SailPoint IdentityNow and AI Services 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 IdentityNow and AI services (hereinafter the "SaaS Services") might impact how data is collected, used, shared, and maintained within your organization. While it is not meant as a substitute for a formal Data 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?

IdentityNow is the name of the SailPoint identity governance service.

The SailPoint AI services currently include Access Insights, Recommendation Engine, and Access Modeling.

2. Who is the data controller?

When using the SaaS Services, the customer is the data controller.

3. Who is the data processor?

SailPoint Technologies, Inc. ("SailPoint") acts as the data processor for our customers that use the SaaS Services.

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.

IdentityNow is a multi-tenant, microservices-based, SaaS identity governance platform that allows organizations to automate and control user provisioning, access requests, separation-of-duties policies, access certification for auditors, and password management.

The SailPoint AI services, Access Modeling, Recommendation Engine, and Access Insights, are multi-tenant, microservices-based, SaaS solutions designed with AI-driven automation, machine learning and analytics, to work in conjunction with SailPoint's IdentityNow service (or on-premises IdentityIQ software) to remove complexity and empower organizations to make intelligent, automated identity decisions.

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

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

7. What types of data will be processed?

The customer will determine what types of data, including personal data, are loaded into the SaaS Services.

Typically, data in IdentityNow is limited to business contact type information, such as employee name, title, email, office and/or mobile phone number, office address, manager, role, etc.; entitlement data (what applications can the employee access and what permissions do they have); and technical information, such as IP address and geolocation data.

Data in the AI services will be the data or a subset of the data in IdentityNow plus activity data from IdentityNow. Some of the information stored in the AI services is required and some is optionally configured by the customer. The information stored in the AI services is restricted to the following information:

1. Lists of objects: identities, applications, accounts, access profiles, roles, access requests, identity request items, entitlements, work groups, certifications, policy violations, and compliance events.

2. For each identity, a non-configurable set of identity attributes is collected: Internal (SailPoint-specific) Identity Identifier, Roles, Access Profiles, Accounts, Applications, and Entitlements. For each identity, a configurable list of identity attributes is also collected. These additional attributes include details such as first name, last name, department, and other attributes. These attributes are at the customer's discretion and are configured during the provisioning of the customer's tenant.

3. For each certification, a non-configurable set of related objects is collected: name of the cert, the certification campaign that the cert is part of, and each individual certification item within the certification.

4. For each compliance event, the following information is stored: date and time of the compliance event and type of event (add/remove access profile, add/remove account, add/remove application, add/remove entitlement, entitlement review, access request, account state change, and password change).

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, or financial account number or tax ID number will be processed in the SaaS Services. SailPoint's standard contractual terms included in the Software as a Service Agreement (available at https://www.sailpoint.com/legal/customer-agreements/) include restrictions against

providing this type of personal data.

> Restrictions. Customer and its Users shall not, and shall not permit any third party to… send or store in the SaaS Service any personal health data, credit card data, personal finance data, government issued identification numbers, or other sensitive data which may be subject to the Health Insurance Portability and Accountability Act, Gramm-Leach-Bliley Act, the Payment Card Industry Data Security Standards, or similar laws…

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 IdentityNow is typically pulled from other systems in the customer's environment, and data in the AI services is pulled from IdentityNow (or the on-premises IdentityIQ software). Data is aggregated in IdentityNow to provide better visibility into who has access to what applications and systems. IdentityNow allows customers to certify user access privileges, which may be required to meet legal, regulatory and/or corporate governance requirements. IdentityNow 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 AI services use artificial intelligence (AI) and machine learning (ML) to enhance the utility of IdentityNow (or the on-premises IdentityIQ software).

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

The SaaS Services are 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. SailPoint 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 the SaaS Services by the customer. As such, the customer will determine whether the data they load into the SaaS Services is necessary for and limited to a specific purpose. SailPoint, as the data processor, will only process the data as instructed by the customer, who is the data controller.

11. Will processing include automated decision making and profiling?

This will be determined by the customer. SailPoint does not expect that the SaaS Services will be used for automated decision making or profiling. 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 in the SaaS Services?

A customer's SaaS Services environment is accessible by SailPoint DevOps and support personnel for support purposes. DevOps and support personnel are able to access data in your SaaS Services environment similar to the customer's system administrator.

This data is generally limited to name, email address, other business contact information and entitlement information (what applications can an employee access and what permissions do they have). SailPoint personnel are not able to access sensitive information, including passwords and challenge questions, which is encrypted.

If SailPoint is engaged to provide professional services, SailPoint professional services personnel will have access to the customer's SaaS Services environment during the engagement.

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

For the SaaS Services, SailPoint is a data processor who will receive the personal data from the customer, who is the data controller.

SailPoint leverages Amazon Web Services (AWS) to host the SaaS Services. While AWS doesn't have access to information in the SaaS Services, they do have physical control of the systems and data. SailPoint leverages Twilio to provide two-factor authentication via mobile device within IdentityNow. If this functionality is enabled by the customer's system administrators, mobile phone numbers are shared with Twilio for this purpose.

A list of other third-party and affiliate sub-processors who may assist in provision of the services 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 they access the data. The customer will also determine the location where the SaaS Services are hosted. SailPoint leverages Amazon Web Services (AWS) for hosting the SaaS Services. The SaaS Services can be hosted in any one of the following AWS Regions, AWS US East (Northern Virginia) Region, AWS US West (Oregon), AWS Canada (Montreal), AWS Europe (Frankfurt) Region, AWS Europe (London) Region, AWS Asia Pacific (Tokyo), or AWS Asia Pacific (Sydney) Region. Although the data in the SaaS Services will physically reside in the chosen location, the customer's SaaS Services environment will be managed and maintained by SailPoint DevOps and support personnel located in the US, UK, India, Singapore and Australia.

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 contract, posted policies or other means prior to collecting data and should insure that information provided to individuals includes all required information. IdentityNow supports a customer configurable 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 information. In the event that an individual makes a request directly to SailPoint, we will not respond without getting the customer's prior 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 the SaaS Services. 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 the SaaS Services 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 the SaaS Services 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 use the information loaded to the SaaS Services for marketing or advertising purposes.

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 them 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?

SailPoint will only process customer data in the SaaS Services for the duration of the SaaS Services subscription term. The customer can edit and delete data in IdentityNow during the subscription term, and the customer can request that SailPoint delete data in the AI services during the subscription term. Within 30 days of termination or expiration of the SaaS Services, SailPoint will delete the customer instance of the SaaS Services and all customer data stored therein. Customer data from the SaaS Services that is archived on back-up systems will be securely isolated and protected from any further processing for the 30-day duration that the backup is held.

Where SailPoint maintains customer business and personal data, we will update or delete that information on request.

21. What security measures exist to protect the data?

The SaaS Services encrypt data in transit and at rest. For a description of the technical and organizational security measures employed by SailPoint, please see SailPoint's SaaS Data Security Program at https://www.sailpoint.com/legal/customer-agreements/.

The SaaS Services are ISO 27001 certified, and the certificate is available at https://docs.sailpoint.com/wp-content/uploads/SailPoint-ISO-27001-Certificate.pdf. SailPoint completes a SOC 1 Type 2 and SOC 2 Type 2 audit of the SaaS Services annually. The SOC 3 report for

the SaaS Services is available at https://docs.sailpoint.com/wp-content/uploads/SailPoint-IdentityNow-SOC-3-Report.pdf.

The SaaS Services are hosted on Amazon Web Services (AWS) cloud platform, which provides substantial protection for the base infrastructure, including the virtual servers, data storage, databases, network, and other resources. AWS follows a rigorous approach to security and maintains compliance with ISO 9001, ISO 27001, HIPAA, PCI, SOC, CSA, FedRAMP, FERPA, and other compliance programs. Please see https://aws.amazon.com/compliance/programs/ for additional information.

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

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 the SaaS Services, 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?

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. In addition, 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 Information originates from the European Economic Area and is transferred to the United States, SailPoint agrees to comply with the EU-U.S. Privacy Shield Framework and makes an affirmative commitment to adhere to EU-U.S. Privacy Shield Principles. Where Personal Information originates from Switzerland and is transferred to the United States, SailPoint agrees to comply with all 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, as part of the Software as a Service Agreement. This is included in the standard terms for EMEA customers and is an option for all other customers to include where appropriate. 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")?

In providing the SaaS Services to the customer, SailPoint acts as a Service Provider as defined in CCPA section 1798.140(v). The customer discloses data to SailPoint solely for a valid business purpose for SailPoint to provide the SaaS Services, including support and maintenance 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.