

Privacy Policy

Last updated: September 2026

1. Data Controller

AXOUND is the brand under which Danoux Olivier, a Swiss sole proprietorship, provides its services.

Danoux Olivier AXOUND
Chemin de Riantbosson 19
1217 Meyrin
Switzerland

For questions regarding the protection of your personal data or to exercise your rights, you may contact AXOUND through the contact form available on axound.ch or by post at the address above.

2. Scope

This Privacy Policy explains how AXOUND processes personal data, in particular when you:

- visit axound.ch;
- contact AXOUND or request a Digital Survival Assessment;
- are a prospect, customer, supplier, partner or professional contact;
- use the AXOUND customer portal;
- communicate with AXOUND in connection with a business or contractual relationship.

Some AXOUND services also involve processing data on behalf of customers, including backup, restoration, Brand Monitoring and Incident Response services.

Where the customer determines the essential purposes and means of processing and AXOUND processes data on its behalf, the applicable conditions are specified in the relevant contract and, where required, in a Data Processing Agreement (“DPA”).

3. Data We Process

Depending on your relationship with AXOUND, we may process the following categories of personal data.

Identification and professional data: first and last name, company, job title and professional contact details.

Requests and communications: email address, telephone number, message content, service requests, commercial proposals and communication history.

Contractual and administrative data: contracts, orders, invoices and information required for invoicing and managing the customer relationship.

Customer portal data: username, email address, information required to manage the account and information relating to requests made through the portal.

Technical and security data: including IP address, date and time, requested resource, browser or device information and events required for website operation, diagnostics, abuse prevention and security.

Professional information from public sources: information available on company websites, professional registers, professional networks and other publicly accessible sources where relevant in a professional context.

Service-related data: information relating to systems, accounts, domains, incidents, technical logs or other information which a customer authorises AXOUND to access in connection with a service.

As part of Brand Monitoring, AXOUND may process domain names, website content, technical information, screenshots and other information publicly accessible on the Internet.

4. Sources of Data

Personal data may be obtained:

- directly from you;
- from your company or organisation;
- from AXOUND customers where required to perform a service;
- from professional or publicly accessible sources;
- from systems or services which a customer authorises AXOUND to access;
- automatically when the website or customer portal is used where required for operation or security.

5. Purposes of Processing

AXOUND processes personal data where required in particular to:

- respond to enquiries;
- arrange a Digital Survival Assessment or meeting;
- prepare a quotation or proposal;
- establish and manage a business relationship;
- enter into and perform contracts;

- provide and administer AXOUND services;
- operate the customer portal;
- manage backup and restoration requests;
- provide digital resilience, Brand Monitoring and Incident Response services;
- communicate with customers, prospects, suppliers and partners;
- manage invoicing, accounting and administrative obligations;
- protect systems, services and the website;
- diagnose technical issues and prevent abuse;
- establish, exercise or defend legal rights;
- comply with legal obligations;
- reasonably develop AXOUND's business;
- measure aggregate use of the website and the effectiveness of its content.

AXOUND does not sell personal data.

6. Legal Framework and Grounds for Processing

Under Swiss law, AXOUND processes personal data in accordance with the Swiss Federal Act on Data Protection ("FADP"), including the principles of transparency, purpose limitation, proportionality and security.

Where the European Union General Data Protection Regulation ("GDPR") applies, processing may in particular be based on:

- performance of a contract or pre-contractual steps;
- compliance with a legal obligation;
- legitimate interests pursued by AXOUND or a third party, including operating a B2B business, ensuring security, reasonably developing the business and defending legal rights;
- consent where the relevant processing actually requires consent.

Where processing relies on consent, consent may be withdrawn for the future.

7. Website Forms

When you complete an AXOUND form, the information provided is used to handle your request and contact you.

Submissions may be retained in the website database to ensure proper follow-up and continuity in handling requests, in addition to the email notification sent to AXOUND.

Submissions are generally retained for **12 months following the last meaningful interaction**.

Where a person becomes a customer, information required for the contractual relationship may become part of the customer record and is then retained according to the rules applicable to that relationship.

Longer retention may also be necessary where required by law or reasonably necessary to establish, exercise or defend legal claims.

8. Customer Portal

AXOUND operates a customer portal allowing authorised users to access certain service-related functions.

Information required for authentication and account management is stored within AXOUND's WordPress environment.

The portal uses technologies required in particular for authentication, session management, preferences and security.

AXOUND does not currently use a tool designed to systematically record all actions performed by users within the customer portal.

9. Hosting and Email

The AXOUND website, its database and AXOUND's primary email infrastructure use **Infomaniak** services in Switzerland.

Data processed through these services are hosted within Infomaniak's Swiss infrastructure.

The hosting provider also generates technical access and error logs required for operation, diagnostics and hosting security.

Such logs are retained according to the provider's applicable technical retention cycles.

10. Audience Measurement with Plausible Analytics

AXOUND uses **Plausible Analytics** to measure aggregate use of the website, including pages viewed, traffic sources, devices and browsers used and approximate geographical information.

Plausible does not set audience-measurement cookies and does not use persistent identifiers designed to track a visitor across different days or websites.

The IP address and User-Agent received with a request may be used transiently to calculate a daily identifier. The raw IP address and full User-Agent are not stored by Plausible.

Visitor data used for audience measurement are processed and stored within the European Union.

AXOUND uses these statistics solely to understand overall website use, evaluate traffic sources and improve its content. They are not used for targeted advertising or individual profiling.

11. Website Security and Wordfence

AXOUND uses security mechanisms designed to detect and block unauthorised access attempts, attacks, malicious requests and other security events.

Wordfence traffic logging is configured for **security-related events** only and is not used by AXOUND as an audience measurement tool.

Wordfence processes IP addresses required for certain security functions and exchanges certain technical information with its infrastructure in order to provide its protection services.

The provider, **Defiant, Inc.**, is established in the United States.

Where personal data are transferred in this context, AXOUND relies on the contractual safeguards applicable to the service, including the provider's Data Processing Addendum and applicable Standard Contractual Clauses.

12. Providers and Recipients

Where necessary, personal data may be disclosed or made accessible to the following categories of recipients:

- hosting and email providers;
- information security providers;
- audience measurement providers;
- storage and backup providers;
- technical providers required to perform a service;
- professional advisers such as accountants or lawyers;
- registrars, hosting providers, platforms, search engines or other relevant parties where Brand Monitoring or takedown services require this;
- public authorities where disclosure is legally required or necessary to establish, exercise or defend legal rights.

Where AXOUND acts as a processor on behalf of a customer, relevant subprocessors and corresponding conditions may be specified in the applicable DPA.

13. External Communication Services

The website may provide links or shortcuts to communication services operated by third parties.

Where you voluntarily choose to use such a service, a connection may be established with the relevant provider or you may leave AXOUND's technical environment.

Subsequent processing by that provider is governed by its own terms and privacy policy.

14. International Transfers

AXOUND favours providers and infrastructure located in Switzerland or the European Economic Area where reasonably possible.

Certain technical functions may nevertheless involve providers established in other countries, including the US provider used for certain website security functions.

Where personal data are transferred to a country that is not recognised as providing an adequate level of protection under applicable Swiss law, AXOUND implements, where required, appropriate safeguards permitted by applicable law, such as recognised Standard Contractual Clauses or another appropriate legal mechanism.

Transfers relating to processing performed on behalf of customers are, where necessary, specified in the applicable DPA.

15. Backup, Restoration and Processing on Behalf of Customers

Certain backup, restoration, Brand Monitoring and Incident Response services may involve processing personal data on behalf of customers.

In these situations, the relevant customer is generally the data controller and AXOUND processes the information in accordance with the contractually agreed instructions.

The scope, providers, locations and retention periods applicable to such processing are defined in the relevant service documentation and, where required, in the applicable DPA.

Backup data may be subject to retention periods and immutability mechanisms which technically prevent alteration or deletion before the relevant retention period expires.

16. Automation and Artificial Intelligence

AXOUND may use automated or artificial-intelligence-assisted tools to support certain technical, analytical or classification tasks.

Within the current Brand Monitoring workflow, information that may be submitted to such tools originates from sources publicly accessible on the Internet.

The fact that information is publicly available does not necessarily prevent it from constituting personal data where it concerns an identifiable person. AXOUND therefore limits such use to information required for the relevant service.

AXOUND does not use such tools to make solely automated decisions concerning individuals which produce legal or similarly significant effects.

Where external tools are used in processing performed on behalf of a customer, relevant conditions are addressed in the contractual documentation and, where necessary, in the applicable DPA.

17. Retention

AXOUND retains personal data only for as long as required for the relevant purposes and subsequently where required by law or justified for establishing, exercising or defending legal rights.

In particular:

- website form submissions are generally retained for 12 months following the last meaningful interaction;
- prospect and professional contact information is retained while reasonably relevant to the professional relationship and deleted when no longer necessary;
- customer portal account data are retained for as long as required to provide the relevant service and subsequently deleted or rendered inaccessible according to applicable contractual terms and technical cycles;
- accounting records are retained for the applicable statutory period under Swiss law;
- technical and security logs are retained according to their purpose and applicable technical cycles;
- backup data follow the retention periods applicable to the relevant service and may remain protected against deletion during an immutability period;

- Brand Monitoring and Incident Response records may be retained for the duration required to provide the service and subsequently where necessary to establish or defend legal rights.

Data which are no longer required are deleted, anonymised or rendered inaccessible where technically and legally possible.

18. Cookies and Similar Technologies

AXOUND uses cookies or similar technologies that are strictly necessary in particular for website operation, security, customer portal authentication, session management, preferences and recording privacy choices.

Audience measurement performed through Plausible Analytics does not rely on cookies or persistent identifiers.

AXOUND does not currently use Google Analytics or technologies intended for targeted advertising or cross-site behavioural tracking.

Where non-essential technologies are introduced, AXOUND adapts the information provided and, where required under applicable law, allows visitors to make the necessary choice.

19. Data Security

AXOUND implements technical and organisational safeguards appropriate to the nature of the information and associated risks.

Depending on the circumstances, these include access controls, authentication mechanisms, confidentiality measures, encryption where appropriate, backups and measures designed to support system continuity.

As no information system or transmission method can guarantee absolute security, AXOUND adapts its safeguards according to relevant risks, the state of the art and the evolution of its services.

20. Your Rights

Depending on applicable law and circumstances, you may in particular request:

- confirmation as to whether AXOUND processes personal data concerning you;
- access to such data;
- correction of inaccurate data;
- deletion where permitted by law;

- cessation or restriction of certain processing where applicable;
- delivery or transmission of certain data where a right to data portability applies;
- withdrawal of consent for future processing where the relevant processing relies on consent.

Where the GDPR applies, you may also benefit in particular from the rights to erasure, restriction, objection and data portability provided by the Regulation.

AXOUND may request information reasonably necessary to verify the identity of the person making a request.

Certain rights may be limited by statutory retention obligations, third-party rights or overriding legitimate interests.

21. Data Processed on Behalf of a Customer

Where AXOUND processes your personal data solely on behalf of one of its customers, that customer will generally be the relevant data controller.

In such circumstances, your request should generally be submitted directly to the relevant customer.

AXOUND will assist the customer where required under the applicable contractual and legal obligations.

22. Complaints

AXOUND encourages you to contact us first with any question or concern regarding your personal data.

In Switzerland, you may also contact the Federal Data Protection and Information Commissioner (FDPIC).

Where the GDPR applies, you may also lodge a complaint with the competent supervisory authority.

23. Changes to this Privacy Policy

AXOUND may amend this Privacy Policy where its activities, services, providers, technical practices or legal requirements change.

The applicable version is the version published on axound.ch.

The date of the latest update appears at the beginning of this Privacy Policy.