some rights may be restricted under applicable laws or contractual obligations (e.g., retention obligations, security requirements).
- Requests that cannot be fulfilled due to such limitations will be communicated to the Data Subject along with the justification.
- Ardoise reserves the right to charge a reasonable fee or refuse requests that are manifestly unfounded, excessive, or repetitive in accordance with Article 12(5) GDPR.

9. Incident & Breach Management

Ardoise maintains a structured Incident & Breach Management Framework to promptly detect, investigate, and respond to security incidents and data breaches that may impact Customer Data or user-provided data. This framework ensures compliance with applicable regulations, including GDPR Articles 33 and 34, and provides Customers with timely and transparent communication.

9.1 Definitions

- Security Incident – any event that may compromise the confidentiality, integrity, or availability of data or systems (e.g., attempted unauthorized access, malware detection, service disruption).

© 2026 Ardoise. All rights reserved.

- Unsuccessful Security Incident – events such as pings, port scans, failed logins, or similar attempts that do not compromise data. Ardoise shall have no obligation to notify Customers of Unsuccessful Security Incidents.
- Personal Data Breach – an incident that results in, or that Ardoise reasonably suspects has resulted in, the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

9.2 Detection and Monitoring

- Continuous monitoring of infrastructure, applications, and AI pipelines to detect anomalies.
- Use of automated alerts, intrusion detection/prevention systems, and log analysis.
- Regular penetration testing and vulnerability scanning to identify weaknesses.

9.3 Incident Response Process

Ardoise follows a documented Incident Response Plan (IRP) structured around the following phases:

1. Identification – Detect and validate the incident through monitoring, user reports, or Sub-Processor notifications.
2. Containment – Apply immediate technical and organizational measures to prevent further impact.
3. Investigation – Assess the scope, root cause, and potential impact on Customer Data or user-provided data.
4. Eradication & Recovery – Remove threats, restore services, and validate system integrity.
5. Post-Incident Review – Document findings, lessons learned, and implement preventive measures.

9.4 Notification Obligations

To Customers:

- Ardoise will notify the affected Customer(s) of a personal data breach without undue delay and, where feasible, within 48 hours of becoming aware of the breach, in accordance with Article 33(1);(2) GDPR.
- In accordance with Article 33(3) GDPR, notifications will include:
    - A description of the nature of the breach (type of data, number of data subjects affected).
    - Likely consequences of the breach.
    - Measures taken or proposed to address and mitigate the breach.

© 2026 Ardoise. All rights reserved.

    - Recommended actions for the Customer.

Notification will be made via secure email or other agreed point of contact as specified in the relevant Agreement, and Ardoise will provide reasonable cooperation and assistance to help the Customer investigate and remediate the breach.

With respect to Customer Data processed by Ardoise as Processor, the Customer remains responsible for determining whether notification to the competent supervisory authority and to the data subjects is necessary, and for carrying out such notifications, with Ardoise providing operational and technical support at the Customer's request. Where Ardoise acts as an independent Controller, Ardoise remains responsible for any notifications required of it under GDPR Articles 33 and 34

To Supervisory Authorities:

- Where Ardoise acts as a Controller (for personalization/AI data), it will notify the relevant data protection authority within 72 hours, unless the breach is unlikely to result in risk to individuals.

To Data Subjects:

- Where required under GDPR Article 34, Ardoise will notify affected individuals directly if the breach is likely to result in a high risk to their rights and freedoms.

Ardoise maintains internal records of all security incidents and personal data breaches, in accordance with Article 33(5) GDPR.

9.5 Roles and Responsibilities

- Ardoise Security Team – leads incident detection, response, and containment.
- Data Protection Officer (DPO) – evaluates regulatory reporting obligations, coordinates notifications, and liaises with authorities.
- Customer – responsible for notifying its own Data Subjects if acting as Controller, with Ardoise's assistance where relevant.
- Sub-Processors – contractually required to notify Ardoise promptly of any security incidents affecting Customer Data.

9.6 Testing and Continuous Improvement

- The Incident Response Plan is tested at least annually through tabletop exercises or simulated breaches.
- Outcomes are reviewed and integrated into security improvements.
- Lessons learned are shared internally to strengthen organizational readiness.

© 2026 Ardoise. All rights reserved.

10. International Data Transfers

Ardoise primarily processes and stores Customer Data and user-provided data within the European Union (EU)/European Economic Area (EEA) whenever possible. However, certain processing activities may involve transfers of data outside the EU/EEA, particularly where Sub-Processors are located or operate global infrastructures.

Ardoise ensures that all international data transfers comply with GDPR and other applicable data protection laws by implementing appropriate safeguards.

10.1 Data Hosting within the EU

- Core hosting and storage are provided through Amazon Web Services (AWS) and Microsoft Azure with EU data center locations (e.g., Frankfurt, Ireland, Paris).
- Transactional communications through Brevo are processed within the EU (France/Germany).
- Wherever possible, Ardoise configures its services to retain data within the EU/EEA.

10.2 Transfers Outside the EU/EEA

Some Sub-Processors may process data outside the EU/EEA (e.g., United States-based providers). Examples include:

- Cloudflare – operates a global CDN and security infrastructure, with some processing potentially occurring outside the EU.
- OpenAI, Gemini (Google), Anthropic Claude – provide AI inference services for personalization and coaching.
- SCORM Cloud (Rustici Software, US) – provides eLearning content delivery and SCORM compliance services.

10.3 Safeguards for International Transfers

To protect Customer Data when transferred outside the EU/EEA, Ardoise applies one or more of the following safeguards:

- Standard Contractual Clauses (SCCs) – incorporated into contracts with Sub-Processors located outside the EU/EEA.
- Data Processing Agreements (DPAs) – ensuring Sub-Processors provide GDPR-equivalent protections.
- Technical Measures – such as encryption in transit and at rest, ensuring that data is protected during transfer.

© 2026 Ardoise. All rights reserved.

- Data Minimization – sharing only the minimal data required for the processing activity.
- Pseudonymization/Minimization – inputs to AI models are reduced to task-necessary data; direct identifiers are removed where not required.
- Transfer Impact Assessments (TIAs) – conducted for non-EU/EEA providers, as required by Schrems II and supervisory guidance.

10.4 Customer Transparency

- Customers are provided with an up-to-date list of Sub-Processors, including their geographic locations, in Section 6 (Sub-Processors).
- Any future changes involving international transfers will be notified to Customers in advance, allowing them to raise objections where contractually permitted.

10.5 Compliance with Local Laws

Ardoise monitors developments in international data transfer regulations (e.g., the EU-US Data Privacy Framework) and will adapt its practices as necessary to maintain compliance.

10.6 Transfer Mechanism

Where a transfer of Personal Data under this DPA is a restricted transfer requiring Standard Contractual Clauses, the Parties agree:

1. The EU SCCs (Implementing Decision (EU) 2021/914) are incorporated by reference Module Two (Controller-to-Processor) where Customer is a controller, and Module Three (Processor-to-Processor) where Customer acts on behalf of a third-party controller.
2. For each Module: the docking clause (Clause 7) applies; Clause 9 Option 2 (general authorisation) applies with the notice period in Section 6.3; the optional independent dispute-resolution language in Clause 11 does not apply; Clause 17 is governed by the law of France; Clause 18(b) disputes are heard by the courts of France.

3. Annexes I, II and III of the SCCs are populated, respectively, by the data inventory in Section 4.5 and the sub-processor list in Section 6.1 (Annex I), the security measures in Section 7 (Annex II), and Section 6.1 (Annex III).

4. The competent supervisory authority (Clause 13) is that of the data exporter's Member State, or the French CNIL where the exporter is not established in the EEA.

5. UK transfers are governed by the UK International Data Transfer Addendum (v.B1.0), completed using the entries above.

© 2026 Ardoise. All rights reserved.

6. Swiss transfers apply the SCCs with FADP amendments (competent authority: the Swiss FDPIC; GDPR references read as FADP references).

© 2026 Ardoise. All rights reserved.

11. Compliance & Audit

Ardoise is committed to ensuring accountability, transparency, and continuous improvement in its data protection and security practices. Compliance is maintained through internal governance, regular external reviews, and alignment with international standards.

11.1 Regulatory Compliance

- Ardoise complies with the General Data Protection Regulation (GDPR) and other applicable data protection laws in the jurisdictions where it operates.
- International data transfers are managed in accordance with GDPR Chapter V (see Section 10).
- Ardoise actively monitors emerging privacy and security regulations (e.g., EU–US Data Privacy Framework, UK GDPR, CCPA) and adapts practices to maintain compliance.

11.2 Independent Security Audits

- Ardoise undergoes independent third-party security audits at least annually, which include penetration testing, vulnerability assessments, and reviews of organizational security controls.
- These external assessments are performed by certified security firms with no operational ties to Ardoise, ensuring unbiased evaluation.
- Audit reports and executive summaries can be shared with Customers upon request and subject to non-disclosure agreements (NDAs).

11.3 Certifications & Roadmap

- Ardoise aligns its security practices with leading international standards, including ISO 27001 and SOC 2 Type II.
- Certification processes are actively underway, with a roadmap to achieve the relevant certifications required by enterprise customers.
- Customers will be informed as certifications are obtained.

© 2026 Ardoise. All rights reserved.

11.4 Customer Audit Rights

- Subject always to the limitations set out in the Agreement, and to the extent required under Data Protection Law, Customers may request audits or inspections of Ardoise's processing activities no more than once in any twelve (12)-month period, and only upon at least thirty (30) days' prior written notice, unless a Personal Data Breach, regulator inquiry, or other reasonable grounds require more frequent audits in accordance with GDPR Article 28(h).
- To minimize operational disruption, Ardoise may provide recent third-party audit reports, certifications, or summaries as an alternative to on-site inspections.
- Where on-site audits are required, they will be coordinated to ensure security and confidentiality.

12. Retention & Deletion

Ardoise applies strict retention and deletion policies to ensure that Customer Data and user-provided data are kept only for as long as necessary to fulfill contractual obligations, provide services, or comply with legal requirements. Data that is no longer required is securely deleted or anonymized in accordance with industry best practices.

12.1 General Retention Principles

- Customer-provided data (Processor role): Retained only for the duration of the Customer's contract and deleted or returned upon termination, unless otherwise required by law.
- User-provided data (Controller role): Retained only for as long as the user account remains active or until the Data Subject requests deletion.
- System-generated data (logs, analytics): Retained for limited periods necessary for security, performance monitoring, and troubleshooting.
- Anonymized or aggregated data: May be retained indefinitely, as it does not identify individual Data Subjects.

12.2 Retention Periods by Data Category

Data Category	Role	Retention Period	Deletion Method

© 2026 Ardoise. All rights reserved.

Customer-provided onboarding data (user identifiers, roles, teams)	Processor	Duration of contract	Secure deletion or return to Customer
Organizational context (team/department info)	Processor	Duration of contract	Secure deletion or return to Customer
Login credentials & authentication data	Processor	Active account lifetime	Secure deletion upon account closure
User-provided personalization data (preferences, goals, self-assessments)	Controller	Active account lifetime or until user request	Secure deletion upon account closure or request
Usage logs, activity history	Hybrid (Processor for Customer reporting / Controller for service optimization)	Typically **6–12 months**	Automated log purging; anonymization for analytics
Security & technical logs	Hybrid	**6–12 months** (longer if required by law/regulation)	Secure deletion or rotation
AI model outputs (recommendations, adaptive pathways)	Hybrid	Retained only as long as necessary for delivery	Ephemeral storage; anonymization if used for improvement
Aggregated / anonymized analytics	Controller	Indefinitely (non-identifiable)	Data permanently anonymized

12.3 Secure Deletion Protocols

- Automated Processes: Regular scheduled tasks enforce retention limits and purge expired records.
- Deletion Upon Request: Both Customers and end-users can request deletion in accordance with their rights (see Section 8).
- Contract Termination: At the end of a Customer contract, Ardoise will, at the Customer's choice, either:
    - Return Customer Data in a commonly used, machine-readable format, or

© 2026 Ardoise. All rights reserved.

- Permanently delete Customer Data from all systems including from backups within the standard backup lifecycle (not exceeding 12 months).
- Verification: Deletion processes are logged and subject to audit.

12.4 Exceptions

- Where retention is required by law (e.g., tax, regulatory, or security obligations), Ardoise may retain limited data for the statutory period.
- Data may also be retained temporarily for dispute resolution or enforcement of contractual rights.

13. Updates & Amendments

Ardoise may update or amend this Data Processing & Protection Policy from time to time in order to:

- Reflect changes in applicable laws, regulations, or industry standards.
- Incorporate new or updated services, features, or Sub-Processors.
- Improve clarity and transparency of our practices.

13.1 Notification of Changes

- Material changes (e.g., new Sub-Processors, changes to processing purposes, international transfer practices) will be communicated to Customers in advance through the agreed notification channels (e.g., email, customer portal).
- Minor or editorial changes (e.g., clarifications, formatting, legal references) may be made without prior notice but will always be reflected in the version history of this Policy.
- Sub-Processor changes will be managed in accordance with the notification and objection procedures set out in *Section 6*.

13.2 Customer Rights

- Where required by contract or regulation, Customers will have the right to review and, where appropriate, object to material changes.
- Continued use of Ardoise services following notification of updates will constitute acceptance of the revised terms, unless otherwise agreed.

© 2026 Ardoise. All rights reserved.

13.3 Version Control

- This Policy is version-controlled. Each published version will include a revision date and timestamp.
- Historical versions will be retained and can be made available to Customers upon request.

© 2026 Ardoise. All rights reserved.

14. Contact

Ardoise has appointed a Data Protection Officer (DPO) and maintains dedicated contact channels for privacy, security, and compliance inquiries.

14.1 Data Protection Officer (DPO)

For questions regarding this Policy, data protection, or to exercise Data Subject rights (see Section 8), you may contact our DPO:

Email: dpo@ardoise.ai
Postal address:
Ardoise – Data Protection Officer
31, rue de Mogador
75009 Paris
France

(Please do not include sensitive personal information in your initial request; identity verification steps will follow.)

14.2 Security Incidents & Vulnerabilities

To report a potential security vulnerability or incident, please use:

Email: security@ardoise.ai

Reports will be reviewed promptly by Ardoise's Security Team. Please send only a high-level description of the issue in the initial contact — do not transmit exploit code or credentials. A secure communication channel will be provided if required.

14.3 General Inquiries

For all other questions about Ardoise services and policies:

Email: info@ardoise.ai
Website: www.ardoise.ai

© 2026 Ardoise. All rights reserved.

15. Liability

Except to the extent that Data Protection Law expressly requires otherwise, each Party's liability arising out of or in connection with this DPA (including the Standard Contractual Clauses, where applicable) shall be subject to the exclusions and limitations of liability set forth in the Agreement, and such limitations shall apply in the aggregate to all claims arising under or in connection with this DPA.

16. Order of Precedence

In the event of any conflict or inconsistency between this DPA and the Agreement, the following order of precedence shall apply (in descending order):
(a) the Standard Contractual Clauses (where applicable),
(b) this DPA, in respect of data protection matters; and
(c) the Agreement, in respect of all other matters.

To the extent this DPA is incorporated into the Agreement, it shall supersede any prior data processing terms between the Parties concerning the same subject matter. In case of ambiguity, the English language version of this DPA shall prevail.

17. Jurisdiction Specific Terms

17.1 Application of Terms

To the extent Ardoise processes Customer Data originating from and protected by Data Protection Laws in one of the specific jurisdictions listed in this Section 17, the terms specified in this Section ("Jurisdiction-Specific Terms") shall apply in addition to the terms of this DPA. In the event of any conflict or ambiguity between the Jurisdiction-Specific Terms and the rest of this DPA, the Jurisdiction-Specific Terms will prevail, but only to the extent they apply to Ardoise's processing of such Customer Data.

17.2 California (United States)

- For the purposes of this DPA, "Data Controller" shall include "Business," "Data Processor" shall include "Service Provider," and "Personal Data" shall include "Personal Information" as defined under the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA/CPRA").
- Ardoise shall not Sell or Share Customer Personal Data and shall process such data solely to perform the Services for Customer as a Service Provider under the CCPA/CPRA.

© 2026 Ardoise. All rights reserved.

- Ardoise shall not retain, use, or disclose Customer Personal Data outside the direct business relationship, except as necessary to perform the Services or comply with law.
- Ardoise may Deidentify Customer Personal Data for internal use, provided it does not attempt to re-identify such information.
- Ardoise shall ensure its Sub-Processors qualify as Service Providers under the CCPA/CPRA, and shall notify Customer if it can no longer comply with the CCPA/CPRA.

17.3 People's Republic of China (PIPL)

- "Personal Data" means "personal information" under the Personal Information Protection Law ("PIPL"). "Data Controller" means a "personal information processor," and "Data Processor" means an "entrusted party."
- Each Sub-Processor authorised in Section 6 is agreed as a "sub-entrusted party."
- Customer shall obtain any required approvals, permissions, or filings from Chinese authorities necessary for the cross-border processing of Personal Data under this DPA.
- Where Ardoise or its Sub-Processors outside China process Personal Data, such processing shall constitute a cross-border transfer under the PIPL and the Parties shall implement any required procedural or contractual measures (including signing the Chinese Standard Contract, where required).

17.4 Japan (Act on the Protection of Personal Information – APPI)

- Where Ardoise processes Personal Data originating from Japan that is subject to the Act on the Protection of Personal Information ("APPI"), Ardoise shall comply with the provisions of the APPI, including the handling of Personal Data in accordance with Customer's instructions, safeguarding Personal Data through appropriate technical and organisational measures, and supporting the exercise of data subject rights under the APPI.
- Cross-Border Transfers – Where Ardoise transfers Personal Data from Japan to a country outside of Japan, Ardoise shall ensure appropriate safeguards are implemented in accordance with the APPI, including the execution of contractual measures to ensure foreign third parties maintain an equivalent level of protection, and shall disclose information regarding the foreign country's data protection regime and the data handling practices of the receiving entity upon request by the Customer or the Data Subject.
- Joint-Use (Shared-Use) – Ardoise shall not engage in "joint use" (shared use) of Personal Data with any third party within the meaning of Article 23(4) APPI, unless agreed in writing with the Customer in advance and subject to the Customer providing the necessary public notice required under APPI.

© 2026 Ardoise. All rights reserved.