

PHARMACEUTICAL SECURITY INSTITUTE, INC.

Last updated: August 2025

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 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 our certification, please visit <https://www.dataprivacyframework.gov/>.

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	5
1.3.	Personal Data Otherwise Provided To and Processed By PSI About Alleged Counterfeiting Incidents	6
1.4.	Disclosures of Your Personal Data Including Onward Transfers Under The DPF Programs	7
1.5.	International Transfers of your Personal Data	8
1.6.	Inquiries and Complaints	9
2.	Choice Under the DPF Programs	10
2.1.	Opt Out for Different Scenarios	10
2.2.	Opt In Regarding Sensitive Information	10
3.	Security	11
4.	Retention Periods	11
5.	Your Rights in Relation to Your Personal Data	11
5.1.	Your Rights Under Applicable Privacy Law	11
5.2.	Your Rights Under the DPF Programs	13
6.	Recourse and Enforcement under the DPF Programs	13
6.1.	Independent Dispute Resolution Procedure	14
6.2.	DPF Programs Verification	14
6.3.	Remedies and Sanctions	14
6.4.	Possibility to Invoke Arbitration	14
6.5.	Jurisdiction of the Federal Trade Commission	14
7.	Other Provisions	15
7.1.	Notice and Procedure for Making Claims of Copyright Infringement	15
7.2.	Counter Notification	15
8.	Disclaimer	16
9.	Modification of This Website's Privacy Statement and Terms of Use	17
10.	Contact Information	17

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), and to ensure that this website remains available and is functioning and displayed properly and effectively for all visitors. All network traffic may be monitored in order to identify unauthorized attempts to (i) upload or change information, or (ii) access your account for our member area, or otherwise cause damage or conduct criminal or unauthorized activity. Further, we will use a cookie to allow you to remain logged in when you log in to our member area.

You may benefit from our use of cookies similar for the aforementioned purposes equally 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 on our website, usage duration, loaded content, screen resolution, information related to your login and use of our member area.

Wix.com Ltd., Yunitsman 5 St, Tel Aviv, Israel is headquartered in Israel, which the European Commission has recognized as a country which provides an adequate level of protection for Personal Data. Further, its U.S. affiliate Wix.com Inc., 100 Gansevoort Street, New York, NY 10014, U.S. is certified under the DPF Programs.

- As it relates to the login page on our website's member area, we have further implemented Google's reCAPTCHA which involves the placing of a related cookie. This allows us to

verify whether a user of our website is a human being as opposed to a bot. reCAPTCHA does this by performing an analysis regarding a user's website usage. Hereby, particularly the following categories of data may be processed: URL of the accessed website and the referral website, IP address, operating system, device settings (such as location), browser and the implemented settings and plug ins, certain usage behavior on our website (such as mouse movements), usage duration, loaded content, screen resolution.

The purpose of our reCAPTCHA use is to ensure the security and safety of our website and, in particular, its member area and your use of it by preventing computer programs from misusing and attacking our website.

Google's parent company, Google LLC, 1600 Amphitheatre Pkwy, Mountain View, CA 94043, U.S., is certified under the DPF Programs.

We cannot rule out that Google could also process your data in connection with the provision of reCAPTCHA for its own purposes. Please check Google's Privacy Policy for details on Google's own processing activities: <https://policies.google.com/privacy#infocollect>

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 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

a) 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.

b) Website Member Area

If you are a representative of one of PSI's members, you may also use our website's member area. You are not obligated to register and use the member area but if you decide to do so, this requires for you to sign up to the member area. 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.

PSI generally processes Personal Data to verify your authorization to use the members area as well to ensure that it remains safe and secure including regarding your access and use of our 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. We may share information from our joint communication with your colleagues at the member you work for or other members where this may be necessary or helpful based on the topic and content of the communication.

The 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, the content of any related correspondence between you and us.

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.

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:

a) 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 a) above.

b) Website Member Area

The legal basis for our aforementioned processing of Personal Data regarding our website's member area 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 b) above.

1.3. Personal Data Otherwise 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, 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 Personal Data to its members.

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 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. 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, and 1.3.1 above, you may find relevant information in relation to our possible further transfers of Personal Data to recipients under Section 1.4.1 below. Section 1.4.2 below sets out relevant requirements applicable to onward transfers under the DPF Programs.

1.4.1. 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.

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 1.4.1 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, and 1.3.1 and share Personal Data with these recipients in relation the provision of their services to us.

1.4.2. 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, or 1.4.1 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.

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.

1.5. 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.

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.

1.6. 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.

8100 Boone Blvd Ste 220

Vienna, Virginia 22182-2683

E-Mail: psi@psi-inc.org

Phone: (703) 848-0161

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

Your unique username and password, or if you did not supply PSI with a username and password when you first submitted the information, 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 specifying the individual's sex life (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. Remote access to the Personal Data is not available.

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.
- **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.

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 August 21, 2025.

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.