XBiotech
Privacy Policy

XBiotech Inc. and XBiotech GmbH ("XBiotech") has adopted this Privacy Policy ("Policy") to establish and maintain an adequate level of Personal Data privacy protection. This Policy applies to the processing of Personal Data that XBiotech obtains from Individuals and Patients located in the European Union and Switzerland.

XBiotech complies with the US-EU Privacy Shield Framework and Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from Individual Patients in the European Union member countries and Switzerland. XBiotech has certified that it adheres to the Privacy Shield Privacy 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 the policies in this privacy policy and the Privacy Shield Privacy Principles, the Privacy Shield Privacy Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov/.

The Federal Trade Commission (FTC) has jurisdiction over XBiotech's compliance with the Privacy Shield. All XBiotech employees who handle Personal Data from Europe and Switzerland are required to comply with the Principles stated in this Policy.

Capitalized terms are defined in Section 14 of this Policy.

I. SCOPE

This Policy applies to the processing of Individual Personal Data that XBiotech receives in the United States concerning Individuals who reside in the European Union and Switzerland that are running or participating in XBiotech clinical study(ies). XBiotech is a biopharmaceutical company that is conducting clinical trials.

II. RESPONSIBILITIES AND MANAGEMENT

XBiotech has designated the Clinical Department to oversee its information security program, including its compliance with the EU and Swiss Privacy Shield program. The Clinical Department shall review and approve any material changes to this program as necessary. Any questions, concerns, or comments regarding this Policy also may be directed to privacy@XBiotech.com.

XBiotech will maintain, monitor, test, and upgrade information security policies, practices, and systems to assist in protecting the Personal Data that it collects. XBiotech personnel will receive training, as applicable, to effectively implement this Policy. Please refer to Section 6 for a discussion of the steps that XBiotech has undertaken to protect Personal Data.

Effective Date: 05 November 2018

III. RENEWAL/VERIFICATION

XBiotech will renew its US-EU Privacy Shield and Swiss-US Privacy Shield certifications annually, unless it subsequently determines that it no longer needs such certification or if it employs a different adequacy mechanism.

Prior to the re-certification, XBiotech will conduct an in-house verification to ensure that its attestations and assertions about its treatment of Individual Personal Data are accurate and that the company has appropriately implemented these practices. Specifically, as part of the verification process, XBiotech will undertake the following:

A. Review this Privacy Shield policy and its publicly posted website privacy policy to ensure that these policies accurately describe the practices regarding the collection of Individual Personal Data
B. Ensure that the publicly posted privacy policy informs Individuals of XBiotech's participation in the US EU Privacy Shield and US Swiss Privacy Shield programs and where to obtain a copy of additional information (e.g., a copy of this Policy)
C. Ensure that this Policy continues to comply with the Privacy Shield principles
D. Confirm that Individuals are made aware of the process for addressing complaints and any independent dispute resolution process (XBiotech may do so through its publicly posted website, Individual contract, or both)
E. Review its processes and procedures for training Employees about XBiotech's participation in the Privacy Shield programs and the appropriate handling of Individual's Personal Data

XBiotech will prepare an internal verification statement on an annual basis.

IV. COLLECTION AND USE OF PERSONAL DATA

XBiotech collects certain personal data from Individual Patients who participate in its clinical studies.

XBiotech may collect personal data from clinical site personnel, and employees, and personal sensitive information through clinical trials and general business activities. XBiotech takes appropriate action where unsolicited confidential data is received to prevent / minimize the risk of recurrence.

The information that we collect from Individual Patients is used for exploring the potential clinical benefit of XBiotech’s pipeline of therapeutic product candidates.

XBiotech does not disclose personal information to third parties for purposes that are materially different than what it was originally collected for. Should this change in the future, we will provide individuals with the option to opt-out.

V. DISCLOSURES/ONWARD TRANSFERS OF PERSONAL DATA

Except as otherwise provided herein, XBiotech discloses Personal Data only to Third Parties who reasonably need to know such data only for the scope of the execution of the clinical study and not for other purposes. Such recipients must agree to abide by confidentiality obligations.

XBiotech may provide Personal Data to Third Parties that act as agents, consultants, and contractors to perform tasks on behalf of and under our instructions. For example, XBiotech may outsource database management and/or processing of patient lab testing to Third Parties. Such Third Parties must agree to use such Personal Data only for the purposes for which they have been engaged by XBiotech and they must either:

A. comply with the Privacy Shield principles or another mechanism permitted by the applicable EU & Swiss data protection law(s) for transfers and processing of Personal Data;
B. or agree to provide adequate protections for the Personal Data that are no less protective than those set out in this Policy;

XBiotech also may disclose Personal Data for other purposes or to other Third Parties when a Data Subject has consented to or requested such disclosure. Please be aware that XBiotech may be required to disclose an individual's personal information in response to a lawful request by public authorities, including to meet national security or law enforcement requirements. XBiotech is liable for appropriate onward transfers of personal data to third parties.

VI. SENSITIVE DATA

An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is:

i. in the vital interests of the data subject or another person;
ii. necessary for the establishment of legal claims or defenses;
iii. required to provide medical care or diagnosis;
iv. carried out in the course of legitimate activities by a foundation, association or any other non-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;
v. necessary to carry out the organization’s obligations in the field of employment law; or
vi. related to data that are manifestly made public by the individual.

VII. DATA INTEGRITY AND SECURITY

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

Further, XBiotech uses secure encryption technology to protect certain categories of personal data. Despite these precautions, no data security safeguards guarantee 100% security all of the time.

VIII. NOTIFICATION

XBiotech notifies Individuals about its adherence to the EU-US Privacy Shield and Swiss-US Privacy Shield principles through its publicly posted website privacy policy, available at: http://www.xbiotech.com/downloads/XBiotech_Privacy_Policy.pdf.

IX. ACCESSING PERSONAL DATA

XBiotech 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.

X. RIGHT TO ACCESS, CHANGE OR DELETE PERSONAL DATA

A. Right to Access. Individuals have the right to know what Personal Data about them is included in the databases and to ensure that such Personal Data is accurate and relevant for the purposes for which XBiotech collected it. Individuals may request to review their own Personal Data stored in the databases and request correction, erasure, or deletion of any data, as permitted by applicable law and XBiotech policies. Upon reasonable request and as required by the Privacy Shield principles, XBiotech allows Individual Patients access to their Personal Data, in order to correct or amend such data where inaccurate. Individual Patients may request access by contacting XBiotech by phone or email. To request access of Personal Data, Individual Patients should submit a written request to XBiotech by emailing privacy@xbiotech.com.

B. Requests for Personal Data. XBiotech 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: (a) legally binding request for disclosure of the Personal Data by a law enforcement authority unless prohibited by law or regulation; or (b) requests received from the Data Subject or Individual.

C. Satisfying Requests for Access, Modifications, and Corrections. XBiotech will endeavor to respond in a timely manner to all reasonable written requests to view, modify, or inactivate Personal Data.

XI. CHANGES TO THIS POLICY

This Policy may be amended from time to time, consistent with the Privacy Shield Principles and applicable data protection and privacy laws and principles. We will make employees available of changes to this policy either by posting to our intranet, through email, or other means. We will notify Individuals if we make changes that materially affect the way we handle Personal Data previously collected, and we will allow them to choose whether their Personal Data may be used in any materially different manner.

XII. QUESTIONS OR COMPLAINTS

EU and Swiss Individuals may contact XBiotech with questions or complaints concerning this Policy at the following address:

privacy@xbiotech.com

XIII. ENFORCEMENT AND DISPUTE RESOLUTION

In compliance with the US-EU and Swiss-US Privacy Shield Principles, XBiotech commits to resolve complaints about your privacy and our collection or use of your personal information. EU and Swiss individuals with questions or concerns about the use of their Personal Data should contact us at: privacy@xbiotech.com.

Effective Date: 05 November 2018

If an Individual's question or concern cannot be satisfied through this process XBiotech has further committed to refer unresolved privacy complaints under US-EU Privacy Shield and Swiss-US Privacy Shield to an independent dispute resolution mechanism operated by the Council of Better Business Bureaus. Dispute resolution will address complaints and provide appropriate recourse free of charge to the individual.

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

XBiotech commits to cooperate with EU and Swiss data protection authorities (DPAs) and comply with the advice given by such authorities with regard to human resources data transferred from the EU and Switzerland in the context of the employment relationship.

XIV. PHARMACEUTICAL AND MEDICINAL PRODUCTS

a. Application of EU Member State Laws/GDPR or the Privacy Shield Principles
   i. EU Member State law/General Data Protection Regulation (GDPR) applies to the collection of the personal data and to any processing that takes place prior to the transfer to the United States. The Privacy Shield Principles apply to the data once they have been transferred to the United States. Data used for pharmaceutical research and other purposes should be anonymized when appropriate.

b. Future Scientific Research
   i. Personal data developed in specific medical or pharmaceutical research studies often play a valuable role in future scientific research. Where personal data collected for one research study are transferred to a U.S. organization in the Privacy Shield, the organization may use the data for a new scientific research activity if appropriate notice and choice have been provided in the first instance. Such notice should provide information about any future specific uses of the data, such as periodic follow-up, related studies, or marketing.
   ii. It is understood that not all future uses of the data can be specified, since a new research use could arise from new insights on the original data, new medical discoveries and advances, and public health and regulatory developments. Where appropriate, the notice should therefore include an explanation that personal data may be used in future medical and pharmaceutical research activities that are unanticipated. If the use is not consistent with the general research purpose(s) for which the personal data were originally collected, or to which the individual has consented subsequently, new consent must be obtained.

c. Withdrawal from a Clinical Trial
   i. Participants may decide or be asked to withdraw from a clinical trial at any time. Any personal data collected previous to withdrawal may still be processed along with other data collected as part of the clinical trial, however, if this was made clear to the participant in the notice at the time he or she agreed to participate.

d. Transfers for Regulatory and Supervision Purposes

i. Pharmaceutical and medical device companies are allowed to provide personal data from clinical trials conducted in the EU to regulators in the United States for regulatory and supervision purposes. Similar transfers are allowed to parties other than regulators, such as company locations and other researchers, consistent with the Principles of Notice and Choice.

e. "Blinded" Studies

i. To ensure objectivity in many clinical trials, participants, and often investigators as well, cannot be given access to information about which treatment each participant may be receiving. Doing so would jeopardize the validity of the research study and results. Participants in such clinical trials (referred to as "blinded" studies) do not have to be provided access to the data on their treatment during the trial if this restriction has been explained when the participant entered the trial and the disclosure of such information would jeopardize the integrity of the research effort.

ii. Agreement to participate in the trial under these conditions is a reasonable forgoing of the right of access. Following the conclusion of the trial and analysis of the results, participants should have access to their data if they request it. They should seek it primarily from the physician or other health care provider from whom they received treatment within the clinical trial, or secondarily from the sponsoring organization.

f. Product Safety and Efficacy Monitoring

i. A pharmaceutical or medical device company does not have to apply the Privacy Shield Principles with respect to the Notice, Choice, Accountability for Onward Transfer, and Access Principles in its product safety and efficacy monitoring activities, including the reporting of adverse events and the tracking of patients/subjects using certain medicines or medical devices, to the extent that adherence to the Principles interferes with compliance with regulatory requirements. This is true both with respect to reports by, for example, health care providers to pharmaceutical and medical device companies, and with respect to reports by pharmaceutical and medical device companies to government agencies like the Food and Drug Administration.

g. Key-coded Data

i. In certain instances, some research data may be uniquely key-coded at their origin by the principal investigator so as not to reveal the identity of individual data subjects. Pharmaceutical companies sponsoring such research do not receive the key. The unique key code is held only by the researcher, so that he or she can identify the research subject under special circumstances (*e.g.*, if follow-up medical attention is required). A transfer from the EU to the United States of data coded in this way would not constitute a transfer of personal data that would be subject to the Privacy Shield Principles.

XV. DEFINED TERMS

Capitalized terms in this Privacy Policy have the following meanings:

"Individual " means an Individual from EU or Switzerland. The term also shall include any individual patient, or an individual connected with the collection of data where XBiotech has obtained his or her personal data as part of its business relationship with XBiotech.

"Data Subject" means an identified or identifiable natural living person. An identifiable person is one who can be identified, directly or indirectly, by reference to a name, or to one or more factors unique to his or her personal physical, psychological, mental, economic, cultural or social characteristics. For Patients residing in Switzerland, a Data Subject also may include a legal entity.

"Employee" means an employee (whether temporary, permanent, part-time, or contract), former employee, independent contractor, or job applicant of XBiotech or any of its affiliates or subsidiaries, who is also a resident of a country within the European Economic Area.
"Europe" or "European" refers to a country in the European Union.

“Personal data” and “personal information” are data about an identified or identifiable individual that are within the scope of the Directive, received by an organization in the United States from the European Union, and recorded in any form.

"Sensitive Data" means Personal Data that discloses a Data Subject's medical or health condition, race or ethnicity, political, religious or philosophical affiliations or opinions, sexual orientation, or trade union membership.

"Third Party" means any individual or entity that is neither XBiotech nor an XBiotech employee, agent, contractor, or representative.