Identity and Access Management of ESMA Systems

Record of ESMA activities processing personal data, based on Article 31 of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

Nr.	Item	Record information
Identity and Access Management of ESMA Systems		
1	**Last update of the record**	06/07/2021
2	**Reference number**	ESMA65-8-7678
3	**Name and contact details of controller**	ESMA's ICT Head of Unit itdpo@esma.europa.eu European Securities and Markets Authority (ESMA) 201-203 Rue de Bercy 75012 Paris France

4	**ESMA area entrusted with processing**	ESMA/RES/Human Resources ESMA/RES/ICT (Infrastructure and Communications Technologies Team) ESMA/RES/CPS (Corporate Services Team)
5	**Processors (if any)**	Sailpoint Technologies
6	**Name and contact details of DPO**	ESMA DPO - dpo@esma.europa.eu
7	**Name and contact details of processor (where applicable)**	Sailpoint Technologies United States 11120 Four Points Drive, Suite 100 Austin, TX 78726 1-512-346-2000 Phone
8	**Purpose of the processing**	IAMAN is an Identity and Access Management system that centralises the provisioning of user accounts to access ESMA business applications. This platform manages the entire user lifecycle: user self-registration, assignment of access permissions to ESMA's business systems, removal of permissions when no longer needed and decommissioning of user accounts. It also provides a selfservice password reset mechanism that allows a user to change or reset his/her password without any third-party intervention.
9	**Description of categories of persons whose data ESMA**	ESMA collects the name, work email address and organisation to identify and authenticate users of

		ESMA business applications. Additionally, the mobile phone number is collected and used to send text

	processes and list of data categories	messages (SMS) with one-time passwords (OTPs) to access systems that require strong authentication. Data is collected from ESMA staff – CA, TA, Trainees –, External Consultants, NCAs, or other external entities having access to ESMA's ICT systems.
10	**Time limit for keeping the data**	Personal data may be retained for as long as the data subject has access to ESMA's business systems. Personal data with regards to non recertified users can be retained for one year.

11	**Recipients of the data**	Information is only accessible to authorised ESMA staff and contractors responsible for the management and support of ESMA user account on systems. SailPoint uses its Affiliates and a range of third party Sub-processors to assist it in providing the Services. These Sub-processors are set out below. For further clarity (i) The Third party Sub-processors relate directly to the SaaS Services being provided and will have no access to any Customer Personal Data at any time (ii); SailPoint Affiliates are where SailPoint's professional services, legal& contracts, Support engineers and DevOps personnel reside (as all of the same may be included in or related to this Agreement), save that only relevant personnel will have access to any Customer Personal Data at any time, solely for the purposes of their specific role. As indicated in the signed DPA, SailPoint will process Customer Personal Data only for the purposes described in this DPA and only in accordance with Customer's documented lawful instructions. The parties agree that this DPA and the Agreement set out the Customer's complete and final instructions to SailPoint in relation to the

processing of Customer Personal Data. Additional processing outside the scope of these instructions (if any) will require prior written agreement between Customer and SailPoint.

Third-Party sub-processors

1 Service-Specific Sub-processors

Entity Name	Location	Purpose
Amazon Web Services, Inc. 410 Terry Avenue North Seattle, WA 98109, USA	USA	Hosting provider for the SaaS Services – hosting will occur in AWS' Frankfurt region (thus all business related data concerning the service, including personal data, will be permanently hosted only in an EU datacentre).
Twilio, Inc. 375 Beale Street, Suite 300 San Francisco, CA 94105, USA	USA	Two-factor authentication communication via mobile device provider for the SaaS Services if Customer elects to enable this feature.
salesforce.com, inc. 415 Mission Street, 3rd Floor San Francisco, CA 94105, USA	USA	ticketing system for Support and Maintenance Services

2 Ancillary Sub-processors

Entity Name	Location	Purpose
SailPoint International, Inc	USA	Head Office and location of SailPoint customer management systems (SalesForce, Twilio
SailPoint Technologies GmbH	DE	
SailPoint Technologies India Private Ltd.	India	DevOps
SailPoint Technologies Netherlands B.V.	NL	IDN Experts
SailPoint Technologies SARL (Switzerland), including registrations in Belgium and France	Switzerland	(Sales and SE and PS services)
SailPoint Technologies UK Ltd.	UK	Legal & Contracts support

12	**Are there any transfers of personal data to third countries or international organisations?**	Yes, All sub-processors listed in cell 11 (Recipients of the Data) may process customer personal data. SailPoint uses the same sub-processors for all customers of a given solution.

	If so, to which ones and with which safeguards?	Types of personal data processed: 1. Identification and contact data (name, address, title, contact details): 2. Employment details (job title, role, manager); and/or 3. IT information (entitlements, IP address, usage data, cookies data, geolocation data). ESMA will not provide or make available to SailPoint or the Services Special categories of Personal Data. SailPoint requires all sub-processors comply with law, including having adequate data protection, security and confidentiality. Upon the first signature of the SaaS services contract, ESMA had already included in the contractual annexes signed with the sub-processor (SailPoint Inc) the Standard Contract Clauses (SCCs) on personal data processing provided by the European Commission, based on the former Data protection Directive (95/46/EC), which was the only instrument available at that time (August 2020), and, as per the data contractual clauses for the hosting of the service this will occur in AWS' Frankfurt region.

13	**General description of security measures, where possible.**	In order to protect your personal data, a number of technical and organisational measures have been put in place. ESMA's IT infrastructure is protected by physical and logical security measures: physical access to the servers is controlled, network firewalls protect the logic perimeter of the ESMA IT infrastructure; and the main computer systems holding the data are security hardened. Administrative measures include the obligation for ESMA staff and service providers maintaining the equipment and systems to have signed non-disclosure and confidentiality agreements. SailPoint IdentityNow service is concerned by two security assessments:
		- ISO/IEC 27001:2013; - SOC 2 Type 2 attestation. The service is hosted on Amazon Web Services (AWS) cloud platform, which provides substantial protection for the base infrastructure, and this includes the virtual servers, data storage, databases, network, and other resources. The AWS' Frankfurt region is chosed for hosting and operating the IAMAN SaaS solution, hence all business related data (e.g. the datastore with user account information and related access rights entitilements) is hosted in EU datacentres. The service provider conducts regular third-party penetration testing on IdentityNow to ensure the continued security of the platform. The user access to the system (login process) is protected by a 2 factor authentication mechanism.

14	**Information on how to exercise your rights to access, rectification, object and data portability (where applicable), including recourse right.**	a) You are entitled to access your information relating to your personal data processed by ESMA, verify its accuracy and, if necessary, correct it in case the data is inaccurate or incomplete; b) You have the right to request the erasure of your personal data, if your personal data is no longer needed for the purposes of the processing , if you withdraw your consent or if the processing operation is unlawful; c) You can ask the Data Controller to restrict the personal data processing, under certain circumstances, such as if you contest the accuracy of the processed personal data or if you are not sure if your personal data is lawfully processed; d) You may also object, on compelling legitimate grounds, to the processing of your personal data;

		e) Additionally, you may have the right to data portability which allows you to make a request to obtain the personal data that the Data Controller holds on you and to transfer it from one Data Controller to another, where technically possible. You may exercise your rights by contacting the Data Controller at itdpo@esma.europa.eu In some cases your rights might be restricted in accordance with Article 25 of the Regulation (EU) 2018/1725. In each case, ESMA will assess whether the restriction is appropriate. The restriction should be necessary and provided by law, and will continue only for as long as the reason for the restriction continues to exist. If you have additional questions or concerns you can also contact ESMA's DPO at DPO@esma.europa.eu You have the right to lodge a complaint with the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under the Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by ESMA. In case of queries please consult ESMA's Data Protection Officer (DPO@esma.europa.eu). You may also contact the European Data Protection Supervisor (edps@edps.europa.eu). For more information please refer to: https://www.esma.europa.eu/about-esma/data-protection