Privacy information for business partners

Biofrontera AG and its affiliated companies pursuant to Section 15 et seq. of the German Stock Corporation Act (***AktG***) (hereinafter also referred to as "***Biofrontera Company***"[1]" "***we***" and "***us***") has set itself the goal to constantly improve the service and range of information offered to our business partners, suppliers, customers or interested parties in order to contribute to the mutual corporate success. In the context of a business relationship and in times of increasing globalisation, personal data (hereinafter referred to as "***data***") is regularly used and processed by us. We take the protection of your data very seriously and consider data protection in all our business processes. In doing so, we comply with the applicable legal rules on data protection. In the following, you will receive a detailed overview of how we process your data. We ask you to also make this data protection information available to your employees who are in business contact with us.

Pursuant to Art. 4 No. 1 of the EU General Data Protection Regulation („***GDPR***"), personal data means any information relating to an identified or identifiable natural person that you provide to us as a business partner in the course of our business relationship. With this privacy information, we inform you about the type, scope and purposes of the collection of personal data by us and how this data is handled. In addition, you will learn about the rights you have regarding the processing of your data.

Person responsible and data protection officer

The Biofrontera Company with which you are in business contact or an ongoing contractual business relationship or the initiation of such a relationship is responsible for the processing of your data.

You can contact the Biofrontera Company for all data protection issues:

- at our central business address for data protection issues

  Hemmelrather Weg 201, 51377 Leverkusen, Germany

  With the addition „data privacy"

  or

- by email under datenschutz@biofrontera.com.

Biofrontera AG, Biofrontera Bioscience GmbH and Biofrontera Pharma GmbH have appointed a data protection officer in accordance with the legal requirements. You can also contact the data protection officer centrally at our above-mentioned e-mail address (datenschutz@biofrontera.com).

[1] ***Biofrontera Companies*** *are Biofrontera AG, Biofrontera Pharma GmbH, Biofrontera Development GmbH, Biofrontera Neuroscience GmbH, Biofrontera Bioscience GmbH, Biofrontera UK Ltd (seat: Cambridge).*

What is the origin of your data and what data is processed?

We process your data in accordance with the principles of data protection law only to the extent necessary, if we are permitted to do so by applicable legal requirements or we are obliged to do so.

Unless otherwise stated below, the terms "process" and "processing" also include, in particular, the collection, use, storage, disclosure and transfer of personal data (Art. 4 No. 2 GDPR).

In principle, the provision of your data is voluntary. However, for the conclusion and implementation of the business relationship, it is mandatory to process certain data about you.

We process the data that we receive from you in the course of our business relationship, i.e. either on the basis of a contractual relationship with you, or your company (such as the purchase and sale of products, services, works services, rights of use, etc.), a pre-contractual contact or any other inquiry on your part (e.g. via the internet, by e-mail or telephone or on the occasion of a trade fair or product event).

In addition, to the extent necessary for the fulfilment of our contractual or legal obligations, we process your data that we permissibly obtain from publicly accessible sources (such as commercial registers and registers of association, the press, the internet) or are legitimately provided by other third parties (e.g. a credit agency).

Relevant data are in particular:

- Contact details of the contact person(s) at the business partner and business address;
- Communication data, such as telephone number and e-mail address;
- Bank and billing data;
- Tax number/VAT-ID; and
- Order data, such as sales data or business partner history;
- Name and business address of directors and shareholders, company representatives as far as this information is obtained from public sources and the Commercial Register.

We generally use and store the following categories of your business and/or personal information:

- Salutation;
- First and last name;
- Postal address;
- E-mail address;
- Landline number, mobile number and fax number;
- Occupation, position, title and academic degree.

What is my data used for (purpose of processing) and on what basis (legal basis) does this happen?

Processing for the fulfilment of contractual obligations

We process your personal data primarily for the fulfilment of contracts with you, or your company, or for the performance of pre-contractual measures (Art. 6 para. 1 lit. b) and f) GDPR) upon request. In the context of our business relationship, you are obliged to provide the data necessary for the establishment, performance and termination of a business relationship and for the fulfilment of the associated contractual obligations, or which we are required to collect by law. Without this data, we will generally not be able to conclude a contract with you, to execute and terminate it, and to take pre-contractual measures to conclude a contract with you upon request. If you do not provide us with the necessary information and documents, we will not be able to establish or continue the business relationship you have requested.

Processing due to legal requirements

In addition, we process your data insofar as this is necessary for the fulfilment of legal obligations (Art. 6 para. 1 lit. c) GDPR).

Processing on the basis of a legitimate interest

In addition, we process your personal data insofar as this is necessary to safeguard the legitimate interests of us or a third party (Art. 6 para.1 lit. f) GDPR). This could include the following cases:

- Providing information (e.g. by mail) about invitations to events and other initiatives to present our products, services, offers, and promotions;
- Assertion of legal claims and defence in legal disputes;
- Measures for optimising our business processes, such as maintaining a supplier database or a "customer relationship management" database;
- For the purpose of advertising products or promotions (with trading partners);
- Measures to ensure operational safety and for business management;
- For reconciliation with European and international embargo lists;
- Credit checks; and
- Collection of debts, also in connection with the appointment of collection agencies.

Recipients of your data and place of processing

Within the context of our business relationships, those who are entrusted with the fulfilment of our contractual and legal obligations and to carry out our internal processes (e.g. sales, purchasing, logistics, financial accounting, human resources) will have access to your data. The employees authorised to access the data are obligated to maintain confidentiality and to protect business and trade secrets as well as data privacy.

To the extent necessary, we also share your data with other affiliated group companies pursuant to Section 15 et seq. of German Stock Corporation Act, which may process it for their own purposes as data controllers. Your data is only accessible to authorized persons and / or departments that have a legitimate reason to access and process it for the above purposes.

We use processors for the provision of special services. The transfer of your data to the processors is carried out in strict compliance with the obligation of confidentiality and the requirements of the GDPR. The processors appointed by us, who may only process the data for our and not for their own purposes, are obliged to comply with the requirements of the GDPR. In these cases, the responsibility for the data processing remains with us.

Recipients of your data may be, for example:

- Public bodies and institutions (e.g. tax authorities, law enforcement agencies) in the event of a legal or regulatory obligation;
- Insolvency administrators or creditors inquiring due to foreclosure;
- Auditors on the occasion of the audits of the annual financial statements;
- Service providers that we use in the context of data processing relationships;
- Affiliated companies within the Group as defined in sections 15 et seq. of the German Stock Corporation Act.

To the extent that these data recipients (affiliated companies or external entities/companies) are located in countries outside the European Union (EU) and the European Economic Area (EEA) that have not been recognised by the European Commission as having an adequate level of data protection, we ensure that appropriate safeguards are in place to ensure a comparable level of data protection, for example by concluding EU Standard Contractual Clauses of the European Commission with the respective data recipients.

How long will your data be stored

We process and store the personal data of our business partners as long as this is necessary for the fulfilment of our contractual and legal obligations arising from the existing business relationship. If your personal data is no longer required for the fulfilment of contractual or legal obligations, it is regularly deleted, unless commercial and tax retention obligations resulting from the German Commercial Code (Handelsgesetzbuch - *HGB*) and the German Tax Code (Abgabenordung - *AO*) (retention periods or documentation periods are, for example, ten years for accounting documents and six years for commercial or business letters) or the preservation of evidence within the statutory limitation periods (these limitation periods can be up to 30 years, whereby the regular limitation period is 3 years) requires its further processing for a limited period of time.

In addition, we will retain your personal data as long as necessary for other relevant processing purposes specified in this information.

Processing of your data in the context of our online events/meetings using Microsoft Teams

Thanks to the audio and video conferencing function, we can offer you participation in our online events/meetings via video/audio. For this purpose, we use Microsoft Teams to organise such online events/meetings. We process the following data as part of our online events/meetings:

- **Communication data**: e.g. your e-mail address, if you provide the eMail address a in personalized way;
- **Log files and log data**;
- **Meeting metadata**: e.g. date, time, meeting ID, telephone numbers, location;
- **User details**: e.g. display name, profile picture (optional) and preferred language;
- **Text, audio and video data**: it is possible to use the chat function in an online event/meeting. In this respect, the text entries made by the respective user are processed in order to display the online events/meetings. In order to enable the display of video and the playback of audio, the data from the microphone of your end device and from any video camera of the end device are processed accordingly for the duration of the online event/meeting. The camera or microphone can be switched off or muted by the user at any time via the Microsoft Teams applications;
- **Telemetry data**: this includes diagnostic data in connection with the use of the service, including transmission quality. This data is used for troubleshooting, securing, and updating the technical service and monitoring it; and
- **Personalising the background, participating in a meeting as an avatar and sharing content**: every user in online events/meetings has the option of personalising their background on a voluntary basis by uploading images, graphics, etc. This function is not intended to collect data. Furthermore, Microsoft Teams is not used to pass on content during an online event/meeting that contains special categories of data (e.g. health data, data on religious preferences, etc.). Avatars for Microsoft Teams make it possible to connect with your presence in Microsoft Teams without having to switch on your cameras. Users can present themselves as they wish to appear by selecting the specific avatar.

Our Microsoft Teams settings mean that no audio or video recordings are made of our online events/meetings. Transcriptions, live subtitles and sharing of the static or live location are also deactivated.

We process your personal data primarily for the fulfilment of contracts with you, or your company, or for the performance of pre-contractual measures (Art. 6 para. 1 lit. b) and f) GDPR), Furthermore, we process the data on the basis of our legitimate interest in accordance with Art. 6 para. 1 lit. f) GDPR. Our legitimate interest in processing your data is the organisation of our online events/meetings.

Microsoft Teams is a Microsoft Office 365 service. It is a productivity, collaboration and exchange platform. Microsoft Office 365 is a software product of the company

Microsoft Ireland Operations Limited
One Microsoft Place
South County Business Park
Leopardstown
Dublin 18
D18 P521 Irland
(hereinafter referred to as "***Microsoft***")

and is part of the Microsoft Office 365 cloud application, for which a user account must be created.

Data processing with Microsoft Office 365 takes place on servers in data centres in the EU. For this purpose, we have concluded a data processing agreement with Microsoft in accordance with Art. 28 GDPR. We have agreed on technical and organisational measures with Microsoft for Microsoft Office 365 that correspond to the current state of the art in IT security, e.g. with regard to access authorisation and end-to-end encryption concepts for data lines, databases and servers.

We have also implemented the "Customer Lock Box" functionality in Microsoft Office 365. This means that Microsoft cannot access our data in Microsoft Office 365.

It cannot be excluded that, in individual cases, companies affiliated with Microsoft outside the EU (so-called third countries) may obtain access to the data. Such third country transfers are only possible if there is an adequacy decision by the EU Commission, the controller or processor has provided appropriate safeguards to protect the personal data or one of the exceptions under Art. 49 GDPR applies. On 10 July 2023, the European Commission adopted an adequacy decision (EU-U.S. Data Privacy Framework - DPF) for transfers of personal data from the EU to companies in the USA. This means that from this date, data from companies in the EU can be transferred to companies in the USA covered by the adequacy decision without further additional guarantees. This adequacy decision only applies if the corresponding recipient of data in the USA is subject to the DPF and complies with the associated data protection obligations as part of a self-certification process. In these cases, a corresponding transfer of data to this recipient is considered as secure. Microsoft has a certification, which can be found here https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active. Although no further measures are required, we have also concluded the so-called standard contractual clauses with Microsoft as part of the das processing agreement. These represent a further guarantee for third country transfers.

Microsoft reserves the right to process customer data (which may include your data) for its own legitimate business purposes. We have no control over this data processing by Microsoft. To the extent that Microsoft Teams processes data in connection with its legitimate business purposes, Microsoft is an independent controller for these data processing activities and as such is responsible for compliance with all applicable data protection laws. If you require information about the processing by Microsoft, please refer to the relevant Microsoft statement (https://privacy.microsoft.com/de-de/privacystatement).

Your data in connection with the use of Microsoft Teams will generally be deleted if there is no need for further storage. In the case of statutory retention obligations, deletion will only be considered after the respective retention obligation has expired. Login data and IP addresses are deleted after 180 days at the latest.

Your rights (rights of data subjects)

You have extensive rights with regard to the processing of your data.

Right to information: You have the right to information about the data stored by us, in particular, for what purpose the processing is carried out and how long the data is stored (Art. 15 GDPR). This right is limited by the exceptions of Section 34 of the Federal Data Protection Act (Bundesdatenschutzgesetz – *BDSG*), according to which the right to information does not apply in particular if the data is stored only due to legal retention requirements or for data security and data protection control, the provision of information would require a disproportionate effort and a misappropriation of the data processing is prevented by appropriate technical and organisational measures.

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. This right is subject to the restrictions set out in Section 35 BDSG, according to which the right to erasure may be waived in particular if, in the case of non-automated data processing, there is a disproportionate effort for erasure and your interest in erasure is to be regarded as 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 personal 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 on grounds relating to your particular 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 para. 3 GDPR, you have the right to revoke your consent at any time. The revocation does not affect the lawfulness of the processing carried out on the basis of 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.

To exercise these rights, please contact the data protection officer (if appointed) or the person named above. If you submit a request for information and there is doubt regarding your identity, we may request information enabling us to satisfy ourselves as to your identity.

Status: 27.03.2024