Data Privacy Policy

The protection of personal data is a priority for Biofrontera AG („***Biofrontera***“, “***us***”, “***our***” or “***we***”). As a website user (“***you***” and “***your***”) your personal data is processed in accordance with the applicable data protection laws, especially the European General Data Protection Regulation (***GDPR***).

According to Art. 4 no. 1 GDPR, personal data refers to any information relating to an identified or identifiable natural person. This includes any data you provide to us (“***data***”).

This privacy policy provides detailed information about the type, scope, and purposes of data processing, as well as how your data is managed. It also outlines your rights concerning the processing of your data.

Responsible person (controller) and data protection officer

Responsible for the processing of your data is:

Biofrontera AG
Hemmelrather Weg 201
51377 Leverkusen

We have appointed an external data protection officer:

DPOint GbR
Aachener Straße 619
50933 Köln

Our data protection officer is available to address any questions or concerns you may have regarding data protection. You can reach the data protection officer

- at our business address above, with the addition of „Datenschutz/Data Privacy“ or
- by E-Mail at datenschutz@biofrontera.com.

External Hosting

This website is hosted externally by tops.net GmbH & Co. KG, Holtorfer Straße 35, 53229 Bonn ("***tops.net***" or "***hoster***"). Data collected via this website, such as IP addresses, contact requests, metadata and communication details, contract and contact information, names, web access logs, and other website-generated data, are stored on the host’s servers.

The external hosting serves the purpose of fulfilling the contract with our potential and existing customers (Art. 6 (1) lit. b) GDPR) and in the interest of secure, fast, and efficient provision of our online services by a professional provider (Art. 6 (1) lit. f) GDPR).

Our hoster processes your data only to the extent necessary to fulfil its service obligations and adheres to our instructions regarding data processing.

We have concluded a data processing agreement for the use of the above-mentioned service.

Collection and storage of data as well as type and purpose of their use

Website visit

Each time you access our website, your browser automatically transmits data that is stored in the server's log files. These are the following data ("***log files data***"):

- Browser type and browser version;
- Name und URL of the accessed file;
- Date and time of the server request;
- Report about successful access (HTTPS response code);
- Operating system in use;
- Referrer URL;
- Websites that are accessed by the user's system via our website;
- Internet service provider of the user; and
- IP-address (anonymized) and the requesting provider.

We analyse log files data anonymously to continuously improve the website, tailor it to user interest and address errors more efficiently. These activities align with our legitimate interest in data processing as outlined in Art. 6 (1) lit. f) GDPR.

Requests by email, telephone or fax

If you contact us via email, phone, or fax, your request and associated data will be stored and processed to address your inquiry. We do not share this data without your consent.

The processing of these data is based on Art. 6 (1) lit. b) GDPR, as far as your request is related to the fulfilment of a contract or is necessary for the performance of pre-contractual measures. In all other cases, the processing is based on our legitimate interest in the effective handling of the requests addressed to us (Art. 6 (1) lit. f) GDPR) or on your consent according to Art. 6 (1) lit. a) GDPR, if this has been requested; the consent can be revoked at any time.

The data you send us via contact requests will be retained until you request its deletion, revoke consent, or the purpose for storing it no longer applies (e.g., after processing your request). Statutory retention periods remain unaffected.

Newsletter

To register for the newsletter, we collect necessary data such as title, name, and email address. The registration is confirmed via a "double opt-in" process, where you must confirm your subscription through a link sent to your email. We track whether you open the email and which issues of the newsletter you read, including frequency and timing. By subscribing, you will regularly receive updates about our offers.

In certain cases, we use the service provider pressetext Nachrichtenagentur GmbH, located at Josefsträdter Straße 44, 1080 Vienna, Austria ("***pressetext***"), to send newsletters. Pressetext specializes in press distribution and regulatory technology (RegTech). The data you provide for newsletter subscription (see para. 1) will be stored on pressetext's servers in Vienna.

The data collected during newsletter registration will be used solely for advertising purposes via the newsletter. The legal basis for sending the newsletter is your consent under Art. 6 (1) lit. a) and Art. 7 GDPR, Section 7 (3) of Act against Unfair Competition - ***UWG***. The legal basis for recording the registration is our legitimate interest (Art. 6 (1) lit. f) GDPR) in proving that the newsletter was sent with your consent.

You can revoke your consent at any time by sending a message in text form (e.g., email) to the contact details provided above. The legality of data processing prior to the revocation remains unaffected.

The data you provide for subscribing to the newsletter will be stored by us or pressetext until you unsubscribe. After unsubscribing or when the purpose no longer applies, your data will be deleted from the distribution list. We may also delete or block email addresses at our discretion, in line with our legitimate interest (Art. 6(1) lit. f) GDPR). The logging of registration and dispatch details will be retained as long as there is a need to prove the original consent.

After unsubscribing from the newsletter, your email address may be stored in a blacklist by us or pressetext to prevent future mailings. The data will only be used for this purpose and not merged with other data. This serves both your interest and our legitimate interest in complying with legal requirements (Art. 6(1) lit. f) GDPR). The blacklist storage is indefinite, but you may object if your interests outweigh our legitimate interest.

Further information on pressetext's data protection provisions can be found at the following link: https://www.pressetext.com/privacy.

We have concluded a data processing agreement with pressetext to ensure that data is processed in compliance with data protection regulations.

Cookies

On our website we use so-called "cookies". Cookies are small text files and do not cause any damage on your device. They are either stored temporarily for the duration of a session (session cookies) or permanently (permanent cookies) on your device. Session cookies are automatically deleted after the end of your visit while permanent cookies stay on your device until you delete them, or they are automatically removed by your browser.

In some cases, third-party cookies may be stored on your device when visiting our website. These cookies allow us or third-party providers to offer certain services or features.

Cookies have various functions. Many cookies are technically necessary, as certain website functions would not work without them (e.g. the shopping cart function). Other cookies are used to analyse user behaviour or display targeted advertising.

Cookies necessary for electronic communication (necessary cookies), providing certain functions (functional cookies, e.g. shopping cart), or optimizing the website (e.g. to audience measurement cookies) are stored based on Art. 6 (1) lit. f) GDPR, unless another legal basis applies. The website provider has a legitimate interest in storing cookies for the technically error-free and optimized provision of its services. If consent to the storage of cookies has been requested, the storage of the cookies concerned is based exclusively on this consent (Art. 6 (1) lit. a) GDPR and Section 25 (1) of Telecommunications-Telemedia Data Protection Act - ***TDDDG***); the consent can be withdrawn at any time.

If third-party companies or analysis tools use cookies, we will inform you about this separately in this privacy policy and, if required, ask for your consent.

You can configure your browser to notify you when cookies are about to be set, allowing you to decide whether to accept them on a case-by-case basis, exclude them entirely, or allow them for specific instances. Please note that disabling cookies may affect the functionality of the website.

Please refer to the user menu of your web browser or the website of your browser's manufacturer for guidance on adjusting cookies settings. Typically, the help function in your browser's menu will show how to be notified about cookies, reject new ones, and delete existing ones

Cookie-Consent-Management - Usercentrics

Our website uses Usercentrics' consent technology to obtain your consent for storing certain cookies on your device or for using specific technologies, and to document this in compliance with data protection laws. The provider of this technology is Usercentrics GmbH, Sendlinger Straße 7, 80331 Munich, Germany ("***Usercentrics***").

When you visit our website, a connection is established with Usercentrics' servers to obtain your consent and provide further explanations about cookie usage. Usercentrics then stores a cookie in your browser to track your consent or its withdrawal. The collected data (e.g., settings, login data, consent ID, consent time, opt-in/out, language, and device data) is deleted after 12 months or earlier if you request deletion, you delete the Usercentrics cookie by yourself, or if the purpose no longer applies. Legal retention obligations remain unaffected. Usercentrics is used to obtain the legally required consent for the use of cookies. The legal basis for this is Article 6 (1) lit. c) of the GDPR.

We have concluded a data processing agreement with Usercentrics to ensure that data is processed in compliance with data protection regulations.

Recipients of data

In the scope of our business activities, we cooperate with various external parties. In some cases, this also requires the transfer of data to these external parties. We only disclose data to external parties if this is required as part of the fulfilment of a contract (Art. 6 (1) lit. b) GDPR, if we are legally obligated to do so (e.g., disclosure of data to tax authorities) based on Art. 6 (1) lit. c) GDPR, if we have a legitimate interest in the disclosure pursuant to Art. 6(1) lit. f) GDPR, or if another legal basis permits the disclosure of this data. When using processors, we only disclose your data based on a valid data processing agreement. In the case of joint processing, a joint controllership agreement is concluded.

Transfer to recipients outside the European Economic Area (EEA)

We may transfer data to recipients located outside the EEA, known as third countries. Before such transfers, we ensure that the recipient offers an adequate level of data protection, for example, using EU Commission's Standard Contractual Clauses (***SCCs***), or that you have explicitly consented to the transfer.

Transfer to recipients in the USA

Please note that, as a safe third country, the USA generally has a level of data protection comparable to that of the EU. Data transfer to the USA is therefore permitted when the recipient is certified under the EU-US Data Privacy Framework (***DPF***). You can verify certifications through the https://www.dataprivacyframework.gov/s/participant-search/participant-detail?contact=true&id=a2zt0000000TT9jAAG&status=Active. If certification is unavailable, equivalent safeguards must be established by the US recipient (e.g. SCC).

Integration of third-party services and contents

Google Services

In the following we describe the use of data using services of Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.

The responsible service provider in the EU is the Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland ("***Google***").

Depending on the service, Google may act as a data processor or joint controller under relevant agreements. Data transfers to the U.S. occur under the SCCs to ensure appropriate data protection. We have concluded corresponding contracts with Google.

Please find details here:

https://support.google.com/publisherpolicies/answer/10437486?hl=en,

https://business.safety.google/adsprocessorterms/ and

https://business.safety.google/adscontrollerterms/.

Furthermore, Google LLC is certified under DPF. For more information, please follow the link: https://www.dataprivacyframework.gov/s/participant-search/participantdetail?contact=true&id=a2zt000000001L5AAI&status=Active.

For more information about Google's use of data, settings, and opportunities to raise objections, please refer to Google's privacy declaration https://policies.google.com/privacy?hl=en-US.

Google Analytics (GA4)

We use functions of the web analysis service Google Analytics. The service provider of this service is Google.

Google Analytics enables the website provider to analyse the behaviour of the website visitors. To that end, the website provider receives a variety of user data, such as pages accessed, time spent on the page, the utilized operating system and the user's origin. The data collected is associated with the user's device but is not linked to a specific user ID.

Furthermore, Google Analytics allows us to record your mouse and scroll movements and clicks, among other things. Google Analytics uses various modelling approaches to augment the collected data sets and uses machine learning technologies in data analysis.

Google Analytics uses technologies that make the recognition of the user for the purpose of analysing the user behaviour patterns (e.g., cookies or device fingerprinting).

In Google Analytics 4, the anonymization of IP addresses is enabled by default. This ensures that your IP address is anonymized by Google within EU or EEA member states.

The use of Google Analytics is based on Art. 6 (1) lit. f) GDPR as the website provider has a legitimate interest in analysing user behaviour to improve its offerings and advertising. If an explicit consent has been requested (e.g. consent to store cookies), the processing is based exclusively on Art. 6 (1) lit. a) GDPR and Section 25 (1) TDDDG; the consent can be withdrawn at any time.

The data sent by us and linked to cookies are automatically deleted after 2 months. Deletion of data that has reached its retention period occurs automatically once a month. If you revisit

our website within the two-month retention period, the retention duration is extended by an additional two months.

You can prevent the recording and processing of your data by Google by downloading and installing the browser plugin available under the following link: https://tools.google.com/dlpage/gaoptout?hl=en.

For more information about the handling of user data by Google Analytics, please consult Google's Google Analytics Terms of Service at: https://marketingplatform.google.com/about/analytics/terms/us/.

Social media

We maintain publicly accessible profiles on social networks as detailed below. The social media icons on our website function solely as links. no data is processed by the social media providers when you visit our site. If you click on the "plug-ins", you will be redirected to our respective social media profiles.

Social networks such as Facebook, Instagram, etc. often analyse user behaviour comprehensively when visiting their websites or encountering embedded content (e.g. like buttons or advertising banners). Accessing our social media accounts may trigger numerous data processing operations, which are subject to applicable data protection regulations.

In detail

If you are logged into your social media account while visiting our social media profiles, the provider of the social media can allocate this visit to your user account. However, your data may also be collected if you are not logged in or do not have an account with the respective social media portal. This can occur through cookies stored on your device or by recording your IP address.

By collecting data, the social media providers can create user profiles based on your preferences and interests. This allows for targeted advertising both within the social media platform and across other websites. If you have an account with the respective social network, the interest-based advertising may be displayed on all devices on which you are or were logged in.

Please also note that we are not able to track all processing on the social media platforms. Depending on the provider, further processing operations may therefore be carried out by the operators of the social media portals. For details, please refer to the terms of use and data protection provisions of the respective social media provider.

Legal basis

Our social media presence aims to maximize visibility on the internet, aligning with our legitimate interest under Art. 6 (1) lit. f) GDPR. The data analysis processes initiated by social networks may be based on different legal grounds, which should be specified by the respective social media providers, such as consent under Art. 6 (1) lit. a) GDPR.

Data controller and enforcement of rights

When you visit one of our social media profiles (e.g. Facebook), we share joint responsibility with the platform provider for the resulting data processing. In principle, you may exercise your rights (such as access, correction, deletion, restriction of processing, data portability, and complaint) against both, us and the respective platform provider (e.g. Facebook).

Please note that despite the joint responsibility with the social media provider, we do not have full influence on the data processing operations of the social media portals. Our possibilities are significantly determined by the company policy of the respective provider.

Storage period

The data directly collected by us via the social media presence will be deleted from our system as soon as the purpose for storing it no longer applies, you request us to delete it, or you withdraw your consent to store it. Stored cookies remain on your terminal device until you delete them. Binding legal conditions – in particular retention periods and limitation periods – will remain unaffected.

We have no influence on the storage period of your data, which is stored by the operators of the social networks for their own purposes.

For details, please contact the social media provider directly (e.g. in their privacy policy, see below).

Our social networks in detail

YouTube

Our website integrates videos from YouTube, provided by Google.

We use YouTube's enhanced privacy mode, which ensures that YouTube does not store information about visitors before they play a video. Data is only transferred to Google once you actively play the video (by clicking on it). We do not have control over this data transfer.

Once you play a YouTube video on this website, a connection to YouTube's servers is established, and the following data may be transmitted to Google:

- Your IP address,
- Information about the browser and operating system used,
- The page from which you accessed the video (Referrer URL),
- Date and time of your access,
- Other data required by YouTube for service provision and optimization

If you are logged into a Google or YouTube account, the collected data can be directly linked to your profile. If you prefer not to have this association, make sure to log out of your account before playing a YouTube video.

Additionally, YouTube may store data in the local storage of your browser in extended privacy mode. This technology functions similarly to cookies and can be used for analysing your usage behaviour. Google uses this data, among other things, to generate video statistics, improve website usability, and prevent fraud.

Under certain circumstances, once a YouTube video starts playing, additional data processing operations may be triggered that are beyond our control. These operations can involve the collection of information for various purposes such as analytics or user behaviour tracking, which may be managed directly by YouTube.

The use of YouTube on our website is based on our interest in presenting our online offerings in an engaging manner, which qualifies as a legitimate interest under Art. 6 (1) lit. f) GDPR. If consent is obtained, processing will be based solely on Art. 6 (1) lit. a) GDPR and Section 25 (1) TDDDG, if the consent includes the storage of cookies or access to device information (e.g., device fingerprinting). This consent can be withdrawn at any time.

LinkedIn

We have a profile on LinkedIn. This service is provided by LinkedIn Ireland Unlimited Company, Wilton Plaza, Wilton Place, Dublin 2, Ireland ("***LinkedIn***").

If you contact us via LinkedIn, we process your name and any other information you provide. We are solely responsible for the processing of your data. This processing is based on Art. 6 (1) lit. f) GDPR, as it serves our legitimate interest in maintaining a proper and interactive corporate presentation.

LinkedIn collects logfiles (URL, referrer-URL, IP-address, device and browser information and access times). Die IP-addresses are shortened or (if they are used to reach LinkedIn members across devices) hashed (pseudonymized). The direct identifiers of LinkedIn members are deleted by LinkedIn after seven days. The remaining pseudonymized data is then deleted within 180 days (https://www.linkedin.com/help/linkedin/answer/a1445756/linkedin-marketing-solutions-und-die-datenschutz-grundverordnung-dsgvo-?lang=de).

The data collected by LinkedIn cannot be assigned by us to specific persons. LinkedIn may store the data collected from website visitors on its servers in the USA and use it for its own purposes. LinkedIn uses cookies and other technologies to collect data from you. For details, please refer to LinkedIn's privacy policy and cookie policy: https://www.linkedin.com/legal/privacy-policy#choices-oblig https://de.linkedin.com/legal/cookie-policy?trk=homepage-basic_footer-cookie-policy.

If you have given your consent, the use of the above-mentioned service is based on Art. 6 (1) lit. a) GDPR and Section 25 (1) TDDDG. This consent can be withdrawn at any time. If your consent has not been requested, the service is used based on Art. 6 (1) lit. f) GDPR; the website operator has a legitimate interest in effective advertising measures that include the use of social media.

Storage period

Unless otherwise stated, we store data only as long as is necessary to fulfil the purposes for which it was collected. In some cases, data must be stored to comply with legal obligations, such as tax or commercial law. In these cases, we will only continue to store the data for these legal purposes but will not process it in any other way and will delete it after the legal retention period has expired.

Data security

We make every effort to ensure the security of your data within the scope of the applicable data protection laws and technical possibilities.

For security reasons and to protect the transmission of confidential content, such as purchase orders or inquiries you submit to us as the website provider, this website uses the SSL (Secure Socket Layer) coding system. We would like to point out that data transmission on the Internet (e.g. when communicating by email) can have security gaps. Complete protection of the data against access by third parties is not possible.

To secure your data, we maintain technical and organisational security measures in accordance with Art. 32 GDPR, which we continually adapt to the state of the art.

Furthermore, we do not guarantee that our service will be available at certain times; disruptions, interruptions or failures cannot be ruled out.

Your rights (rights of data subjects)

You have extensive rights regarding the processing of your data.

Right of access

You have the right to access information about the data we store, including its purpose and storage duration (Art. 15 GDPR). This right is limited by exceptions under Section 34 of the Federal Data Protection Act - ***BDSG***, such as when data is retained solely for legal purposes or security, or when providing the information would require disproportionate effort. Furthermore, the prevention of misuse through technical and organizational measures may also limit access.

Right to rectify inaccurate data

You have the right to request the rectification of your data without delay if it should be inaccurate (Art. 16 GDPR).

Right to erasure

You have the right to request the erasure (Art. 17 GDPR) of your data. These conditions exist in particular if a) the respective processing purpose has been achieved or otherwise ceases to apply, b) we have processed your data unlawfully, c) you have revoked a consent without the data processing may not be continued on another legal basis, d) you successfully object to the data processing, or e)the obligation to delete your data based on the law of the EU or an EU member state, to which we are subject, exists. The right to erasure is limited by Section 35 BDSG, particularly if deleting the data would require disproportionate effort, especially for non-automated data, and if your interest in deletion is considered low.

Right to restriction of processing

You have the right to request restriction of the processing of your data (Art. 18 GDPR). This right exists in particular if a) the accuracy of the data is disputed, b) you request restricted processing instead of erasure under the conditions of a legitimate request for erasure, c) the data is no longer necessary for the purposes pursued by us, but you need the data to assert, exercise or defend legal claims or d) the success of an objection is still disputed.

Right to data portability

You have the right to obtain your data that were provided to us in a structured, common, machine-readable format (Art. 20 GDPR), if the data has not already been deleted.

Right to object

You have the right to object to the processing of your data at any time based on your specific situation (Art. 21 GDPR). We will stop processing your data unless we can demonstrate compelling legitimate grounds for the processing which outweigh your interests, rights, and freedoms, or if the processing serves the purpose of asserting, exercising or defending legal claims.

According to Art. 7 (3) GDPR, you have the right to withdraw your consent at any time. The revocation does not affect the lawfulness of the processing carried out based on the previous consent. The only consequence of the revocation is that we may no longer continue the data processing based on this consent for the future. However, please note that we may not be able to provide certain services or additional services if we are not able to process the data required for this purpose.

Right in relation to automated decision making

You have the right (Art. 22 GDPR) not to be subject to automated decision making, including profiling, that has legal consequences or similar significant effects for you. We generally do not use automated decision making or profiling. However, if you have been subjected to automated decision-making and do not agree with the outcome, you may contact us in the ways set out below and ask us to review the decision.

Right to complain to the supervisory authority

You have the possibility to contact the above-mentioned data protection officer (if appointed) or a data protection supervisory authority if you believe that the processing of your data violates the GDPR.