

# Privacy Policy

This **privacy policy** provides information on the processing of personal data in connection with our **activities and operations**, including our **website** under the domain name xatla.net. In particular, we explain why, how and where we process personal data. We also provide information on the rights of individuals whose data we process.

We may publish further privacy policies or other information on data protection for specific or additional activities and operations.

## 1 Contact details

Responsibility for the processing of personal data:

### **xatla AG**

Dorfmatweg 8a  
3110 Münsingen  
Switzerland  
[datenschutz@xatla.net](mailto:datenschutz@xatla.net)

In individual cases, third parties may be responsible for the processing of personal data, or there may be joint responsibility with third parties.

## 2 Terms and legal basis

### 2.1 Definitions

**Data subject:** A natural person whose personal data we process.

**Personal data:** Any information relating to an identified or identifiable natural person.

**Sensitive personal data:** Data concerning trade union, political, religious or philosophical views and activities; data concerning health, sexual life or membership of an ethnic or racial group; genetic data; biometric data that uniquely identifies a natural person; data concerning criminal or administrative sanctions or proceedings; and data concerning social welfare measures.

**Processing:** Any handling of personal data, regardless of the means and procedures used, for example, the retrieval, comparison, adaptation, archiving, storage, reading, disclosure, acquisition, collection, erasure, disclosure, sorting, organisation, saving, alteration, dissemination, linking, destruction and use of personal data.

### 2.2 Legal basis

We process personal data in accordance with Swiss data protection law, in particular the [Federal Act on Data Protection](#) (Data Protection Act, DPA) and the [Ordinance on Data Protection](#) (Data Protection Ordinance, DPO).

### 3 Nature, scope and purpose

We process the personal data necessary to carry out our activities and operations in a sustainable, people-friendly, secure and reliable manner. The personal data processed may fall, in particular, into the categories of browser and device data, content data, communication data, metadata, usage data, master data (including inventory and contact details), location data, transaction data, contract data and payment data.

We also process personal data that we receive from third parties, obtain from publicly available sources or collect in the course of our activities and operations, provided that such processing is permitted for legal reasons.

We process personal data, where necessary, with the consent of the data subjects. In many cases, we may process personal data without consent, for example to comply with legal obligations or to safeguard overriding interests. We may also seek the consent of data subjects even where their consent is not required.

We process personal data for the period necessary for the respective purpose. We anonymise or delete personal data, in particular in accordance with statutory retention and limitation periods.

### 4 Disclosure of personal data

We may disclose personal data to third parties, have it processed by third parties, or process it jointly with third parties. Such third parties are, in particular, specialist providers whose services we use.

We may, for example, disclose personal data to banks and other financial service providers, public authorities, educational and research institutions, consultants and solicitors, interest groups, IT service providers, cooperation partners, providers of API services for communication and calendar functions such as email and appointment management, credit and business information agencies, logistics and shipping companies, marketing and advertising agencies, media organisations, associations, social institutions, telecommunications companies and insurance providers.

For the dispatch of invoices in physical or electronic form, we use the services of Pingen AG, Zurich (Switzerland). Invoice and address data are processed on our behalf. Data processing takes place in Switzerland. Where, for logistical reasons, dispatch is carried out via international printing or postal service providers, appropriate data protection is ensured in accordance with the requirements of the Swiss Data Protection Act.

### 5 Personal data abroad

We generally process personal data in Switzerland. However, we may also disclose or export personal data to other countries, in particular to process it there or have it processed there.

We may disclose personal data to any [country on Earth](#) and elsewhere in [the universe](#), provided that the law in that jurisdiction guarantees adequate data protection in accordance with [a decision by the Swiss Federal Council](#).

We may disclose personal data to countries whose laws do not guarantee adequate data protection, provided that appropriate data protection is ensured for other reasons, in particular on the basis of standard data protection clauses or other suitable safeguards. In exceptional cases, we may export personal data to countries without adequate or appropriate data protection if the specific data protection requirements are met, for example the explicit consent of the data subjects or a direct connection to the conclusion or performance of a

contract. We are happy to provide data subjects with information on any safeguards upon request or to supply a copy of such safeguards.

## 6 Communication

We process personal data in order to communicate with individuals, as well as with public authorities, organisations and companies. In particular, we process data that a data subject provides to us when contacting us, for example by post or email. We may store such data in an address book or using similar tools.

Third parties who provide us with data about other individuals are obliged to ensure the data protection of those data subjects themselves. In particular, they must ensure that such data is accurate and may be disclosed.

We use selected services from suitable providers to enable and improve communication with individuals and other communication partners. We may also use such services to manage and otherwise process the data of data subjects beyond the scope of direct communication.

In particular, we use:

- **Intercom**: Customer service and support chat system; providers: Intercom R&D Unlimited Company (Ireland) / Intercom Inc. (USA). Data processing is safeguarded by a data processing agreement (DPA) including EU standard contractual clauses. The processing of highly sensitive patient data within this chat system is prevented by the system itself: [Privacy Policy](#), [Security](#).
- **Nylas**: Programming interface for the data protection-compliant integration of email, calendar and contact data; provider: Nylas Inc. (USA). Data processing takes place on the basis of a Data Processing Addendum (DPA) exclusively on Nylas's European cloud infrastructure: [Privacy Policy](#), [Security](#).

## 7 Data security

We take appropriate technical and organisational measures to ensure data security commensurate with the respective risk. However, we cannot guarantee absolute data security.

Access to our website is secured via transport encryption ([SSL/TLS](#), in particular using the [Hypertext Transfer Protocol Secure, abbreviated to HTTPS](#)). Most browsers indicate transport encryption with a padlock icon in the address bar.

Our digital communications are subject – as *is generally the case with* all digital communications – to mass surveillance without cause or suspicion, as well as other forms of surveillance by security authorities in Switzerland, the rest of Europe, the United States of America (USA) and other countries. We have no direct influence over the processing of personal data by intelligence services, police forces and other security authorities.

## 8 Rights of data subjects

### 8.1 Data protection rights

We grant data subjects all rights in accordance with applicable data protection law. Data subjects have the following rights in particular:

- **Right of access:** Data subjects may request information as to whether we process personal data concerning them and, if so, what personal data is involved. Data subjects shall also receive the information necessary to assert their data protection rights and to ensure transparency. This includes the personal data being processed as such, but also, amongst other things, details regarding the purpose of processing, the duration of storage, any disclosure or export of data to other countries, and the origin of the personal data.
- **Rectification and restriction:** Data subjects may have inaccurate personal data rectified, incomplete data completed, and the processing of their data restricted.
- **Erasure and objection:** Data subjects may have personal data erased ('right to be forgotten') and object to the processing of their data with effect for the future.
- **Data disclosure and data portability:** Data subjects may request the disclosure of personal data or the transfer of their data to another controller.

We may defer, restrict or refuse the exercise of data subjects' rights within the limits permitted by law. We may inform data subjects of any conditions that must be met for them to exercise their data protection rights. For example, we may refuse to provide information in whole or in part on the grounds of trade secrets or the protection of other individuals. We may, for example, also refuse to delete personal data in whole or in part on the grounds of statutory retention obligations.

*In exceptional cases*, we may charge a fee for the exercise of these rights. We will inform data subjects in advance of any such costs.

We are obliged to identify data subjects who request information or assert other rights by taking appropriate measures. Data subjects are obliged to cooperate.

### 8.2 Legal protection

Data subjects have the right to enforce their data protection claims through legal channels or to lodge a complaint with a competent data protection supervisory authority.

The data protection supervisory authority for private controllers and federal bodies in Switzerland is the [Federal Data Protection and Information Commissioner](#) (FDPIC).

## 9 Use of the website

### 9.1 Cookies

We may use cookies. Cookies – both our own cookies (first-party cookies) and cookies from third parties whose services we use (third-party cookies) – are data stored in the browser. Such stored data need not be limited to traditional text-based cookies.

Cookies can be stored temporarily in the browser as ‘session cookies’ or for a specific period as so-called permanent cookies. ‘Session cookies’ are automatically deleted when the browser is closed. Permanent cookies have a specific storage period. In particular, cookies enable us to recognise a browser the next time it visits our website and thereby, for example, measure the reach of our website. However, permanent cookies can also be used for online marketing, for example

Cookies can be disabled in full or in part, or deleted, at any time via your browser settings. Without cookies, our website may no longer be available in its entirety. We actively seek your express consent to the use of cookies – at least where and to the extent necessary.

### 9.2 Logging

We may collect the following information for every visit to our website, provided that this is transmitted by your browser to our server infrastructure or can be determined by our web server: Date and time, including time zone, Internet Protocol (IP) address, access status (HTTP status code), operating system including user interface and version, browser including language and version, individual sub-pages of our website accessed, including the amount of data transferred, and the last webpage accessed in the same browser window (referrer).

We store such information, which may also constitute personal data, in server log files. This information is necessary to ensure that our website is available on a permanent, user-friendly and reliable basis, and to guarantee data security and, in particular, the protection of personal data – including by or with the assistance of third parties.

### 9.3 Web beacons

We may use tracking pixels on our website. Tracking pixels are also known as web beacons. Tracking pixels – including those from third parties whose services we use – are small, usually invisible images that are automatically retrieved when you visit our website. Tracking pixels can be used to collect the same information as in server log files.

## 10 Notifications and communications

We send notifications and communications via email and other communication channels such as instant messaging or SMS.

### 10.1 Performance and reach measurement

Notifications and messages may contain web links or web beacons that track whether an individual message has been opened and which web links were clicked. Such web links and web beacons may also track the use of notifications and messages on a personal basis. We require this statistical tracking of usage for performance and reach measurement in order to be able to send notifications and communications effectively and in a user-friendly manner, as well as permanently, securely and reliably, based on the needs and reading habits of the recipients.

### 10.2 Consent and objection

You must, *in principle*, expressly consent to the use of your email address and other contact details, unless such use is permitted for other legal reasons. Where possible, we use the 'double opt-in' procedure to obtain consent; this means you will receive an email containing a web link which you must click to confirm, thereby preventing misuse by unauthorised third parties. We may log such consents, including [your Internet Protocol \(IP\) address](#) and [the date and time](#), for evidential and security purposes.

You may, *in principle*, object at any time to receiving notifications and communications such as newsletters. By doing so, you may also object to the statistical recording of usage for the purposes of measuring success and reach. This is without prejudice to any necessary notifications and communications relating to our activities and operations.

## 11 Social media

We are present on social media platforms and other online platforms in order to communicate with interested parties and provide information about our activities and operations. In connection with such platforms, personal data may also be processed outside Switzerland.

The General Terms and Conditions (GTC) and Terms of Use, as well as privacy policies and other provisions of the individual operators of such platforms, also apply in each case. These provisions provide information in particular on the rights of data subjects directly vis-à-vis the respective platform, including, for example, the right of access.

## 12 Third-party services

We use services provided by specialist third parties to enable us to carry out our activities and operations in a sustainable, user-friendly, secure and reliable manner. These services allow us, amongst other things, to embed functions and content into our website. When such embedding takes place, the services used collect users' Internet Protocol (IP) addresses, at least temporarily, for technically necessary reasons.

For necessary security-related, statistical and technical purposes, third parties whose services we use may process data relating to our activities and operations in an aggregated, anonymised or pseudonymised form. This includes, for example, performance or usage data required to provide the respective service.

- **[Microsoft services](#)**: Providers: Microsoft Corporation (USA) / Microsoft Ireland Operations Limited (Ireland) for users in the European Economic Area (EEA), the UK and Switzerland; General information on data protection: '[Privacy at Microsoft](#)', '[Privacy \(Trust Center\)](#)', [Privacy Statement](#).

### 12.1 Digital infrastructure

We use services from specialist third parties to access the digital infrastructure required in connection with our activities and operations. These include, for example, hosting and storage services from selected providers.

In particular, we use:

- **[Myra Security GmbH](#)**: Provision of cyber protection shields, Content Delivery Network (CDN) and Web Application Firewall (WAF) to defend against DDoS attacks and malicious traffic. Data processing is carried out in accordance with the GDPR and the Swiss Data Protection Act exclusively within the European Union (EU): [Privacy Policy](#).
- **[cloudscale.ch](#)**: Cloud server platform; provider: cloudscale.ch AG (Switzerland); information on data protection: [Privacy Policy](#).
- **[ServerBase](#)**: Cloud hosting; Provider: ServerBase AG (Switzerland); Data protection information: [Privacy policy](#), '[Swiss data centre](#)'.
- **[Infomaniak Network SA](#)**: Provision of AI services compliant with data protection regulations. Data processing takes place in real time and is carried out entirely in certified Swiss data centres. Data entered is processed temporarily and is not used for training public models. [Privacy Policy](#).

### 12.2 Online collaboration

We use third-party services to enable online collaboration. In addition to this privacy policy, any directly visible terms and conditions of the services used, such as terms of use or privacy policies, also apply.

In particular, we use:

- **[Microsoft Teams](#)**: A platform for productive collaboration, particularly via audio and video conferencing; Provider: Microsoft; Teams-specific information: '[Security and compliance in Microsoft Teams](#)', in particular '[Data protection](#)'.
- **[Fullview ApS](#)**: Provision of visual support tools (co-browsing). Data processing is carried out in compliance with the GDPR and the Swiss Data Protection Act exclusively on servers within the European Union (Frankfurt, Germany). To protect

sensitive patient data, fields requiring protection are automatically redacted in real time prior to screen sharing (data masking). Support access is granted only after explicit authorisation by the end user. [Privacy policy](#).

### 12.3 Contact options

We use services from selected providers to communicate more effectively with third parties, such as potential and existing customers

### 12.4 Maps

We use third-party services to embed maps on our website.

In particular, we use:

- [map.search.ch](https://www.map.search.ch): Map service; Provider: Swisscom Directories AG (Switzerland); Information on data protection: [Privacy Policy](#), [‘Terms of Use’](#), in particular [‘Rights of use for own purposes’](#).

### 12.5 Digital audio and video content

We use services provided by specialist third parties to enable the direct playback of digital audio and video content, such as music or podcasts.

In particular, we use:

- [cloudscale.ch](https://www.cloudscale.ch): Cloud server platform; Provider: cloudscale.ch AG (Switzerland); Data protection information: [Privacy Policy](#).

## 13 Final provisions

We may amend and supplement this privacy policy at any time. We will provide information about such amendments and supplements in an appropriate manner, in particular by publishing the current privacy policy on our website.