# Global Privacy Policy (websites & accounts)

*Last updated: 2025-12-08*

**Important – French version prevails.**
This English version is provided for convenience. In case of any discrepancy or conflict between this version and the French version of this Privacy Policy ("Politique de confidentialité globale"), the **French version shall prevail** and be the only legally binding version.

This Global Privacy Policy ("**Policy**") explains how INAI ("**inAi**", "**we**", "us", "our") processes personal data in connection with its public websites and certain generic accounts and corporate relationships.

This Policy is intended to comply with Regulation (EU) 2016/679 ("**GDPR**"), the French "Informatique et Libertés" Law, and applicable e-privacy rules on cookies and similar technologies.

---

## 1. Scope, purpose and hierarchy

### 1.1 Scope of this Policy

This Policy applies when inAi acts as **controller** for the following situations:

- visitors of our public websites:
    - `https://www.inai.fr`
    - `https://www.inai.world`
    - `https://www.pagemind.fr`
    - `https://www.emplo.fr`
- individuals who:
    - submit **contact, demo, pilot or partnership requests**,
    - subscribe to **newsletters** or similar communications,
- holders of **generic inAi accounts** not governed by a product-specific privacy policy (for example, a cross-product portal or legal hub account, if such services are offered),
- **business contacts** (prospects, partners, suppliers, investors, incubators, public bodies),
- **job applicants** applying for roles at inAi.

## 1.2 What is not covered here

This Policy does **not** replace product-specific privacy policies and data-processing agreements. In particular:

- **PageMind** customer data (such as supplier files, catalog documents, configuration and outputs) is primarily processed by inAi as **processor** on behalf of PageMind customers (retailers, brands, marketplaces) and is governed by:
    - the **PageMind-specific Privacy Policy**, and
    - the relevant **Data Processing Agreement (DPA)** and product Terms of Service.
- **Emplo** candidate data (including CVs, job preferences, applications and connected accounts) is governed by the **Emplo Privacy Policy**.
- Any employer-side data processed through Emplo in a B2B configuration is governed by the relevant product-specific and contractual documents.

When you use PageMind or Emplo, you must refer to the **specific privacy policy and terms** for that service. In case of inconsistency between this Policy and a product-specific privacy policy, the **product-specific privacy policy prevails** for the corresponding service.

## 1.3 Relationship with other legal documents

This Policy forms part of inAi's broader legal stack, which also includes:

- the **Legal Notice / Mentions légales**,
- the **Website Terms of Use** (for access to the public sites),
- the **Cookie & Tracking Technologies Policy** (the "Cookie Policy"),
- the **Security & Data Protection Overview (Trust)**,
- product-specific **Terms of Service**, **DPAs**, **MSAs** and other agreements.

For the matters they each cover, and subject to mandatory law, the following hierarchy applies:

1. Any individually negotiated contract (MSA, pilot agreement, order form),
2. Product-specific Terms of Service and DPA,
3. Product-specific privacy policies (PageMind, Emplo),
4. This **Global Privacy Policy** (websites & generic accounts),
5. Cookie Policy and Security & Data Protection Overview (informational, non-contractual),
6. FAQ and other purely informational content.

### 1.4 Non-contractual nature of this Policy

This Policy is provided to comply with GDPR transparency obligations (Articles 12–14) and relevant CNIL guidance. It **does not create contractual rights or obligations** beyond those already provided by:

- applicable laws and regulations, and
- the contracts and terms that apply to your relationship with inAi.

In particular, detailed commitments regarding service levels, security, data location and liability are set out in the applicable Product Terms, DPA and/or MSA, and **not** in this Policy.

---

## 2. Identity of the controller and contact details

### 2.1 Controller

Unless expressly stated otherwise in a product-specific document, the controller for the processing covered by this Policy is:

> **INAI**
> Société par actions simplifiée à associé unique (SASU)
> Share capital: **1 000 €**
> Registered with **RCS Lille Métropole** under number **987 977 386**
> Registered office: **142 rue d'Iéna, apt. 21, 59000 Lille, France**
> Official domains: `inai.fr`, `inai.world`, and associated product domains including `pagemind.fr` and `emplo.fr`.

### 2.2 Contact details

For general questions about this Policy or data protection at inAi:

- Email: `contact@inai.fr`
- Postal address:
  **INAI – Data Protection**
  142 rue d'Iéna, apt. 21
  59000 Lille, France

For privacy-specific or data-protection questions (including exercising your rights), you can contact our dedicated address:

- Email: `privacy@inai.fr` (or any other dedicated address indicated on our Sites or Legal Hub).

If inAi appoints a Data Protection Officer (“DPO”) or equivalent contact, the relevant contact details will be published in this Policy or on our Sites. You may contact that person for any question related to personal-data protection and your rights.

### 2.3 Roles by product

- For **websites, marketing, support and recruitment**, inAi acts as **controller**.
- For **PageMind** catalog workflows, inAi acts mainly as **processor** on behalf of its business customers, who remain controllers of their catalogs and related personal data.
- For **Emplo**, the Emplo Privacy Policy specifies when inAi acts as controller and, where applicable, in which situations inAi may act as processor for employer-side integrations.

---

## 3. Key concepts and roles

### 3.1 Definitions

In this Policy:

- **“Personal data”** means any information relating to an identified or identifiable natural person.
- **“Processing”** means any operation performed on personal data (collection, storage, use, disclosure, etc.).
- **“Controller”** means the entity that determines the purposes and means of the processing.
- **“Processor”** means the entity that processes personal data on behalf of the controller.
- **“Recipient”** means an entity to which personal data is disclosed.
- **“EEA”** means the European Economic Area.
- **“Sites”** means the public websites operated by inAi (`inai.fr`, `inai.world`, `pagemind.fr`, `emplo.fr` and associated public pages).
- **“Apps”** or **“Services”** means inAi’s web applications and online services, including PageMind and Emplo.
- **“Customer”** means a business customer (retailer, brand, marketplace, employer) using inAi’s services under a contract.
- **“User”** means any natural person using the Sites or Apps (for example, a visitor, candidate, or user of a customer account).
- **“Candidate”** means a job-seeker using Emplo or applying for roles at inAi.

### 3.2 Where inAi is controller

inAi acts as **controller** for:

- visitors of the Sites (browsing, technical logs, cookies),
- individuals completing contact, demo, pilot, partnership or newsletter forms,
- generic inAi accounts that are not governed by a product-specific privacy policy (if any),
- business contacts, suppliers, partners, incubators, investors and public bodies with whom inAi communicates directly,
- **job applicants to inAi** (recruitment for roles at inAi),
- Emplo candidates and certain other product users, as described in the relevant product-specific privacy policies.

## 3.3 Where inAi is processor

inAi acts as **processor** when it processes personal data on documented instructions from a customer. This is typically the case for:

- **PageMind**: catalog files and related data provided by retailers, brands or marketplaces, and any personal data they may contain (for example, supplier contact details in documents).
- Certain **Emplo** employer-side data, where Emplo is integrated into an employer or partner workflow under a B2B arrangement.

In these cases, the **customer remains the controller** and is responsible for:

- determining the purposes and legal bases for processing,
- providing information to data subjects,
- complying with its own obligations under GDPR and other laws.

## 3.4 Responsibilities where inAi is processor

Where inAi processes personal data as processor on behalf of a customer:

- inAi acts only on the customer's **documented instructions** and within the framework of the applicable DPA and agreements;
- the customer remains solely responsible for:
    - its own controller obligations (information, legal basis, DPIAs, etc.),
    - the decision to upload particular data,
    - the use made of outputs (for example, catalog texts or analytics);
- inAi assists the customer in fulfilling certain obligations (such as handling data-subject requests or security incidents) as specified in the DPA.

To the maximum extent permitted by applicable law, inAi is **not responsible** for a customer's independent decisions about how they use our products, what data they

upload, or how they interpret or rely upon outputs, except where applicable law expressly requires joint responsibility.

---

## 4. Data we process, purposes, legal bases and retention

This section summarises the main processing activities for which inAi acts as **controller** in relation to the Sites and generic accounts. It specifies, for each context:

- categories of personal data,
- purposes of processing,
- legal bases under GDPR,
- retention periods, and
- main categories of recipients.

The actual data processed may vary depending on your interactions with us.

### 4.1 Website visitors (no account)

When you browse our Sites, we process technical and usage data to provide and secure the websites.

| Data categories | Purposes | Legal basis | Retention | Main recipients |
|---|---|---|---|---|
| Technical identifiers (IP address, date/time, URLs visited, HTTP headers, user-agent, device/browser information, error logs) | Provide access to the Sites, ensure routing, detect incidents and abuse, maintain security and performance | Legitimate interests (Art. 6(1)(f) GDPR): operation, security and improvement of the Sites | Web server logs are typically kept for up to **12 months**, unless a longer period is required for security investigations or legal purposes, in line with CNIL guidance that technical connection data should generally not be retained beyond around one year.([CNIL][1]) | Hosting and infrastructure providers (processors), security/monitoring tools |
| Strictly necessary cookies and similar identifiers (see Cookie Policy) | Maintain sessions, remember cookie choices, provide basic security and | Legitimate interests; exemption under e-privacy rules for strictly | Duration of the cookie (session or short persistence), as detailed in the Cookie Policy | Hosting and security providers |

| Data categories | Purposes | Legal basis | Retention | Main recipients |
|---|---|---|---|---|
| | load-balancing | necessary cookies | | |
| Non-essential cookies (analytics, preferences, marketing – where used) | Measure audiences, understand usage, improve the Sites, manage marketing campaigns | Consent (Art. 6(1)(a) GDPR) via banner and cookie settings | Non-essential cookies usually have a lifetime of up to **13 months**, and data derived from them is kept for limited periods (typically up to 25 months) in line with CNIL recommendations for audience measurement.([CNIL][2]) | Analytics and marketing providers (some act as independent controllers, see Section 6.3) |

Details of cookie types, providers and durations are set out in the **Cookie & Tracking Technologies Policy** and its cookie list.

## 4.2 Contact forms, demo / pilot requests, newsletter and commercial relations

When you contact us or subscribe to communications, we process your contact details and messages.

| Data categories | Purposes | Legal basis | Retention | Main recipients |
|---|---|---|---|---|
| Identification and contact data (name, job title, company, email, phone, country, language) | Respond to your enquiries (contact, demo or pilot request, partnership proposal, press enquiry) and maintain a record of interactions | Pre-contractual measures / contract (Art. 6(1)(b)) where your request relates to a potential contract; legitimate interests (Art. 6(1)(f)) for general B2B contact and follow-up | For prospects and non-customer contacts, data is generally kept up to **3 years** after the last meaningful contact (e.g. click, reply, meeting), in line with CNIL recommendations on commercial prospection.([CNIL][3]) | Internal teams (founder, sales, partnerships); CRM, email and support tool providers (processors) |
| Message content and | Understand your | Same as above | Same as above | Same as above |

| Data categories | Purposes | Legal basis | Retention | Main recipients |
|---|---|---|---|---|
| related context (company details, use case description, notes from calls) | request, prepare responses and proposals, document pilot or partnership discussions | | | |
| Newsletter or similar opt-in subscription data (email, subscription preferences) | Send newsletters and updates about our products, research and activities | Consent (Art. 6(1)(a)) obtained via opt-in; legitimate interests (Art. 6(1)(f)) for some B2B communications with opt-out | Until you unsubscribe or for up to **3 years** after your last meaningful interaction in the absence of other legal bases, unless a shorter period is chosen | Email delivery and newsletter platforms (processors); internal teams |

You can object to or unsubscribe from marketing communications at any time, for example by using the unsubscribe link in emails or by contacting us.

### 4.3 Generic inAi accounts (non-product-specific)

If we offer generic accounts not governed by a product-specific privacy policy (for example, a cross-product portal or a legal hub account), we process your account data to provide that service.

| Data categories | Purposes | Legal basis | Retention | Main recipients |
|---|---|---|---|---|
| Account credentials (email, hashed password, identifiers) | Create and manage your account, authenticate you | Contract (Art. 6(1)(b)) – providing the account | For as long as the account is active; after deletion we retain minimal technical logs and account events for a limited period (typically 1–3 years) for security and legal defence | Hosting, authentication and email providers (processors); internal operations team |
| Profile and usage data (name, role, company, | Provide access, manage authorisations, detect misuse | Legitimate interests (Art. 6(1)(f)) – ensure | Security logs and technical events are kept for limited periods, typically up to **12** | Same as above |

| Data categories | Purposes | Legal basis | Retention | Main recipients |
|---|---|---|---|---|
| language; last login, account status; basic security logs) | and security incidents | security, prevent fraud and abuse | **months**, unless a longer period is necessary for security investigations or legal obligations.([CNIL][1]) | |

For PageMind and Emplo accounts specifically, please refer to the relevant product privacy policies.

## 4.4 Business partners, suppliers, incubators, investors and public bodies

We process information about professional contacts in the context of our business relationships.

| Data categories | Purposes | Legal basis | Retention | Main recipients |
|---|---|---|---|---|
| Professional contact details (name, job title, company, business email/phone), communication history | Manage contracts and relationships with partners, suppliers, incubators (e.g. EuraTechnologies), investors and public funding bodies | Legitimate interests (Art. 6(1)(f)) – managing B2B relationships and corporate governance | For the duration of the relationship and then for applicable limitation periods (typically up to **5 years** after the end of the relationship, longer where accounting or legal obligations require; certain accounting documents must be kept up to **10 years** under French law).([orcom.fr][4]) | Internal management, finance and legal; accountants, banks, lawyers, auditors, public funding bodies (some acting as independent controllers) |
| Contract and billing data (contracts, purchase orders, invoices, payment | Contract management, accounting, legal compliance (tax, audit) | Legal obligation (Art. 6(1)(c)) – corporate, tax and accounting rules; | Accounting records are typically retained for up to **10 years** in accordance with French law.([orcom.fr][4]) | Accountants, payment providers, banks, auditors, tax authorities and other |

| Data categories | Purposes | Legal basis | Retention | Main recipients |
|---|---|---|---|---|
| details) | | legitimate interests (Art. 6(1)(f)) – managing our business | | competent authorities where required |

## 4.5 Job applicants to inAi (recruitment)

When you apply for a role at inAi, we process your application data.

| Data categories | Purposes | Legal basis | Retention | Main recipients |
|---|---|---|---|---|
| Identification and contact data (name, email, phone, LinkedIn or similar profile) | Manage applications, communicate with candidates | Pre-contractual measures (Art. 6(1)(b)); legitimate interests (Art. 6(1)(f)) – recruiting staff | For the duration of the recruitment process; if you are not hired, we may keep your file for up to **2 years** after the last contact, in line with CNIL guidance, so that we can recontact you about future opportunities.([CNIL][5]) | Internal hiring managers and founders; HR tools and recruitment platforms (processors); external recruiters where applicable (independent controllers or processors depending on role) |
| Application content (CV, cover letter, portfolio, interview notes, references you provide) | Assess your profile, skills and experience; build a candidate pool | Same as above | Same as above; if you are hired, relevant data may be transferred to your HR file and kept in accordance with HR and employment-law requirements (outside this Policy's scope) | Same as above |

We do not require you to include **special-category data** (e.g. health data, political opinions, religious beliefs) in your application. If you nevertheless provide such data, we

will treat it with particular care and may delete obviously inappropriate or excessive information where feasible.

### 4.6 High-level processing where inAi acts as processor (PageMind, some Emplo flows)

For completeness, we note that inAi also processes certain personal data as **processor** on behalf of customers, especially for PageMind catalog workflows and some Emplo employer-side integrations.

In these cases:

- the **customer** is the controller and defines:
    - which data is uploaded,
    - for which purposes,
    - on which legal bases;
- inAi processes the data only:
    - according to the customer's documented instructions, and
    - under the terms of the applicable DPA and contracts;
- data subjects should in principle **contact the customer** to exercise their rights; inAi will assist the customer as processor as described in the DPA.

This Policy does **not** attempt to exhaustively describe those processor-level activities.

---

## 5. How we collect personal data

### 5.1 Data collected directly from you

We collect personal data directly from you when you:

- browse the Sites (via technical logs and cookies),
- complete contact, demo, pilot, partnership or newsletter forms,
- create a generic inAi account (if applicable),
- communicate with us by email, phone or through other channels,
- apply for a position at inAi (via email, forms or recruitment platforms),
- use our products where we are controller (see product-specific privacy policies).

Providing certain data may be mandatory to process your request (for example, a valid email address to respond). Where applicable, we indicate which fields are mandatory.

### 5.2 Data obtained indirectly

We may also receive personal data from third parties, for example:

- from business contacts who introduce you (for example, incubators, partners, other customers),
- from **job boards** or recruitment platforms when you apply to inAi through those platforms,
- from PageMind customers or Emplo employer-side partners, where they provide us with documents or user lists in contexts where they are controllers,
- from public sources (such as official registries, professional directories or public websites) in a B2B context.

Where we receive personal data indirectly from controllers (for example, from a PageMind customer or an employer using Emplo), it is primarily the responsibility of that controller to inform the individuals concerned, and we assist them as processor under the DPA.

---

## 6. Recipients and data sharing

We only share personal data where necessary and in accordance with applicable law.

### 6.1 Internal recipients

Within inAi, personal data is accessible only to staff and contractors who need it for their tasks, such as:

- founders and management,
- engineering and operations teams,
- customer-success and sales teams,
- legal, finance and administrative staff.

All such persons are bound by confidentiality obligations.

### 6.2 Processors and sub-processors

We use third-party service providers acting as **processors** (or sub-processors) to support our activities, including:

- cloud hosting and storage providers,
- managed database, backup and monitoring services,
- email delivery and newsletter platforms,
- CRM and support tools,
- recruitment and HR platforms,
- AI model vendors and infrastructure providers.

We take appropriate steps to select processors that provide sufficient guarantees in terms of security and confidentiality and to ensure that:

- their access to personal data is limited to what is necessary,
- they process data only on our documented instructions,
- they are bound by written data-processing agreements,
- they implement appropriate technical and organisational measures.

An up-to-date list or description of key sub-processors is available in our **Legal Hub**, Privacy documentation and/or DPA. This list may evolve over time.

### 6.3 Independent third-party controllers

Some third parties process personal data obtained in connection with our Sites or products as **independent controllers** (or joint controllers), under their own terms and policies. This may include:

- payment service providers and banks,
- certain analytics or advertising providers,
- job boards and platforms from which you apply or to which you connect Emplo,
- public registries (e.g. in the context of retail compliance),
- some recruitment agencies or external advisers.

Their handling of personal data is governed by their own privacy and cookie policies, which we encourage you to consult separately.

To the maximum extent permitted by applicable law, inAi is **not responsible** for processing carried out independently by such third-party controllers for their own purposes, outside the scope of its documented relationship with them. This does not affect any responsibilities we may have where we act as joint controller with a given partner under applicable law.

### 6.4 Legal and regulatory disclosures

We may disclose personal data where required or authorised by law, regulation or court order, or in response to validated requests from competent public authorities, including:

- courts and law-enforcement authorities,
- regulatory and supervisory authorities (e.g. CNIL),
- tax and social-security authorities.

Such disclosures are limited to what is strictly necessary and, where permitted, we may inform the affected customers or individuals.

### 6.5 Business transfers

If inAi is involved in a merger, acquisition, restructuring, sale of assets or similar transaction, personal data may be transferred as part of that transaction, subject to

applicable legal requirements and appropriate safeguards. In such cases, we will take reasonable steps to inform affected individuals.

---

## 7. International data transfers

### 7.1 EU-centric hosting

We design our systems so that primary storage and processing of customer data at rest take place within **European Union** data centres, in particular for PageMind and Emplo, using EU-based virtual private cloud (VPC) environments, as described in our Security & Data Protection Overview.

For the website and corporate data covered by this Policy, we likewise favour EEA-based hosting and service providers where feasible.

This EU-centric design is a general rule and not an absolute guarantee that no personal data will ever transit to or be processed in countries outside the EEA, as explained in Sections 7.2 to 7.4.

### 7.2 When transfers outside the EEA may occur

Despite our EU-centric design, some processing may involve transfers of personal data outside the **European Economic Area (EEA)**, for example:

- when we use global service providers whose support teams or infrastructure are partly located outside the EEA (for example, certain email, CRM, analytics or AI providers),
- when our own staff or contractors located outside the EEA need limited access to data for support or maintenance purposes, under strict access controls,
- when users access the Sites or Apps from outside the EEA (in which case data necessarily transit between their device and our systems).

### 7.3 Safeguards for international transfers

Where personal data is transferred outside the EEA and there is no adequacy decision for the destination country, we implement appropriate safeguards, such as:

- **Standard Contractual Clauses (SCCs)** adopted by the European Commission,
- other recognised transfer mechanisms under GDPR,
- additional technical and organisational measures (such as encryption, minimisation, and access restrictions),
- contractual restrictions on onward transfers and on processing for purposes independent of our relationship with the provider.

We aim to limit such transfers to what is strictly necessary to provide and support our services.

### 7.4 Customer choices

Certain enterprise customers may have specific localisation or data-sovereignty requirements. In such cases, we encourage customers to contact us so we can discuss possible configurations and contractual clauses. Our ability to support particular configurations may depend on technical and commercial feasibility.

We do **not** promise that no data will ever leave the EEA, as this would not be realistic given the way modern internet services function.

---

## 8. Retention periods and deletion

### 8.1 General principles

We retain personal data only for as long as necessary to:

- provide the services or information requested,
- pursue our legitimate interests (for example, security, fraud prevention, defence of legal claims),
- comply with legal obligations (for example, accounting, tax, employment, or regulatory requirements).

Retention periods depend on the context and purpose of the processing. When determining them, we take into account CNIL and other supervisory-authority guidance, legal limitation periods and operational needs.([CNIL][5])

### 8.2 Illustrative retention periods

Subject to specific legal obligations or customer agreements, typical retention periods include:

- **Website technical logs**: up to **12 months**, unless extended for security or legal reasons.([CNIL][1])
- **Non-essential cookies and related identifiers**: typically up to **13 months** for cookies themselves, with derived analytics data kept for limited periods (often up to **25 months**) in line with CNIL guidance.([CNIL][2])
- **Cookie consent choices**: remembered typically for around **6 months**, consistent with CNIL recommendations on consent storage practices.([Village de la Justice][6])
- **Prospects / commercial contacts**: up to **3 years** after the last meaningful contact (e.g. click, reply, meeting).([CNIL][3])

- **Job applicants not hired**: generally up to **2 years** after the last contact, unless you consent to a longer period or request earlier deletion.([CNIL][5])
- **Customer, supplier and partner contracts and invoices**: kept for statutory periods, typically up to **10 years** for certain accounting and tax records.([orcom.fr][4])
- **Generic account data**: for the life of the account; after closure, certain data may be kept for a limited period (typically 1–3 years) for security and legal defence.

The concrete period actually implemented may be shorter where technically and operationally possible.

### 8.3 Deletion and anonymisation

When data is no longer needed, we:

- delete it from our active systems, or
- anonymise or aggregate it so that it is no longer personal data.

Backups are generally overwritten on a rolling basis and are not normally restored solely to delete individual records, except where required by law or by a controller exercising its rights under a DPA.

### 8.4 Legal holds and exceptions

We may retain certain data beyond standard periods where:

- required by law (for example, in connection with investigations, litigation or regulatory obligations), or
- reasonably necessary to establish, exercise or defend legal claims.

In such cases, access is restricted and data is used only for the relevant legal or security purposes.

---

## 9. Cookies and similar technologies

Our use of cookies and similar tracking technologies is described in detail in the separate **Cookie & Tracking Technologies Policy**, which forms an integral part of our legal framework.

In summary:

- We use **strictly necessary cookies** to operate the Sites and Apps (including session management, security and cookie preference storage) without prior consent, as permitted by e-privacy rules.

- We use **non-essential cookies** (such as analytics, preference, functional or marketing cookies) only with your **prior consent** via the cookie banner and settings interface.
- You can manage your preferences at any time using:
    - our cookie settings centre, and/or
    - your browser or device settings.

Refusal of non-essential cookies may degrade certain features. If you block strictly necessary cookies or essential scripts, the Sites or Apps may not function correctly. In such cases, we cannot guarantee availability or performance and, to the maximum extent permitted by law, any malfunction resulting solely from your choices is outside our responsibility.

---

## 10. Security of processing

We implement appropriate technical and organisational measures to protect personal data against unauthorised access, loss, alteration or disclosure, having regard to the risks and to the state of the art, as required by Article 32 GDPR.

These measures include, in particular:

- **Access control and identity management**:
    - least-privilege access,
    - strong authentication for internal systems,
    - role-based permissions and periodic review of rights.
- **Encryption**:
    - encryption of data in transit (TLS) and at rest (industry-standard algorithms) where supported.
- **Network and infrastructure security**:
    - use of virtual private cloud (VPC) architectures, security groups and firewalls,
    - reliance on reputable cloud providers with robust security programmes.
- **Application security and development practices**:
    - version control, code review and protected branches,
    - vulnerability and dependency management,
    - testing and controlled deployment pipelines.
- **Logging and monitoring**:

    - logging of security-relevant events,
    - monitoring and alerts for incidents or anomalies.
- **Backups and continuity**:
    - regular backups stored in secure locations,
    - tested restore procedures to support disaster recovery.
- **Organisational measures**:
    - confidentiality undertakings for staff and contractors,
    - onboarding and training on security and data protection,
    - documented incident-response procedures.

Further information is provided in our **Security & Data Protection Overview (Trust)**. That document is descriptive and informational and **does not create contractual obligations**. In case of conflict, the applicable contracts and this Policy prevail.

No system can be guaranteed to be 100% secure. You are responsible for the security of your own devices, networks and credentials and for any configuration choices you make (for example, installing third-party tools that may interfere with our services).

---

## 11. Profiling and automated decision-making

We may perform limited forms of **profiling** within the meaning of GDPR, such as:

- analysing website usage and engagement with communications to understand interest in our products,
- aggregating usage metrics in our products to improve features and performance (as further detailed in product-specific privacy policies).

For PageMind and Emplo, certain AI-driven features (for example, matching and ranking, or suggestion of actions) may be described in more detail in the respective product privacy policies.

We do **not**:

- use profiling via the Sites to take decisions that produce legal effects concerning you or similarly significantly affect you within the meaning of Article 22 GDPR,
- make hiring decisions or catalog publication decisions **solely** on the basis of automated processing without human involvement; such decisions are made by controllers (employers, retailers, brands) using their own processes and systems.

If this were to change in the future for specific services, we would update the relevant product privacy policies and, where applicable, implement the safeguards required by law.

---

## 12. Your rights

Under GDPR and, where applicable, other data-protection laws, you have a number of rights regarding your personal data. These include, in particular:

- **Right of access**: to obtain confirmation as to whether we process your personal data and, where applicable, a copy of that data.
- **Right to rectification**: to have inaccurate or incomplete personal data corrected or completed.
- **Right to erasure ("right to be forgotten")**: to request deletion of your personal data in certain circumstances (for example, where it is no longer necessary for the purposes for which it was collected, or where you withdraw consent and there is no other legal basis).
- **Right to restriction of processing**: to request that processing be restricted in certain cases (for example, while a dispute about accuracy or lawfulness is being resolved).
- **Right to data portability**: to receive certain data you have provided to us in a structured, commonly used and machine-readable format and to transmit that data to another controller, where the processing is based on consent or contract and carried out by automated means.
- **Right to object**:
    - to processing based on our legitimate interests, on grounds relating to your particular situation;
    - to processing for **direct marketing**, in which case we will stop processing for that purpose.
- **Right to withdraw consent**: where processing is based on your consent, you may withdraw that consent at any time, without affecting the lawfulness of processing carried out before withdrawal.
- **Rights related to automated decision-making**: where you are subject to a decision based solely on automated processing that produces legal effects concerning you or similarly significantly affects you, you may have the right to obtain human intervention, express your point of view and contest the decision. As noted above, we do not currently use such decisions in the scope of this Policy.

These rights are not absolute and may be subject to conditions and exceptions under applicable law (for example, where processing is necessary to comply with legal obligations, or for the establishment, exercise or defence of legal claims).

---

## 13. Exercising your rights and contacting us

### 13.1 How to contact us

To exercise your rights or ask questions about this Policy, you can contact us by:

- Email: `privacy@inai.fr` (or any updated privacy contact indicated on the Sites), or
- Post:
  **INAI – Data Protection**
  142 rue d'Iéna, apt. 21
  59000 Lille, France

Where available, you may also be able to use in-product tools (for example, account-deletion functions) or online forms specifically dedicated to privacy requests.

### 13.2 Verification of identity

For security and confidentiality reasons, we may need to verify your identity before responding to certain requests (for example, by asking you to confirm access to a specific email address or account).

If we have reasonable doubts about your identity, we may request additional information that is strictly necessary to confirm it. If we cannot verify your identity with reasonable efforts, we may refuse to act on your request.

### 13.3 Time limits and fees

We aim to respond to requests within **one month** of receipt. This period may be extended by up to two additional months in case of complex or numerous requests; in such cases, we will inform you of the extension and the reasons for it.

Exercising your rights is generally **free of charge**. However, if a request is manifestly unfounded or excessive (for example, due to its repetitive nature), we may either:

- charge a reasonable fee reflecting the administrative costs of responding, or
- refuse to act on the request.

### 13.4 Where inAi is controller vs processor

- Where inAi is **controller** (for example, for website visitors, business contacts, Emplo candidates where specified in the Emplo Privacy Policy, and job applicants to inAi), we handle your request directly.

- Where inAi acts only as **processor** for a customer (for example, for PageMind catalog files):

    - you should preferably address your request to the **customer/controller** (retailer, brand, employer);

- if you contact us directly, we may forward your request to the controller and support them in responding, in accordance with the DPA.

### 13.5 Right to lodge a complaint

You also have the right to lodge a complaint with a competent data-protection authority, in particular:

- in France, the **Commission Nationale de l'Informatique et des Libertés (CNIL)**,
- or the authority of your habitual residence, place of work, or place of the alleged infringement.

The CNIL can be contacted via its website and at the following address:

CNIL
3 Place de Fontenoy
TSA 80715
75334 Paris Cedex 07
France
Website: `https://www.cnil.fr`

We encourage you to contact us first so that we can try to resolve your issue, but you are not obliged to do so before contacting a supervisory authority.

---

## 14. Children

Our Sites and services are **not directed at children** below the minimum age required to consent to online services in their country of residence (commonly 15 or 16 in the EU, depending on the Member State).

- **Emplo** is intended for adult job-seekers capable of entering into employment relationships.
- We do not knowingly collect personal data from children in the context of this Policy. If we become aware that we have collected personal data from a child contrary to our intentions, we will take reasonable steps to delete such data and, where appropriate, close the relevant account.

Parents or legal guardians who believe that their child has provided personal data to us without consent may contact us using the details in Section 13.

---

## 15. Changes to this Policy

We may update this Policy from time to time, for example to:

- reflect changes in our processing activities, products or organisational structure,
- take into account changes in applicable laws or regulatory guidance,
- improve clarity and transparency.

When we make changes, we will:

- update the **"Last updated"** date at the top of this page; and
- where appropriate, provide additional notice (for example, via a banner on the Sites or an email, especially if the changes are material).

Where changes involve new processing activities that require consent, or where the legal basis changes, we will obtain new consent where required by law.

Your continued use of the Sites after the effective date of the updated Policy implies your acknowledgement of the changes, without prejudice to any specific consent that may be required for certain processing.

---

## 16. Relationship with other documents and applicable law

### 16.1 Relationship with other documents

This Policy should be read together with:

- the **Website Terms of Use** (governing access to and use of the Sites),
- the **Legal Notice / Mentions légales**,
- the **Cookie & Tracking Technologies Policy**,
- the **Security & Data Protection Overview (Trust)**,
- the product-specific **Terms of Service**, **Privacy Policies**, **DPAs** and **MSAs**.

In case of inconsistency:

- product-specific Terms of Service, Privacy Policies and DPAs prevail for the corresponding products and services,
- the Cookie Policy prevails for details on cookies and similar technologies,
- the Website Terms of Use and Legal Notice prevail for rules on access to and use of the Sites.

### 16.2 Applicable law

This Policy and any dispute relating to it are governed by **French law** and, where applicable, by EU law (in particular the GDPR), without prejudice to any mandatory provisions of the law of the country where you habitually reside if you are a consumer and those provisions provide you with greater protection.

## 16.3 Non-contractual nature

Nothing in this Policy should be interpreted as:

- creating contractual rights or obligations beyond those provided by applicable law and the agreements you have with inAi,
- modifying any limitations of liability, warranties, or other contractual provisions set out in the applicable Terms of Service, DPA, MSA or other contracts.

In case of conflict between this Policy and a signed contract or product-specific terms, the latter prevail for the relevant subject-matter.