

THE PHARMACEUTICAL SECURITY INSTITUTE, INC.

Last updated: September 2026

Privacy Statement

The Pharmaceutical Security Institute, Inc. ("**PSI**" or "**we**") is a membership organization whose activities implicate efforts to remedy the Counterfeiting and distribution of pharmaceuticals in violation of law ("**Counterfeiting**"), through interaction with its members and coordination as need be with governments, medical control agencies, and law enforcement and other authorities.

PSI respects your privacy and provides this Privacy Statement to inform you particularly of our privacy practices and choices you can make about the way your Personal Data is collected and how that information is used as well as your privacy rights. "**Personal Data**" means any information relating to an identified or identifiable natural person.

PSI operates the publicly available website psi-inc.org ("**Website**"). The Website also includes a dedicated section reserved for members (the "**Member Area**") which member representatives can access with their login information.

PSI complies with the EU-U.S. Data Privacy Framework ("**EU-U.S. DPF**") and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework ("**Swiss-U.S. DPF**") (altogether "**DPF Programs**") as set forth by the U.S. Department of Commerce. PSI has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles ("**EU-U.S. DPF Principles**") with regard to the processing of Personal Data received from the European Union ("**EU**") and the United Kingdom ("**UK**") in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. PSI has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of Personal Data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this Privacy Statement and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles (altogether the "**DPF Programs Principles**"), the DPF Programs Principles shall govern. To learn more about the Data Privacy Framework (DPF) Program and to view PSI's current certification, please visit the Data Privacy Framework website (<https://www.dataprivacyframework.gov/>) and search for The Pharmaceutical Security Institute, Inc. in the Data Privacy Framework List. PSI will respond to verified requests concerning Personal Data in accordance with applicable law and the DPF Program Principles.

PSI is the data controller who is responsible for the processing of your Personal Data as described in this Privacy Statement, unless states otherwise in the following.

Table of Contents

1. Notice	3
1.1. Information Collected and Stored Automatically on Our Website	3
1.2. Personal Data Otherwise Processed on Our Website	4
1.3. Personal Data Provided to and Processed by PSI About Alleged Counterfeiting Incidents	8
1.4. Personal Data Processed as Part of Our E-Mail Correspondence with You	9
1.5. Disclosures of Your Personal Data Including Onward Transfers Under the DPF Programs	10
1.6. International Transfers of your Personal Data	12
1.7. Inquiries and Complaints	13
2. Choice Under the DPF Programs	144
2.1. Opt Out for Different Scenarios	14
2.2. Opt In Regarding Sensitive Information	14
3. Security	14
4. Retention Periods	15
5. Your Rights in Relation to Your Personal Data	15
5.1. Your Rights Under Applicable Privacy Law	15
5.2. Your Rights Under the DPF Programs	17
6. Recourse and Enforcement under the DPF Programs	17
6.1. Independent Dispute Resolution Procedure	17
6.2. DPF Programs Verification	18
6.3. Remedies and Sanctions	18
6.4. Possibility to Invoke Arbitration	18
6.5. Jurisdiction of the Federal Trade Commission	18
7. Other Provisions	18
7.1. Notice and Procedure for Making Claims of Copyright Infringement	18
7.2. Counter Notification	19
8. Disclaimer	20
9. Modification of This Website's Privacy Statement and Terms of Use	20
10. Contact Information	21

1. Notice

1.1. Information Collected and Stored Automatically on Our Website

PSI does process and store information automatically collected on its Website.

1.1.1. Cookies

A "cookie" is a file placed on your computer's hard drive or in its memory by a website that can possibly be used for different purposes, such as, to recognize you when you come back to a website, to maintain your settings on a website (such as the language settings), to prevent a security incident or fraud, or to monitor your use of a website. PSI particularly uses cookies for security and safety reasons as well as to ensure the proper and effective functioning of our Website, including to establish state and flow control for applications accessible over the web as specified in the following.

1.1.2. Descriptions On Our Related Data Processing Activities

PSI uses cookies for website security purposes (including for the protection from unauthorized use, fraud, abuse, and malicious attacks on our Website). Cookies also ensure that this Website including its functions remain available to, function properly, and can be used effectively by all visitors. We may monitor network traffic to identify unauthorized attempts to (i) upload or change information, or (ii) access your account in the Member Area, or otherwise cause damage or engage in criminal or unauthorized activity. Additionally, we will use a cookie to keep you logged in to the Member Area, so you will not have to reenter your login information.

You may also benefit from our use of cookies for the aforementioned purposes to us as they enable you to properly, safely, and securely use our Website and its functionalities.

In general, we rely on our IT service provider Wix regarding our aforementioned use of cookies. We have engaged Wix regarding the hosting and provision of our Website including its functionalities via its the cloud solution. This also includes the placing of cookies on your device and the accessing of them later on. Different cookies will be used for the aforementioned purposes. In the majority of cases, the duration of the cookies is the duration of the session of your website visit, whereas some of the cookies may be stored for a longer period of time until they have fulfilled their respective purpose. Our use of cookies may include the processing of data categories, such as identifier, URL of the accessed website and the referral website, IP address, operating system, device settings, browser and the implemented settings and plug ins, certain usage activities and interactions on our Website, usage duration, loaded content, screen resolution, information related to your login and use of our Member Area.

For the duration of the processing of data as such by PSI itself in relation to cookies, please see Section 4 below.

Unauthorized attempts to upload or change information, or otherwise cause damage to this Website, are strictly prohibited and may be punishable under applicable law.

Except for visitors who voluntarily provide PSI with Personal Data and users of our Members Area, and except for the aforementioned purposes, PSI will not attempt to discover the identify of individual visitors to this Website or their usage habits while visiting this Website.

1.1.3. Legal Bases for Our Data Processing Activities

If you are located in the European Economic Area ("**EEA**") or UK, or your Personal Data is (otherwise) governed by their privacy laws, the following applies:

For PSI's own processing activities regarding the storing of data on your device via cookies or the accessing of such data on your device, we rely on the legal basis pursuant to Art. 5 para. 3 s 2 of the Directive 2002/58/EC as amended by the Directive 2009/136/EC (ePrivacy Directive) in conjunction with the respectively implementing provision under applicable EEA Member State law which allows for processing for the purpose of carrying out the transmission of a communication, or as strictly necessary in order for us to provide the requested service to you. For our related subsequent processing activities of Personal Data, we rely on the legal basis of the legitimate interests pursued by PSI or by a third party pursuant to Art. 6 para 1 s 1 lit. f EU and UK General Data Protection Regulation ("**GDPR**"). The relevant legitimate interests correspond with the purposes and interests described under Section 1.1.2 above.

1.2. Personal Data Otherwise Processed on Our Website

Personal Data may be collected or provided to PSI via the contact form on our Website as well as processed by us under the Member Area of our Website and we may process such Personal Data as described in the following.

1.2.1. Descriptions on Our Related Personal Data Processing Activities

1.2.1.1. Website Contact Form

You can send us a message via our Website contact form. You are free to use the contact form and provide us with the information you want under the "*Subject*" and the "*Message*" - fields. If you decided to use the contact form, we need you to provide us with your name and e-mail address which enables us to get back to you regarding your inquiry and properly deal with it.

PSI generally processes Personal Data under our contact form for the purpose of giving you the opportunity to contact us regarding your inquiries as well as for us to communicate with you in relation thereto while we may also share information with our members if this is necessary to respond to and deal with your inquiry. If you use the Website contact form to provide us with information about alleged Counterfeiting incidents and related activities, the descriptions under Section 1.3 below apply in relation to the related processing.

1.2.1.2. Website Member Area

If you are a representative of one of PSI's members, you may also use our Website's Member Area which may involve the following processing activities.

1.2.1.2.1. Registration, Account Information, and General Use of the Member Section

You are not obligated to register and use the Member Area and its embedded dashboard with incident summaries (the "**Dashboard**") section but if you decide to do so, this requires you to respectively sign up to the Member Area and its Dashboard

section. Hereby, we need certain information from you, including particularly your login information including your e-mail address and password, to allow you to safely access and use the Member Area including its Dashboard section, whereas the password of this section differs from the Member Area as such.

PSI generally processes this Personal Data to verify your authorization to use the Members Area, including its Dashboard section, as well to ensure that it remains safe and secure including regarding your access and use of our Member Area, including its Dashboard section.

Under the "*My Account*" section of the Member Area you can update the e-mail address or password used for the Member Area.

Your use of our Member Area which particularly enables us to provide you with relevant information about our activities and allows you to provide us with your input and communicate with us in relation thereto.

The general processing related to our Member Area may involve data categories, such as your name, e-mail address, company, password, information on your use of our Website's Member Area (including your join date)

If you provide us with information about alleged Counterfeiting incidents and related activities, the descriptions under Section 1.3 below apply in relation to the related processing. If you otherwise correspond with us via e-mail, the descriptions under Section 1.4 below apply in relation to the related processing.

You can find further information on the processing of Personal Data by PSI in relation to specific parts of the Member Area in the following. Information on the processing of Personal Data in relation to the Member Area's Dashboard section can be found under Section 1.3 below.

1.2.1.2.2. Resource Request Form

You can send us a message via the "*Resource Request Form*" under the "*Resources*" section in our Member Area. You are free to use the form and provide us with the information / request you want under the "*Subject*" and the "*Type your message here ...*" - fields. If you decide to use the contact form, we need your name and e-mail address so that we can identify and process your request.

We then use your Personal Data to fulfil your request and engage with you in relation thereto. We may also share information with our members if necessary to respond to and deal with your request.

1.2.1.2.3. Monthly Member Reports

Under the "*Monthly Member Reports*" section of our Member Area, we provide our member representatives with monthly reports about our relevant activities which may also include related information about PSI Directors and Officers.

PSI generally processes this Personal Data to keep our member representatives informed about our activities.

1.2.1.2.4. Registration for Events

The aforementioned monthly reports under the "*Monthly Member Reports*" section of our Member Area may also mention upcoming events for whom member representatives can register. The monthly report will then include a link to an online form.

You are free to use the form and register for an event. If, however, you want to register, we mandatorily need some information about you and your attendance, including your name, e-mail address, company, and whether you want to attend in person or virtually (where applicable) which we then use to facilitate your event attendance, to properly prepare and organize these events, and to communicate with you in relation to your registration and attendance of the event.

1.2.1.2.5. Member Directory

Under the "*Member Directory*" section of our Member Area, we list all the PSI Directors and Officers as well as other Member Representatives. This list generally includes the name, position at PSI, his/her respective company, business postal and e-mail address, and phone number for each individual.

We use such information to provide all member representatives with relevant information about all of the listed individuals and to give them the opportunity to contact these individuals.

1.2.1.2.6. Subject Matter Expert (SME) Directory

Under the "*Subject Matter Expert (SME) Directory*" section of our Member Area, PSI provides member representatives with information regarding designated subject matter experts affiliated with PSI member companies. This information may include an individual's name, employer, professional title, areas of expertise, professional background and qualifications, business e-mail address, business telephone number, and other business contact information that has been provided for inclusion in the SME Directory.

PSI generally processes this Personal Data for the purpose of facilitating collaboration, information exchange, professional consultation, and member engagement among authorized representatives of PSI member organizations. The SME Directory enables member representatives to identify and communicate with individuals possessing specialized expertise relevant to pharmaceutical security, counterfeit prevention, investigations, regulatory matters, supply chain security, and related subject areas.

The information contained in the SME Directory is intended solely for use by authorized PSI member representatives and may not be used for marketing, solicitation, or any unrelated commercial purpose.

1.2.1.2.7. Q&A Forum

Under the "*Q&A Forum*" section of our Member Area, authorized member representatives may submit questions, comments, responses, and other content concerning subject areas designated by PSI. The Q&A Forum serves as a moderated discussion platform intended to facilitate information sharing, professional dialogue, and collaboration among PSI members.

When you participate in the Q&A Forum, PSI may process Personal Data including your name, employer, position, business contact information, user account information, questions submitted, responses posted, comments made, attachments submitted, and information relating to your participation in forum discussions.

All questions, comments, responses, and other submissions are subject to review by authorized PSI personnel before publication. PSI conducts such reviews for the purpose of ensuring compliance with applicable usage rules, maintaining the integrity of the forum, protecting confidential information, promoting appropriate discussions, and preventing the posting of content that violates applicable law, PSI policies, or the rights of third parties.

PSI generally processes this Personal Data for the purposes of administering and operating the Q&A Forum, facilitating member communications and collaboration, responding to member inquiries, maintaining records of forum activity, enforcing forum rules, and protecting the security and integrity of PSI's systems and services.

PSI reserves the right to decline, remove, edit, restrict access to, or archive content submitted to the Q&A Forum where PSI reasonably determines that such content violates forum rules, applicable law, confidentiality obligations, intellectual property rights, or the interests of PSI and its members.

1.2.2. Legal Bases for Our Personal Data Processing Activities

If you are located in the EEA or UK, or your Personal Data is (otherwise) governed by their privacy laws, the following applies:

1.2.2.1. Website Contact Form

The legal basis for our processing of Personal Data via the contact form on our Website and any follow up communication with you is the legitimate interests pursued by PSI or by a third party, particularly, our members, pursuant to Art. 6 para 1 s 1 lit. f EU and UK GDPR. The relevant legitimate interests correspond with the purposes and interests described under Section 1.2.1.1 above.

1.2.2.2. Website Member Area

The legal basis for our aforementioned processing of Personal Data regarding our Website's Member Area, including the Dashboard, Resource Request Form, Monthly Member Reports, Registration for Events, Member Directory, Subject Matter Expert (SME) Directory, and Q&A Forum, is the legitimate interests pursued by PSI or by a third party, particularly our members, pursuant to Art. 6 para 1 s 1 lit. f EU and UK GDPR. The relevant legitimate interests correspond with the purposes and interests described above.

1.3. Personal Data Provided to and Processed by PSI About Alleged Counterfeiting Incidents

Personal Data may be collected or provided to PSI about alleged Counterfeiting incidents and related activities by telephone, letter, facsimile, e-mail to psi@psi-inc.org or another e-mail address of PSI or its personnel, the contact form on our Website, or other means of communication. Where we do not obtain your Personal Data directly from yourself, we may particularly obtain it (i) through someone else's report of an alleged Counterfeiting incident that contains your Personal Data, (ii) from our members, (iii) publicly available sources, such as the internet, or (iv) in the course of litigation or authority proceedings from involved parties including public authorities.

1.3.1. Descriptions on Our Personal Data Processing Activities

PSI uses such Personal Data only for the purposes for which it was voluntarily submitted or originally collected or subsequently authorized by the individual or for which it was obtained from other sources, namely (i) the collection of data about alleged pharmaceutical Counterfeiting and related activities, (ii) the analysis of such data, the use of such data or analyses in connection with formulating and implementing anti-Counterfeiting strategies, (iii) facilitating investigations of suspected criminal activity, and/or (iv) communicating and sharing information with courts, public authorities (including but not limited to law enforcement authorities), or legal counsel.

Personal Data may particularly comprise one or more of the following: names and nationalities, dates of birth, the grounds for suspecting that the subjects are engaged in illegal conduct and related background information, and any prior criminal activity. The described processing is necessary for the purposes of the legitimate interests pursued by PSI or third parties, particularly its members, to protect the public health, share information on the counterfeiting of pharmaceuticals as well as to establish, exercise or defend of legal claims and initiate enforcement action through the appropriate authorities.

For the aforementioned purposes, PSI may also forward such Personal Data to its members.

Dashboard Section of the Member Area

One way for PSI to disclose such Personal Data to its members and their representatives is through the Dashboard section of the Member Area which has its own login with a different password than the Member Area (as described above under Section 1.2.1.2.1). This Dashboard section displays incident summaries which may include the Personal Data described above. These summaries are generally only available to the member representatives whose members are respectively affected by such an incident. The summaries may also

include some Personal Data about the member representative who submitted the relevant information to PSI, such as their name, position, member / employer, and business contact information.

Apart from the disclosures and related purposes described above, we could also become subject to lawful requests by public authorities, including to meet national security or law enforcement requirements, which could require us to disclose Personal Data in response.

1.3.2. Legal Bases for Our Personal Data Processing Activities

If you are located in the EEA or UK, or your Personal Data is (otherwise) governed by their privacy laws, the legal basis for the processing activities described under Section 1.3.1 are the legitimate interests pursued by PSI or by a third party, particularly, our members, pursuant to Art. 6 para 1 s 1 lit. f EU and UK GDPR or the performance of a task carried out in the public interest laid down by EEA or EEA Member State law or UK law pursuant to Art. 6 para 1 s 1 lit. e EU and UK GDPR. The relevant legitimate interests correspond with the purposes and interests described under Section 1.3.1 above. As an exception, to the extent that our processing of Personal Data is necessary for compliance with any other legal obligation based on EEA or EEA Member State law or UK law, such as if we are legally obligated to provide certain data to a court or an authority in the EEA or UK, the relevant legal basis would be Art. 6 para 1 s 1 lit. c EU and UK GDPR in relation thereto.

PSI does not generally solicit or collect Sensitive Information, as defined under Section 2.2 below, but if PSI may process such Personal Data, the legal basis would be your consent pursuant to Art. 9 para 2 lit. a EU and UK GDPR, the establishment, exercise or defense of legal claims pursuant to Art. 9 para 2 lit. f EU and UK GDPR, or reasons of public interest in the area of public health on the basis of EEA or EEA Member State law or UK law pursuant to Art. 9 para 2 lit. i EU and UK GDPR.

1.4. Personal Data Processed as Part of Our E-Mail Correspondence with You

We may collect Personal Data or receive via e-mail psi@psi-inc.org or another e-mail address of PSI or our personnel and we may process such Personal Data as described in the following.

1.4.1. Descriptions on Our Personal Data Processing Activities

When you send an e-mail to psi@psi-inc.org or another e-mail address of PSI or its personnel or if PSI or its personnel corresponds with you via e-mail, PSI may generally process your name, e-mail address, the information in your e-mail signature, your employer, the subject matter and the content of the e-mails, and metadata related to each e-mail (such as the data and time of its sending).

PSI generally processes Personal Data as part of the e-mail correspondence for the purpose of allowing you to contact us and us to contact you as well as for corresponding with each other. We may also share information about our correspondence with our members and their representatives where this is necessary or helpful to respond to and deal with your inquiry or the relevant matter that we are corresponding with you about. If you send us an e-mail to

provide us with information about alleged Counterfeiting incidents and related activities, the descriptions under Section 1.3 below apply in relation to the related processing.

1.4.2. Legal Bases for Our Personal Data Processing Activities

If you are located in the EEA or UK, or your Personal Data is (otherwise) governed by the privacy laws in the EEA or UK, the legal basis for the processing activities described under Section 1.4.1 are the justifications based on the legitimate interests pursued by PSI or by a third party, particularly, our members, pursuant to Art. 6 para 1 s 1 lit. f EU and UK GDPR or the performance of a task carried out in the public interest laid down by EEA or EEA Member State law or UK law pursuant to Art. 6 para 1 s 1 lit. e EU and UK GDPR. The relevant legitimate interests correspond with the purposes and interests described under Section 1.4.1 above. As an exception, to the extent that our processing of Personal Data is necessary for compliance with any other legal obligation based on EEA or EEA Member State law or UK law, such as if we are legally obligated to provide certain data to a court or an authority in the EEA or UK, the relevant legal basis would be Art. 6 para 1 s 1 lit. c EU and UK GDPR in relation thereto.

PSI does not generally solicit or collect Sensitive Information, as defined under Section 2.2 below, but if PSI processes such Personal Data, the legal basis would be your consent pursuant to Art. 9 para 2 lit. a EU and UK GDPR, the establishment, exercise or defense of legal claims pursuant to Art. 9 para 2 lit. f EU and UK GDPR, or reasons of public interest in the area of public health on the basis of EEA or EEA Member State law or UK law pursuant to Art. 9 para 2 lit. i EU and UK GDPR.

1.5. Disclosures of Your Personal Data Including Onward Transfers Under the DPF Programs

Apart from the disclosures respectively described under the Sections 1.1.2, 1.2.1, 1.3.1, and 1.4.1 above, you may find relevant information in relation to our possible further transfers of Personal Data to recipients under Section 1.5.1 below. Section 1.5.2 below sets out relevant requirements applicable to onward transfers under the DPF Programs.

1.5.1. Descriptions on Disclosures of Your Personal Data

As it relates to the processing activities described under this Privacy Statement, PSI may (also) transfer Personal Data to a court, a public authority (including but not limited to law enforcement authorities), or legal counsel and at a minimum only for the purpose of establishing, exercising, or defending of legal claims including for the prevention, investigation, or detection of violations of law or for important reasons of public interest. PSI may also transfer Personal Data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. Neither PSI nor any of its members has control over courts or public authorities that may be potential transferees. Applicable law in different jurisdictions may affect the confidentiality of the information voluntarily submitted by an individual to PSI and transferred to such courts or authorities. As a result, PSI cannot make any assurances as to whether or not any such court or authority will keep such Personal Data confidential.

Personal Data included in the Subject Matter Expert (SME) Directory and information submitted to or displayed within the Q&A Forum may be disclosed to authorized representatives of PSI member organizations in accordance with the purposes described above. Such disclosures are limited to facilitating collaboration, consultation, information sharing, and other legitimate PSI member activities consistent with this Privacy Statement.

If you are located in the EEA or UK, or your Personal Data is (otherwise) governed by their privacy laws, the legal basis for the transfers set out above is the legitimate interests pursued by PSI or by a third party, particularly, our members, pursuant to Art. 6 para 1 s 1 lit. f EU and UK GDPR or the performance of a task carried out in the public interest laid down by EEA or EEA Member State law or UK law pursuant to Art. 6 para 1 s 1 lit. e EU and UK GDPR. The relevant legitimate interests correspond with the purposes and interests stated above. As an exception, to the extent that our processing of Personal Data is necessary for compliance with any other legal obligation based on EEA or EEA Member State law or UK law, such as if we are legally obligated to provide certain data to a court or an authority in the EEA or UK, the relevant legal basis would be Art. 6 para 1 s 1 lit. c EU and UK GDPR in relation thereto.

If and to the extent such a transfer may include Sensitive Information, as defined under Section 2.2 below, the legal basis would be your consent pursuant to Art. 9 para 2 lit. a EU and UK GDPR, the establishment, exercise or defense of legal claims pursuant to Art. 9 para 2 lit. f EU and UK GDPR, or reasons of public interest in the area of public health on the basis of Union or Member State law pursuant to Art. 9 para 2 lit. i EU and UK GDPR.

As it relates to disclosures already covered under Section 1.3 above, the specific descriptions on disclosures set out under Section 1.3 prevail over the general descriptions under this Section 1.5.1 in case of any discrepancy.

PSI may further engage IT service providers in relation to the processing activities described under the Sections 1.1.2, 1.2.1, 1.3.1, and 1.4.1 and share Personal Data with these recipients in relation the provision of their services to us. In particular, PSI

- has engaged Wix regarding the hosting and provision of our Website including its functionalities via its the cloud solution as also described under Section 1.1.2.
- relies on Microsoft in relation to its correspondence via e-mails and messages, which also includes the messages and information which you may send us by using the different forms available on our Website, and the Dashboard as described under Sections 1.2.1.1, 1.2.1.2.2, 1.2.1.2.4, 1.3.1, and 1.4.1.

1.5.2. Onward Transfers Under the DPF Programs and Our Related Liability

If any of the transfers to a recipient described under Sections 1.1.2, 1.2.1, 1.3.1, 1.4.1, or 1.5.1 above relate to Personal Data which PSI has received under the DPF Programs, such a transfer is considered an onward transfer under the DPF Programs and is thus subject to the applicable requirements for onward transfers as set out therein.

PSI requires third-party agents and service providers that process Personal Data on its behalf to provide at least the same level of privacy protection as required by the DPF Program

Principles and will take reasonable and appropriate steps to ensure that such processing is conducted consistent with those obligations.

In the context of an onward transfer, PSI has the responsibility for the processing of Personal Data it receives under the DPF Programs and subsequently transfers to a third party acting as an agent on its behalf. PSI remains liable under the DPF Program Principles if its agent processes such Personal Data in a manner inconsistent with the DPF Program Principles, unless PSI proves that it is not responsible for the event giving rise to the damage.

1.6. International Transfers of your Personal Data

Your Personal Data may be transferred to and stored in countries outside of the jurisdiction you are in where we and the recipients of the data have operations.

If you are located in the EEA, UK or Switzerland, or your Personal Data is (otherwise) governed by such privacy laws, the following applies:

Your Personal Data will particularly be processed in the United States of America and may also be processed in other countries outside of the EEA, UK, and Switzerland.

Our own processing of your Personal Data, including any onward transfer performed by us, is generally subject to the DPF Programs to ensure an adequate level of protection for that Personal Data.

When we transfer your Personal Data to a recipient outside the EEA, UK, or Switzerland: Either of the following applies:

- The recipient is located in a country, territory, or sector which provides an adequate level of protection for the processing of personal data based on a decision from the European Commission or the respectively competent authority in the UK or Switzerland. Decisions from the European Commission are available [here](#).
- The recipient is itself certified under the DPF Programs or otherwise subject to a similar program which provides adequate level of protection for the processing of personal data based on a decision from the European Commission or the respectively competent authority in the UK or Switzerland.
- PSI transfers the Personal Data to the recipient pursuant to appropriate safeguards, such as the EU Standard Contractual Clauses approved by the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 or equivalent clauses for the UK or Switzerland. The EU Standard Contractual Clauses can be reviewed under the [Annex of the aforementioned Implementing Decision](#).
- Outside of the aforementioned cases, PSI may receive and/or transfer Personal Data pursuant to a derogation under applicable privacy law, such as, where the transfer is necessary for (i) important reasons of public interest or (ii) the establishment, exercise or defense of legal claims or (iii) based on your explicit consent.

Below you can find relevant information regarding IT service providers Wix and Microsoft (see descriptions under Section 1.1.2 and at the end of Section 1.5.1):

- Wix.com Ltd., Yunitsman 5 St, Tel Aviv, Israel. The European Commission has recognized Israel as a country providing for an adequate level of protection for Personal Data, whereas the related Commission Decision is available [here](#). Further, its U.S. affiliate Wix.com Inc., 100 Gansevoort Street, New York, NY 10014, U.S. is certified under the DPF Programs.
- Microsoft's U.S. parent company, Microsoft Corporation, 1 Microsoft Way, Redmond, WA 98052, U.S. is certified under the DPF Programs.

In the event that you wish to learn more about the specifics of international transfers and the respective transfer mechanism which we use, please contact PSI at psi@psi-inc.org.

1.7. Inquiries and Complaints

If you have any questions or complaints in relation to this Privacy Statement or PSI's processing of Personal Data, please contact us under the following contact information.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, PSI commits to resolve DPF Programs Principles-related complaints about our collection and use of your Personal Data. EEA and UK and Swiss individuals with inquiries or complaints regarding our handling of Personal Data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF should first contact PSI at:

The Pharmaceutical Security Institute, Inc.

526 King St., Ste. 203

Alexandria, VA 22314

E-Mail: psi@psi-inc.org

Phone: (703) 705-5930

PSI will investigate and attempt to resolve complaints relating to its processing of Personal Data in accordance with the DPF Program Principles and applicable law.

Please include the following information to enable PSI to verify that it originates from you:

Your username or other information reasonably necessary to verify your identity, or, if you did not establish login credentials with PSI, a physical or electronic signature;

Identification of the individually identifying information to which your inquiry or complaint relates;

Identification of any material that you are requesting that PSI remove or disable access to, and information reasonably sufficient to permit PSI to locate the material;

Information reasonably sufficient to permit PSI to contact you, such as your address, telephone number, and if available, an electronic mail address at which PSI may contact you; and

A statement that the information in the inquiry or complaint is accurate.

2. Choice Under the DPF Programs

To the extent that PSI processes Personal Data under the DPF Programs the following applies:

2.1. Opt Out for Different Scenarios

PSI will give the opportunity to any individual about whom Personal Data has been provided to choose ("opt out") that PSI will not (a) disclose such individual's Personal Data to a third party except as consistent with the DPF Programs, or (b) use such Personal Data for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by such individual. Please note that this choice does not apply to disclosures to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of PSI.

2.2. Opt In Regarding Sensitive Information

PSI does not generally solicit or collect Personal Data specifying an individual's medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information concerning an individual's sex life or sexual orientation (collectively "*Sensitive Information*"). PSI will only collect and use Sensitive Information as permitted by the DPF Programs and applicable law and will obtain affirmative consent ("*opt in*") from an individual if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice, if no exception to the requirement to obtain affirmative consent applies under the DPF Programs, such as, where processing is necessary for the establishment of legal claims or defenses.

In the event that you wish to exercise any of your (opt out or opt in) choices, please contact PSI at psi@psi-inc.org.

3. Security

PSI has taken reasonable measures to assure that Personal Data that it collects or has been supplied to it is retained in a secure manner. Only authorized personnel, bound by confidentiality agreements, are granted access to the data stored by PSI. PSI maintains administrative, technical, and physical safeguards designed to protect Personal Data from unauthorized access, use, alteration, disclosure, or destruction. Access to Personal Data is restricted to authorized personnel with a legitimate business need to access such information.

PSI has appointed a Chief Security Officer ("CSO") who is in charge of PSI's security policy and who monitors compliance with this policy. PSI also requires employees to review and adhere to this Privacy Statement, in addition to their general agreement as to the maintenance of confidentiality.

PSI holds periodic security training and compliance evaluation sessions for all its employees which include a discussion of PSI's Privacy Statement, awareness of its discipline process, how to take action to protect data and equipment in the event of disaster, and training on PSI's back-up procedures and methods of safe disposal of data.

Data Integrity

PSI seeks to ensure that all Personal Data that it maintains is up to date, accurate, complete and relevant.

4. Retention Periods

PSI will retain Personal Data only for as long as necessary to fulfil the purposes it was collected it for as set out above. To determine the appropriate retention period for Personal Data, PSI consider the amount, nature, and sensitivity of the Personal Data, the potential risk of harm from unauthorized use or disclosure of Personal Data, the purposes for which PSI processes that Personal Data and the applicable legal requirements.

If you are located in the EEA or UK, or your Personal Data is (otherwise) governed by their privacy laws, the following applies:

In general, PSI will only retain your personal data (i) for as long as necessary to fulfil the purposes we collected or otherwise processed it for, (ii) until you withdraw your consent on which the processing is based, where there is no other legal basis for the processing, or (iii) until you successfully exercise your right to object as described under Section 5 below, in each case to the extent that neither of the exceptions under the following paragraph do not apply.

We may particularly refrain from erasing your personal data if its continued processing is necessary for compliance with a legal obligation (including statutory retention obligations, such as under tax law) or for the establishment, exercise or defense of legal claims.

5. Your Rights in Relation to Your Personal Data

5.1. Your Rights Under Applicable Privacy Law

If you are based in the EEA or the UK or another jurisdiction with similar privacy laws, or your Personal Data is (otherwise) governed by such privacy laws, subject to any exemptions and limitations provided for under applicable law that may apply, you generally have the following rights in respect of Personal Data that we hold about you:

- **Right of access.** Your right of access allows you to receive information on
 - the purposes of our processing of your Personal Data and the processed categories of Personal Data;
 - the envisaged storage period or the criteria used to determine the period;
 - the source of your Personal Data where the Personal Data are not collected from you;
 - the recipients or categories of recipients to whom we may disclose your Personal Data and, in case of transfers to countries outside of the EEA or UK, information about the appropriate safeguards;
 - the existence of automated decision-making, including profiling, and relevant information in relation thereto; and
 - a copy of the Personal Data undergoing processing.

- **Automated Decision-Making.** PSI does not use Personal Data received under this Privacy Statement for solely automated decision-making, including profiling, that produces legal effects concerning individuals or similarly significant effects on individuals.
- **Right of portability.** Under certain conditions, you have the right, to (i) receive Personal Data which you have provided to us in a structured, commonly used and machine-readable format and (ii) transmit such data to another controller without hindrance or, where technically feasible, have the personal data transmitted directly to another controller.
- **Right to rectification.** You have the right to obtain rectification or completion of inaccurate or incomplete Personal Data we hold about you without undue delay.
- **Right to erasure.** You have the right to demand from us to erase your Personal Data without undue delay under certain conditions. This may particularly be the case if the processing of your Personal Data is no longer necessary in relation to the purposes for which they were collected or otherwise processed. However, we may particularly refrain from erasing your Personal Data to the extent that its continued processing is necessary for compliance with a legal obligation (including statutory retention obligations, such as under tax law) or for the establishment, exercise or defense of legal claims.
- **Right to restriction.** You have the right, to demand from us restriction of the processing of your Personal Data under certain conditions. This may particularly be the case where (i) the accuracy of the Personal Data is contested by you, for a period enabling us to verify the accuracy of such Personal Data, or (ii) the processing is unlawful and you oppose the erasure of your Personal Data and request the restriction of its use instead.
- **RIGHT TO OBJECT. YOU HAVE THE RIGHT TO OBJECT TO THE PROCESSING OF YOUR PERSONAL DATA**
 - **BASED ON THE LEGITIMATE INTERESTS BY US OR A THIRD PARTY ON GROUNDS RELATING TO YOUR PARTICULAR SITUATION WHILE WE WILL NO LONGER PROCESS THE PERSONAL DATA UNLESS (I) WE ARE ABLE TO DEMONSTRATE COMPELLING LEGITIMATE GROUNDS FOR THE PROCESSING WHICH OVERRIDE YOUR INTERESTS, RIGHTS AND FREEDOMS OR (II) FOR THE ESTABLISHMENT, EXERCISE OR DEFENCE OF LEGAL CLAIMS; OR**
 - **FOR DIRECT MARKETING PURPOSES.**

If you wish to exercise any of these rights, please contact PSI at psi@psi-inc.org.

Right to Lodge a Complaint with an Authority. You also have the right to lodge a complaint to a data protection authority, in particular, in the country of your habitual residence, your place of work or the place of the alleged infringement.

You can find a list of the data protection authorities in the EEA and their contact information under the following link: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en

The competent data protection authority in the UK and its contact information are as follows:

Information Commissioner's Office
Wycliffe House

Water Lane
Wilmslow, Cheshire
SK9 5AF
United Kingdom

Helpline number: +44 303 123 1113

You can find its contact form here: <https://ico.org.uk/global/contact-us/contact-us-public/>

5.2. Your Rights Under the DPF Programs

Irrespective of the aforementioned rights under Section 5.1 above, if your Personal Data is subject to the DPF Programs, with the exemptions and limitations permitted thereunder, you particularly have the right, without the need for justification, to obtain from PSI confirmation of whether it is processing Personal Data related to you and have the data communicated to you as well as to have the Personal Data corrected, amended or deleted where it is inaccurate or processed in violation of the DPF Programs Principles.

In the event that you wish to exercise any of these rights, please contact PSI at psi@psi-inc.org.

PSI may restrict access to Personal Data to any individual as may be permitted under the DPF Programs or applicable law. Under DPF Programs, such restrictions may particularly arise to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security, defense, or public security; or generally for the following reasons (i) interference with the execution or enforcement of the law or with private causes of action, including the prevention, investigation or detection of offenses or the right to a fair trial; (ii) disclosure where the legitimate rights or important interests of others would be violated; (iii) breaching a legal or other professional privilege or obligation; (iv) prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and corporate re-organizations; or (v) prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound management, or in future or ongoing negotiations involving the organization.

PSI may charge a reasonable fee for providing access to Personal Data under the DPF Programs.

6. Recourse and Enforcement under the DPF Programs

The DPF Programs Principle which covers the recourse and enforcement particularly involves the following aspects:

6.1. Independent Dispute Resolution Procedure

If you have an inquiry or complaint regarding PSI's compliance with the DPF Programs Principles, you should first contact PSI in writing to inform us of any specific inquiry or complaint you may have about PSI's collection, retention or usage of your Personal Data.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, PSI commits to refer unresolved complaints concerning our handling of Personal Data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF to the International Centre for Dispute Resolution of the American Arbitration Association, an alternative dispute resolution provider based in the United States. If you do not

receive timely acknowledgment of your DPF Programs Principles-related complaint from us, or if we have not addressed your DPF Programs Principles-related complaint to your satisfaction, please visit [ICDR-AAA DPF IRM Service](#) for more information or to file a complaint. The services of International Centre for Dispute Resolution of the American Arbitration Association are provided at no cost to you.

6.2. DPF Programs Verification

On a periodic basis, but not less frequently than once every year, PSI conducts its own objective DPF Programs compliance review procedure. PSI also verifies that its Privacy Statement, as set forth herein, is accurate, comprehensive, prominently displayed, and completely implemented, including implementation of appropriate employee training and other internal procedures. Additional information regarding the Data Privacy Framework Program is available from the U.S. Department of Commerce through the Data Privacy Framework website (<https://www.dataprivacyframework.gov/>).

6.3. Remedies and Sanctions

The result of any remedies provided by the independent dispute resolution body should be that the effects of non-compliance are reversed or corrected by the organization, insofar as feasible, and that future processing by the organization will be in conformity with the DPF Programs Principles and, where appropriate, that processing of the personal data of the individual who brought the complaint will cease.

The sanctions for non-compliance with the DPF Programs Principles range from suspension from the DPF Programs to compensation for individuals for losses incurred as a result of non-compliance. Other sanctions include public notice of non-compliance and injunctions.

6.4. Possibility to Invoke Arbitration

For resolution of any claimed violations of the DPF Programs Principles not resolved by any of the other DPF Programs mechanisms, you have the option to invoke arbitration to determine, for residual claims, whether PSI has violated its obligations under the DPF Programs Principles as to you, and whether any such violation remains fully or partially unremedied. This option is available only for these purposes. You may find more information on this option under [Annex I](#) of the DPF Programs.

6.5. Jurisdiction of the Federal Trade Commission

The Federal Trade Commission has jurisdiction over PSI's compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF.

7. Other Provisions

7.1. Notice and Procedure for Making Claims of Copyright Infringement

Alleged Copyright Infringement: If you believe that material posted on this Website infringes your copyright, you must submit a notification in writing. To be effective, your notification must include the following:

A physical or electronic signature of a person authorized to act on behalf of the owner of the exclusive right that you claim has been infringed;

Identification of the copyrighted work you claim has been infringed;

Identification of the material that you are requesting that PSI remove or disable access to, and information reasonably sufficient to permit PSI to locate the material;

Information reasonably sufficient to permit PSI to contact you, such as your address, telephone number, and if available, an electronic mail address at which PSI may contact you;

A statement that you have a good faith belief that use of the material in the manner complained of is not authorized by you, or the law; and

A statement that the information in the notification is accurate, and under penalty of perjury, that you are authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Upon receipt of the written Notification containing the information set forth above:

PSI shall remove or disable access to the material that you allege is infringing;

PSI shall forward your written notification to the party who provided the material;

PSI shall take reasonable steps to promptly notify the party who provided the material that PSI has removed or disabled access to the material.

7.2. Counter Notification

If you object to PSI's removal or disabling of access to your material in response to a written notification, you may serve PSI with a Counter Notification. To be effective, a Counter Notification must be a written communication provided to PSI's Designated Agent that includes substantially the following:

A physical or electronic signature of the person submitting the Counter Notification;

Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before PSI removed it or disabled access to it;

A statement under penalty of perjury that the person submitting the Counter Notification has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material;

The name, address, and telephone number of the person submitting the Counter Notification, and a statement that the person submitting the Counter Notification consents to the jurisdiction of Federal District Court for the judicial district in which the person submitting the Counter Notification is located, or if the address of the person submitting the Counter Notification is outside of the United States, for any

judicial district in which PSI may be found, and that the person submitting the Counter Notification will accept service of process from the party who provided the original Notification or an agent of such person.

Upon receipt of a Counter Notification containing the information set forth above:

PSI shall promptly provide the party who served the original Notification with a copy of the Counter Notification; and

PSI shall inform the party who served the original Notification that it will replace the removed material or cease disabling access to it within ten (10) business days.

PSI shall replace the removed material or cease disabling access to the material within ten (10) to fourteen (14) business days following receipt of the Counter Notification, **provided** PSI's Designated Agent has not received notice from the party who served the original Notification that an action has been filed seeking a court order to restrain the person submitting the Counter Notification from engaging in infringing activity relating to the material on PSI's Website.

8. Disclaimer

PSI is not responsible for the content of any off-site pages that are referenced by or that reference to the PSI Website. PSI is not responsible for any defamatory, offensive, misleading, or illegal conduct of other users, links, or third parties, and the risk of injury from the foregoing rests entirely with the visitor.

Links from the PSI Website to other sites, or from other sites to the PSI home page, do not constitute an endorsement by PSI. The links are for convenience only. It is the responsibility of the visitor to evaluate the content and usefulness of information obtained from other sites.

All information provided by PSI at this Website is for the convenience of interested visitors and visitors. The information is based on reports from various third party sources whose credibility and knowledge are unknown to PSI. PSI has not independently verified the accuracy of any information. PSI updates information only as new information is submitted. Individual visitors may use the information as they see fit. PSI does not guarantee the accuracy, completeness, timeliness, or correct sequencing of information, PSI is not responsible for errors or omissions, or for the use of, or results obtained from the use of, the information.

Reference to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply endorsement, recommendation, or favoring by PSI.

9. Modification of This Website's Privacy Statement and Terms of Use

PSI reserves the right to amend this Website's Privacy Statement and Terms of Use and will alert you that changes have been made by indicating the date they were last updated. Your continued use of this Website after the Website Privacy Statement and Terms of Use have been amended signifies that you have agreed to any and all new terms.

PSI'S WEBSITE PRIVACY STATEMENT AND TERMS OF USE WERE LAST UPDATED ON SEPTEMBER 7, 2026.

10. Contact Information

If you have any questions or comments regarding PSI's Privacy Statement, privacy practices or Terms of Use, please contact PSI at psi@psi-inc.org.