Direct Supervision

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
Direct Supervision		
1	**Last update of the record**	04/12/2023
2	**Reference number**	ESMA40-133-1357
3	**Name and contact details of controller**	**EUROPEAN SECURITIES AND MARKETS AUTHORITY (ESMA)** 1. For Central Counterparties (CCPs): Head of CCP Directorate (CCPD) email: ccpd.data-protection@esma.europa.eu 2. For all other directly supervised entities, namely credit rating agencies (CRAs), securitisation repositories (SRs) and Benchmark administrators, trade repositories (TRs), TRs reporting SFT transactions (SFTRs) and Data Reporting Services Providers (DRSPs):

		Head of Conduct Supervision and Convergence Department (CSC) email: CSC-Support-office@esma.europa.eu Address of the controller: **European Securities and Markets Authority (ESMA)** **201-203 Rue de Bercy** **75012 Paris** **France**
4	**ESMA area entrusted with processing**	For CCPs: CCP Directorate For all other directly supervised entities (namely CRAs, SRs, TRs, SFTRs, DRSPs and benchmark administrators): CSC Department
5	**Processors (if any)**	NUIX Ireland Limited for processing, analysing, and investigating large volumes of data Tresorit AG for secure communication or exchange with an external recipient, and as a temporary storage of documents
6	**Name and contact details of DPO**	ESMA DPO 201-203 rue de Bercy 75012 Paris

		France dpo@esma.europa.eu
7	**Name and contact details of processor (where applicable)**	Nuix (NUIX Ireland Limited) Times House, 2nd Floor South 5 Bravingtons Walk, Kings Cross London N1 9AW, United Kingdom Tresorit (Tresorit AG) Franklinstrasse 27, 8050 Zurich, Switzerland
8	**Purpose of the processing**	ESMA supervisory mandates are enshrined in Union law and cover different categories of legal persons. However, in the exercise of its supervisory duties, ESMA may have to process personal data, for example to assess the fit and proper nature of managers or to check whether conflict of interest rules are complied with. The legal basis for ESMA's processing of personal data in this context stems from specific provisions in the following regulations applied together with their relevant delegated acts: for CRAs - Regulation (EC) No 1060/2009 (CRAR); for SRs - Regulation (EU) 2017/2402 (Securitisation Regulation); for Benchmark administrators- Regulation (EU) 2016/1011 (Benchmarks Regulation); for TRs - Regulation (EU) No 648/2012 (EMIR); for TRs reporting SFT transactions - Regulation (EU) 2015/2365 (SFTR); For DRSPs - Regulation (EU) No 600/2014 (MiFIR);

		for third-country CCPs - Regulation (EU) No 648/2012 (EMIR). In particular, the purpose of the processing is to enable ESMA to assess and to ensure: For Benchmark administrators: • adequate experience, knowledge and reputation of the members of the management body, the board and the oversight function; • adequate experience and knowledge of internal control functions (compliance function, risk assessment, review function, internal audit); • management of potential conflicts of interests related to managers, board members or any board committees or any other person directly or indirectly linked to provision of the benchmark; • compliance with other requirements relating to outsourcing arrangements which are examined in the framework of the registration process (they typically contain personal data of the signatories representatives). For CRAs, SRs, TRs, SFTRs, DRSPs: • adequate experience, knowledge and reputation of the supervised entities' senior management and board members; • compliance with other requirements relating to outsourcing arrangements which are examined in the framework of the registration process (they typically contain personal data of the signatories representatives). Specifically for CRAs:

		• adequate experience and knowledge of persons in charge of internal control functions (compliance function, risk assessment, review function, internal audit), managers of CRAs' branches and rating analysts; • sufficient in-depth knowledge and expertise in structured finance markets required for board members of CRAs that issue credit ratings on structured finance instruments; • that entities issuing credit ratings are registered under CRAR with ESMA (Perimeter activity); • that CRAs report to ESMA information on credit ratings and pricing practices and fees charged for these credit ratings and ancillary services through the RAtings DAta Reporting tool (RADAR) and the European Rating Platform (ERP); • independence and avoidance of conflicts of interest of CRAs's shareholders, Board members, persons in charge of the review function, compliance function, internal audit. Specifically for DRSPs: • That the management body shall possess adequate collective knowledge, skills and experience to be able to understand the activities of the data reporting services provider. Each member of the management body shall act with honesty, integrity and independence of mind to effectively challenge the decisions of the senior management where necessary and to effectively oversee and monitor management decision-making where necessary. Specifically for SRs, TRs, DRSPs and SFTRs: • appropriateness of human resources, including the fit-and-proper assessments of relevant technology staff and individuals who are responsible for internal control functions (compliance, risk assessment, internal audit);

		• management of potential conflicts of interests related to managers, board members or any person directly or indirectly linked to SR/TR by close links. Specifically for third country Tier 2 CCPs: • adequate experience, knowledge and reputation of the CCP's shareholders, senior management and board members; • other information potentially received on the basis of MoUs or in the context of College participation (e.g., information received from third-country NCAs concerning an enforcement action, should such be directed against/involve specific individuals). Specifically for other third-country Tier 1 CCPs: • basic information about managers and contact details of the CCP applying for recognition by ESMA; • other information potentially received on the basis of MoUs or in the context of College participation (e.g., information received from third-country NCAs concerning an enforcement action, should such be directed against/involve specific individuals). Additional purpose of the processing of personal data is related to the handling of complaints received by ESMA about potential wrong-doing and/or infringements by the above categories of supervised entities. As part of investigating a potential wrong-doing/infringement of these entities ESMA may collect information through Tresorit (Secure Documention Vault). As part of this data collection, ESMA

		tries as much as possible to exclude unnecessary personal data through the selection process of the Evidence data set. The collected information can be processed and analysed by ESMA staff using an e-Discovery tool called Nuix. Nuix provides advanced capabilities for collecting, indexing, searching, and extracting information from various sources, including emails, documents, databases, social media, and more. It is mainly used for investigation and (pre-)enforcement cases. Finally, as part of investigating a potential wrong-doing/infringement of the supervised entities ESMA may also conduct online interviews and record such interviews. For more information please consult: ICT Audio and Video Communication and Collaboration (europa.eu). The purpose of personal data processing in such context is the exercise of ESMA's supervisory mandate and gathering evidence while ensuring the highest level of accuracy of the content discussed during interviews.
9	**Description of categories of persons whose data ESMA processes and list of data categories**	I. Categories of persons: I.1.For all supervised entities (unless otherwise specified): (a) senior managers / members of the administrative or supervisory board, persons appointed to direct the business of the branches, staff responsible for internal audit, internal control, compliance function, risk assessment function, review function and technology staff; (b) independent non-executive directors (INEDs) for CRAs only;

		(c) shareholders, managers, rating analysts, employees and other natural persons whose services are placed at the disposal or under the control of the supervised entity or persons linked to it by control; (d) employees of supervised entities or individuals working for them and persons involved in credit rating activities, trade repository and benchmark activities, rated entities and related third parties, third parties to whom the supervised entities have outsourced operational functions or activities and persons closely related or connected to a supervised entity or its activities. I.2. Complaints: (a) complainant; (b) staff / board member of the supervised entity (including former employees acting as whistleblowers), in cases where complainant refers to personal data of this staff / board member. I.3 Perimeter activity: (a) senior manager/representative of the identified company; (b) shareholders and key function holders related to the activities of the company; (c) analysts. I.4. RADAR: (a) lead analysts.

		II. Categories of personal data processed: (a) name and family name; (b) address; (c) professional experience; (d) personal data relating to criminal convictions and offences; (e) declarations on the independence of INEDs of CRAs; (f) documents, containing information on whether shareholders of CRAs/SRs/TRs/SFTRs/CCP hold shares and financial instruments in other undertakings; (g) documents, containing personal data collected in the supervisory work related to compliance with ESMA's direct supervision related regulations and CCPs (e.g. appraisals of CRAs' senior staff, information regarding litigation procedures or disciplinary actions against supervised entities staff); (h) incidents reports of supervised entities, containing information on personal data of respective staff involved; (i) complaints, containing personal data such as contact details, employment details of the complainant and if relevant, of the supervised entities including CCP's staff;

		(j) name, start date, end date and country of CRAs' lead analysts; (k) personal data (e.g. name, position and any other identifying information on the professional experience and economic background of the senior managers / members of the supervisory or administrative body/shareholders/staff of supervised entities; (l) personal data of supervised entities' staff and third parties (individuals) included in electronic stored information ("ESI", including but not limited to emails, chat messages, and data from collaboration and relevant systems) gathered for ongoing supervision, investigation, pre-enforcement or enforcement work; (m) video recording, voice recording in the context of online interviews during investigations, when necessary.
10	**Time limit for keeping the data**	1. Personal data as per point II.(a) to (k)above are kept for 15 years following receipt of the respective document / information, containing personal data. 2. Personal data as per point II.(l) and (m) gathered through electronic stored information and online interview recordings need to be retained for the necessary period until the end of the investigation and of any other relevant follow-up actions (pre-enforcement or enforcement work) as explained below: (i) for cases that do not trigger pre-enforcement work: ESI and online interview recordings that are part of the evidence set (ESI identified as relevant to the subject of the investigation, pre-enforcement or enforcement work) are kept for 15 years following their receipt. The rest of ESI

		and/or online interview recordings that are not part of the evidence set are kept for 6 months after decision not to refer the case for pre-enforcement work. (ii) for cases that are classified as low- and intermediate- priority in terms of serious indications of the possible existence of facts liable to constitute one or more of the infringements: the selected data set is kept available to the Supervision Officers until: (i) the RAP or closing letter is communicated to the entity; and (ii) the classification into intermediate or low priority is approved by the HoD. If no pre-enforcement work is started on these cases, the selected data set is maintained until the quarter when the maximum limitation period for the imposition of penalties has elapsed. After this, in six months the selected data set will be identified and removed. Evidence data set is considered part of the investigation file and is kept for 15 years following receipt of the respective document / information, containing personal data. (iii) for cases classified as high-priority in terms of serious indications of the possible existence of facts liable to constitute one or more of the infringements: the selected data set is kept available to Supervision Officers until the RAP or closing letter is communicated to the entity. The selected data set and evidence data set are kept available to the Supervision Officers that are involved in the pre-enforcement work until the completion of all proceeding related to the investigation, i.e. ESMA's Board of Supervisors (BoS) has taken its decision regards the IIO report results and any other decision follow-up procedures are finalised (appeal to the Board of Appeal, etc.). After this, in six months the selected data set will be identified and removed. Evidence data set (including also any electronic message requested during the pre-enforcement work or that support the findings of the pre-enforcement report) is considered part of the investigation file and is kept for 15 years following receipt of the respective document / information, containing personal data.In case of initiated administrative or judicial proceedings, the retention period shall be extended to

		one year after these proceedings are sanctioned by a decision having acquired the authority of a final decision.
11	**Recipients of the data**	Personal data can only be accessed by ESMA staff from the Supervision Departments, designated for the purpose of supervisory activities related the supervised entities they are in charge of
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**	ESMA will transfer personal data outside of the EU/EEA only where necessary and appropriate to fulfil its obligations in the context of international cooperation in accordance with Article 33 of the ESMA Regulation and, as far as third-country CCPs are concerned, with Article 25 of EMIR, as may be further amended, repealed or replaced. The transfers will be done in accordance with Chapter V of the Regulation (EU) 2018/1725, i.e. where there is a Commission's adequacy decision recognising a third country as ensuring an adequate level of protection of personal data, or for important reasons of public interest, as recognised in Union or Member State law. In the absence of an adequacy decision adopted by the Commission, where these transfers are made in the usual course of business or practice, your personal data might be transferred only to third country authorities that are signatories to the IOSCO-ESMA Administrative Arrangement (AA) for the transfer of personal data between EEA and non-EEA securities regulators adopted with the approval of the European Data Protection Supervisor and in accordance with Article 48(3) of the Regulation and available at:

		https://www.esma.europa.eu/sites/default/files/administrative_arrangement_aa_for_the_transfer_of_personal_data_between_eea_and_non-eea_authorities.pdf
13	**General description of security measures, where possible.**	All information concerning the direct supervision of ESMA is: (a) treated confidentially by all staff involved in the supervisory process. In addition, the relevant regulations provide for the obligation of professional secrecy, applicable to all the persons who work or have worked for ESMA; (b) classified as “ESMA Restricted Use” according to ESMA Data Classification Policy; (c) accessed only by the respective Supervision Officers working on the relevant supervisory activity (registration procedures, ongoing monitoring, investigations, etc, through restricted access to the folder on ESMA electronic document centre. Measures on the circulation, transmission, storage, usage and destruction or disposal of the restricted and confidential documents information are strictly applied by the Supervision Officers in accordance with ESMA Classified Documents Handling Procedure (ESMA/2014/INT/168). All supervisory activities are documented and saved. Hard copies are kept in locked cupboards. Electronic versions are saved in ESMA electronic document centre access to which is limited only to Supervision Officers. For example, the following measures are applicable:

		1)Transmission: Information in paper format and other non-reusable media: For internal circulation, sealed envelopes are used. For external transmission, sealed mail envelopes are used with registered mail or email service with tracking capabilities (e.g. DHL). Information in electronic format: An ESMA e-mail address is used to send documents. The use of online web messaging providers is not allowed. When sending the document to another ESMA email address, there is no need to encrypt the document. When sending the document outside ESMA, 'ESMA RESTRICTED USE' documents are to be sent on an encrypted medium. ESMA may also exchange information with supervised entities through Tresorit, which is a cloud-based solution that allows a high level of security for external exchange of restricted and confidential documents and messages, and which allows for controlling the access and content. 2) Storage: Information in paper format and other non-reusable media:

		When not in use, ‘ESMA RESTRICTED USE’ documents are kept in locked cupboards. ‘ESMA RESTRICTED USE’ documents must not be left on the desks when the user leaves the office. Information in electronic format: ‘ESMA RESTRICTED USE’ files can be saved on a network folder with controlled access, established on the "need-to-know" basis. The Data Owner determines which persons will access each folder that contains ‘ESMA REGULAR USE’ documents and sends a request to the IT Helpdesk. 3) Usage: The use of ‘ESMA RESTRICTED USE’ documents. 4) Destruction / Disposal: Information in paper format and other non-reusable media: ‘ESMA RESTRICTED USE’ paper documents must be shredded or disposed in containers designated for collection of sensitive documents for secure disposal. CDs and DVDs should be given to the Physical Security Officer for proper destruction and disposal. Information in electronic format:

		On encrypted devices (PCs/laptops with encrypted hard drives or USB flash drives), the simple file deletion in the computer operating system is sufficient.
14	**Information on how to exercise your rights to access, rectification, object and data portability (where applicable), including recourse right.**	You may exercise your rights by contacting the relevant Data Controller (see contact details above). Your rights are the following: 1) 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. 2) You have the right to request the erasure of your personal data, if your personal data is no longer needed for the purpose of the processing, if you withdraw your consent or if the processing operation is unlawful. 3) 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. 4) You may also object, on compelling legitimate grounds, to the processing of your personal data. 5) 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.

		Please note that restrictions to your data subject's right may apply under Article 25 of Regulation (EU) 2018/1725 and 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. If you have additional questions or concerns, you can also contact: 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 because of the processing of your personal data by ESMA. For further information, please see contact ESMA DPO at DPO@esma.europa.eu or consult the website: www.esma.europa.eu/data-protection.