Sitero Privacy Policy

Updated May 6, 2024

Contents

1. Policy Purpose

Sitero prioritizes the confidentiality and security of personal data. This Privacy Policy ("Policy") applies to our processing of personal data that you provide to Sitero via one of the channels enumerated below. In this Policy, we explain the guidelines that apply to our processing of your personal data and provide information to which you are entitled under applicable data protection laws.

The purpose of this Policy is to ensure the compliance of Sitero, LLC ("Sitero") with our obligations under state, federal, and international privacy regulations; including the EU-U.S. Data Privacy

Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) set forth by the United States Department of Commerce (DoC) with respect to the collection, use and retention of Personal Data transferred from the European Union, United Kingdom (and Gibraltar), and Switzerland to the United States as further described herein (collectively, the "DPF Policy"). This DPF Policy outlines our commitment to the DPF Principles (the "Principles") and our practices for implementing the Principles.

Please read this Policy in its entirety to ensure that you are fully informed. If you have any questions or concerns about how Sitero processes your personal data, please contact us at privacy@sitero.com.

Sitero complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the DoC. Sitero has certified to the DoC 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 in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Sitero has certified to the DoC 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 policy and the EU-U.S. DPF Principles, the UK Extension to the EU-U.S. DPF, and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the DoC Data Privacy Framework (DPF) program, and to view Sitero's DPF certification, please visit https://www.dataprivacyframework.gov/. The DoC Data Privacy Framework List is available here. Sitero complies with the Principles with respect to the Personal Data it receives from its Customers or their Users in the European Union, United Kingdom (and Gibraltar), and Switzerland in connection with the use of (i) applications downloaded to a User's mobile device ("Mobile Applications"); and (ii) Sitero's hosted software applications (the "Subscription Service") and related support services ("Support Services"), as well as expert services (including professional services, training and certification) (the "Expert Services") that we provide to Customers and Users. In this DPF Policy, the Subscription Service, Support Services and the Expert Services are collectively referred to as the "Service."

2. What is Personal Data?

For purposes of these Policy, personal data broadly refers to any information relating to an identified or identifiable individual that directly or indirectly identifies the individual by reference to one or more factors specific to their physical, physiological, mental, economic, cultural, or social identity. Personal data does not include such information if it is anonymous (i.e., the personal data can no longer be traced back to the individual to whom it relates).

Examples of personal data include:

- Your first and last name
- Your employee identification number

- Your home address
- Your home or personal mobile telephone number
- Your personal email address
- The names of your family members
- Your date of birth
- Specific employment information about you (i.e., information from your CV or resume)

What is sensitive personal data?
Sensitive personal data is a category of personal data that may be more sensitive in nature compared to the personal data listed above.
Examples of sensitive personal data include:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Genetic data or biometric data (processed solely to identity an individual)
- Health-related data
- Financial data (in certain jurisdictions)
- Data concerning an individual's sex life or sexual orientation
- Trade-union membership (in some regions)

3. Types of Personal Data Provided to Sitero.

3.1 If you visit our website (www.sitero.com), use the contact form, contact Sitero for customer services or otherwise communicate with us.

Sitero collects, processes, and stores the following types of personal data (if provided by you):

- Name, job title, email address, phone number
- Information about the subject matter of your inquiry
- Date of your inquiry
- Other information you provide in connection with your inquiry
- Product-specific interest(s)
- Description of business question or need

We encourage you not to provide sensitive personal data to us unless it is strictly necessary for the processing of your inquiry. In this context, the information should only be sent in a highly encrypted form if you send the information by e-mail.

Your personal data will be processed only for the following purposes:

- Handling of your inquiry
- General communication with you

Sitero's legal basis for processing:

The basis depends on the nature of your inquiry.

Legitimate interests: We may process your personal data on the basis of our legitimate interests in handling and responding to your inquiry, communicating with you, and developing our products and services (Article 6(1)(f) of the General Data Protection Regulation).

Contractual obligations: If your inquiry concerns a (potential) formation of contract, we process your data to implement measures before the formation of contract (Article 6(1)(b) of the General Data Protection Regulation).

Retention Period:

Your personal data will be stored for as long as may be required to handle your inquiry. However, the data can be stored for a longer period in anonymized form.

3.2 Sitero's use of Cookies.

Sitero may also collect information about how you use our website using essential and non-essential cookies. Cookies are small text files sent by the website you are visiting to the computer or device you are using. If accepted, these cookies, which may include an anonymous unique identifier, are stored on the web browser of your device. Cookies can then track and collect data from your browser, sending that data back to the website owner. Once cookies are accepted by the user, the website is able to recognize repeated visits and track the user's usage patterns to better serve the user when they return to the website. Cookies do not extract personal data. Website visitors typically are able to follow a simple procedure to control the website host's use of cookies by indicating whether they want to permit the host to collect cookies at all and, if so, which type (essential or non-essential).

Essential cookies guarantee certain functionality without which the user may be unable to use the website as intended. Non-essential cookies collect information about the way the website is used or to store information that the user enters into the website (such as username, language preferred, or user location). Whereas essential cookies are used to ensure the basic functionality of the website, non-essential cookies are used to improve the performance of the website and offer the user personalized features.

Sitero uses both essential and non-essential cookies on www.sitero.com. We offer you the option to refuse or limit our use of cookies in connection with your visits to the site. Please be advised that if you do not accept any cookies, you may not be able to use some portions of our website.

3.3 If you sign up to receive marketing materials and/or newsletters from Sitero.

Sitero may collect, process, and store the following types of personal data (if provided by you):

- Your name and email address
- Your consent
- Your interests
- Your click-behavior in relation to published material

Sitero purpose for processing:

- Your personal data may be processed for the purposes of Sitero's marketing activities, which may include statistical analysis.

Sitero's legal basis for processing:

- Consent: Sitero will only use your personal data for direct marketing, including for sending out newsletters, if you have given your prior and explicit consent to our doing so (Article 6(1)(a) of the General Data Protection Regulation). You can always withdraw your consent by clicking on the unsubscribe link at the bottom of each email or by contacting us as described below. Note, however, withdrawing your consent does not affect the legality of the processing that preceded the withdrawal.
- Legitimate interests: The processing of your personal data will, in connection with analysis and statistics, be based on our legitimate interests in being able to improve and develop our service (Article 6(1)(f) of the General Data Protection Regulation).

Retention period

Your personal data will be stored for as long as your consent to receive newsletter(s) or other marketing materials is active.

Documentation relating to your marketing consent is kept for two (2) years from the time you have withdrawn your consent to receive direct marketing material. The retention period is determined based on Sitero's legitimate interest in being able to document that direct marketing has been carried out in accordance with the applicable legislation (Article 6(1)(f) of the General Data Protection Regulation).

3.4 If you apply to work at Sitero.

Sitero may, as permitted by law depending on your country of residence, collect, process, and store the following personal data:

- Personal data that you disclose in your job application and CV as well as any attachments
- Personal data that you disclose during any job interviews
- Information about you, including information regarding your previous jobs, activities, competencies, performance, as well as information about you that is publicly available, including information posted on social media
- Criminal records

- References from your previous and/or current employers
- Additional information you will provide in relation to the recruitment process

Sitero's purposes for processing:

- Your personal data will be processed for the purpose of determining your qualifications for employment and to reach a hiring decision.

Sitero's legal bases for processing:

- Request to enter into an employment contract with Sitero: We may process your personal data on the basis of your request to enter into an employment contract with Sitero (Article 6(1)(b) of the GDPR).
- Legitimate interests: We may process your personal data on the basis of our legitimate interests in carrying out further assessments to aid in reaching a hiring decision, including on the basis of personality tests (where permitted) and publicly available information on the internet (Article 6(1)(f) of the GDPR).
- Consent: In exceptional cases and only when no other legal basis can be applied, Sitero may ask separately for your consent to process your personal data (Article 6(1)(a) and 9(2)(a) of the GDPR). Sitero will, for instance, only take references from your previous and/or current employers or collect your health information or criminal records if you have consented to this.

Retention period

If you are offered a position with Sitero, your job application and additional relevant personal data obtained during the recruitment and hiring process will be stored in your employee file for the duration specified by applicable laws. If no such duration is specified, Sitero will retain your personal data in accordance with its record retention policy.

If you are not offered a position with Sitero we will store your job application and any additional personal data obtained during the recruitment process for a period of time following your rejection as required under local applicable law. If no such duration is specified, Sitero will retain your personal data in accordance with its record retention policy.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Sitero, LLC commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of human resources 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 in the context of the employment relationship.

<u>3.6 If you are a Vendor or Supplier of Sitero.</u>

Sitero may collect, process, and store the following types of personal data about you:

- Your name and job title
- Your business contact information (telephone, email, mailing address)
- Individual information (e.g., preferred language(s), CV, qualifications)
- Organizational information such as the nature of the work performed by your employer and your specific role/responsibilities for your employer
- Information related to the product(s) or service(s) you provide to Sitero
- We may receive such information directly from you (primarily through emails and other correspondence with you) or from a third party such as your employer.

Your personal data may be processed for the following purposes:

- General planning, fulfilment, and the management of the business relationship, including the negotiation, execution, and amendment of contracts or other agreements
- Administration such as the processing of payments, rating evaluations, accounting, auditing, as well as providing support
- Providing newsletters and other marketing communications
- Responding to inquiries from you
- General communication with you in connection with the business relationship

Sitero's legal bases for processing

- Contractual obligations: In certain cases, the processing of your personal data is necessary to fulfil a contract (Article 6(1)(b) of the General Data Protection Regulation).
- Legitimate interests: We may process your personal data on the basis of our legitimate interests in, for example, managing day-to-day operations in accordance with legitimate and fair business practices, including planning, execution and management of the cooperation or our legitimate interest in, for example, performing marketing activities (where consent is not required) and providing support. The processing may also be necessary for our legitimate interest in preventing fraud or establishing, defending, or asserting legal claims (Article 6(1)(f) of the General Data Protection Regulation).
- Legal obligations: The processing of your personal data will in some cases be necessary for compliance with legal obligations, such as our obligation to prevent illegal activities (Article 6(1)(c) of the General Data Protection Regulation.

Retention period

Your personal data will be stored for as long as is necessary to fulfil the business relationship.

<u>3.7 If you engage with Sitero's social media pages.</u>

Sitero and the social media providers through which Sitero posts and maintains content are jointly responsible for the processing of personal data collected in connection with your visit to any profile(s) maintained by Sitero.

Types of personal data collected
When you visit or interact with Sitero's social media profiles, Sitero [and the social media provider] may collect, process, and store the following types of personal data about you (if provided):

- Information available on your applicable social media profile, including your name, gender, civil status, workplace, interests, image, and your city
- Whether you "like" or have applied other reactions to our profile
- Comments you leave on our posts
- Data confirming that you have visited our profile(s)

Sitero processes your personal data for the following purposes:

- Improving our products and services, including our social media profiles and pages
- Conducting analysis about stakeholder engagement with our social media presence
- To be able to communicate with you
- General marketing purposes

Social media providers process for their own purposes and each has its own privacy notice that you should review to become familiar with their purposes for processing.

Sitero's legal basis for processing:
Legitimate interests: Sitero bases the processing of your personal data on our legitimate interests in being able to communicate with and market to you on our social media profiles, as well as our legitimate interest in improving our products and services (Article 6(1)(f) of the General Data Protection Regulation).

Retention period
Please refer to the privacy policy of the provider for each of the social media platforms for information on how long they store your personal data.

3.8 If you are a Customer of Sitero.
Sitero hosts and processes Customer Data, including any Personal Data contained therein, as a Processor at the direction of and pursuant to the instructions of Sitero's Customers.

Sitero also collects several other types of information from our Customers, and may process those data as a Controller, including:

- Information and correspondence our Customers and Users submit to us in connection with Support Services and Expert Services or other requests related to our Service.
- Information we receive directly from Customers or from our business partners in connection with our Customers' and Users' use of the Service or in connection with services provided by our business partners on their behalf, including configuration of the Subscription Service.
- Information related to Users' use of the Mobile Applications, including geographic location data and information regarding Users' Devices and OS identification, login credentials, language, and time zone.

- General information about Customers, including a Customer's company name and address, payment information, and the Customer representative's contact information for billing, marketing and contracting purposes ("General Information").

Purposes of Collection and Use
Sitero may use Personal Data submitted by our Customers and Users as necessary to provide the Service and Software Applications, including updating, enhancing, securing, and maintaining the Software Applications and to carry out Sitero's contractual obligations to its Customers. Sitero also obtains General Information in connection with providing the Service and maintaining Sitero's relationships with its Customers. Data will be retained in accordance with our internal policies on record retention unless otherwise required by law or contract agreement.

Third Party Disclosures
We may disclose Personal Data that our Customers and Users provide to our Services and Software Applications pursuant to our contract with our Customer:

- To our subsidiaries and affiliates;
- To contractors, business partners and service providers we use to support our Service;
- In the event Sitero sells or transfers all or a portion of its business or assets (including in the event of a merger, acquisition, joint venture, reorganization, dissolution, or liquidation), in which case Personal Data held by us about Users or relating to Customers may be among the assets transferred to the buyer or acquirer;
- If required to do so by law or legal process;
- In response to lawful requests from public authorities, including to meet national security, public interest, or law enforcement requirements.

4. Rights of California Residents

Subject to legal limitations, if you are a resident of California, you may have the right to make the following choices regarding your personal information:

Access to Your Personal Information. You may request access to your personal information by contacting us as described below. If required by law, upon request, we will grant you reasonable access to the personal information that we have about you. You may be entitled to ask us for a notice describing what categories of personal information (if any) we share with third parties or affiliates for direct marketing.

Changes to Your Personal Information. You may have a right to modify your personal information. You may contact us as described below in order to request that your information be modified. Note that we may keep historical information in our backup files as permitted by law.

Deletion of Your Personal Information. You may request that we delete your personal information by contacting us as described below. If required by law, we will grant a request to delete information,

but you should note that in many situations we must keep your personal information to comply with our legal obligations, resolve disputes, enforce our agreements, or for another one of our business purposes.

Objection to Certain Processing. You may object to our use or disclosure of your personal information by contacting us as described below.

Promotional Emails. You may choose to provide us with your email address for the purpose of allowing us to send communications and promotional materials to you. You can stop receiving most emails by following the unsubscribe instructions in emails that you receive. If you decide not to receive these emails, we may still send you service-related communications.

Revocation of Consent. If you revoke your consent for the processing of personal information then we may no longer be able to provide you services. In some cases, we may limit or deny your request to revoke consent if the law permits or requires us to do so, or if we are unable to adequately verify your identity. You may revoke consent to processing (where such processing is based upon consent) by contacting us at the address described below.

Please note that, as required by law, we will require you to prove your identity. We may verify your identity by telephone call or email. Depending on your request, we will ask for information such as your name, your physical address, or the name of the clinical trial in which you participated. We may also ask you to provide a signed declaration confirming your identity. Following a request, we will use reasonable efforts to supply, correct or delete personal information about you in our files.

5. Access & Correction

Individuals in the European Union, United Kingdom (and Gibraltar), and Switzerland generally have the right to access their Personal Data. As a Processor processing Personal Data on behalf of its Customers in the course of providing the Subscription Service, Sitero does not own or control such data and does not have a direct relationship with the Users whose Personal Data may be processed in connection with providing the Subscription Service. Since each Customer is in control of what information, including any Personal Data, it collects from its Users, how that information is used and disclosed, and how that information can be changed, Users of the Subscription Service should contact the applicable Customer administrator with any inquiries about how to access or correct Personal Data contained in Customer Data. To the extent a User makes an access or correction request to Sitero, we will refer the request to the appropriate Sitero Customer and will support such Customer as needed in responding to any request.

To access or correct any General Information Customer has provided, or other personal data in respect of which Sitero acts as a Controller, the relevant individual should contact us at privacy@Sitero.com.

6. Choice

Subject to the below paragraph, in accordance with the Principles, Sitero will offer Customers and Users the ability to request that Sitero limit the use and disclosure of their Personal Data to the extent it: (i) discloses their Personal Data to third party Controllers, or (ii) uses their Personal Data for a purpose that is materially different from the purposes for which the Personal Data was originally collected or subsequently authorized by the Customer or User. To the extent required by the Principles and applicable laws, Sitero also will obtain opt-in consent if it engages in certain uses or disclosures of Sensitive Data. Unless permitted by applicable laws and the Principles, Sitero uses Personal Data only for purposes that are materially the same as those indicated in this Policy.

Sitero may disclose Personal Data of Customers and Users without offering an opportunity to opt out, and may be required to disclose the Personal Data, (i) to third-party Processors that Sitero has retained to perform services on its behalf and pursuant to its instructions, (ii) if it is permitted or required to do so by law or legal process, or (iii) in response to lawful requests from public authorities, including to meet national security, public interest, or law enforcement requirements. Sitero also reserves the right to transfer Personal Data in the event of an audit or if the company sells or transfers all or a portion of its business or assets (including in the event of a merger, acquisition, joint venture, reorganization, dissolution, or liquidation).

7. Liability for Onward Transfers

Sitero complies with the DPF's Principle regarding accountability for onward transfers as demonstrated in our customer agreements and agreements with sub-processors and vendors. Sitero remains liable under the Principles if its onward transfer recipients process Personal Data in a manner inconsistent with the Principles, unless Sitero proves that it was not responsible for the event giving rise to the damage.

8. Dispute Resolution

If Sitero maintains your Personal Data in one of the Services within the scope of our DPF certification, you may direct any inquiries or complaints concerning our DPF compliance to privacy@Sitero.com. Sitero shall respond within 45 days.

If your complaint cannot be resolved through Sitero's internal processes, Sitero will cooperate with the International Centre for Dispute Resolution-American Arbitration Association (ICDR-AAA) pursuant to the applicable ICDR-AAA procedures, available on the ICDR-AAA website (https://go.adr.org/dpf_irm.html). In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Sitero 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-American Arbitration Association (ICDR-AAA), an alternative dispute resolution provider based in the United States. 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 here for more information or to file a complaint. The services of the ICDR-AAA are provided at no cost to you.

The ICDR-AAA alternative dispute resolution process may be commenced as provided for in the relevant ICDR-AAA rules and procedures. The ICDR-AAA neutral may propose any appropriate remedy, such as deletion of the relevant Personal Data, publicity for findings of non-compliance, payment of compensation for losses incurred as a result of non- compliance, or cessation of processing of Personal Data of the Customer or User who brought the complaint. The ICDR-AAA neutral, or the Customer or User, also may refer the matter to the U.S. Federal Trade Commission (FTC). As the FTC has jurisdiction over Sitero's compliance 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), Sitero is subject to the investigatory and enforcement powers of the FTC. Under certain circumstances, Customers and Users may be able to invoke binding arbitration to address complaints about Sitero's compliance with the Principles.

9. How to Contact Sitero

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Sitero commits to resolve DPF Principles-related complaints about our collection and use of your Personal Data. EU and UK and Swiss individuals with inquiries (including if you need to update, change, or remove your information) 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 Sitero at: privacy@Sitero.com.

If it's not possible to contact Sitero at privacy@Sitero.com, you can contact us by regular mail addressed to:
Sitero, LLC
Attn: Privacy
3119 Ponce de Leon
Coral Gables, Florida 33134

Alternatively, regular mail may also be directed to our UK -based subsidiary, Sitero UK, Ltd., by addressing it to:
Sitero UK, Ltd
Attn: Legal Department
6th Floor, 9 Appold Street, London, EC2A 2AP, United Kingdom

10. Adherence to Policies and Procedures

All Sitero Employees and contractors are required to comply with all established Sitero policies, procedures, and standards, as amended from time to time. Failure to do so will be considered just cause for disciplinary action, up to and including termination.

11. Policy Distribution and Awareness

Sitero intends that all Sitero Policies will be retained in the controlled document management system and active Sitero Policies will be made available on the quality assurance portal, as well as applicable intranet and external sites. Certain Sitero Policies may require that the parties to whom the policy applies, complete training or acknowledge that they have read, understood, and agree to comply with the policy. Any such trainings, attestations, or communications are determined and managed by the Policy Owner and Owning Department.

Role	Description	Frequency	Document Retention
All Employees	Live or Web Based Training	Annual	Learning Management System Training Records

12. Program Governance

This policy provides general guidance regarding compliance with the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework set forth by the United States Department of Commerce with respect to the collection, use and retention of Personal Data transferred from the European Union, United Kingdom (and Gibraltar), and Switzerland to the United States. More specific information concerning Sitero's role and responsibilities regarding data transfer can be found in our customer agreements.

The below roles, departments, and teams are key to the implementation of this policy and include those parties who are responsible for completing activities described within this document and/or those who enforce, distribute, or must adhere to this policy.

Privacy Team

· Review this policy annually.

· Adhere to this policy when reviewing Vendor Risk Assessments, contract agreements, Data Protection Impact Assessments and any other areas that involve the transfer of personal data from the European Union, United Kingdom, and Switzerland to the United States.

Data Protection Officer

Advise the business in relation to enforcing this policy when Sitero or its Affiliates transfers personal data from the European Union, United Kingdom, and Switzerland to the United States.