EU-US Privacy Shield

Last updated January 31, 2021

Privacy Shield Policy

1. EU-U.S. Privacy Shield Policy

Valis Biosciences, Inc. (Valis Bioscience) respects the privacy of its customers, employees, business partners, individuals whose personal information with which we are entrusted, and others. Valis Bioscience collects and uses any collected personal health information in accordance with the laws and regulations of the countries in which the information is collected, and in which it does business.

Valis Bioscience complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. Valis Bioscience has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view ourcertification, please visit https://www.privacyshield.gov/

2. PURPOSE

In the course of our business, it is necessary for us to access, collect, process, use, transmit, disclose, store and otherwise handle personal data (defined below) about individuals. This Policy provides the basis for protecting such data while ensuring compliance with legal requirements. The United States Department of Commerce, and the European Commission,have agreed on a set of data protection principles and frequently asked questions (the "EU-U.S. Privacy Shield") to enable U.S. companies to satisfy the requirement under European Union law that adequate protection be given to personal information transferred from the EUand from the United Kingdom to the United States. The EEA also has recognized the EU-U.S. Privacy Shield as providing adequate data protection.

3. SCOPE

This Policy applies to all personal data accessed, collected, processed, used, transmitted, disclosed, or stored (hereinafter collectively referred to as "processed") in any format including electronic, paper or verbal by Valis Bioscience. All employees, whether permanent,temporary or on contract or third parties working on behalf of us shall adhere to this Policy.

4. POLICY

We are committed to using reasonable commercial measures to ensure the safeguarding of personal data of individuals and that such data is used only as intended and that precautions preventing misuse are both effective and appropriate. Personal data must therefore be:

(a) Accessed, used and disclosed fairly and lawfully;

(b) Obtained for specified business and/or legal purposes and not used or disclosed in away which is incompatible with the purpose(s) for which it was collected;

(c) Adequate, relevant and not excessive for the purpose(s) for which it is collected or maintained;

(d) Accurate and, where necessary, kept up to date;

(e) Not kept for longer than is necessary to fulfill the purpose(s) it is used for, subject to the Company's document retention policy;

(f) Used and disclosed in accordance with relevant legal requirements;

(g) Appropriately protected against unauthorized, inadvertent, or illegal access, use and/or disclosure through administrative, technical, and physical safeguards; and

(h) Restricted to designated countries unless the rights and freedom of individuals are protected therein.

We will strive to prevent breaches of personal data security and will notify individuals of a breach of personal data if the law so requires. We will train our employees regarding the safeguarding of personal data. We will update this Privacy Policy as necessary to comply with legal standards. Breach of legal requirements concerning personal data may result in censure, enforcement proceedings, fines, and/or damages. It may also result in personal liability for our employees and/or officers, adverse publicity and damage to our reputation, brand or to commercial interests. The Privacy Officer, who will report on compliance with thisPrivacy Policy, will manage all data privacy policies, procedures, and issues. All employees are required to support the Privacy Officer discharging obligations for protecting data privacy.

5. WHAT PERSONAL DATA MAY BE COLLECTED?

We may collect the following examples of personal data: full name, address, telephone or mobile number, business and home contact details including e-mail addresses and telephone numbers, health information, video information including images of a user's face,audio information, and demographic information. Personal data may further include any information that identifies an individual, but does not include information that has been encoded, encrypted, or otherwise anonymized.

Data that may be collected will be used for the purpose of supporting clinical research or programs supporting population health management, and for maintaining and improving Company internal systems and offerings.

6. HOW WE COLLECT PERSONAL DATA AND HOW IT IS USED

We collect personal data to the extent necessary to establish and manage our relationship with our employees, customers, and contractors and to perform any related functions. We may also collect personal data through information technology when users are interacting with Company offerings, and other communications systems used to assist with the performance and administration of Human Resources activities, customer and other business functions, as well as to implement our hardware and software solutions related to electronic clinical outcomes assessments, training on assessments and procedures and monitoring of study visits with clinical trials. These systems may be updated from time to time and interface with each other to share and update any personal data they hold. Some of the personal data that we maintain will be kept in paper files, while other personal data will be included in computerized files and electronic databases as described in the protection of personal data section of this Privacy Policy below. Employees or potential employees will be advised of the Company's Privacy Policy. We may also access, use, process or disclose customer and contractor personal data during the course of conductingour business. We take reasonable steps to ensure that data we collect from our employees,customers and contractors is reliable for its intended use, accurate, complete, and current.

7. DISCLOSURE OF PERSONAL DATA

Personal data may be made available for the purposes mentioned above to responsible management, human resources, accounting, audit, compliance, legal, information technology and other corporate staff who need to know these details for their functions within the Company, including maintenance and improvement of Company offerings, some of which may not be based in the US. The identity of personnel within the Company having access to personal data shall be controlled on the basis of business and security requirements, shall be consistent with the job requirements of such person having access, and shall be modified to the extent their job requirements change. Employees with access topersonal data shall be made aware of their responsibilities for maintaining the privacy of that information, particularly regarding the protection of both hard-copy, soft-copy, and electronic information. Personal data may also be made available to third parties providing relevant services under contract to us (see the protection of personal data section of this Policy below for further details), such as auditors and compliance managers, background verification, legal and IT hosting and maintenance providers. We must have appropriate security and privacy measures in place with such third parties covering how they hold and maintain any personal data that we provide to them.

Certain personal data will also be reported to government and regulatory authorities where required by law and for tax or other purposes. Personal data may also be released to external parties as required or permitted by employment or other statutes and regulations, or by legal process, as well as to parties to whom an individual authorizes us to release theirpersonal data. Personal data may also be used internally to improve Company solutions, or otherwise improve Company's overall service offerings, the privacy of such data being maintained according to the terms of this Policy. We will not sell any personal data to any third party other than as part of any restructuring of the Company or sale of a relevant Company business. If we do provide any data to a third party, we will enter into a written

agreement with the third party that requires the third party provide at least the same level of privacy and security protections as is implemented by Company.

Valis Bioscience may be forced to disclose an individual's personal information when compelled by a lawful request made by a recognized public authority or where required to meet national security and or law enforcement requirements. Valis Bioscience is subject tothe investigatory and enforcement powers of the Federal Trade Commission ("FTC") and orthe Food and Drug Administration ("FDA").

Personal Information may be shared with third party business entities. The entities to whomValis Bioscience may disclose personal information includes, but it is not limited to clinical trial sponsors and or their contracted agents as well as public health entities including but not limited to local, state or national health organizations.

In cases of onward transfer to third parties of data of EU or United Kingdom individualsreceived pursuant to the EU-US Privacy Shield, Valis Bioscience is potentially liable.

8. PROTECTION OF PERSONAL DATA

We are committed to ensuring that personal data is secure. To prevent unauthorized loss, alternation, destruction, access, use or disclosure, we have put in place and will maintain suitable physical, administrative and technical safeguards to secure the data we process. Where appropriate and consistent with the risk, personal data shall be kept securely. Accessto information systems containing personal data shall be controlled, at a minimum, by an individual user identification and password with appropriate requirements for re-logging after passage of an inactive time and/or use of password-protected screensavers. Firewall protection and operating system patches shall be installed on all computers containing personal data. Up-to-date versions of security agency software, including malware, patches and antivirus and pest patrol shall be installed on all computers containing personal data.
All items of equipment containing storage media shall be checked to ensure that any personal data has been removed or securely overwritten prior to disposal. Personal data that is transmitted across public networks or wirelessly or stored on portable devices shallbe encrypted.

Appropriate contractual arrangements shall be implemented for the responsibility and physical protection of personal data when such information is made available to third parties. Personal data, other than that normally required by mobile users, shall only be taken off site, as necessary. Any member of staff using personal data when working from home or during off-site meetings should take necessary precautions to ensure its security, including not leaving such information unattended. Any member of staff dealing with telephone inquiries should be careful about disclosing any personal information held by us.

Any individuals who are provided with access to personal data may only use such information for the purposes set out in this Privacy Policy (or as otherwise notified from timeto time) taking steps to provide reasonable safeguards to protect the personal information at all times. Access to personal data by terminated employees shall be promptly withdrawn. Employees who have access to personal information will be trained on privacy and security

measures. Unless required to be reported to government or regulatory authorities, sensitive personal data, as defined below will not be disclosed without the express written consent ofthe individual (which may be given by acknowledgement of policies setting out such disclosure requirements). Personal data shall be retained and destroyed in accordance withthe Company's data retention policies.

Sensitive personal data is defined as an individual's first name and last name or first initialand last name in combination with one or more the following data elements that relate to such individual: Substance abuse treatment; Alcohol abuse treatment; HIV/Aids; Genetic Information; and Information related to sexually transmitted diseases.

Individuals whose personal information has been collected by Valis Bioscience shall havethe right to access that data for review, modification or deletion. Access to review, modifyand or delete personal information or otherwise manage the use and disclosure of your personal data may be initiated by contacting Valis Bioscience:

Valis Bioscience
Attn: Christian Yavorsky, Senior Management1426
Parker Street
Berkeley, CA 94702
United States
Phone: (925)338-0000
help@valisbioscience.com

Valis Bioscience will follow their corporate approved policies and procedures when handlingany personal data requests.

9. ACCESS TO PERSONAL DATA

Individuals may opt out of providing personal data, upon request. To the extent that personaldata has been collected, individuals have the right to review personal data held about them and have certain inaccurate information corrected, unless the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated. If you wish to do so, or to notify us of a change in your details, please contact the Privacy Officer.

A formal request from an individual for information that we hold about them must be made in writing. A fee is payable by the data subject for provision of this information. Any member of staff who receives a written request should forward it to the Privacy Officer immediately.

10. NOTICE

In addition to this posting, we will provide either a copy of this Privacy Policy or a separate privacy notice to each employee, customer and contractor if we collect and use informationfrom them, which will include the type of information we collect, our Company's contact information for any inquiries or complaints, the identity of third parties to which we will

disclose the information, and the choices and means that we offer individuals for limitinguse and disclosure of their information upon request.

11. CHANGES TO THIS EU-U.S. PRIVACY SHIELD POLICY

This policy may be amended from time to time, consistent with the requirements of the Privacy Shield Framework. A notice will be posted on the Valis Bioscience web page (www.valisbioscience.com/eu-us-privacy-shield) for 60 days whenever this policy is changedin a material way.

12. EFFECTIVE DATE

This policy became effective on 31JAN2021 and was last updated on 31JAN2021.

13. INDEPENDENT RECOURSE FOR PRIVACY COMPLAINTS

In compliance with the Privacy Shield Principles, Valis Bioscience commits to resolve complaints about our collection or use of your personal information. EU individuals withinquiries or complaints regarding our Privacy Shield policy should first contact Valis Bioscience at:

Valis Bioscience
Attn: Christian Yavorsky, Senior Management1426
Parker Street
Berkeley, CA 94702
United States
Phone: (925)338-0000
help@valisbioscience.com

Valis Bioscience has further committed to cooperate with the panel established by theEU data protection authorities (DPAs) with regard to unresolved Privacy Shield complaints concerning data transferred from the EU.

Under certain limited conditions it is possible to seek recourse through last resort binding arbitration. Please note the name of the website or other online resource to which you provided the information, as well as the nature of the information that you provided. Valis Bioscience will use reasonable efforts to respond promptly to requests, questions or concerns you may have regarding our use of personal information about you. Except where required by law, the Company cannot ensure a response to questions or comments regarding topics unrelated to this Policy or our privacy practices.