Nr.	Item	Security Logging and Auditing
1	Name of the Controller	Head of Resources Department: itdpo@esma.europa.eu
1,1	Address of the Controller	ESMA, 201-203 Rue de Bercy, 75012 Paris
1,2	ESMA Parts Entrusted with Processing	ESMA/RES/Information and Communications Technologies (ICT)
1,3	Processors (If any)	Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU); Security audit monitoring is performed with the collaboration of Airbus Cyber SAS acting a data processor. Note that ESMA internally also uses third party monitoring solutions to proactively detect potential security incidents, handling risks and to perform forensic investigations.
2	Name and contact details of DPO	ESMA´s Data Protection Officer (DPO): dpo@esma.europa.eu
3	Name and contact details of joint controller (where applicable)	Not applicable
4	Name and contact details of processor (where applicable)	Security audit monitoring is performed by ESMA with the collaboration of the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) and Airbus Cyber SAS located in 1 Boulevard Jean Moulin - ZAC de la Clef Saint Pierre - 78990 Elancourt (France).
5	Purpose of the processing	To perform holistic Information Security Incident - and Personal Data breach -, detection, prevention, contention, mitigation, analysis and support of security investigations and inquiries concerning ESMA´s resources, including but not limited to: Data, Applications, Services and Information and Communications systems. The applicable data protection Regulation (EU) 2018/1725 considers the security of electronic communication networks as an enabler to the protection of individuals and more generally of Union institutions, bodies and agencies. In particular, according to Articles 4, 29 and 33: personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
6	Description of categories of persons whose data ESMA processes and list of data categories	ESMA staff, SNEs, trainees, external consultants and third parties including NCAs/CRAs/TVs and any other stakeholder or external party interacting or accessing ESMA´s ICT systems, networks and applications. The purpose is to identify threats affecting ESMA´s ICT systems, networks, applications and data and to perform security incident handling and forensic investigations. The following personal data are handled: data subject's system identifiers (user accounts or UserIDs), email addresses, computer names and identifiers, IP addresses and MAC addresses, activity concerning with ESMA´s systems, networks, applications and data - any data stored in, transmitted from / to an ESMA's system involved in a possible incident (as victim, relay or perpetrator), authentication record events including the timestamp (date and time) as well as the ESMA´s ICT resources or data involved.
7	Time limit for keeping the data	Audit Data is kept up to 24 months. Exceptions could apply on ad-hoc basis in case of investigations and inquiries which might require to keep data for longuer periods, either to derive further conclussions or as evidences in support of legal and/or regulatory procedures. For more information please refer to the "Decision of the Management Board of the European Securities and Markets Authority of 1 October 2019 adopting internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of ESMA (OJ L 303, 25.11.2019, p. 31–36) at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1575129513769&uri=CELEX:32019Q1125(01)"
8	Recipients of the data	The Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) and Airbus authorized staff. ESMA´s Information Security Officer and Security personnel with a valid need-to-know. ESMA´s Staff designated on ad-hoc basis by The Data Controller with a valid need-to-know dealing with a potential incident, an incident, investigation or inquiry.
9	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	No
10	General description of security measures, where possible.	ESMA applies security controls aligned with security policies and procedures. Notably aligned with ISO 27001. Airbus has only access to the specific data mentioned in point 6.
11	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	**INFORMATION SECURITY AND DATA PRIVACY BUSINESS USE NOTICE** In order to meet ESMA's Security Policies and Procedures, as well as the applicable data protection regulation, ESMA needs to collect, correlate, analyse and store user's activity data in relation to ESMA's assets (including but not limited to ESMA's data, applications, networks and ICT systems). • As a general principle, ESMA only processes personal data for the performance of tasks carried out in the public interest on the basis of the Treaty on the Functioning of the European Union, on the basis of the relevant legislation or in the legitimate exercise of official authority vested in ESMA or in a third party to whom the data are disclosed. • Users acknowledge that ESMA's assets (including but not limited to ESMA's ICT systems, data and applications) must only be accessed and used to conduct activities approved by ESMA. • Users ackowledge that user's activity resulting from the interactions with ESMA's assets (including but not limited to ESMA's ICT systems, data and applications) will be collected, correlated, analysed, stored and used to verify personal accountability of user's actions on ESMA's assets. • This data processing operation does not target 'private' users communications but actions performed on ESMA's assets. • ESMA has the right to proactively review logged in user's activity data, in particular in cases of suspected breaches of legal or security compliance obligations. The analysis of the compiled and registered information will take place on a case by case basis; following ESMA's risks and incident handling procedures, when performing Information Security compliance health checks or when there is a legitimate suspicion that an individual has infringed ESMA's Security policies or is engaged in other unlawful activity. • The recorded information will be kept up to 24 months and can be extended in case of justified inquiries, investigations and to resolve potential security incidents or risks. • ESMA processes personal data in line with Regulation (EU) 2018/1725. In some cases your rights might be restricted in accordance with Article 25 of this Regulation. In each case, ESMA will assess whether the restriction is appropriate and Decision on Restrictions of Data Subject Rights ESMA40-133-716. For more information, please see ESMA's Data Protection Statement on https://www.esma.europa.eu/data-protection. 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. 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).