Smarsh EU-U.S., UK Extension & Swiss-U.S. Data Privacy Framework

Smarsh Inc. ("Smarsh") is a Software Development Company that partners with regulated organizations of all sizes to capture, retain, and oversee solutions that help them identify regulatory and reputational risks within their communications data. Smarsh is committed to individual privacy and reveres the confidence of its customers, business partners and others. We strive to collect, use, and disclose personal information in a manner consistent with the laws of the countries in which we do business, while upholding the highest ethical standards in our business practice.

The EU – U.S. Data Privacy Framework, UK extension to the EU – U.S. Data Privacy Framework, and Swiss – U.S. Data Privacy Framework set forth the privacy principles Smarsh follows in regard to transfer of personal information from the European Economic Area ("EEA") (which includes the twenty-seven (27) member states of the European Union ("EU") plus Iceland, Liechtenstein and Norway), the United Kingdom ("UK"), and Switzerland, respectively, to the United States ("U.S.").

Smarsh complies with the EU – U.S. Data Privacy Framework, UK extension to the EU – U.S. Data Privacy Framework, and Swiss – U.S. Data Privacy Framework, as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the EU, the UK, and Switzerland to the U.S. in reliance on the Data Privacy Framework. Smarsh has certified to the U.S. Department of Commerce that it adheres to the Data Privacy Framework principles. If there is any conflict between the Smarsh privacy statement and the Data Privacy Framework principles, the Data Privacy Framework principles shall govern. To learn more about the Data Privacy Framework program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

EU – U.S. Data Privacy Framework

The United States Department of Commerce and the European Commission have agreed on a set of data protection principles and frequently asked questions to enable U.S. companies to satisfy the requirement, under EU law, that adequate protection be given to personal information transferred from the EEA to the U.S. (the "EU – U.S. Data Privacy Framework"). On July 10, 2023, the European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework. The adequacy decision concludes that, for the purpose of Article 45 of Regulation (EU) 2016/679 ("EU GDPR"), the U.S. ensures an adequate level of protection for personal data transferred from the EU to U.S. companies participating in the EU-U.S. Data Privacy Framework.

The EU – U.S. Data Privacy Framework is publicly displayed on our website at www.Smarsh.com. For more information about EU – U.S. Data Privacy Framework principles and to view Smarsh's certification, visit the U.S. Department of Commerce's website at https://www.dataprivacyframework.gov/.

Dispute Resolution

In compliance with the Data Privacy Framework principles, Smarsh commits to resolve complaints about our collection or use of your personal information. EU, UK, and Swiss individuals with inquiries or complaints regarding our Data Privacy Framework policy should first contact Smarsh at:

Smarsh GLOBAL HEADQUARTERS

Call us: **1-866-Smarsh-1**

Write us: **851 SW 6th Avenue - Portland, Oregon 97204**

Smarsh EEA & UK:

Call us: **+44 (0) 20 3608 1209**

Write us: **One Canada Square, Level 39 - London, E14 5AB**

privacy@Smarsh.com

Smarsh has further committed to refer unresolved Data Privacy Framework 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 JAMS, an alternative dispute resolution provider based in the U.S.

If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit ***https://www.jamsadr.com/DPF-Dispute-Resolution*** for more information or to file a complaint. The services of JAMS are provided at no cost to you.

If your DPF complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf.

SCOPE

This Framework applies to all personal information received by Smarsh in the U.S. from the EEA, in any format, including electronic, paper, or verbal.

DEFINITIONS

For purposes of this policy, the following definitions shall apply:

"Agent" means any third party that collects or uses personal information under the instructions of, and solely for, Smarsh or to which Smarsh discloses personal information for use on Smarsh's behalf.

"Customer" means any individual, corporation, or other entity which contracts Smarsh to perform services involving the transfer, processing, or reporting of personal information on behalf of and under the instructions of said "Customer."

"Smarsh" means Smarsh, its predecessors, successors, subsidiaries, divisions, and groups in the U.S. and globally.

"Associate" means an individual employed by Smarsh, or an affiliate located in one of the EU member countries or the UK.

"Subcontractor" means any individual, corporation, or other entity under written contract with Smarsh to assist in fulfilling the responsibilities assigned by the Customer or to meet business needs.

"Personal information" means any information or set of information that identifies or could be used by or on behalf of Smarsh to identify an individual. This includes but is not limited to information that: pertains to a specific individual, can be uniquely linked to that individual (e.g., by name, social security number, driver's license), originated in an EU Member State, the UK, or Switzerland, and is provided in any form. Personal information does not include information that is encoded or

anonymized, or publicly available information that has not been combined with non-public personal information.

“Sensitive personal information” means personal information that reveals race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, views or activities that concern health or sex life, information about social security benefits, or information on criminal or administrative proceedings and sanctions other than in the context of pending proceedings. In addition, Smarsh will treat as sensitive personal information any information received from a third party where that third party treats and identifies the information as sensitive.

PRIVACY POLICY

Smarsh is committed to respecting the privacy of individuals. Smarsh has internal procedures to repeatedly review and monitor the use of personal information and to confirm it is used responsibly and that we comply with internationally recognized standards of privacy protection. Internationally recognized standards require that the processing of personal data, both automated and manual, meet the data protection principles as described in this EU-U.S. Data Privacy Framework, UK extension to the EU-U.S. Data Privacy Framework, and Swiss-U.S. Data Privacy Framework.

NOTICE: Where Smarsh collects personal information directly from website visitors, customers or other sources in the EU, UK, and Switzerland, they will be informed regarding the purpose and use of the personal information, the types of non-agent third parties to which Smarsh discloses that information and the choices, if any, that Smarsh offers individuals for limiting the use and disclosure of their personal information. Notice will be provided in clear and conspicuous language at the time of collection, or as soon as practicable thereafter and before Smarsh uses the information for a purpose other than for which it was originally collected. Notice may be given in person, by email, post, telephone, or by posting on the Smarsh intranet or website.

CHOICE: Smarsh will offer individuals the opportunity to choose (opt out) if their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. Affirmative or explicit (opt in) choice must be given if sensitive information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized by the individual.

ACCOUNTABILITY FOR ONWARD TRANSFER: Smarsh may share personal information with its subcontractors or other agents of the Customer as required to successfully complete Customer activities or to meet business needs. Smarsh will obtain assurances from its subcontractors that they will protect personal information consistently with this EU – U.S. Data Privacy Framework, UK extension to the EU-U.S. Data Privacy Framework, and Swiss – U.S. Data Privacy Framework. Examples of appropriate assurances that may be provided by third-party business partners include: a contract obligating or agreement with the third party to provide at least the same level of protection as is required by the relevant EU – U.S. Data Privacy Framework, UK extension to the EU-U.S. Data Privacy Framework, and Swiss – U.S. Data Privacy Framework principles, being subject to the EU General Data Protection Regulation, EU – U.S. Data Privacy Framework certification, UK extension to the EU-U.S. Data Privacy Framework certification, and Swiss – U.S. Data Privacy Framework certification by the third party, or being subject to another European Commission adequacy finding. Where Smarsh. has knowledge that an agent is using or disclosing personal information in a manner contrary to this policy, Smarsh will take reasonable steps to prevent or stop the use or disclosure. Smarsh’s accountability for personal information that it receives in the U.S. under the Data Privacy Framework and subsequently transfers to a third party is described in the Data Privacy Framework Principles. In particular, Smarsh remains responsible and liable under the Data Privacy Framework

Principles if third-party agents that it engages to process personal data on its behalf do so in a manner inconsistent with the Principles, unless Smarsh proves that it is not responsible for the event giving rise to the damage.

Please be aware that Smarsh may be required to disclose an individual's personal information in response to a lawful request by public authorities, including meeting national security or law enforcement requirements.

ACCESS AND CORRECTION: Upon request, Smarsh may grant reasonable access to personal information it holds about individuals. Smarsh will take reasonable steps to permit individuals to correct, amend, or delete information that is demonstrated to be inaccurate or incomplete except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy or where the rights of persons other than the individual would be violated. Those rights may be honored by Smarsh following proper authentication and verification.

SECURITY: Smarsh has implemented reasonable and appropriate physical, electronic, and quality system procedures to safeguard and secure personal information. Computer equipment, networks, programs, data, and documentation are maintained to high standards, and precautions to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and/or destruction are in place.

DATA INTEGRITY AND PURPOSE LIMITATION: Smarsh will use personal information in ways that are compatible with the purpose for which it was collected or authorized by the individual. Smarsh will take reasonable steps to confirm that personal information is relevant to its intended use, accurate, complete, and current.

ENFORCEMENT: Any questions or concerns regarding the use or disclosure of personal information should be directed to Smarsh. Smarsh will investigate and attempt to resolve complaints and disputes regarding the use and disclosure of personal information in accordance with the principles contained in this policy. EU, UK, and Swiss citizens with inquiries or complaints regarding this privacy policy should first contact Smarsh at:

Smarsh World Headquarters
851 SW 6th Ave #800
Portland, OR 97204
+ 1 866 SMARSH 1 (toll-free)
+44 (0) 20 3608 1209 (outside of U.S.)
privacy@Smarsh.com

Smarsh will provide an annual self-certification letter to confirm appearance on the list of EU – U.S. Data Privacy Framework, UK extension to the EU-U.S. Data Privacy Framework, and Swiss – U.S. Data Privacy Framework participants.

TRAINING: Smarsh has provided its Associates with appropriate training to guarantee that all individuals who process personal information are fully aware of their responsibility with respect to data protection.

LIMITATION ON APPLICATION OF PRINCIPLES

Adherence by Smarsh to these EU – U.S. Data Privacy Framework, UK extension to the EU-U.S. Data Privacy Framework, and Swiss – U.S. Data Privacy Framework principles may be limited (a) to the

extent required to respond to a legal or ethical obligation; (b) to the extent necessary to meet national security, public interest, or law enforcement obligations; and (c) to the extent expressly permitted by an applicable law, rule, or regulation.

INTERNET PRIVACY

Smarsh sees the Internet and the use of other technology as valuable tools to communicate and interact with consumers, Associates, business partners, and others. Smarsh recognizes the importance of maintaining the privacy of information collected online and has created a specific Privacy Policy (the "PP") governing the treatment of personal information collected through the website that it operates. With respect to personal information that is transferred from the EEA or the UK to the U.S., the PP is subordinate to this policy. However, the PP also reflects additional legal requirements and evolving standards with respect to Internet privacy. Smarsh's Privacy Policy can be found at: https://www.smarsh.com/legal-website-privacy-policy.

CHANGES TO THIS DATA PRIVACY FRAMEWORK PRIVACY POLICY

This EU-U.S. Data Privacy Framework, UK Extension, and Swiss-U.S. Data Privacy Framework page, as well as our Privacy Policy, may be amended from time to time consistent with the requirements of the EU-U.S. Data Privacy Framework, UK extension to the EU-U.S. Data Privacy Framework, and Swiss-U.S. Data Privacy Framework. We will post any revised policies on the Smarsh website.

EFFECTIVE DATE

October 1, 2025