SailPoint IdentityIQ Privacy FAQs

Many organizations are required by law to identify, assess, and minimize privacy risks associated with data processing activities, especially as they relate to new systems or technology. The purpose of this Data Privacy Questionnaire is to answer common questions related to how SailPoint's IdentityIQ software might impact how data is collected, used, shared, and maintained within your organization. While it is not meant as a substitute for a formal Privacy Impact Assessment, it may assist you in evaluating and managing your organization's data privacy risks.

1. What is the name of the product or service?

IdentityIQ is the name of the on-premises software product provided by SailPoint.

2. Who is the data controller?

When using the IdentityIQ software, the customer is the data controller.

3. Who is the data processor?

When using the IdentityIQ software, the customer is the data controller.

IdentityIQ is on-premises software that is operated in your data center or the data center or cloud service of your choosing. SailPoint does not need and does not expect to receive access to the information loaded into the IdentityIQ software in your environment in order to provide the software and the support and maintenance services. Support does not require or include remote access to your environment.

If we are engaged to provide professional services, SailPoint will likely have limited access to at least some of the information in the software during the project, but the means by which we access information and the information we can access is determined by you.

SailPoint will receive business and personal data, as you would expect in the course of maintaining a business relationship. Where we process personal data received in the context of our business relationship, SailPoint acts as the data processor for our customer, who is the data controller.

4. What is your address?

SailPoint's corporate headquarters is located at:

11120 Four Points Dr, Ste 100, Austin, Texas 78726, USA

Other office locations are listed at https://www.sailpoint.com/contact-us/.

5. Description of the product or service.

IdentityIQ is our on-premises identity security solution, which can be hosted in the public cloud or deployed in a customer's data center. It provides large, complex enterprise customers a unified and highly configurable identity security solution that consistently applies business and security policies as well as role and risk models across applications and data on-premises or hosted in the cloud. IdentityIQ enables organizations to:

- Empower users to request and gain access to enterprise applications and data;
- Enable business users to reset their passwords via self-service tools without the need for IT involvement;
- Provide on-demand visibility to IT, business, and risk managers into "which identities have access to what resources" to help make business decisions, improve security, and meet audit requirements;
- Improve security and eliminate common weak points associated with data breaches, including weak passwords, orphaned accounts, entitlement creep and separation-of-duties policy violations; and
- Manage compliance using automated access certifications and policy management.

We package and price IdentityIQ into Core Modules and Advanced Integration Modules. All customers leverage the IdentityIQ Governance Platform, which provides the base features of the solution, including the identity warehouse, workflow engine and governance models. The three Core Modules include:

- Lifecycle Manager: This module provides a business-oriented solution that delivers access securely and cost effectively. The self-service access request capabilities feature an intuitive user interface that empowers business users to take an active role in managing changes to their access while greatly reducing the burden on IT organizations. Automated provisioning manages the business processes of granting, modifying and revoking access throughout a user's lifecycle with an organization, whether that user is an employee, contractor, or business partner. Changes to user access can be automatically provisioned via a large library of direct connectors for applications such as Workday and SAP or synchronized with IT service management solutions such as ServiceNow.
- Compliance Manager: This module enables the business to improve compliance and audit performance while lowering costs. It provides business user friendly access certifications and automated policy management controls (e.g., separation-of-duty violation reporting) that are designed to simplify and streamline audit processes across all applications and data. Built-in audit reporting and analytics give IT, business, and audit teams visibility into, and management over, all compliance activities in the organization.
- File Access Manager: This module secures access to the growing amount of data stored in file servers, collaboration portals, mailboxes, and cloud storage systems. It helps organizations identify where sensitive data resides, which identities have access to it, and how they are using it and then puts effective controls in place to secure it. File Access Manager is designed to interoperate with the Compliance Manager and Lifecycle Manager modules to provide comprehensive visibility and governance over user access to all data. By augmenting identity data from structured systems with

data from unstructured data targets, organizations can more quickly identify and mitigate risks, spot compliance issues, and make the right decisions when granting or revoking access to sensitive data.

The Advanced Integration Modules provide connectivity to target application platforms such as SAP, mainframes, and file storage systems.

6. Individuals from or about whom data will be collected and processed.

The customer will determine whose data is loaded into IdentityIQ. The IdentityIQ software is typically licensed for use in managing the customer's employees and contractors, in which case only employee and contractor data is processed.

7. What types of data will be processed?

The customer will determine what types of data, including personal data, are loaded into IdentityIQ. Typically, data in IdentityIQ is limited to business contact information, such as employee name, title, email, office and/or mobile phone number, and office address; employment information such as manager, role, etc.; entitlement data (what applications can an individual access and what permissions do they have); and metadata, such as IP address.

8. What sensitive categories of data will be processed?

SailPoint does not expect sensitive personal data, including special categories of personal data as referenced in Art. 9 GDPR, such as health data, political opinions, religious or philosophical beliefs, trade union membership, race or ethnic origin, sexual orientation, genetic data, biometric data, criminal activity data, financial account number or tax ID number will be loaded in IdentityIQ or provided to SailPoint for any purpose.

9. What are the sources of the data to be processed?

The customer will determine from whom the data is collected and whether this is done on an automated or voluntary basis. SailPoint will not collect personal information on the customer's behalf.

10. What are the purposes of the processing?

Data loaded in IdentityIQ is typically pulled from other systems in the customer's environment. Data is aggregated in IdentityIQ to provide better visibility into who has access to what applications or systems. IdentityIQ allows customers to certify user access privileges, which may be required to meet legal, regulatory, and/or corporate governance requirements. IdentityIQ also allows customers to streamline the onboarding and off-boarding process, enabling IT to quickly grant employees access to the applications they need to do their jobs or quickly remove access when it is no longer needed.

The customer will determine its purpose in using IdentityIQ and processing personal data within IdentityIQ. Because IdentityIQ aggregates data from other applications in the customer environment, the purpose for data processing in IdentityIQ will likely be consistent with the purpose for which it was collected and processed in the other applications.

IdentityIQ is typically used to provide identity governance capabilities for employees and contractors. Identity governance is designed to ensure the right people have access to the right applications and information in an organization. The customer is solely responsible for determining the legal basis for its data processing. The customer's legal basis for processing may be legitimate business interests and/or legal requirements. We would not expect customers to process employee data on the basis of consent, but the customer is responsible for that determination.

Information is loaded into IdentityIQ by the customer. As such, the customer will determine whether the data they load into IdentityIQ is necessary for and limited to a specific purpose.

Where SailPoint acts as the data processor, we will only process the data as instructed by the customer, who is the data controller, and as required to fulfill our contractual obligations.

11. Will processing include automated decision making and profiling?

This will be determined by the customer. SailPoint does not expect that the IdentityIQ software will be used to make automated decision making or profiling decisions that result in legal effects for the data subject. To the extent the service is used for these purposes, the customer will be responsible for determining the legal basis for such processing.

12. Will SailPoint have access to the data?

IdentityIQ is on-premises software that is operated in your datacenter or the datacenter or cloud service of your choosing. SailPoint does not need and does not expect to receive access to the data loaded into the IdentityIQ software in your environment in the course of providing the software and the support and maintenance services. Support does not require or include remote access to the customer environment.

If we are engaged to provide professional services, SailPoint will likely have limited access to at least some of the data in the software during the project, but the means by which we access the data and the data we can access will be determined by you.

SailPoint will receive business and personal data in the course of maintaining the business relationship. SailPoint stores elements of your business information, including business contact information (employee name, title, email, phone number, address, manager, role, etc.) for the customer personnel who interact directly with SailPoint, contract details (copies of fully executed agreements and summary details such as products and services purchased, contract effective date and renewal dates, amounts, etc.) and information about the customer IT environment in which the IdentityIQ software is installed (software version and related operating system, application server, database, hardware specifications, etc.). This information is stored in a CRM database that physically resides in the US and is accessible to certain SailPoint personnel worldwide (access is granted by role on a least privileged access/need to know basis).

Troubleshooting information that may be provided to SailPoint support by your system administrators or project team members is in addition to the business information described above and may include screenshots, log files, or XML objects. This troubleshooting information can be sanitized to remove or redact personal or sensitive data before being provided to SailPoint. Once transmitted to SailPoint, this troubleshooting information will physically reside on servers in the US and be accessible to SailPoint support personnel worldwide (access is granted by role on a least privileged access/need to know basis).

Some of your employees may be granted access to certain portals/websites made available by SailPoint to its customers (i.e. Compass and Identity University sites). Access to such portals/websites will require each user to provide their name, company name, and work email in order to establish an account that will allow access to the site. The user may also provide other business contact information, such as title, phone number, office address, etc. A limited subset of your employees and contractors will require access to these SailPoint sites. The user information provided for this purpose will be stored on servers physically located in the US and will be visible to SailPoint staff with a need to access such information from locations worldwide.

13. What third parties will assist SailPoint with the data processing?

SailPoint Technologies, Inc. is a data processor who will receive the personal data from the customer, who is the data controller. SailPoint leverages its Affiliates and a range of third-party sub-processors to assist it in providing the contracted services. SailPoint uses third-party sub-processors to provide ancillary support services and account administration. Depending on the geographic location of customer and the nature of the services provided, SailPoint may use one or more of its Affiliates as sub-processors. A list of sub-processors is available at https://www.sailpoint.com/legal/sub-processors/.

14. Where will the data be processed? From where may it be accessed?

The customer will determine from where the data comes and from where the customer and its users access the data. The customer will also determine the location where the IdentityIQ software is hosted.

Where personal data is provided by the customer and processed by SailPoint, it may be processed in the US and any of the locations shown in the list of sub-processors. SailPoint's corporate systems, such as email and support ticketing, reside in the US. The data in these corporate systems will physically reside in the US and be accessible to SailPoint employees worldwide (access is granted by role on a least privileged access/need to know basis).

15. What notice or information will be provided to individuals regarding information collection and processing?

The customer is responsible for providing any notices to individuals through employment contracts, posted policies or other means prior to collecting data and should insure that information provided to individuals includes all required information. IdentityIQ supports a configurable "click-through" usage agreement or notice. SailPoint will not collect personal information on the customer’s behalf.

16. How will individuals exercise their rights granted under data protection laws?

SailPoint will assist the customer in responding to any requests regarding individual privacy rights, including any right to access, erase, edit, restrict, export, or object to processing of personal data by SailPoint. In the event that an individual makes a request directly to SailPoint related to personal data provided by the customer, we will not respond without the customer's authorization.

17. Will individuals be allowed to withdraw their consent to processing, if applicable?

The customer is responsible for determining the legal basis under which they are processing information in IdentityIQ. The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone’s life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

As the information in IdentityIQ is generally obtained in the context of the employment relationship and used as required for the customer to satisfy legal obligations and/or for the legitimate interests of the business (such as security and compliance), consent may not be applicable.

Where SailPoint is a data processor acting on behalf of the customer, who is the data controller, SailPoint processes customer information for legitimate business purposes and in fulfillment of our contractual obligations and does not rely on consent as the legal basis for processing customer information.

18. Is personal information kept accurate and up-to-date?

The customer loads information into IdentityIQ and is responsible for ensuring that this information is kept accurate and up-to-date.

Where SailPoint maintains customer business and personal data, we will update that information on request and we periodically remove inactive accounts from our portals.

19. What marketing communications, if any, will individuals receive?

SailPoint does not have access to the information loaded into IdentityIQ and would not use the information loaded into IdentityIQ for marketing or advertising purposes should we be given access during a professional services engagement.

For the users in your company who sign up for an account through our Compass customer portal or through www.sailpoint.com, we may send messages related to SailPoint events or products. These users can determine what type of information they receive and always have the option of opting out of communications.

20. For how long will data be processed and what will happen to the data once it has been processed?

The customer determines how long data is processed in its instance of IdentityIQ and how data is updated in and/or deleted from its instance of IdentityIQ.

SailPoint will return or destroy customer data upon request following termination or expiration of the contractual relationship, unless customer data must be retained to meet legal, accounting, or corporate governance requirements. Elements of customer data retained will only be used for the purpose for which they were retained and will be protected from any further processing.

21. What security measures exist to protect the data?

The customer is responsible for establishing and maintaining the security controls in its environment.

IdentityIQ utilizes AES-256 encryption for all sensitive data and passwords. Keys are generated and managed within the IdentityIQ application and are stored in a local, password-protected key-store. IdentityIQ can also leverage a third-party tool for encryption. In addition, data masking can be accomplished for attributes classified by the customer. IdentityIQ supports encryption over the wire when reading and writing data from/to managed systems exploiting available encryption technologies such as TLS and SSH when connecting to directories, systems, and databases. IdentityIQ provides encryption via TLS for many other systems while data is in transit.

In the web layer, IdentityIQ uses JavaServer Faces (JSF) which is an industry standard, official Java API for rendering web application pages. JSF makes sure that all aspects of the component rendering are appropriately escaped to prevent instruction of scripting vulnerabilities. For the portions of the product where JavaScript toolkits and AJAX are used to improve the usability and scalability of the product, all input is passed through cross-site scripting checks to make sure that the data is not returned to the browser in a way that will cause it to be executed.

In the persistence layer, IdentityIQ uses the industry standard Hibernate package. SQL injection is prevented through the use of parameterized prepared statements in Hibernate. IdentityIQ has a few instances where direct SQL is used through Hibernate's Query Language (HQL) and in these cases automated test suites are used to inspect and catch any issues that might be introduced.

IdentityIQ is certified for Common Criteria ISO/IEC 15408 conformance, specifically the Common Criteria IT Security Evaluation Enterprise Security Management Identity and Credential Management Protection Profile. Common Criteria Certification provides independent, objective validation of the reliability, quality, and trustworthiness of IT products. Common Criteria Certification is a rigorous process that includes product testing by a third-party laboratory that has been accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) to perform evaluation of products against security requirements. Common Criteria Certification is a requirement for software used by the US government on national security systems. The international scope of Common Criteria, currently adopted by 31 countries, allows users from other countries to purchase IT products with the same level of confidence, due to the recognition of the certification across the 31 complying nations. More information on Common Criteria Certification is available at https://www.commoncriteriaportal.org/, and the IdentityIQ certification documents are available at https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11043.

SailPoint is ISO 27001 certified, and the certificate is available at https://docs.sailpoint.com/wp-content/uploads/SailPoint-ISO-27001-Certificate.pdf. Information on security measures used to protect information on SailPoint systems can be provided on request.

22. Have privacy by design and default principles been implemented?

The customer is responsible for implementing privacy principles in its environment.

SailPoint includes risk assessment in all elements of our business, including technology acquisition and implementation, policy and procedure design, physical security, and product design and build. As it relates to IdentityIQ, security and privacy considerations are integrated throughout the software development lifecycle (SDLC).

23. Is there a personal data security breach management policy and team in place for incident response?

The customer is responsible for its IdentityIQ environment, including security breach management.

SailPoint maintains a Security Incident Response Plan, which specifies the steps, roles, and responsibilities should a security incident occur. This policy addresses remediation and follow-through to ensure the issue is understood and fully addressed. SailPoint will notify the customer of any security incident that involves loss of customer data.

24. If the data will be transferred from its country of origin to the US, what measures are in place to legitimize those data exports?

Where personal data originates from the European Economic Area and is transferred to the United States, SailPoint agrees to comply with the provisions of the EU-U.S. Privacy Shield Framework and makes an affirmative commitment to adhere to EU- U.S. Privacy Shield Principles. Where personal data originates from Switzerland and is transferred to the United States, SailPoint agrees to comply with the provisions of the U.S.-Swiss Privacy Shield Framework and makes an affirmative commitment to adhere to the U.S.-Swiss Privacy Shield Principles.

On July 16, 2020, the Court of Justice of the European Union (CJEU) issued a judgment which made the EU-U.S. Privacy Shield Framework no longer a valid mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States. Following the CJEU's decision, the Swiss Federal Data Protection and Information Commissioner also concluded that the Swiss-U.S. Privacy Shield no longer provides a valid mechanism for the transfer of personal data from Switzerland to the United States. However, SailPoint continues to honor its commitments under the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework, along with reliance on alternative mechanisms to legitimize international personal data transfers from the European Union or Switzerland to the United States, such as by implementing Standard Contractual Clauses.

SailPoint will enter into a Data Protection Addendum, including Standard Contractual Clauses/Model Clauses (using the form specified by the European Commission), as part of the Software License Agreement. Standard contract terms are available at https://www.sailpoint.com/legal/customer-agreements/.

25. Does SailPoint have an appointed representative for data protection matters in the EU?

SailPoint has appointed a Data Protection Officer who can be reached at privacy@sailpoint.com.

26. Has SailPoint allocated sufficient resources (in time and money) for mitigating identified privacy risks?

SailPoint allocates resources as appropriate to mitigate identified risks.

27. What is SailPoint’s role with regard to the California Consumer Privacy Act of 2018 (“CCPA”)?

IdentityIQ is an on-premises software application. The only ongoing services provided as part of IdentityIQ are support and maintenance services for the software. In addition, the customer may choose to engage SailPoint to provide professional services (e.g. implementation services, expert services, and training services). In providing these services to the customer, SailPoint acts as a Service Provider as defined in CCPA section 1798.140(v). To the extent that a customer discloses any data to SailPoint, it is solely for a valid business purpose for SailPoint to provide these services.

28. Will SailPoint sell customer data?

SailPoint will not sell customer data, including all definitions of “sell” included in section 1798.140(t) of the CCPA.

29. What are the restrictions under which SailPoint operates with respect to the customer’s data?

In addition to not selling customer data, as a service provider under the CCPA SailPoint will not retain, use, or disclose a customer’s data for a commercial purpose other than in providing the services specified in the agreement with the customer.

30. How will data processing responsibilities be determined?

Each party’s responsibilities will be outlined in a mutually agreed upon contract. Responsibilities specific to data processing can be set forth in a Data Processing Addendum or other privacy related addendum.