
Privacy Policy of breathe medical AG

Version 1.0 – 18.07.2025 - superseded - for reference only

About us

This privacy policy ("**Privacy Policy**") explains how we process and protect your personal data when you use the web application UpLeap, the mobile applications available on Android and IOS, and related services (together the "**Services**"). The Services are available through the website <https://www.upleap.me/> ("**Website**"), as well as the official UpLeap mobile apps ("**Mobile Apps**") available on the Google Play Store and the Apple App Store.

These Services are operated by breathe medical AG, c/o ETH Zürich, Institut für Design, Materialien und Fabrikation, ML E39, Sonneggstrasse 3, 8092 Zurich Switzerland (the "**Company**", "**we**", "**our**", or "**us**"). The Company is the controller for the data processing described below.

Unless otherwise defined in this Privacy Policy, the definitions used in this Privacy Policy have the same meaning as in the EU General Data Protection Regulation (GDPR).

For all questions on the subject of data protection, you can also contact us at:

by e-mail to: privacy@upleap.me

by mail to: breathe medical AG, c/o ETH Zürich, Institut für Design, Materialien und Fabrikation, ML E39, Sonneggstrasse 3, 8092 Zurich Switzerland

1 Personal data we collect

We may collect or receive personal information for a number of purposes connected with our business operations when you use our Services, namely:

- Contact information (e.g. email, phone, address)
- IP address and log-in data
- Account information (if applicable, e.g. profession, birth date)

There is no obligation to provide your personal data. However, please note that our Services cannot be provided if you do not provide the required data strictly necessary for performing the contract between you and us.

2 How we collect personal data

We collect information about our users when they use our Services, including taking certain actions within it.

Directly

- Via our Mobile Apps, our Website, and electronic communication
- When you use our Services
- When you provide services to us
- When you correspond with us by electronic means using our Services
- When you browse, complete a form or make an inquiry while using our Services

Indirectly

- Through public sources
- From public registers (such as commercial registers), news articles and internet searches
- When our business customers engage us to perform professional services which involve them sharing personal data they control with us as part of that engagement
- From external Service Providers (see section 5)

3 Legal Basis and purposes

Our legal basis for collecting and using the personal data described in this Privacy Policy depends on the personal data we collect and the specific purposes for which we collect it.

Contract: To perform our contractual obligations or take steps linked to a contract with you. In particular:

- To provide our Services.
- As part of an application process.

Consent: We may rely on your freely given consent at the time you provided your personal data. In particular:

- To provide you with news, special offers, newsletters, and general information about the goods and Services we offer.

Legitimate interests: We rely on legitimate interests based on our assessment that the processing is fair and reasonable and does not override your interests or fundamental rights and freedoms. In particular:

- To maintain and improve our Mobile Apps, Website and Services.
- To develop new services.
- To provide you with news, special offers, newsletters and general information about the Services we offer.

Necessity for compliance with legal obligations: To meet regulatory and public interest obligations.

In particular:

- To notify you about changes to our Services and our Privacy Policy
- To comply with applicable regulations and legislation.
- For the legal enforcement of claims and rights.

4 Data retention

We retain personal data for so long as it is needed for the purposes for which it was collected and in line with legal and regulatory requirements or contractual arrangements. After this period, we delete or fully anonymise your personal data.

5 Data recipients

We engage third-party companies ("**Service Providers**") to facilitate the operation of our Services, assist in analysing the usage of the Services, or perform necessary services, such as payment and the provision of IT services. These third parties have access to your personal data only to the extent necessary to perform these tasks.

Type(s) of Service Providers who might access your personal data:

- Payment providers
- Development service providers
- Software infrastructure service provider
- Accountants and lawyers

6 Data transfers

We and/or our Service Providers may transfer your personal data to and process it in the following countries:

- In the EU/EEA/CH
- US

We may use Service Providers partly located in so-called third countries (outside the European Union or the European Economic Area) or process personal data there, i.e., countries whose level of data protection does not correspond to that of the EU.

We safeguard your personal data per our contractual obligations and applicable data protection legislation when transferring data abroad.

Such safeguards may include:

- The transfer to countries where there is an adequacy decisions by the European Commission in place;
- Applying standard data protection model clauses, binding corporate rules or other standard contractual obligations that provide appropriate data protection.

7 Data disclosure

We may disclose your personal data in the good faith belief that such action is necessary:

- To comply with a legal obligation (i.e., if required by law or in response to valid requests by public authorities, such as a court or government agency)
- To protect the security of our Services and defend our rights or property
- To prevent or investigate possible wrongdoing in connection with us

8 Data Security

We take reasonable technical and organisational security measures that we deem appropriate to protect your stored data against manipulation, loss, or unauthorised third-party access. Our security measures are continually adapted to technological developments.

We also take internal data privacy very seriously. Our employees and the service providers that we engage are required to maintain secrecy and comply with applicable data protection legislation. In addition, they are granted access to personal data only insofar as this is necessary for them to carry out their respective tasks or mandate.

The security of your personal data is important to us but remember that no method of transmission over the internet or electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your personal data, we cannot guarantee its absolute security. We recommend using antivirus software, a firewall, and other similar software to safeguard your system.

9 Your rights

You have the below data protection rights. To exercise these rights, you may contact the above address or send an e-mail to: privacy@upleap.me. Please note that we may ask you to verify your identity before responding to such requests.

- **Right of access:** You have a right to request a copy of your personal data, which we will provide to you in an electronic form.
- **Right to amendment:** You have the right to ask us to correct our records if you believe they contain incorrect or incomplete information about you.
- **Right to withdraw consent:** If you have provided your consent to the processing of your personal data, you have the right to withdraw your consent at any time with effect for the future. This includes cases where you wish to opt-out from marketing communications. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose(s) to which you initially consented to unless there is another legal basis for processing. To stop receiving emails from us, please click on the 'unsubscribe' link in the email you received or contact us at privacy@upleap.me.
- **Right to erasure:** You have the right to request that we delete your personal data when it is no longer necessary for the purposes for which it was collected or when it was unlawfully processed.
- **Right to restriction of processing:** You have the right to request the restriction of our processing of your personal data where you believe it to be inaccurate, our processing is unlawful, or where we no longer need to process it for the initial purpose, but where we are not able to delete it due to a legal obligation or because you do not want us to delete it.
- **Right to portability:** You have the right to request that we transmit your personal data to another data controller in a standard format such as Excel, if this is data which you have provided to us and if we are processing it on the legal basis of your consent or to perform our contractual obligations.
- **Right to object to processing:** Where the legal basis for our processing of your personal data is our legitimate interest, you have the right to object to such processing on grounds relating to your particular situation. We will abide by your request unless we have a compelling legal basis for the processing which overrides your interests or if we need to continue to process the personal data for the exercise or defence of a legal claim.
- **Right to lodge a complaint with a supervisory authority:** You have the right of appeal to a data protection supervisory authority if you believe that the processing of your personal data violates data protection law. In the EU and EEA, you can exercise this right, for example, before

a supervisory authority in the Member State of your residence, your place of work or the place of the alleged infringement. You can find a list of the relevant authorities here: https://edpb.europa.eu/about-edpb/board/members_en.

10 Cookies

Our Services use cookies and similar technologies (collectively “Tools”) provided either by us or by third parties.

A cookie is a small text file that is stored on your device by the browser. Comparable technologies are web storage (local / session storage), fingerprints, tags or pixels. Most browsers are set by default to accept cookies and similar technologies. However, you can usually adjust your browser settings so that cookies or similar technologies are rejected or only stored with your prior consent. If you refuse cookies or similar technologies, you may not be able to use all of our Services without problems.

In the following, the Tools we use are listed by category, whereby we inform you in particular about the providers of the Tools, the storage period, and their purpose. If personal data is transferred to third countries, we refer you to section 6 of our Privacy Policy, also with regard to the risks this may entail.

10.1 Essential tools

- **Wix CMS** – core page rendering, routing, and security cookies
- **Wix FAQ widget** – stores state so the FAQ expands/collapses.

10.2 Non-essential tools

- **Google Tag Manager (gtag/js)** – loads analytics/marketing tags; no cookies of its own, but transmits IP address to Google servers.

11 Social Media and Links to Third-Party Apps and Websites

Our Services contain links to websites or apps that are not operated by us. When you click on a third-party link, you will be directed to that third party's website or app. We have no control over the content, privacy policies, or practices of any third-party websites or services.

We maintain online presences on social networks to, among other things, communicate with customers and prospective customers and to provide information about our products and Services. If you have an account on the same network, it is possible that your information and media made available there may be seen by us, for example, when we access your profile. In addition, the social network may allow us to contact you. As soon as we transfer personal data into our own system, we are responsible for this independently. This is then done to carry out pre-contractual measures and to fulfil a contract. For the

legal basis of the data processing carried out by the social networks under their own responsibility, please refer to their data protection declarations. Below is a list of social networks on which we operate an online presence:

- Facebook: [Privacy Policy](#)
- Instagram: [Privacy Policy](#)
- LinkedIn: [Privacy Policy](#)

12 Newsletter

We send newsletters and other notifications by email and through other communication channels and may deliver them with the help of third parties.

In principle, you must expressly consent to receive newsletters and other notifications from us, unless this is permitted for other legal reasons.

Newsletters and other notifications may contain web links or tracking pixels that record whether an individual newsletter or notification has been opened and which web links were clicked (performance measurement). Such web links and tracking pixels record the use of newsletters and other notifications. We use this statistical recording of usage, including success and reach measurement, in order to be able to offer newsletters and other notifications effectively and in a user-friendly manner, as well as permanently, securely and reliably, based on the reading habits of the recipients.

You can unsubscribe from newsletters and other notifications at any time and thereby object in particular to the aforementioned collection of usage. You can do so by contacting us directly or following the link included in the footer of each newsletter we send you.

13 Changes to this Privacy Policy

We may update our Privacy Policy from time to time. We therefore encourage you to review this Privacy Policy periodically for any changes.

Changes to this Privacy Policy are effective when they are posted on this page.

14 Contact us

If you have any questions about this Privacy Policy, do not hesitate to get in touch with us at:

breathe medical AG
c/o ETH Zürich, Institut für Design, Materialien und Fabrikation
ML E39
Sonneggstrasse 3
8092 Zurich Switzerland

privacy@upleap.me