PUBLIC

Register of Processing Activities carried out as a Processor

Processor	European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA)
Address:	Vesilennuki 5, 10415 Tallinn, Estonia
Data Protection Officer:	dpo@eulisa.europa.eu
General description of security measures:	Personal data is stored on eu-LISA ICT infrastructure with restricted access. Standard ICT security measures are implemented to protect this ICT infrastructure (e.g. firewalls, antivirus protection, data encryption and passwords). Data is backed-up regularly and security software is kept up-to-date. eu-LISA premises are not publicly accessible and secured. Access to the personal data is restricted to authorised users requiring it for the purposes of the processing. eu-LISA contracts include data protection provisions as standard which must be complied with by contractors.

Case Nr	Reception Date	Last update	Processor(s)	Processing Operation Name/Description	Purpose	Category of Data Subjects	Category of Personal Data	Joint Controllers	Controller(s)	Sub-processor(s)	Retention Period	Recipients	International Transfers	Prior Consultation	Opinion of the EDPS
0006/2026	12/06/2026		Programme and Solutions Management Unit	European Search Portal (ESP)	According to art. 6 (3) and 41 of Regulation (EU) 2019/817 and Regulation (EU) 2019/818, euLISA is mandated to develop the ESP and ensure its technical management acting as data processor responsible for the technical management – including maintenance and technological developments -of the central infrastructure for the interoperability components.	Eu-LISA statutory staff having access to the ESP for management and monitoring Stakeholders of eu-LISA, including Member States representatives Other categories of data subjects: - ESP operators (Member States Authorities and Union Agencies -Frontex, Europol, Eurojust, EPPO-). - EU and Third-country national citizens (Article 17 of the Regulations (EU) 2019/817 and 2019/818). - TCNs subject to screening Regulation (EU) 2024/1356.	Name, contact details and affiliation: - ESP Operator Username e-Communication and/or connection data: Logs, endUserID Other personal data: - ESP Profile used; EU System queried; Europol data queried; System ID; Authority. Biometric data for unique identification: Biometric data (fingerprints, facial images); Personal data relating to criminal convictions and offences or related security measures (e.g. copies of the criminal records certificates)	No	Member States Authorities (including Screening Authorities) and European Union Agencies (Frontex, Europol, Eurojust, EPPO)	No	12 months as per Article 10(3) of Regulation (EU) 2019/817 and Regulation (EU) 2019/818. The ESP can temporarily store personal data in two specific situations: 1. in case of a delay in receiving all the data collected from the different CBSs: if the ESP doesn't receive simultaneously all data requested in the query, the system can store temporarily (from 0,8 to 2 seconds) the personal data in the ESP Gateway before sending the final result to the user. 2. in case of backup during the temporary storage: in case the backup of the interoperability components is done during the temporary storage of personal data in the ESP Gateway, those data cannot be stored in the ESP beyond the agreed retention period.	Designated eu-LISA staff members Other recipients: EDPS, EPPO, competent authorities or EUI Agencies	No	**No**	No
0005/2026	12/06/2026		Programme and Solutions Management Unit	Common Identity repository (CIR)	eu-LISA ensures a safe connection network to CIR for the authorised users from the MSs competent authorities. Also, eu-LISA develops, tests and maintains the databases included in CIR.	Eu-LISA statutory staff having access to the CIR: As stated in Reg (EU) 818 art 62 (2), duly authorized staff shall have access to the CIR for the following purposes: management and monitoring (PA011 and PA012) Stakeholders of eu-LISA, including Member States representatives Member State or Union agency staff having access to the CIR (Article 24 of the Regulations (EU) 2019/817 and 2019/818) Other categories of data subjects: EU and Third-country national citizens (Article 17 of the Regulations (EU) 2019/817 and 2019/818). Some systems ask also for personal data of the parental authority, meaning their data are processed. TCNs subject to screening in the cases foreseen in Articles 5 and 7, Regulation (EU) 2024/1356.	Name, contact details and affiliation: Identity (name, surname), First name of the parents, Date of birth, Place of birth (town and country), Year of birth, Nationality/nationalities, Gender, SIS biographic data User email. e-Communication and/or connection data: Logs (with pseudonymised usernames), as per Article 24 of Regulation (EU) 2019/817 and 818 with the following data: the Member State or Union agency launching the query; the purpose of access of the user querying via the CIR; the date and time of the query; the type of data used to launch the query; the results of the query and where a link is created; the data used to launch the query and the results of the query indicating the EU information system from which the data were received; Administrator credentials. Personal identification numbers: Travel Document number; Type of the travel document or documents and the three-letter code of the issuing country of the travel document or documents; The authority which issued the travel document; Travel Document issue date; Travel Document expiration date. Other personal data: SIS identity group reference; CIR identity group reference; Link reference; Identity confirmation file reference; CBS record reference. Biometric data for unique identification:Biometric data (Regulations (EU) 2019/817 and 2019/818 Article 18.1): DAT.15 - fingerprints of the applicant in accordance with the relevant provisions of the Common Consular Instructions; sourced from EES, VIS, ECRIS-TCN; DAT.14 - facial images, in accordance with Regulation (EC) No 1683/95. These data are sourced from EES, VIS, ECRIS-TCN. Personal data relating to criminal convictions and offences or related security measures: Convicted Person: Convicting Member State. These data are sourced from ECRIS-TCN; Serious crime flag ETIAS Consequential Amendment, art. 7 in chapter I).	No	Member States, European Border and Coast Guard Agency	No	Data retention periods depend on the CBSs that provided and/or update the data in CIR, being CIR agnostic on this topic. Once received the automatic expiration of the retention period in the original CBS, CIR deletes immediately and automatically the personal data affected (Article 23, IO Regs.)	Designated eu-LISA staff members eu-LISA Administrators. Other recipients: - MSs competent authorities, designated by national laws - Europol accessing CBS record references for law enforcement purposes. - SIRENE National Bureau and National SIS Office - European Data Protection Supervisor accessing technical logs from the CIR the purposes of monitoring, audit and compliance	No	**No**	No
0003/2026	16/06/2026		Programme and Solution Management Unit	**Dublinet**	DubliNet is the secure electronic communication network that connects the national authorities responsible for asylum and migration management across EU Member States and associated states. Dublinex allows Asylum and Migration Member States' (MSs) competent authorities to exchange data and documents over the secure electronic communication channels and using TESTA Network – Art. 52(4), Art. 72 of Regulation (EU) 2024/1351 (hereinafter the Regulation or AMMR), Art. 48 of Regulation (EU) 2024/1358, Art. 1(4), Regulation (EU) 2018/1726. DublinEx: DublinEx is a web-based application developed and managed by eu-LISA that facilitates the creation, completion, updating of existing forms, management, validation, digital signing, and preparation for exchange of the standard forms and attach files required under the AMMR. It operates alongside DubliNet: DublinEx produces the structured XML form files, and DubliNet transmits them between Member States.	eu-LISA statutory staff (ID users) Stakeholders of eu-LISA, including Member States representatives (users from white-listed IP addresses of the national competent Asylum authorities)	e-Communication and/or connection data:Range of IP address from whitelists included in the logs for the MS users; user ID for the euLISA's users (logging the changes in the DublinEx Web)	**No**	Member States Asylum and Migration competent authorities		At least 6 months, and for no longer than 12 month, eu-LISA Security Standard on Logging and Monitoring.	Designated eu-LISA staff members (ID users for internal security controls) Other recipients: Asylum and Migration MSs Authorities (for possible auditing purposes due to national legislation – IP range addresses)	No	No	No
0001/2026	12/03/2026		Transition and Automation Unit	**IT Service Management Tool** **Service Now** **managing incidents, problems, and related changes, and standard requests for all the core business systems**	The usage of ITSM tool by eu-LISA is for managing incidents, problems, and related changes, and standard requests for all the core business systems concerning the Large-scale IT systems as external IT support to Member States.	Relatives of the data subject Other categories of data subjects: Third country nationals	Name, contact details and affiliation (e.g. address, first name, surname, e-mail, phone number, citizenship) Personal identification numbers (e.g. national IDs/passports, staff ID) Image, audio (e.g. pictures, ID photo, CCTV record, video/audio recording) -Images may contain fingerprint screenshots and information about criminal convictions and offences. Biometric data for unique identification (e.g. hashes of fingerprint images, fingerprints template and not the actual image of the fingerprint)	**No**	Member States, Authorised Agencies or Bodies	N/A	General personal data Until the ticket is closed. Data is redacted once it is closed or when it is not necessary for the resolution of the ticket. Sensitive personal data Until the ticket is closed. Data is redacted once it is closed or when it is not necessary for the resolution of the ticket.	Designated eu-LISA staff members: - Access coordinator -eu-LISA staff members using SERVICENOW Other recipients: -MWO Contractors	No	No	No
0006/2022			Operations Department - Planning and Standards Unit - Product Management Sector - Eurodac Product Owner	Operational management of Eurodac	eu-LISA is in charge of the operational management of Eurodac and corresponding Communication Infrastructure according to Art. 4 of Eurodac Regulation. This includes operations such as: keeping Eurodac and corresponding Communication Infrastructure functioning 24 hours a day, 7 days a week; ensure its security through the implementation of necessary measures such as incident investigation in relation to troubleshooting (in line with Art. 34(2) and 34(4) of Eurodac Regulation); keeping of records pursuant to Article 28(1) of the Eurodac Regulation; and, provision of statistics, as per Art. 8 of the Eurodac Regulation, relating to the processing operations performed in the Central System as requested by Controllers, including the provision of such data for reporting purposes (as per Art. 8(2) and 40 of Eurodac Regulation).	• Applicants for international protection (including minors except children under the age of 14 and persons unable for fingerprinting due to health reasons or protection of public health) – Art. 9 of Eurodac Regulation (Category "1" and "9" as per Art. 24(4) and 29 thereof). • Beneficiaries of international protection (including minors except children under the age of 14 and persons unable for fingerprinting due to health reasons or protection of public health) – Art. 18 of Eurodac Regulation. • Third-country nationals (TCN) or stateless persons of at least 14 years of age apprehended in connection with the irregular crossing of an external border – Art. 14(1) of Eurodac Regulation (Category "2" and "9" as per Art. 24(4) and 29 thereof). • TCN or stateless persons found illegally staying in a Member-State (MS) of at least 14 years of age – Art. 17 of Eurodac Regulation (Category "3" and "9" as per Art. 24(4) and 29 thereof). • Individuals who are subject to comparisons for law enforcement purposes by MS authorities under Art.19 of Eurodac Regulation. • Individuals who are subject to comparisons for law enforcement purposes by MS authorities under Art. 20 of Eurodac Regulation (Category "4" as per Art. 24(4) thereof).	• e-Communication and/or connection data (Technical and configuration data that can be linked to data subjects' set of information making them Identifiable Personal Information such as "operator user ID", "date on which the data were transmitted to the central system", "e-mail metadata", "originating agency indicator" and "Logs", which might be found in Eurodac Regulation or system-supporting documentation like Interface Control Document ("ICD") or system's user manual). • Personal identification numbers (such as "Eurodac Reference Number" used by MS to identify record files and corresponding data subjects in the system and "link ID" where applicable to relate e.g. record files throughout the system). • Information on the status of the data subject in line with Art. 10 of Eurodac Regulation. • Sensitive data (Biometric data from fingerprints) • Other data recorded in the Central system following an application for international protection that is not already covered here in a different category of personal data such as biometric data (fingerprint data), in line with Art. 11 of Eurodac Regulation (e.g. "sex" and "Member State of origin, place and date of the application for international protection"). • Other data transferred to the Central system in relation to third-country national or stateless person as per 14(2) of Eurodac Regulation that is not already covered here in a different category of personal data, such as biometric data (fingerprint data) (e.g., gender and date on which the fingerprints were taken).	**Yes**	Each of the Competent Authorities for the EU Member States (MS) and Associated Countries (Iceland, Norway, Liechtenstein, Switzerland)'s Immigration and Asylum authorities managing National Access Points are designated as joint controllers, and Eurodac regulation serves as the joint controllership agreement. A list of Member States competent authorities having access to data recorded in the Central System for asylum and immigration purposes (2021/C 45/01) can be found here: https://op.europa.eu/en/publication-detail/-/publication/fab5221d-69af-11eb-aeb5-01aa75ed71a1.	For the purpose of technical and security incident investigation when strictly necessary in line with data minimization principle and security measures: S3BIS Consortium: • Sopra Steria Benelux SA • Thales DIS France SA • ATOS Belgium SA/NV	Personal data kept in the record file owned by MS that belongs to: • Applicants for/beneficiaries of international protection (including minors except children under the age of 14 and persons unable for fingerprinting due to health reasons or protection of public health): 10 (ten) years from the date on which the fingerprints were taken, as per Article 12 of Eurodac Regulation, or until MS initiates deletion of data. The data of beneficiaries of international protection stored in the Central System and marked pursuant to Art 18(1) of Eurodac Regulation shall be made available for comparison for law enforcement purposes, as laid down in Art. 1(2) of Eurodac Regulation, for a period of three years after the date on which the data subject was granted international protection, whilst leaving those data available for comparison for the purposes laid down in Art. 1(1) (Asylum and Immigration) of Eurodac Regulation until the point of their erasure. • Third-country nationals (TCN) or stateless persons apprehended in connection with the irregular crossing of an external border:	For the purposes of the system operational management: • eu-LISA designated staff members For Law Enforcement purposes: • Designated authorities - Art. 5(1) of Eurodac Regulation • Verifying authority - Art. 6(1) of Eurodac Regulation • Specialized/dedicated unit of EUROPOL - Art. 7 of Eurodac Regulation For the purpose of incident investigation during Troubleshooting only when strictly necessary in line with data minimization principle and security measures: • Sub-processor identified in corresponding column of this register	**Yes**	**No**	**No**
0005/2022	21/10/2022		Operations Department - Planning and Standards Unit - Product Management Sector - VIS Product Owner	Operational management of Visa Information System (VIS)	eu-LISA is in charge of the operational management of VIS and corresponding Communication Infrastructure according to Art. 26 of VIS Regulation. This includes operations such as: keeping VIS and its corresponding Communication Infrastructure functioning 24 hours a day, 7 days a week; ensure the security of the central VIS and its communication infrastructure through the implementation of necessary measures such as incident investigation in relation to troubleshooting (in line with Art. 26(9), 29(2) of VIS Regulation and Art. 32 of both VIS Regulation and Commission Decision of 4 May 2010 on the Security Plan for the operation of the Visa Information System (2010/260/EU); ensure that procedures are in place for the keeping of records pursuant to Article 34 of VIS Regulation, point 5 of Commission Decision of 30 November 2009 (2009/876/EC), and Article 16 of Council Decision 2008/633/JHA of 23 June 2008; and, ensure that procedures are in place to monitor the functioning of the VIS, including through statistics, as per Art. 17 and 50 of VIS Regulation and Art. 17 of Council Decision 2008/633/JHA of 23 June 2008.	• Applicant under Article 4(5) of VIS Regulation, including group members under Art. 4(6) thereof. • Visa holder (e.g., Article 7(2) of VIS Regulation). • Third-country nationals apprehended within the Schengen Area with fraudulent or without documents, including those who may not, or may no longer, fulfil the conditions for entry to, stay, or residence in the EU (in accordance with Council Decision 2008/633/JHA of 23 June 2008 but processed through VIS - Article 5). • Individuals who are subject to comparisons and search carried out by MS authorities responsible for law enforcement and Europol - Art. 3 of VIS Regulation. • Individuals who are subject to comparisons and search carried out by MS Central visa authorities and authorities having central responsibility for issuing visas at the border in the Member State concerned - Art. 15 of VIS Regulation. • Individuals who are subject to comparisons and search carried out by MS competent authority/authorities having central responsibility for checks at external border crossing points in accordance with the Schengen Borders Code (border authorities) in the MS concerned – Art. 18 of VIS Regulation. • Individuals who are subject to comparisons and search carried out by MS authority/authorities having central responsibility for checks within the territory of the Member States - Art. 19 of VIS Regulation. • Individuals who are subject to comparisons and search carried out by MS competent authorities having central responsibility for carrying out checks at external border crossing points in accordance with the Schengen Borders Code (border authorities) in the MS concerned, or MS authorities competent for doing so within the territory of the Member States - Art. 20 of VIS Regulation. • Individuals who are subject to comparisons and search carried out by MS authorities responsible for examining asylum applications - Art. 21 and 22 of VIS Regulation. • eu-LISA Officers administrating the system (eu-LISA application administrator). • MS Central visa authority/authorities and authority/authorities having central responsibility for issuing visas at the border in the Member State concerned (Operator User ID) – as per Art. 6(2)(a) of VIS Regulation. • MS competent authority/authorities having central responsibility for checks at external border crossing points in accordance with the Schengen Borders Code (border authorities) in the MS concerned (Operator User ID) – Art. 18 and 20 of VIS Regulation. • MS authority/authorities having central responsibility for checks within the territory of the Member States (Operator User ID) – Art. 19 of VIS Regulation. • MS Officers for Law enforcement (MS Operator User for law enforcement) - Art. 3 of VIS Regulation. • Europol Officials (Europol Operator User) - Art. 3 of VIS Regulation. • MS Officers in charge of asylum and immigration who are authorized to work with the Central System (MS Operator User) - Art. 21 and 22 of VIS Regulation.	• Name, contact details and affiliation (such as "surname", "residence", in the case of minors, "surname and first name(s) of the applicant's father and mother"). • e-Communication and/or connection data (Technical and configurational data that can be linked to data subjects' set of information making them Identifiable Personal Information such as "links to other applications and files" and "Logs", which might be found in VIS Regulation or system-supporting documentation like Interface Control Document ("ICD") or system's user manual). • Personal identification numbers (such as "application number" used by MS to identify record files and corresponding data subjects in the system, "number of the travel document or documents" and "number of the visa sticker"). • Image (photographs). • Details on education, expertise, profession of the person (like "current occupation and employer" and, for students, "name of school"). • Data on family, lifestyle and social circumstances (mainly related to Visa application procedures, such as "main destination and duration of the intended stay", "purpose of travel" or "purposes of the expulsion", and even "information on whether the applicant is travelling in a group or with his spouse and/or children"). • Alphanumeric data on the applicant and on visa requested, issued, refused, annulled, revoked or extended, as defined by article 4 of VIS Regulation (this will include other information recorded in the system such as "status information, indicating that a visa has been requested" and "current nationality and nationality at birth"). • Data related to Visa procedures (including not only data in application forms but also data to be added for a visa issued, for a visa refusal, for a visa annulled or revoked, for a visa extended, or where the examination of the application is discontinued in accordance with Art. 10-14 of VIS Regulation, and even other documents supporting the application in case of a consultation/document request under article 16 of VIS Regulation). • Travel document data, as defined by article 4 of VIS Regulation, including copies of travel documents • Records/logs of processing operations within VIS system including data such as: i) purpose of access ('TypeOfAction'); ii) date and time; iii) type if data transmitted; iv) type of data used for interrogation; v) name of the authority entering/retrieving data (includes: User ID; status: sender/receiver); vi) timestamp; vii) visa application number. • Sensitive data (Biometric data from fingerprints)	**Yes**	Member State's National Authority considered as controller and having central responsibility for the processing of data as per the List of "competent authorities the duly authorised staff of which shall have access to enter, amend, delete or consult data in the Visa Information System (VIS) (2016/C 187/04)". Link to the list can be found in the Official Journal of the EU, here: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016XC0526(01)&from=EN.	For the purpose of technical and security incident investigation when strictly necessary in line with data minimization principle and security measures: Bridge Consortium: • Accenture NV - SA / Idemia Identity and Security France SAS	Application file's data and corresponding links to other applications and files referred to in Article 8(3) and (4) of VIS Regulation, as per Article 23 of VIS Regulation: • 5 (five) years: (a) on the expiry date of the visa, if a visa has been issued; (b) on the new expiry date of the visa, if a visa has been extended; (c) on the date of the creation of the application file in the VIS, if the application has been withdrawn, closed or discontinued; (d) on the date of the decision of the visa authority if a visa has been refused, annulled or revoked. OR • Upon request of the MS, as per Articles 24(2) and 25 of VIS Regulation. For the purpose of keeping of records/logs pursuant to Article 34 of the VIS Regulation and point 5 of Commission Decision of 30 November 2009 (2009/876/EC): • 1 (one) year after the retention period referred to in Article 23(1) of VIS Regulation has expired, if they are not required for monitoring procedures which have already begun (Art. 34(2) of VIS Regulation and point 5.1 of above-mentioned Commission Decision of November 2009)	For the purposes of the system operational management: • eu-LISA designated staff members. For issuing visas at the border in the Member State concerned: • Central visa authority/authorities and authority/authorities - Art. 15 and 17 of VIS Regulation. • Authority/authorities having central responsibility for checks at external border crossing points in accordance with the Schengen Borders Code (2) in the Member State concerned - Art. 18 and 20 of VIS Regulation. Authority/authorities having central responsibility for checks within the territory of the Member State concerned - Art. 19 and 20 of VIS Regulation. For the purpose of determining the Member State ("MS") responsible for examining an asylum application, as per Art. 21 of VIS Regulation: • Competent asylum authority/authorities - Art. 21 and 22 of VIS Regulation. For the purpose of examining an application for asylum, as per Art. 22 of VIS Regulation: • Competent asylum authority/authorities - Art. 21 and 22 of VIS Regulation. For the purpose of law enforcement: • Designated authorities of MS - Art. 3 of VIS Regulation • Europol - Art. 3 of VIS Regulation. For the purpose of incident investigation during Troubleshooting only when strictly necessary in line with data minimization principle and security measures: • Sub-processor identified in corresponding column of this register.	**Yes**	**No**	**No**
0004/2022			Operations Department - Planning and Standards Unit - Product Management Sector - VIS Product Owner	Operational management of Visa Information System (VIS) - Recast	eu-LISA is in charge of the operational management of VIS and corresponding Communication Infrastructure according to Art. 26 of VIS Regulation. This includes operations such as: keeping VIS and its corresponding Communication Infrastructure functioning 24 hours a day, 7 days a week; ensure the security of the central VIS and its communication infrastructure through the implementation of necessary measures such as incident investigation in relation to troubleshooting (in line with Art. 26(9), 29(2) of VIS Regulation and Art. 32 of both VIS Regulation and Commission Decision of 4 May 2010 on the Security Plan for the operation of the Visa Information System (2010/260/EU); ensure that procedures are in place for the keeping of records pursuant to Article 34 of VIS Regulation, point 5 of Commission Decision of 30 November 2009 (2009/876/EC), and Article 16 of Council Decision 2008/633/JHA of 23 June 2008; ensure that procedures are in place to monitor the functioning of the VIS, including through statistics, as per Art. 17 and 50 of VIS Regulation and Art. 17 of Council Decision 2008/633/JHA of 23 June 2008; establish interoperability between EES and VIS, the national interface in each Member State, and the communication infrastructure, as per Article 17a of VIS Regulation.	• Applicant under Article 4(5) of VIS Regulation, including group members under Art. 4(6) thereof. • Visa holder (e.g., Article 7(2) of VIS Regulation). • Individuals who are subject to comparisons and search carried out by MS authorities responsible for law enforcement and Europol - Art. 3 of VIS Regulation. • Individuals who are subject to comparisons and search carried out by MS Central visa authorities and authorities having central responsibility for issuing visas at the border in the Member State concerned - Art. 15 of VIS Regulation. • Individuals who are subject to comparisons and search carried out by MS competent authority/authorities having central responsibility for checks at external border crossing points in accordance with the Schengen Borders Code (border authorities) in the MS concerned – Art. 18 of VIS Regulation. • Individuals who are subject to comparisons and search carried out by MS authority/authorities having central responsibility for checks within the territory of the Member States - Art. 19 of VIS Regulation. • Individuals who are subject to comparisons and search carried out by MS competent authorities having central responsibility for carrying out checks at external border crossing points in accordance with the Schengen Borders Code (border authorities) in the MS concerned, including those at which the EES is operated, or MS authorities competent for doing so within the territory of the Member States - Art. 20 of VIS Regulation. • Individuals who are subject to comparisons and search carried out by MS authorities responsible for examining asylum applications - Art. 21 and 22 of VIS Regulation. • Visa-exempt third-country nationals (under Art. 17a(3)(d) and 19a of VIS Regulation) • eu-LISA Officers administrating the system (eu-LISA application administrator). • MS Central visa authority/authorities and authority/authorities having central responsibility for issuing visas at the border in the Member State concerned (Operator User ID) – as per Art. 6(2)(a) of VIS Regulation. • MS competent authority/authorities having central responsibility for checks at external border crossing points in accordance with the Schengen Borders Code (border authorities) in the MS concerned (Operator User ID) – Art. 18 and 20 of VIS Regulation. • MS authority/authorities having central responsibility for checks within the territory of the Member States (Operator User ID) – Art. 19 of VIS Regulation. • MS Officers for Law enforcement (MS Operator User for law enforcement) - Art. 3 of VIS Regulation. • Europol Officials (Europol Operator User) - Art. 3 of VIS Regulation. • MS Officers in charge of asylum and immigration who are authorized to work with the Central System (MS Operator User) - Art. 21 and 22 of VIS Regulation.	• Name, contact details and affiliation (such as "surname", "residence", in the case of minors, "surname and first name(s) of the applicant's father and mother"). • e-Communication and/or connection data (Technical and configurational data that can be linked to data subjects' set of information making them Identifiable Personal Information such as "links to other applications and files" and "Logs", which might be found in VIS Regulation or system-supporting documentation like Interface Control Document ("ICD") or system's user manual). • Personal identification numbers (such as "application number" used by MS to identify record files and corresponding data subjects in the system, "number of the travel document or documents" and "number of the visa sticker"). • Image (photographs). • Details on education, expertise, profession of the person (like "current occupation and employer" and, for students, "name of school"). • Data on family, lifestyle and social circumstances (mainly related to Visa application procedures, such as "main destination and duration of the intended stay", "purpose of travel" or "purposes of the expulsion", and even "information on whether the applicant is travelling in a group or with his spouse and/or children"). • Alphanumeric data on the applicant and on visa requested, issued, refused, annulled, revoked or extended, as defined by article 4 of VIS Regulation (this will include other information recorded in the system such as "status information, indicating that a visa has been requested" and "current nationality and nationality at birth"). • Data related to Visa procedures (including not only data in application forms but also data to be added for a visa issued, for a visa refusal, for a visa annulled or revoked, for a visa extended, or where the examination of the application is discontinued in accordance with Art. 10-14 of VIS Regulation, and even other documents supporting the application in case of a consultation/document request under article 16 of VIS Regulation). • Travel document data, as defined by article 4 of VIS Regulation, including copies of travel documents • Records/logs of processing operations within VIS system including data such as: i) purpose of access ('TypeOfAction'); ii) date and time; iii) type if data transmitted; iv) type of data used for interrogation; v) name of the authority entering/retrieving data (includes: User ID; status: sender/receiver); vi) timestamp; vii) visa application number. • Sensitive data (Biometric data from fingerprints)	**Yes**	Member State's National Authority considered as controller and having central responsibility for the processing of data as per the List of "competent authorities the duly authorised staff of which shall have access to enter, amend, delete or consult data in the Visa Information System (VIS) (2016/C 187/04)". Link to the list can be found in the Official Journal of the EU, here: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016XC0526(01)&from=EN.	For the purpose of technical and security incident investigation when strictly necessary in line with data minimization principle and security measures: Bridge Consortium: • Accenture NV - SA / Idemia Identity and Security France SAS	Application file's data and corresponding links to other applications and files referred to in Article 8(3) and (4) of VIS Regulation, as per Article 23 of VIS Regulation: • 5 (five) years: (a) on the expiry date of the visa, if a visa has been issued; (b) on the new expiry date of the visa, if a visa has been extended; (c) on the date of the creation of the application file in the VIS, if the application has been withdrawn, closed or discontinued; (d) on the date of the decision of the visa authority if a visa has been refused, annulled or revoked. OR • Upon request of the MS, as per Articles 24(2) and 25 of VIS Regulation. For the purpose of keeping of records/logs pursuant to Article 34 of the VIS Regulation and point 5 of Commission Decision of 30 November 2009 (2009/876/EC): • 1 (one) year after the retention period referred to in Article 23(1) of VIS Regulation has expired, if they are not required for monitoring procedures which have already begun (Art. 34(2) of VIS Regulation and point 5.1 of above-mentioned Commission Decision of November 2009)	For the purposes of the system operational management: • eu-LISA designated staff members. For issuing visas at the border in the Member State concerned: • Central visa authority/authorities and authority/authorities - Art. 15, 17 and 19a of VIS Regulation. • Authority/authorities having central responsibility for checks at external border crossing points in accordance with the Schengen Borders Code (2) in the Member State concerned - Art. 18, 18a and 20 of VIS Regulation. Authority/authorities having central responsibility for checks within the territory of the Member State concerned - Art. 17a, 19, and 20 of VIS Regulation. For the purpose of determining the Member State ("MS") responsible for examining an asylum application, as per Art. 21 of VIS Regulation: • Competent asylum authority/authorities - Art. 21 and 22 of VIS Regulation. For the purpose of examining an application for asylum, as per Art. 22 of VIS Regulation: • Competent asylum authority/authorities - Art. 21 and 22 of VIS Regulation. For the purpose of law enforcement: • Designated authorities of MS - Art. 3 of VIS Regulation • Europol - Art. 3 of VIS Regulation. For the purpose of incident investigation during Troubleshooting only when strictly necessary in line with data minimization principle and security measures: • Sub-processor identified in corresponding column of this register.	**Yes**	**No**	**No**

0003/2022	21/10/2022		Operations Department - Planning and Standards Unit - Product Management Sector - SIS II Product Owner	Operational management of SIS II information system. **Withdrawn, replaced by 0002/2022**	eu-LISA is in charge of the operational management of SIS II and corresponding Communication Infrastructure according to Art. 15 of SIS II Regulation and Council Decision 2007/533/JHA. In regard to the SIRENE Bureaux and communication between the SIRENE Bureaux, its security as per Art. 16(2) of SIS II Regulation and technical functioning (Art. 8(4) and 50(4) of SIS II Regulation and Art. 8(4) and 66(4) of Council Decision 2007/533/JHA). This includes operations such as: keeping SIS II and corresponding Communication Infrastructure functioning 24 hours a day, 7 days a week, 365 days a year; ensure the security of the central SIS II and its communication infrastructure through the implementation of necessary measures such as incident investigation in relation to troubleshooting (in line with Art. 16 and 17 of SIS II Regulation and of Council Decision 2007/533/JHA); ensure that procedures are in place for the keeping the records of all data access and exchange of personal data operations within the CS-SIS as per Art. 18 of SIS II Regulation and of Council Decision 2007/533/JHA; and, ensure that procedures are in place to monitor the functioning of the SIS IIS, including statistics, as per Art. 50 of that Regulation and as per Art. 66 of Council Decision 2007/533/JHA.	In the context of SIS II in the field of border checks (SIS II Regulation): • Third-country nationals in respect of whom an alert has been issued, for the purposes of refusing entry or stay - Art. 24 of SIS II Regulation. • Third-country nationals who are beneficiaries of the right of free movement within the Union - Art. 25 of SIS II Regulation. • Third-country nationals subject to restrictive measures intended to prevent entry into or transit through the territory of Member States - Art. 26 of SIS II Regulation. • Person whose identity has been misused - Art. 36 of SIS II Regulation. • Person who complaints that he/she is not the person wanted by an alert - Art. 34(5) of SIS II Regulation. • eu-LISA Officers administrating the system (eu-LISA Operator User). • Operator on Member-States side - Authority which shall have central responsibility for its N.SIS II (the 'N.SIS II Office') - Art. 7(1) of SIS II Regulation. • Operator on Member-States side/end-user - Authorities responsible for border controls - Art. 27(1)(a) of SIS II Regulation. • Operator on Member-States side - Authorities responsible for customs checks - Art. 27(1)(b) of SIS II Regulation. • Operator on Member-States side- Law enforcement authorities - Art. 27(1)(b) of SIS II Regulation. • Operator on Member-States side - National judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charge - Art. 27(2) of SIS II Regulation. • Operator on Member-States side - Authorities responsible for examining visa applications, issuing visas, and for issuing residence permits - Art. 27(3) of SIS II Regulation. • Operator on Member-States side - SIRENE Bureau - Art. 7(1) of SIS II Regulation. In the context of SIS II in the field of police cooperation and judicial cooperation in criminal matters (Council Decision 2007/533/JHA): • Persons wanted for arrest for surrender or extradition purposes - Art. 26 of Council Decision 2007/533/JHA. • Missing persons who: (i) need to be placed under protection; (ii) missing persons who do not need to be placed under protection - Art. 32 of Council Decision 2007/533/JHA. • Persons sought to assist with a judicial procedure, including: (i) witnesses, (ii) persons summoned or persons sought to be summoned to appear before the judicial authorities in connection with criminal proceedings in order to account for acts for which they are being prosecuted; (iii) persons who are to be served with a criminal judgment or other documents in connection with criminal proceedings in order to account for acts for which they are being prosecuted; (iv) persons who are to be served with a summons to report in order to serve a penalty involving deprivation of liberty - Art. 34 of Council Decision 2007/533/JHA. • Persons for the purposes of discreet checks or specific checks - Art. 36 of Council Decision 2007/533/JHA. • Person whose identity has been misused - Art. 51 of Council Decision 2007/533/JHA. • Data subjects whose data is connected to objects sought for the purposes of seizure or use as evidence in criminal proceedings - Art. 38 of Council Decision 2007/533/JHA. • Person who complaints that he/she is not the person wanted by an alert - Art. 49(5) of Council Decision 2007/533/JHA. • eu-LISA Officers administrating the system (eu-LISA Operator User). • Operator (Authority which shall have central responsibility for its N.SIS II (the 'N.SIS II Office') - Art. 7(1) of Council Decision 2007/533/JHA. • Operator (Authorities responsible for border controls) - Art. 40(1)(a) of Council Decision 2007/533/JHA. • Operator (Authorities responsible for police and customs checks) - Art. 40(1)(b) of Council Decision 2007/533/JHA. • Operator (National Judicial Authorities) - Art. 40(2) of Council Decision 2007/533/JHA. • Operator (Europol) - Art. 41 of Council Decision 2007/533/JHA. • Operator (Eurojust) - Art. 42 of Council Decision 2007/533/JHA. • Operator (Interpol) - Art. 55 of Council Decision 2007/533/JHA. • Operator (SIRENE Bureau) - Art. 7(2) of Council Decision 2007/533/JHA.	• Name, contact details and affiliation (such as "surname", "name(s) at birth and previously used names and any aliases, which may be entered separately"). • e-Communication and/or connection data (Technical and configurational data that can be linked to data subjects' set of information making them Identifiable Personal Information such as "links ID to other alerts issued in SIS II", which might be found in SIS Regulation or system-supporting documentation like Interface Control Document ("ICD") or system's user manual). • Personal identification numbers (such as "number(s) of identity paper(s) and date of issue"). • Image (photographs). • Sensitive data (Biometric data from fingerprints). • Other information on persons in relation to whom an alert has been issued that is not already covered here in a different category of personal data such as biometric data (fingerprint data), such as "any specific, objective, physical characteristics not subject to change" as per Art. 20(2)(b) of SIS II Regulation, "place and date of birth" as per Art. 20(2)(c) of SIS II Regulation, "sex" as per Art. 20(2)(d) of SIS II Regulation, and even "decisions giving rise to an alert" as per Art. 20(2)(k) of SIS II Regulation. • Records of every access and all exchanges of personal data within CS-SIS II central system (includes data such as "history of the alerts", "date and time of the data transmitted", "data used to perform searches" and "reference to the data transmitted" in line with Art. 18(1) and (2) of SIS II Regulation). In addition, and only in the context of SIS II in the field of police cooperation and judicial cooperation in criminal matters: • Data related to criminal convictions and offences ("type of offence" as per Art. 20(3)(n) of Council Decision 2007/533/JHA, and "copy of the original of the European Arrest Warrant/ copy of a translation of the European Arrest Warrant" as per Art. 27 thereof). • Data associated to objects sought for the purposes of seizure or use as evidence in criminal proceedings (such as "objects carried" as per Art. 37(1)(f) of Council Decision 2007/533/JHA, "issued identity papers such as passports, identity cards, driving licenses, residence permits and travel documents which have been stolen, misappropriated, lost or invalidated" as per Art. 38(2)(e) thereof, and even "vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost or invalidated" as per Art. 38(2)(f) via Art. 40(2), 43 and Art. 51(6) of Council Decision 2007/533/JHA).	Yes	Member States competent authorities having central responsibility for its N.SIS II (the N.SIS II Office), and authorities which ensuring the exchange of supplementary information, are to be considered controllers. The list of competent authorities which are authorised to search directly the data contained in the second generation Schengen Information System was released (2021/C 287/01) and can be found here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2021.287.01.0172.01.ENG&toc=OJ%3AC%3A2021%3A287%3ATOC.	For the purpose of technical and security incident investigation when strictly necessary in line with data minimization principle and security measures: • Sopra Steria Group	• Data related to alerts entered in the system in general: for the time required to achieve the purposes for which the alerts were entered (Art. 29(1) of SIS II Regulation) and Art. 44(1) of Council Decision 2007/533/JHA). In any case, MS issuing an alert shall, within three years of its entry in SIS, review the need to keep it (Art. 29(2) of SIS II Regulation and Art. 44(2) of Council Decision 2007/533/JHA). Where the MS decides to retain de alert longer than the review period, that MS shall, within three years of the extension of the period to keep the alert entered in SIS, review the need to keep it (Art. 29(4) of SIS II Regulation and Art. 44(4) of Council Decision 2007/533/JHA). • Technical copies of the information processed which result in offline databases: may be retained for a period not exceeding 48 hours (Art. 31(3) of SIS II Regulation and Art. 46(3) of Council's Decision). • Data on persons whose identity has been misused: shall be deleted at the same time as the corresponding alert or earlier where the person so requests (Art. 36(5) of SIS II Regulation and Art. 51(a) of Council Decision 2007/533/JHA). • Records: shall be deleted at the earliest 1(one) year, and at the latest three years, after their creation. The records which include the history of alerts shall be erased one to three years after deletion of the alerts. Records may be kept longer if they are required for monitoring procedures that are already under way. Art. 18(3) and (4) of both SIS II Regulation and Council Decision 2007/533/JHA). • Data on persons associated to objects sought for the purposes of seizure or use as evidence in criminal proceedings: alerts on objects shall be kept only for the time required to achieve the purposes for which they were entered (Art. 45(1) of Council Decision 2007/533/JHA), and for a maximum of 10 (ten) years (Art. 45(3) thereof), unless extended by MS (Art. 45(4) Council Decision 2007/533/JHA).	For the purposes of the system operational management: • eu-LISA designated staff members For the operation and security of the N.SIS II: • Authority which shall have central responsibility for its N.SIS II (the 'N.SIS II Office') - Art. 7(1) of both SIS II Regulation and Council Decision 2007/533/JHA. Within the context of supplementary information, namely: i) to ensure the exchange and availability of all supplementary information; ii) to be able to react to requests for supplementary information swiftly and within the deadlines provided by law; and, iii) for the verification of the quality of the information entered in SIS: • SIRENE Bureau - Art. 7(1) of both SIS II Regulation and Council Decision 2007/533/JHA. For the identification of third-country nationals for the purpose of border control, namely, in accordance with Regulation (EC) No 562/2006 of the European Parliament and the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code): • Authorities responsible for border controls/border authorities - Art. 27(1)(a) of SIS II Regulation and Art. 40(1)(a) Council Decision 2007/533/JHA. For the identification of third-country nationals for the purposes of police and customs checks: • Authorities responsible for customs checks - Art. 27(1)(b) of SIS II Regulation and Art. 40(1)(b) of Council Decision 2007/533/JHA. • National Law enforcement authorities - Art. 40(1)(b) of Council Decision 2007/533/JHA. For the identification of third-country nationals, in line with the need to the performance of their tasks, as provided for in national legislation, and by their coordinating authorities: • National judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charging a person - Art. 27(2) of SIS II Regulation and Art. 40(2) of Council Decision 2007/533/JHA. In the context of the application of the Community acquis relating to the movement of persons: • Authorities responsible for issuing visas, central authorities responsible for examining visa applications and authorities responsible for issuing residence permits - Art. 27(3) of SIS II Regulation. For the identification of third-country nationals for the purpose of prevention, detection, investigation or prosecution of terrorist offences or other serious criminal offences or the execution of criminal penalties: • MS Law enforcement authorities - Art. 27(1)(b) of SIS II Regulation. For the purpose of monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of CS-SIS, data integrity and security: • Competent authorities in charge of checking whether a search is lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of CS-SIS, data integrity and security as per article 18(5) of SIS II Regulation. Where necessary to fulfil its mandate, including within the exchange and further request of supplementary information in accordance with the provisions of the SIRENE Manual, as per Art. 41(1) Council Decision 2007/533/JHA: • Europol - Art. 41 of Council Decision 2007/533/JHA. Within their mandate: • Eurojust - Art. 42 of Council Decision 2007/533/JHA. Exchange of data on stolen, misappropriated, lost or invalidated passports: • Interpol - Art. 55 of Council Decision 2007/533/JHA (subject to an agreement with European Union on the data flows).	Yes	No	No
0002/2022	21/10/2022	05/06/2026	Programme and Solutions Management Unit	Operational management of SIS information system - Information Alert on third-country nationals and Screening Regulation	eu-LISA is in charge of the operational management of SIS and corresponding Communication Infrastructure according to Art. 15 of Regulation 2018/1861 and Regulation 2018/1862 in regard to the SIRENE Bureaux and communication between the SIRENE Bureaux, its security as per Art. 16(2) of Regulation 2018/1861 and technical functioning (Art. 8(4) of Regulation 2018/1861 and Art. 8(4) of Regulation 2018/1862). This includes operations such as: keeping SIS and corresponding Communication Infrastructure functioning 24 hours a day, 7 days a week, 365 days a year; ensure the security of the central SIS and its communication infrastructure through the implementation of necessary measures such as incident investigation in relation to troubleshooting (in line with Art. 16 and 17 of Regulation 2018/1861 and of Regulation 2018/1862); relating to the Communication Infrastructure: supervision, security; and the coordination of relations between the Member States and the provider (Art. 15(2) of Border checks Regulation 2018/1861 and Judicial Cooperation Regulation 2018/1862); Ensuring its security, namely, by adopting a security plan, including contingency measures, to protect data and critical infrastructure and prevent unauthorised access or use, and applying appropriate rules of professional secrecy and confidentiality in line with Art. 16 and 17 of Border checks Regulation 2018/1861 and Judicial Cooperation Regulation 2018/1862; keeping the logs of all data access and exchange of personal data operations within the CS-SIS as per Art. 18 of Border checks Regulation 2018/1861 and Judicial Cooperation Regulation 2018/1862; ensure that procedures are in place for the keeping the records of all data access and exchange of personal data operations within the CS-SIS as per Art. 18 of Regulation 2018/1861 and of Regulation 2018/1862; and, ensure that procedures are in place to monitor the functioning of the SIS, including statistics, as per Art. 60 of Regulation 2018/1861 and as per Art. 74 of Regulation 2018/1862.In line with Article 14 and Article 15 of the Screening Regulation, the Screening Authorities will be able to conduct searches to SIS according to 2018/1860, 2018/1861 and 2018/1862 Regulations. The processing by the processor does not change so the search and read alert data operations as described below cover all the case a search is conducted for Screening Purposes.	eu-LISA statutory staff: eu-LISA Officers administrating the system (eu-LISA Operator User) Other categories of data subjects: For SIS on the return of illegally staying third-country nationals (TCN Regulation 2018/1860): • Third-country nationals in respect of whom an alert has been issued, for the return of illegally staying (Art. 1 of TCN Regulation 2018/1860) data subject category; • System Operator - Authority which shall have central responsibility for its N.SIS (the 'N.SIS Office'), as per Art. 7(1) of Border checks Regulation 2018/1861 via Art. 19 of TCN Regulation 2018/1860) • System Operator - Authorities responsible for border controls (Art. 34(1)(a) of Border checks Regulation 2018/1861 via Art. 19 of TCN Regulation 2018/1860) • System Operator - Authorities responsible for customs checks (Art. 34(1)(b) of Border checks Regulation 2018/1861) • System Operator - Law enforcement authorities (Art. 34(1)(b) of Border checks Regulation 2018/1861) • System Operator – Authorities responsible for the prevention, detection, investigation or prosecution of terrorist offences or other serious criminal offences or the execution of criminal penalties, within the Member State concerned, provided that Directive (EU) 2016/680 applies (Art. 34(1)(c) of Border checks Regulation 2018/1861) • System Operator – Authorities responsible for examining the conditions and taking decisions related to the entry and stay of third-country nationals on the territory of the Member States, including on residence permits and long-stay visas, and to the return of third-country nationals, as well as carrying out checks on third-country nationals who are illegally entering or staying on the territory of the Member States (Art. 34(1)(d) of Border checks Regulation 2018/1861) • System Operator – Authorities responsible for security checks on third-country nationals who apply for international protection, insofar as authorities performing the checks are not 'determining authorities' as defined in point (f) of Art. 2 of Directive 2013/32/EU of the European Parliament and of the Council6, and, where relevant, providing advice in accordance with Council Regulation (EC) No 377/200413(Art. 34(1)(e) of Border checks Regulation 2018/1861) • System Operator – Authorities responsible for examining visa applications and taking decisions related to those applications including on whether to annul, revoke or extend visas, in accordance with Regulation (EC) No 810/2009 of the European Parliament and of the Council14 (Art. 34(1)(f) of Border checks Regulation 2018/1861) • System Operator – Authorities responsible for verifying different identities and combating identity fraud in accordance with Chapter V of Regulation (EU) 2019/817 (Art. 34(1)(g) of Border checks Regulation 2018/1861) • System Operator – Authorities responsible for naturalisation, as provided for in national law, for the purposes of examining an application for naturalisation (Art. 34(2) of Border checks Regulation 2018/1861) • System Operator - National judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charge (Art. 34(3) of Border checks Regulation 2018/1861) for the purpose of Art. 24 and 25 of Border checks Regulation 2018/1861) • System Operator Authorities responsible for the manual processing of ETIAS applications by the ETIAS National Unit, pursuant to Art. 8 of Regulation (EU) 2018/1240 (Art. 34(1)(h) of Art. 36 of Border checks Regulation 2018/1861 via Art. 19 of TCN Regulation 2018/1860) • System Operator ETIAS Central Unit (Art. 36b of Border checks Regulation 2018/1861 via Art. 19 of TCN Regulation 2018/1860) • System Operator European Border and Coast Guard teams, teams of staff involved in return related tasks, and members of the migration management support teams (Art. 36 of Border checks Re) •System Operator - SIRENE Bureau (Art. 7(1) of Border checks Regulation 2018/1861 via Art. 19 of TCN Regulation 2018/1860. In the context of SIS in the field of border checks (Regulation 2018/1861): • Third-country nationals in respect of whom an alert has been issued, for the purposes of refusing entry or stay - Art. 24 of Regulation 2018/1861. • Third-country nationals who are beneficiaries of the right of free movement within the Union - Art. 26 of Regulation 2018/1861. • Third-country nationals subject to restrictive measures intended to prevent entry into or transit through the territory of Member States - Art. 25 of Regulation 2018/1861. • Person whose identity has been misused - Art. 47 of Regulation 2018/1861. • Operator on Member-States side - Authority which shall have central responsibility for its N.SIS (the 'N.SIS Office') - Art. 7(1) of Regulation 2018/1861. • Operator on Member-States side/end-user - Authorities responsible for border controls - Art. 34(1)(a) of Regulation 2018/1861. • Operator on Member-States side - Authorities responsible for customs checks - Art. 34(1)(b) of Regulation 2018/1861. • Operator on Member-States side- Law enforcement authorities - Art. 34(1)(b) of Regulation 2018/1861. • Operator on Member-States side - National judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charge - Art. 34(3) of Regulation 2018/1861. • Operator on Member-States side - Authorities responsible for examining visa applications, issuing visas, and for issuing residence permits - Art. 34(1)(f) of Regulation 2018/1861. • System Operator – Authorities responsible for security checks on third-country nationals who apply for international protection; • System Operator – Authorities responsible for verifying different identities and combating identity fraud in accordance with Chapter V of Regulation (EU) 2019/817 (Art. 34(1)(g) of Border checks Regulation 2018/1861) • System Operator – Authorities responsible for naturalisation, as provided for in national law, for the purposes of examining an application for naturalisation (Art. 34(2) of Border checks Regulation 2018/1861) • System Operator Authorities responsible for the manual processing of ETIAS applications by the ETIAS National Unit, pursuant to Art. 8 of Regulation (EU) 2018/1240 (Art. 34(1)(h) of Art. 36 of Border checks Regulation 2018/1861) • System Operator ETIAS Central Unit (Art. 36b of Border checks Regulation 2018/1861) • System Operator European Border and Coast Guard teams, teams of staff involved in returnrelated tasks, and members of the migration management support teams (Art. 36 of Border checks Regulation 2018/1861) • System Operator - SIRENE Bureau (Art. 7(1) of Border checks Regulation 2018/1861) In the context of SIS in the field of police cooperation and judicial cooperation in criminal matters (Regulation 2018/1862) • Persons wanted for arrest for surrender or extradition purposes - Art. 26 of Regulation 2018/1862. • Missing persons who: (i) need to be placed under protection; (ii) missing persons who do not need to be placed under protection - Art. 32 of Regulation 2018/1862. • Persons sought to assist with a judicial procedure, including: (i) witnesses; (ii) persons summoned or persons sought to be summoned to appear before the judicial authorities in connection with criminal proceedings in order to account for acts for which they are being prosecuted; (iii) persons who are to be served with a criminal judgment or other documents in connection with criminal proceedings in order to account for acts for which they are being prosecuted; (iv) persons who are to be served with a summons to report in order to serve a penalty involving deprivation of liberty - Art. 34 of Regulation 2018/1862. • Persons for the purposes of discreet checks or specific checks - Art. 36 of Regulation 2018/1862. • Person whose identity has been misused - Art. 62 of Regulation 2018/1862. • Third-Country Nationals in the interest of the Union (Art. 37a(1) Judicial Cooperation Regulation 2018/1862). • Data subjects whose data is connected to objects sought for the purposes of seizure or use as evidence in criminal proceedings - Art. 38 of Regulation 2018/1862. • Operator (Authority which shall have central responsibility for its N.SIS (the 'N.SIS Office') - Art. 7(1) of Regulation 2018/1862. • Operator (Authorities responsible for border controls) - Art. 44(1)(a) of Regulation 2018/1862. • Operator (Authorities responsible for police and customs checks) - Art. 44(1)(b) of Regulation 2018/1862. • Operator (Responsible authority for granting and withdrawing international protection) - Art. 44(1)(e) of Judicial Cooperation Regulation 2018/1862). • Operator Authorities responsible for the prevention, detection, investigation or prosecution of terrorist offences or other serious criminal offences or the execution of criminal penalties, within the Member State concerned, provided that Directive (EU) 2016/680 applies (Art. 44(1)(c) of Judicial Cooperation Regulation 2018/1862). • Operator Authorities responsible for examining the conditions and taking decisions related to the entry and stay of third-country nationals on the territory of the Member States, including on residence permits and long-stay visas, and to the return of third-country nationals, as well as carrying out checks on third country nationals who are illegally entering or staying on the territory of the Member States (Art. 44(1)(d) of Judicial Cooperation Regulation 2018/1862). • Operator Authorities responsible for verifying different identities and combating identity fraud in accordance with Chapter V of Regulation (EU) 2019/818 (Art. 44(1)(f) of Judicial Cooperation Regulation 2018/1862). • Operator (National Judicial Authorities) - Art. 44(3) of Regulation 2018/1862. • Operator (Europol) - Art. 48 of Regulation 2018/1862. • Operator (Eurojust) - Art. 49 of Regulation 2018/1862. • Operator (Frontex) - Art. 50 of Regulation 2018/1862. • Operator (ETIAS Central Unit) -Art. 49a of Judicial Cooperation Regulation 2018/1862. • Operator (SIRENE Bureau) - Art. 7(2) of Regulation 2018/1862.	• Name, contact details and affiliation (such as "surname(s) and forename(s)", "name(s) at birth and previously used names and any aliases, which may be entered separately"). • e-Communication and/or connection data (Technical and configurational data that can be linked to data subjects' set of information making them Identifiable Personal Information such as "links ID to other alerts issued in SIS", which might be found in Regulation 2018/1861 or system-supporting documentation like Interface Control Document ("ICD") or system's user manual; Logs (history of the alerts, timestamp of transmission, data used to perform the searches, Schengen ID, Request Number, name of competent authority responsible for processing the data) as per Art. 18(2)(3) of Border checks Regulation. 2018/1861 via Art. 19 of TCN Regulation 2018/1860). • Personal identification numbers (such as: the category of the person's identification documents, the country of issue of the person's identification documents, number(s) of identity paper(s) and date of issue;vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost or invalidated). • Image (photographs). • Other personal data:place of birth (Art. 4(1)(e) of TCN Regulation 2018/1860; date of birth (Art. 4(1)(f) of TCN Regulation 2018/1860); gender (Art. 4(1)(g) of TCN Regulation 2018/1860); any nationalities held (Art. 4(1)(h) of TCN Regulation 2018/1860); whether the person concerned: (i) is armed, (ii) is violent, has absconded or escaped, (iv) poses a risk of suicide, poses a threat to public health or (vi) is involved in an activity referred to in Articles 3 to 14 of Directive (EU) 2017/541 (Art. 4(1)(i) of TCN Regulation 2018/1860); the reason for the alert (Art. 4(1)(j) of TCN Regulation 2018/1860); the authority which created the alert (Art. 4(1)(k) of TCN Regulation 2018/1860); a reference to the decision giving rise to the alert (Art. 4(1)(l) of TCN Regulation 2018/1860); the action to be taken in the case of a hit (Art. 4(1)(m) of TCN Regulation 2018/1860); whether the return decision is issued in relation to a thirdcountry national who poses a threat to public policy, to public security or to national security (Art. 4(1)(o) of TCN Regulation 2018/1860). • Records of every access and all exchanges of personal data within CS-SIS central system (includes data such as "history of the alerts", "date and time of the data transmitted", "data used to perform searches" and "reference to the data transmitted" in line with Art. 18(1) and (2) of Regulation 2018/1861). • Special categories of personal data: • Sensitive data (Biometric data). • Data related to criminal convictions and offences ("type of offence" as per Art. 20(3)(n) of Regulation 2018/1861 and (Art. 20(2)(r) of Border checks RegulationArt. 4(1)(p) of TCN Regulation 2018/1860, and "copy of the original of the European Arrest Warrant/ copy of a translation of the European Arrest Warrant" as per Art. 27 thereof). • Data associated to objects sought for the purposes of seizure or use as evidence in criminal proceedings (such as "objects carried" as per Art. 37(1)(g) of Regulation 2018/1862, "issued identity papers such as passports, identity cards, driving licenses, residence permits and travel documents which have been stolen, misappropriated, lost or invalidated" as per Art. 38(2)(l) thereof, and even "vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost or invalidated" as per Art. 38(2)(m) via Art. 40(3), 52 and Art. 62(6) of Regulation 2018/1862).	Yes	Member States competent authorities having central responsibility for its N.SIS II (the N.SIS II Office), and authorities which ensuring the exchange of supplementary information, are to be considered controllers. The list of competent authorities which are authorised to search directly the data contained in the second generation Schengen Information System can be found here:https://www.eulisa.europa.eu/our-publications/sis-list-competent-authorities-2025-updated	For the purpose of technical and security incident investigation when strictly necessary in line with data minimization principle and security measures: • Tef Lot 2	• Data related to the return of illegally staying third country nationals (TCN Regulation 2018/1860 Retention and Renew period for alert on return (Art. 19 of TCN Regulation 2018/1860, via Art. 39 of Border checks Regulation 2018/1861): (a) Alerts shall be kept only for the time required to achieve the purposes for which they were entered, Art. 39 (1) of Border checks Regulation 2018/1861. (b) An issuing Member State shall, within three years of the entry of an alert into SIS, review the need to retain it. However, if the national decision on which the alert is based provides for a longer period of validity than three years, the alert shall be reviewed within five year Art. 39 (2) of Border checks Regulation 2018/1861 • SIS in the field of border checks (Border checks Regulation 2018/1861): Alerts in general: For the time required to achieve the purposes for which the alerts were entered (Art. 39(1) of Border checks Regulation 2018/1861). In any case, MS issuing an alert shall, within three years of its entry in SIS, review the need to keep it (Art. 39(2) of Border checks Regulation 2018/1861). • Data on persons whose identity has been misused: shall be deleted at the same time as the corresponding alert or earlier where the person so requests (Art. 47(5) of Border checks Regulation 2018/1861). • SIS in the field of police cooperation and judicial cooperation in criminal matters (Judicial Cooperation Regulation 2018/1862): Alerts in general: For the time required to achieve the purposes for which they were entered (Art. 53(1) Judicial Cooperation Regulation 2018/1862). Data on persons who complaints that they are not the person wanted by an alert: shall be deleted at the same time as the corresponding alert or earlier where the person so requests (Art. 62(5) Judicial Cooperation Regulation 2018/1862). Data on persons whose data is connected to objects sought for the purposes of seizure or use as evidence in criminal proceedings: Alerts on objects shall be kept only for the time required to achieve the purposes for which they were entered (Art. 54(1) Judicial Cooperation Regulation 2018/1862), and for a maximum of 10 years (Art. 54(3) thereof), unless extended by MS (Art. 54(4) Judicial Cooperation Regulation 2018/1862). SIS Central System: Records/logs: shall be deleted at the earliest one year, and at the latest three years, after their creation. The records which include the history of alerts shall be erased one to three years after deletion of the alerts. Records may be kept longer if they are required for monitoring procedures that are already under way. Art. 18(4) and (5) of Border checks Regulation 2018/1861 and Judicial Cooperation Regulation 2018/1862. Technical copies which result in offline databases: may be retained for a period not exceeding 48 hours (Art. 41(3) of Border checks Regulation 2018/1861) a) SIS on the return of illegally staying thirdcountry nationals (TCN Regulation 2018/1860 Retention and Renew period for alert on return (Art. 19 of TCN Regulation 2018/1860, via Art. 39 of Border checks Regulation 2018/1861): (a) Alerts shall be kept only for the time required to achieve the purposes for which they were entered, Art. 39 (1) of Border checks Regulation 2018/1861. (b) An issuing Member State shall, within three years of the entry of an alert into SIS, review the need to retain it. However, if the national decision on which the alert is based provides for a longer period of validity than three years, the alert shall be reviewed within five year Art. 39 (2) of Border checks Regulation 2018/1861 b) SIS in the field of border checks: Alerts in general: For the time required to achieve the purposes for which the alerts were entered (Art. 39(1) of Border checks Regulation 2018/1861). In any case, MS issuing an alert shall, within three years of its entry in SIS, review the need to keep it (Art. 39(2) of Border checks Regulation 2018/1861). Where the MS decides to retain de alert longer than the review period, that MS shall, within three years of the extension of the period to keep the alert entered in SIS, review the need to keep it (Art. 39(4) of Border checks Regulation 2018/1861). Technical copies which result in offline databases: may be retained for a period not exceeding 48 hours (Art. 41(3) of Border checks Regulation 2018/1861). Data on persons whose identity has been misused: shall be deleted at the same time as the corresponding alert or earlier where the person so requests (Art. 47(5) of Border checks Regulation 2018/1861). c) SIS in the field of police cooperation and judicial cooperation in criminal matters (Judicial Cooperation Regulation 2018/1862): Alerts in general: For the time required to achieve the purposes for which they were entered (Art. 53(1) Judicial Cooperation Regulation 2018/1862). In any case, MS issuing an alert shall review the need to keep it within one or three years of its entry into SIS depending on the nature of the Alert. Alerts regarding "Person whose identity has been misused (Art. 47 of Border checks Regulation 2018/1861)" data subjects shall be reviewed in one year (Art.53(2) Judicial Cooperation Regulation 2018/1862). Where the MS decides to retain de alert longer than the review period, that MS shall, within the extension period, review the need to keep it (Art. 53(6) Judicial Cooperation Regulation 2018/1862). Data on persons whose identity has been misused: Shall be deleted at the same time as the corresponding alert or earlier where the person so requests (Art. 62(5) Judicial Cooperation Regulation 2018/1862). Data on persons who complaints that they are not the person wanted by an alert: shall be deleted at the same time as the corresponding alert or earlier where the person so requests (Art. 62(5) Judicial Cooperation Regulation 2018/1862). Data on persons whose data is connected to objects sought for the purposes of seizure or use as evidence in criminal proceedings: Alerts on objects shall be kept only for the time required to achieve the purposes for which they were entered (Art. 53(1) Judicial Cooperation Regulation 2018/1862), and for a maximum of 10 years (Art. 54(2)) thereof, unless extended by MS (Art. 54(4) Judicial Cooperation Regulation 2018/1862).	For the purposes of the system operational management: • eu-LISA designated staff members For the operation and security of the N.SIS: • Authority which shall have central responsibility for its N.SIS (the 'N.SIS Office') - Art. 7(1) of both Regulation 2018/1861 and Regulation 2018/1862. Within the context of supplementary information, namely: i) to ensure the exchange and availability of all supplementary information; ii) to be able to react to requests for supplementary information swiftly and within the deadlines provided by law; and, iii) for the verification of the quality of the information entered in SIS: • SIRENE Bureau - Art. 7(1) of both Regulation 2018/1861 and Regulation 2018/1862. For the identification of third-country nationals for the purpose of border control, namely, in accordance with Regulation (EC) No 562/2006 of the European Parliament and the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code): • Authorities responsible for border controls/border authorities - Art. 34(1)(a) of Regulation 2018/1861 and Art. 44(1)(a) of Regulation 2018/1862. For the identification of third-country nationals for the purposes of police and customs checks: • Authorities responsible for customs checks - Art. 34(1)(b) of Regulation 2018/1861 and Art. 44(1)(b) of Regulation 2018/1862. • National Law enforcement authorities - Art. 34(1)(b) of Regulation 2018/1861 and Art. 44(1)(b) of Regulation 2018/1862. For the identification of third-country nationals, in line with the need to the performance of their tasks, as provided for in national legislation, and by their coordinating authorities: • National judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charging a person - Art. 34(3) of Regulation 2018/1861 and Art. 44(3) of Regulation 2018/1862. In the context of granting and withdrawing international protection: • Responsible authorities for the security checks on third-country nationals who apply for international protection, in accordance with Art. 34(1)(e) of Regulation 2018/1861 and Art. 44(1)(e) of Regulation 2018/1862 In the context of the application of the Community acquis relating to the movement of persons: • Authorities responsible for issuing visas, central authorities responsible for examining visa applications and authorities responsible for issuing residence permits - Art. 34(1)(d) and (f) of Regulation 2018/1861. For the identification of third-country nationals for the purpose of prevention, detection, investigation or prosecution of terrorist offences or other serious criminal offences or the execution of criminal penalties: • MS Law enforcement authorities - Art. 34(1)(c) of Regulation 2018/1861 and Art. 44(1)(c) of Regulation 2018/1862. For the purpose of monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of CS-SIS, data integrity and security: • Competent authorities in charge of checking whether a search is lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of CS-SIS, data integrity and security as per article 18(5) of Regulation 2018/1861. For the purpose of carrying out checks in accordance with Art. 44(1) of Regulation 2018/1862, and within their mandate: • Frontex - Art. 50 of Regulation 2018/1862 Where necessary to fulfil its mandate, including within the exchange and further request of supplementary information in accordance with the provisions of the SIRENE Manual, as per Art. 41(1) Council Decision 2007/533/JHA: • Europol - Art. 41 of Council Decision 2007/533/JHA and Regulation 2018/1862. Within their mandate: • Eurojust - Art. 42 of Council Decision 2007/533/JHA and Art. 49 of Regulation 2018/1862. Exchange of data on stolen, misappropriated, lost or invalidated passports: • Interpol - Art. 55 of Council Decision 2007/533/JHA (subject to an agreement with European Union on the data flows). As per Art.4(e) of Regulation (EU) 2018/1240, ETIAS, shall support the objectives of SIS related to alerts on third-country nationals subject to a refusal of entry and stay, alerts on persons wanted for arrest for surrender purposes or extradition purposes, alerts on missing persons, alerts on persons sought to assist with a judicial procedure and alerts on persons for discreet checks or specific checks. • Authorities responsible for the manual processing of ETIAS applications by the ETIAS National Unit, pursuant to Art. 8 of Regulation (EU) 2018/1240 (Art. 34(1)(h) of Border checks Regulation 2018/1861 and Art. 19 of TCN Regulation 2018/1860). As per Art. 26 of Regulation (EU) 2018/1240 where the automated process laid down in Art. 20(2) to (5) of this Regulation has reported one or several hits, the application shall be processed manually by the ETIAS National Unit of the Member State responsible • System Operator ETIAS Central Unit (Art. 36b of Border checks Regulation 2018/1861 and Art. 19 of TCN Regulation 2018/1860) • System Operator European Border andCoast Guard teams, teams of staff involved in returnrelated tasks, and members of the migration management support teams (Art. 36 of Border checks Regulation 2018/1861 and Art. 19 of TCN Regulation 2018/1860)	Yes	No	No
					•Keeping EES functioning 24 hours a day, 7 days a week in accordance with EES Regulation, in particular, the maintenance work and technical developments necessary to ensure that the EES functions at a satisfactory level of operational quality, in particular as regards the response time for interrogation of the EES Central System by border authorities, in accordance with the technical specifications (Art. 37(3), 2nd par. of EES Regulation). •Ensuring adequate security of EES, including the adoption of a security plan and a business continuity and disaster recovery plan (Art. 5, 7, 37 and 43(3) of EES Regulation). •Hosting EES Central System (Art. 7(2) of EES Regulation)	Eu-LISA statutory staff: Other categories of data subjects • Third-country nationals admitted for a short stay to the territory of the Member States who are subject to border checks in accordance with Regulation (EU) 2016/399 when crossing the borders at which the EES is operated (Art. 2(1)(a) of EES Regulation) • Third-country nationals, on entry to and exit from the territory of the Member States, who: are members of the family of a Union citizen to whom Directive 2004/38/EC applies or of a national of a third country enjoying the right of free movement equivalent to that of Union citizens under an agreement between the Union and its Member States, on the one hand, and a third country, on the other (Art. 2(1)(b)(i) of EES Regulation)	• Name, contact details and affiliation (such as "surname", "name(s) at birth and previously used names and any aliases, which may be entered separately"). • e-Communication and/or connection data (EU Login Credentials (username, authentication status, token responses encrypted and decrypted, authentication request URL), Logs). • Personal identification numbers (Number of the travel document or documents and the three letter code of the issuing country of the travel document or documents, Individual file ID/ individual reference number created by the EES, Entry/exit record ID/ Traveller ID created by the EES). • Image (facial images). • Sensitive data (facial images, fingerprints data). • Other personal data: Date of birth, Sex, Nationality,Type of the travel document or documents, Date of expiry of the validity of the travel		Member State (MS) designated authority having responsibility for its EES use, point (7) of Article 4 of Regulation (EU) 2016/679 and which shall have central responsibility for the processing of data by that MS. Each MS shall communicate the details of that authority to the Commission. (Art. 39(1), 1st par. of EES Regulation) The list of competent authorities which are authorised to use the EES system will be published by each MS by the start of operation	For the purpose of technical and security incident investigation when strictly necessary in line with data minimization principle and security measures: Any subprocessors will be identified by the start of operation.	Data on Third-country nationals subject to a visa requirement (Art. 16 of EES Regulation): • 3 years for entry/exit record or refusal of entry record linked to an individual file, following the date of the exit record or of the refusal of entry record (Art. 34(1) of EES Regulation) and the individual file is kept for 3 years and 1 day, following the date of the last exit record or of the refusal of entry record if there is no entry record within three years from the date of the last exit record or refusal of entry record (Art. 34(2) of EES Regulation). With the following exceptions: • 5 years for third-country nationals data who do not have an exit record following the	Designated eu-LISA staff members Other recipients: • Border authorities (Art. 9(2) and 23 of EES Regulation) • Visa authorities (Art. 9(2) and 24 of EES Regulation) • Immigration authorities (Art. 9(2) and 26 of EES Regulation) • European Data Protection Supervisor (Art. 56 of EES Regulation) • MS Law enforcement authorities (art. 29 of EES Regulation) • MS Central Access Point (art. 29(3) of EES Regulation) • Europol (Art. 30 of EES Regulation) • Carriers (Art. 13(3), 13(4) and 13(6) of EES Regulation) • Frontex (Art. 62(1) EES Regulation)			

0001/2022	2/10/2022		Operations Department - Planning and Standards Unit - Product Management Sector – EES Product Owner	erational management of EES information sys	•Hosting EES Central System (Art. 15(1) of EES Regulation). •Developing and operating the public website referred in Art. 7 of Regulation of Commission Implementing Decision of 30.6.2021 laying down rules for the application of Regulation (EU) 2017/2226 of the European Parliament and of the Council as regards the specifications and conditions for the public website •Hosting, security and operation of the EES web service referred to in Article 13 of EES Regulation, including the separate read-only database referred to in Article 13(5) of EES Regulation, that shall be updated on a daily basis by the VIS via a one-way extraction of the minimum necessary subset of VIS data. •Establishing a Secure Communication Channel between the EES Central System and the VIS Central System to enable interoperability between the EES and the VIS that allows for the retrieval of visa-related data from the VIS, their importation into the EES and the updating of data from the VIS in the EES (Art. 7, 8 and 37 of EES Regulation). •Keeping logs of all data processing operations carried out within the web service by carriers, as per article 13(d) of EES Regulation and articles 10 and 11 of the Regulation 2021/328 on the operation, data protection and security, as well as development and technical implementation of the web service. •Keeping logs of all data processing operations carried out within the EES, as per article 46 of EES Regulation, with the measures set out in the Commission Implementing Decision 2019/328, for keeping and accessing logs in the EES . •Security incident management as per art. 44 of EES Regulation.	Other (Art. 2(1)(b)(i) of EES Regulation) • Third-country nationals, on entry to and exit from the territory of the Member States, who: do not hold a residence card pursuant to Directive 2004/38/EC or a residence permit pursuant to Council Regulation (EC) No 1030/2002 (Art. 2(1)(b)(ii) of EES Regulation) • Third-country nationals whose entry for a short stay to the territory of the Member States is refused in accordance with Article 14 of EES Regulation: Third-country nationals subject to a visa requirement (Art. 2(2) and 18 of EES Regulation) •Third-country nationals whose entry for a short stay to the territory of the Member States is refused in accordance with Article 14 of Regulation (EU) 2016/399: Visa-exempt third-country nationals (Art. 2(2) and 18 of EES Regulation) •Third-country nationals who cross a border on the basis of a valid Facilitated Transit Document issued in accordance with Council Regulation (EC) No 693/2003 (FTD) (Art. 12(2) of EES Regulation) •Third-country nationals subject to a visa requirement (All Third-country nationals listed here, excluding: Visa-exempt third-country nationals (Art. 17 of EES Regulation) (Art. 16 of EES Regulation) •Visa-exempt third-country nationals (Art. 17 of EES Regulation) •MS Border authorities (Operator User ID) (Art. 9(2) and 23 of EES Regulation) •Visa authorities (Operator User ID) (Art. 9(2) and 24 of EES Regulation) •Immigration authorities (Operator User ID) (Art. 9(2) and 26 of EES Regulation) •MS Law enforcement authorities (Operator User ID) (art. 29 of EES Regulation) •Europol Officials (Operator User ID) (Art. 30 of EES Regulation) •Carriers (Operator User ID) (Art. 13(3), 13(4) and 13(6) of EES Regulation) •European Data Protection Supervisor (Operator User ID) (Art. 56 of EES Regulation) •Competent authorities of Member States (Art. 63(1), last par. Of EES Regulation) •European Commission (Art. 63(1), last par. Of EES Regulation) •European Border and Coast Guard Agency (Art. 63(1), last par. Of EES Regulation) Public Website Administrators (Art. 3(1) of Public Website Implementing Decision) Public Website General Public (Art. 6(1) of Public Website Implementing Decision)	• Other personal data: date of birth, sex, nationality; type of the travel documents or documents, date of expiry of the validity of the travel document or documents, National facilitation programme of the Member State concerned, Intended date of entry or exit (optional),MS of destination, Scheduled date of arrival, 'OK'/'NOT OK' reply.	Yes			•3 years for third-country nationals who exceed the authorised stay, from the date of expiry of the above date of expiry of the period of authorised stay, following the date of expiry of the period of authorised stay. (Art. 34(3) of EES Regulation) • 1 year for third-country nationals data, on entry to and exit from the territory of the Member States, who: (i) are members of the family of a Union citizen to whom Directive 2004/38/EC applies or of a national of a third country enjoying the right of free movement equivalent to that of Union citizens under an agreement between the Union and its Member States, on the one hand, and a third country, on the other, and (ii) do not hold a residence card pursuant to Directive 2004/38/EC or a residence permit pursuant to Council Regulation (EC) No 1030/2002 (Article 16(3)(b) and (c) of EES Regulation), after the exit of such third-country nationals. If there is no record of exit, data is stored for a period of five years from the date of the last entry record (Art. 34(4) of EES Regulation). Logs regarding EES Web Service: • 2 years (Art. 13(4), 2nd par. of EES Regulation) Records kept at a central level: • 1 year after the retention period referred to in Article 34 of EES Regulation has expired, unless they are required for monitoring procedures which have already begun (Art. 46(4) of EES Regulation)	• Member States (Art. 63(1) of EES Regulation) • European Commission (Art. 63(1) EES Regulation) • Competent authorities of Member States	Yes	No	No