

# BioFortis Privacy Shield Privacy Policy

---

## 1. OVERVIEW

This Privacy Policy applies to the processing of Personal Data that BioFortis receives about Individuals located in the European Economic Area (“EEA”). The purpose of this Privacy Policy is to demonstrate our commitment to the protection of Personal Data, including Personal Data transferred out of the EEA for the performance of our services and our business operations in the United States.

To support our efforts to ensure the protection of Personal Data, BioFortis complies with the EU-US Privacy Shield Framework issued by the US Department of Commerce, covering the collection, use, and retention of Personal Data collected from individuals in the European Union member countries.

BioFortis certifies that it adheres to the Privacy Shield Principles of notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, access, recourse, enforcement, and liability. If there is any conflict between this Privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles take precedence. The Federal Trade Commission (FTC) has jurisdiction over BioFortis’ compliance with the Privacy Shield Principles.

For more information about Privacy Shield, and to see our certification page, visit <https://www.privacyshield.gov>.

## 2. SCOPE

This Privacy Policy applies to all Personal Data BioFortis receives in the United States concerning individuals who reside in the European Union, including Personal Data of customers, suppliers, vendors, business contacts and partners, and government officials.

This Policy will help you understand how BioFortis collects, uses, discloses, and protects Individuals’ Personal Data and how you can contact BioFortis regarding how your Personal Data are handled.

This Privacy Policy does not cover data from which individuals cannot be identified, or data which has been de-identified (typically by having identifying information redacted or replaced with a code).

## 3. RESPONSIBILITIES AND MANAGEMENT

BioFortis has designated the Quality Management Department to oversee its compliance with the Privacy Shield Principles. The Quality Management Department shall review and approve any changes to this Privacy Policy as necessary.

BioFortis will monitor, maintain, and update its security policies and practices to assist in protecting the Personal Data it collects.

BioFortis personnel receive training, as applicable, to effectively implement this Privacy Policy.

For questions, concerns, or comments regarding this Privacy policy, please contact [support@biofortis.com](mailto:support@biofortis.com).

#### **4. RENEWAL/VERIFICATION**

BioFortis will renew its EU-US Privacy Shield Framework credentials annually, unless and until it determines that it no longer needs such certification or it employs a different adequacy mechanism.

Prior to the recertification, BioFortis will conduct an in-house verification to ensure that its attestations in regards to its treatment of Personal Data are accurate and that BioFortis has appropriately implemented these practices.

Specifically, BioFortis will:

- Review this Privacy Shield Privacy Policy and its Privacy Shield SOP to ensure they accurately describe the practices in the collection and processing of Personal Data
- Ensure that the publicly posted Privacy Policy informs clients of BioFortis' participation in the EU-US Privacy Shield program and how to obtain additional information.
- Ensure that this Privacy Shield Policy and the BioFortis Privacy Shield SOP continues to comply with the Privacy Shield Principles.
- Confirm that clients are made aware of the process for addressing complaints and the availability of an independent recourse mechanism (BioFortis may do this through this Privacy Policy, individual client contract, or both)
- Review its processes and procedures for training employees about BioFortis' participation in the EU-US Privacy Shield program and the appropriate handling of Personal Data

BioFortis will record the verification on the Privacy Shield Compliance Review Form.

#### **5. COLLECTION AND USE OF PERSONAL DATA**

BioFortis collects Personal Data from clients when they purchase its products or services, request information, or otherwise communicate with BioFortis. For example, BioFortis clients may contact the Support Department, or request access to a whitepaper from the website.

The Personal Data that BioFortis collects may vary based on the individual's interaction with BioFortis' website and request for services.

##### **5.1 Collecting Information**

###### **Providing Contracted Services**

BioFortis will collect contact information from your company's assigned project manager in order to determine client requirements, to provide demonstrations and updates, and to collect product approval. The contact information includes name, work title, email address, and telephone number.

###### **Business Contacts**

BioFortis may collect Personal Data concerning contact information for business contacts. The contact information includes name, work title, email address, and telephone number.

## **Billing**

BioFortis collects information from your company's contact for receiving invoices. The contact information includes name, work title, email address, and telephone number.

## **Sales and Marketing**

BioFortis collects information you provide for marketing purposes:

- Business cards provided to BioFortis representatives at conferences and expos
- Name, email, and telephone number information you provide through our website (when requesting whitepapers or other information)
- Other information you choose to provide (browser type, intended use of product)

BioFortis collects information for collecting contract and SOW approvals for BioFortis products and services, including name, work title, email address, and telephone number.

## **Support**

BioFortis collects name and email address from people contacting support by email. BioFortis collects name and telephone number from people contacting support by telephone.

Because of the nature of support, BioFortis may request additional information in order to help resolve the issue. This may include browser type, IP address, and any other information you choose to provide.

## **5.2 Using Information**

### **Providing Contracted Services**

BioFortis will use the collected information to provide and deploy the requested services and to otherwise fulfill contractual obligations (managing transactions, reporting, and other operations related to providing services to a client).

BioFortis may also use the collected information to inform contacts about product upgrades and new releases and BioFortis user events.

### **Business Contacts**

BioFortis will use the collected information for purposes consistent with the provision of information by these contacts, which may include marketing activities focused on sales.

### **Billing**

BioFortis will use the collected information for invoicing and renewal.

BioFortis may also use the collected information for satisfying government reporting, tax, and other financial information requirements.

### **Sales and Marketing**

BioFortis will use the collected information to provide information about BioFortis products, services, and events, such as user group meetings.

### **Support**

BioFortis will use the collected information to solve issues with the service, verify identity to provide access to BioFortis software, or as otherwise requested by the client.

### **Additional Use**

BioFortis uses the Personal Data it collects for the following business purposes, without limitation:

- Storing and processing data, including Personal Data, in computer databases and servers located in the US
- As requested by an individual client
- For other business-related purposes permitted or required under local law and regulation
- As otherwise required by law

## **6. DISCLOSURES/ONWARD TRANSFERS OF PERSONAL DATA**

Except as otherwise provided herein, BioFortis does not disclose Personal Data to Third Parties.

BioFortis may host BioFortis data, including collected Personal Data, on servers hosted by Third Parties, but the Third Parties do not have access to BioFortis data. BioFortis data hosting is covered by contractual agreements.

BioFortis is liable for appropriate onward transfers of Personal Data to Third Parties.

BioFortis also may disclose Personal Data for other purposes or to other Third Parties when that individual has requested such disclosure. Please be aware that BioFortis may be required to disclose an individual's Personal Data in response to a lawful request by public authorities, including to meet national security or law enforcement requirements.

In circumstances in which BioFortis obtains Personal Data as a service provider for its clients, BioFortis' clients are responsible for protecting individual rights with respect to onward transfers.

## **7. SENSITIVE DATA**

BioFortis does not collect Sensitive Data from clients.

In circumstances in which BioFortis-provided services maintain Sensitive Data entered on BioFortis-provided hosting, but input by clients, BioFortis' clients are responsible for collecting the appropriate consent from the individuals whose Sensitive Data are stored on BioFortis-provided servers.

## **8. DATA INTEGRITY AND SECURITY**

BioFortis uses reasonable efforts to maintain the accuracy and integrity of Personal Data and to update it as appropriate. BioFortis has implemented physical, technical, and procedural safeguards to protect Personal Data from loss, misuse, unauthorized access, disclosure, alteration, or destruction. For example, electronically stored Personal Data is stored on a secure network with firewall protection, and access to BioFortis' electronic systems requires user authentication via password. BioFortis also employs access restrictions, limiting the scope of employees who have access to

Personal Data. Despite these precautions, no data security safeguards guarantee 100% security all of the time.

## **9. NOTIFICATION**

BioFortis notifies clients about its adherence to the EU-US Privacy Shield Principles through its publicly posted Privacy Shield Privacy Policy, available at [www.biofortis.com/privacy-faq](http://www.biofortis.com/privacy-faq), within an individual client's contract, or both.

In circumstances in which BioFortis obtains personal data as a service provider for its clients or affiliates, BioFortis' clients or affiliates are responsible for providing appropriate notice to the individuals whose personal data are transferred to the U.S. and obtaining any requisite consent (unless this function has been delegated to BioFortis).

## **10. ACCESSING PERSONAL DATA**

BioFortis personnel may access and use Personal Data only if they are authorized to do so and only for the purpose for which they are authorized.

## **11. RIGHT TO ACCESS, CHANGE, OR DELETE PERSONAL DATA**

### **11.1 Right to Access**

Clients have the right to know what Personal Data about them is included in BioFortis records, and to ensure that such Personal Data is accurate and relevant for the purposes for which BioFortis collected it. Clients may review their own Personal Data and correct, erase, or block any data that is incorrect, as permitted by applicable law and BioFortis policies. Upon reasonable request and as required by the Privacy Shield Principles, BioFortis will provide clients with their collected Personal Data, in order to correct or amend such data where inaccurate. In making modifications to their personal data, clients must provide only truthful, complete, and accurate information. To request access to Personal Data, send an email to [support@biofortis.com](mailto:support@biofortis.com).

In circumstances in which BioFortis maintains personal data as a service provider for its clients, BioFortis' clients are responsible for providing Individuals with access to their personal data and the right to correct, amend or delete the data where it is inaccurate. In these circumstances, Individuals should direct their questions to the appropriate BioFortis client. If they do not receive a response, BioFortis will provide reasonable assistance in forwarding the Individual's request.

### **11.2 Requests for Personal Data**

BioFortis will track each of the following and will provide notice to the appropriate parties under law and contract when either of the following circumstances arise:

- Legally binding request for disclosure of the Personal Data by a law enforcement authority unless prohibited by law or regulation
- Requests received from the individual regarding their own Personal Data

### **11.3 Satisfying Requests for Access, Modification, and Corrections**

BioFortis will endeavor to respond in a timely manner to all reasonable written requests to view, modify, or inactivate Personal Data.

## 12. ENFORCEMENT AND DISPUTE RESOLUTION

In compliance with EU-US Privacy Shield Principles, BioFortis commits to resolve complaints about privacy and the collection or use of Personal Data. EU individuals with questions or concerns about the use of their Personal Data should contact [support@biofortis.com](mailto:support@biofortis.com).

If your question or concern cannot be satisfied through this process BioFortis has further committed to refer unresolved privacy complaints under EU-US Privacy Shield to an independent dispute resolution mechanism operated by JAMS. If a timely acknowledgement of a complaint is not received, or if the complaint is not satisfactorily addressed by BioFortis, EU individuals may contact JAMS using the following link: <https://www.jamsadr.com/file-an-eu-us-privacy-shield-or-safe-harbor-claim>.

Finally, as a last resort and in limited situations, EU individuals may seek redress from the Privacy Shield Panel, a binding arbitration mechanism.

## 13. CHANGES TO THIS PRIVACY POLICY

### 13.1 Modifications to this Policy

This Privacy Policy may be amended from time to time, consistent with Privacy Shield Principles and applicable data protection and privacy laws and principles. BioFortis personnel will be made aware of changes to this Privacy Policy by email or training sessions. BioFortis will notify clients of any changes that materially affect how previously collected Personal Data is handled, and will allow clients to choose whether their Personal Data may be used in any materially different manner.

### 13.2 Version History

Version	Effective Date	Reason for Change
01	March 31, 2017	New
02	May 25, 2018	Updates to comply with GDPR; clearer language and examples of the type of data we collect (Section 5)
03	April 01, 2019	Clarify client's responsibility when BioFortis provides hosting but does not collect information.

## 14. QUESTIONS OR COMPLAINTS

Any questions or complaints should be addressed to [support@biofortis.com](mailto:support@biofortis.com).

## 15. DEFINED TERMS

“European Economic Area” (EEA) means an internal market which is composed of the following thirty-one (31) countries: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Ireland, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands,

Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and United Kingdom.

“Personal Data” as defined under European Union Directive 95/46/EC means data that personally identifies or may be used to identify a person, including an individual’s name in combination with country of birth, marital status, emergency contact, salary information, terms of employment, job qualifications (such as educational degrees earned), address, phone number, email address, user ID, password, and identification numbers. Personal Data does not include information that is de-identified, anonymous, or publically available.

“Sensitive Data” means Personal Data that discloses an individual’s medical or health condition, race or ethnicity, political, religious, or philosophical affiliation or opinions, sexual orientation, or trade union membership.

“Third Party” means any individual or entity that is neither BioFortis or a BioFortis employee, agent, contractor, or representative.