

To: the eu-LISA Management Board

From: Encarna Gimenez, Data Protection Officer (DPO)

Subject: DPO Annual Work Report - 2024

DPO ANNUAL WORK REPORT 2024

European Union Agency for the Operational Management of Large-Scale IT
Systems in the Area of Freedom, Security and Justice

www.eulisa.europa.eu

Document Control Information

Settings	Value
Document Title:	DPO Annual Work Report – 2024
Document Author:	Data Protection Officer (DPO)
Revision Status:	Final
Sensitivity:	Public
Issue Date:	06/01/2025

Summary of Changes:

Revision	Date	Created by	Short Description of Changes
[1]	05/12/2024	DPO	Initial version of the document created
[2]	10/12/2024	DPO	Final version

Contents

Introduction	4
1. Scope.....	6
2. Reappointment of the DPO: Five Years of Strategic Leadership in Data Protection.....	6
2.1. Implementing a New Data Protection Governance Framework.....	7
2.2. Supporting New eu-LISA Systems and Interoperability	7
2.3. Navigating Data Protection During COVID-19	8
2.4. Addressing International Transfers	8
2.5. Enhancing Compliance Through EDPS Audits.....	8
3. DPO Activities and Actions	9
3.1. Awareness	9
3.2. Advice and Guidance	9
3.3. Records of Processing Activities as Controller.....	10
3.4. Records of Processing Activities as Processor	11
3.5. Personal Data Breach Register	11
3.6. Artificial Intelligence and Biometrics: Five Years of Collaborative Effort	11
3.7. Change Management Process.....	12
3.8. EDPS Supervision and Collaboration	13
3.8.1. Follow-up on the EDPS inspections and recommendations	13
3.8.1.1. 'Back-to-green' approach to the implementation of EDPS audit recommendations.....	13
3.8.1.2. 2022 audit on Eurodac, SISII and VIS	14
3.8.1.3. 2023 audit on SIS.....	14
3.8.2. 2024 Audit on VIS	15
3.8.3. EDPS Survey on Data Protection Impact Assessments.....	15
3.8.4. Participation in the EDPS 20th Anniversary Celebrations	16
3.8.5. Supervision Coordination Groups for Eurodac and VIS and Coordinated Supervision Committee for SIS	16
3.9. JHAA DPO Network Meetings	17
3.10. EDPS - EUI DPO Network Meetings.....	18
3.11. Advancing Professional Expertise	18
3.12. Professional Engagement in Data Protection Community Activities.....	19
3.12.1. CPDP - Data Protection Day - 25 January 2024	19
3.12.2. Internet Privacy Engineering Network Event	20
3.12.3. Annual Privacy Forum	20
3.13. Annual Survey	21
4. DPO Function.....	21

Introduction

Article 2 of Regulation (EU) 2018/1726¹ ('eu-LISA Regulation') outlines the objectives of the Agency emphasising the requirement to ensure a high level of data protection in accordance with Union data protection law. This includes adherence to specific provisions tailored for each EU Large-Scale IT System.

The eu-LISA's Data Protection Officer (DPO) plays a central role in this framework, tasked with informing and advising controllers and processors on fulfilling their data protection obligations. The DPO ensures the internal application, in an independent manner, of Regulation (EU) 2018/1725² ('EUDPR'), with ultimate supervision provided by the European Data Protection Supervisor (EDPS).

2024 marked a significant year, defined by milestones such as the reappointment of the DPO in June 2024 following the successful completion of her first five-year mandate. This achievement underscores the Management Board's trust in the DPO's strategic leadership and consistent contributions to enhancing eu-LISA's compliance framework. The year also witnessed eu-LISA's Presidency of the Justice and Home Affairs Agencies Network (JHAAN), with the DPO organising the meetings of the JHAAN DPOs Working Group, chairing discussions, and contributing to the Joint Opinion on the role of DPOs in Artificial Intelligence (AI). This opinion emphasised the importance of maintaining DPOs as central contact points for AI-related matters with the EDPS and proposed actionable recommendations to address ethical and compliance challenges in AI systems.

The report highlights key initiatives undertaken through close collaboration with the DPO, including advancements in Artificial Intelligence and biometrics. These efforts culminated in the completion of the shared Biometric Matching System³ (sBMS) accuracy measurement exercise. This project not only improved the system's reliability but also set benchmarks for ethical compliance in biometric technologies, reinforcing the Agency's commitment to innovation and safeguarding individual rights.

Additionally, the DPO actively participated in EDPS audits and follow-up activities, strengthened awareness across the Agency through training and newsletters, and collaborated with external stakeholders to ensure compliance with evolving data protection standards. The DPO of eu-LISA worked closely with the data controllers, data processors, and EDPS to find effective and compliant solutions that ensure the respect for privacy and personal data. Within the context of limited resources, the DPO effectively prioritised high-impact activities, including support for new IT systems and the implementation of EDPS recommendations, ensuring critical objectives were met without compromising data protection standards. These efforts further sustained eu-LISA's reputation as a leader in operational excellence and data protection.

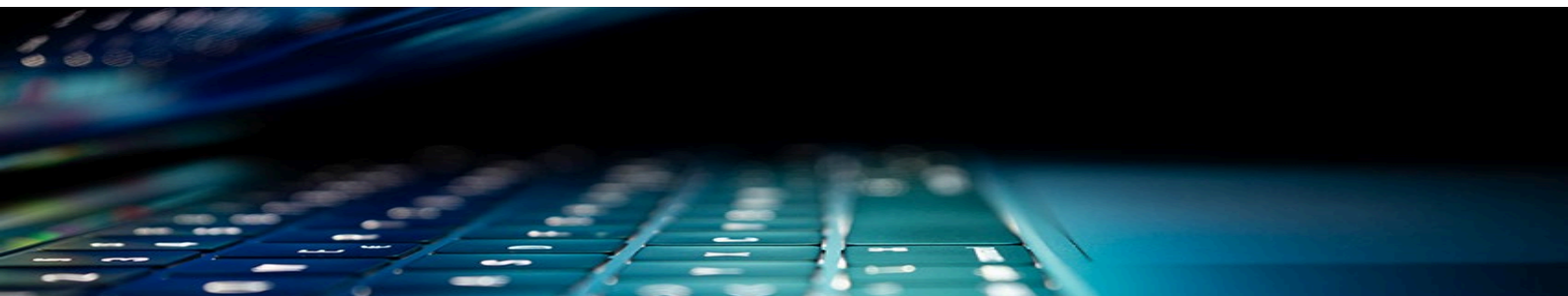
¹ **Regulation (EU) 2018/1726** of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA).

² **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.

³ An EU system established under Regulation (EU) 2019/817 and Regulation (EU) 2019/818, designed to perform biometric matching across multiple large-scale IT systems, including the Entry/Exit System (EES), Visa Information System (VIS), and Eurodac. The sBMS enhances interoperability by enabling efficient and accurate identification, supporting security, and facilitating seamless border management.

Upon reception of the draft report of the EDPS inspection carried out in December 2023 on the Schengen Information System⁴ (SIS), the DPO led a comprehensive exercise to facilitate and support the formal adoption of comments by the Management Board of eu-LISA. This process was conducted in accordance with Article 19(1)(hh) of the eu-LISA Regulation, ensuring that the Agency's feedback was thorough, consistent, and aligned with data protection obligations. The DPO's coordination and guidance were critical in streamlining this process, addressing EDPS recommendations effectively, and reinforcing eu-LISA's commitment to transparency and accountability.

This report reflects the DPO's unwavering commitment to upholding the highest standards of data protection while providing a notable example of addressing challenges with innovation and strategic leadership.



⁴ **Regulation (EU) 2018/1861** of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 and **Regulation (EU) 2018/1862** of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU. Noting that, as defined in Article 19 of **Regulation (EU) 2018/1860** of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals, the entry, processing and updating of alerts, the provisions on responsibilities of the Member States and eu-LISA, the conditions concerning access and the review period for alerts, data processing, data protection, liability and monitoring of statistics, as laid down in Articles 6 to 9, Articles 20(3) and (4), Articles 21, 23, 32, 33, 34(5) and 38 to 60 of Regulation (EU) 2018/1861, apply as well to Regulation (EU) 2018/1860, insofar as this is not specifically arranged in Regulation (EU) 2018/1860 itself.

1. Scope

Under Article 7(4) of the eu-LISA DPO Implementing Rules⁵, the DPO is required to submit an annual report to the Agency's Management Board detailing her activities and providing an overview of the state of play regarding the Agency's data protection activities and compliance.

This report outlines the status of data protection activities within the Agency and summarises the work carried out by the DPO during the year 2024.

2. Reappointment of the DPO: Five Years of Strategic Leadership in Data Protection

First appointed as the Data Protection Officer (DPO) of eu-LISA in June 2019, the DPO has successfully completed her initial five-year mandate, navigating the complexities of an evolving regulatory and operational landscape. During the March 2024 Management Board meeting, the DPO presented a comprehensive review of her tenure, structured around five major challenges and solutions that defined her first mandate.

These key areas included:

1. Implementing and operationalising the new data protection governance framework under EUDPR.
2. Supporting the development and interoperability of new large-scale IT systems in compliance with data protection principles.
3. Addressing data protection challenges during the COVID-19 pandemic, including guidance on workplace policies.
4. Ensuring compliance with complex requirements for international data transfers, including the impact of the Schrems II ruling.
5. Enhancing the Agency's reputation and compliance through the successful implementation of EDPS audit recommendations.

Moreover, the DPO also raised awareness of Section 6 of the EUDPR, which outlines the provisions relating to the Data Protection Officer. This included a focus on:

- Designation under Article 43, ensuring independence and expertise in fulfilling the role.
- Position as detailed in Article 44, highlighting the DPO's direct reporting to the highest management level and protection from penalties for performing their tasks.
- Tasks defined in Article 45, encompassing the DPO's responsibility for ensuring the internal application of the EUDPR and providing guidance on compliance matters.

⁵ **eu-LISA Management Board Decision No 2019-185 REV 1** on implementing rules concerning the Data Protection Officer pursuant to Article 45(3) of Regulation (EU) No 2018/1725 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.

- Following this evaluation, the Management Board formally reappointed the DPO in June 2024, recognising her essential contributions, the trust she has earned through her leadership, and her continued commitment to upholding the highest data protection standards.

This set the stage for sustained strategic leadership, building on the achievements of the past five years and providing a strong foundation for addressing future challenges in data protection with innovation and dedication.

2.1. Implementing a New Data Protection Governance Framework

With the entry into force of the EUDPR in December 2018, eu-LISA faced the challenge of transitioning from the old framework to the new, while ensuring full compliance with data protection requirements. The DPO led the establishment of a new data protection governance framework to strengthen compliance and embed data protection principles into the Agency's operations. Key initiatives included:

- Implementing new rules concerning the DPO as required under Article 45(3) of the EUDPR, formalising the DPO's tasks, duties, and powers within the Agency's governance structure.
- Creating Internal Rules for the restriction of certain data subject rights under Article 25 of the Regulation, ensuring a legally sound approach to balancing operational needs with the protection of individual rights.
- Developing a comprehensive Data Breach Policy to ensure clear processes for identifying, managing, and responding to data breaches.
- Developing a methodology for Data Protection Impact Assessments (DPIAs) to assess and mitigate risks effectively.
- Designing templates for records, risk screening, and threshold assessments, standardising processes and improving efficiency.
- Conducting extensive training on the new EUDPR, fostering awareness and compliance across all levels of the Agency.

These efforts collectively established a robust data protection governance framework that supports operational excellence and ensures compliance with the highest standards within eu-LISA.

2.2. Supporting New eu-LISA Systems and Interoperability

The implementation of new large-scale IT systems and the interoperability framework under Regulation (EU) 2018/1726 introduced complex data protection challenges. The DPO played a fundamental role in:

- Conducting DPIAs for systems such as EES⁶, sBMS, ETIAS⁷, SIS, ECRIS-TCN⁸, CRRS⁹ and others.
- Engaging in prior consultations with the EDPS, including securing a favourable opinion in 2022 on DPIAs related to the accuracy measurement of biometric systems.

⁶ Entry/Exit System (EES): A European Union system designed to register entry, exit, and refusal of entry information of third-country nationals crossing the external borders of the EU. Established under Regulation (EU) 2017/2226, the EES aims to improve border management, enhance security, and streamline the processing of travellers.

⁷ European Travel Information and Authorisation System (ETIAS): A system established under Regulation (EU) 2018/1240, designed to pre-screen and authorise travellers from visa-exempt third countries before they enter the Schengen Area. ETIAS aims to enhance border management, strengthen security, and facilitate travel within the EU by assessing potential risks associated with visa-exempt travellers.

⁸ European Criminal Records Information System for Third Country Nationals and Stateless Persons (ECRIS-TCN): A system established under Regulation (EU) 2019/816, designed to enhance the exchange of information on criminal records of third-country nationals and stateless persons between EU Member States.

⁹ Central Repository for Reporting and Statistics (CRRS): A system established under Regulation (EU) 2019/817 and Regulation (EU) 2019/818, designed to centralise and streamline reporting and statistical data across multiple EU large-scale IT systems.

- Ensuring the application of the Data Protection by Design and by Default (DPbDD) principle throughout the lifecycle of these systems.

This proactive involvement not only underscored eu-LISA's commitment to embedding data protection into its operational management but also highlighted the DPO's strategic leadership and expertise in addressing complex data protection challenges.

2.3. Navigating Data Protection During COVID-19

The COVID-19 pandemic brought unprecedented challenges, requiring swift adaptations to new processing activities and ways of working. The DPO ensured:

- Alignment with European Data Protection Board (EDPB) and EDPS guidelines on pandemic-related data protection issues, including the "Return to Workplace" framework.
- Continuous collaboration with other EU institution DPOs and the EDPS to address emerging risks.

This adaptability reinforced eu-LISA's ability to maintain compliance while addressing novel data protection scenarios.

2.4. Addressing International Transfers

The invalidation of the Privacy Shield by the Schrems II ruling in 2020 required a reassessment of international data transfers. The DPO took the lead in:

- Mapping all international transfers and identifying legitimate mechanisms for compliance.
- Supporting the adoption of Transfer Impact Assessments (TIAs) and supplementary measures.
- Aligning eu-LISA's practices with the EU-US Data Privacy Framework adopted in 2023.

These efforts ensured that eu-LISA remained compliant with evolving international data transfer standards.

2.5. Enhancing Compliance Through EDPS Audits

The DPO played an essential role in addressing EDPS audit recommendations, which were particularly critical in 2019. Through quarterly internal monitoring and proactive updates, the DPO:

- Achieved "Back-to-Green" status by 2023, with all 43 recommendations from the 2018 EDPS audit on SIS and VIS implemented within the deadline.
- Supported the implementation of key recommendations for Eurodac, ensuring positive outcomes in subsequent audits.

These achievements not only enhanced eu-LISA's reputation as a trustworthy IT service provider but also demonstrated the DPO's leadership in navigating complex challenges.

Over the past five years, her strategic leadership and proactive approach have ensured the Agency's compliance with evolving data protection standards. By delivering innovative solutions and fostering a culture of accountability, the DPO has strengthened eu-LISA's position as a leader in safeguarding privacy and managing large-scale IT systems securely.

3. DPO Activities and Actions

The following sections provide a comprehensive overview of the Agency's data protection activities and its compliance with the EUDPR. Particular attention is given to the work performed by the DPO in 2024, highlighting key achievements, initiatives, and contributions to safeguarding data protection standards across the Agency.

3.1. Awareness

In order to raise awareness on data protection, the DPO of eu-LISA makes use of various tools, including general awareness sessions, one-on-one coaching sessions, weekly newsletters and the dedicated Data Protection Officer intranet.

On Data Protection Day, the DPO launched a dedicated webpage, 'Responding to Data Subject Requests,' offering clear, actionable guidance to data controllers across eu-LISA. This initiative empowers teams to uphold data subject rights under the EUDPR effectively.

To mark the publication of the EU Artificial Intelligence Act (Regulation 2024/1689) in the Official Journal, the DPO launched a series of articles in the weekly newsletter, aligned with the *EDPS guidelines on generative Artificial Intelligence and personal data for EU institutions, bodies, offices and agencies (EUIs) of 3 June 2024*. In addition, the Intern to the DPO collaborated with colleagues from the Solutions and Architecture Design Sector, Cybersecurity, Legal, and Research and Development sectors to host an AI Awareness Session.

On 8 March 2024, the EDPS adopted a decision following its investigation into the European Commission's use of Microsoft 365, focusing on compliance with the EUDPR regarding purpose limitation, international transfers, and unauthorised disclosures of personal data. To ensure awareness of this decision across eu-LISA, the DPO included a dedicated article in the internal newsletter and provided additional guidance to relevant stakeholders on how the EDPS findings may impact the use of similar tools within the Agency.

To optimise support for the data controllers and processors, the DPO Intranet was regularly updated with templates, step-by-step instructions, and relevant resources.

Other efforts to raise awareness included a dedicated Data Protection Corner in the weekly eu-LISA newsletter, distributed to all staff members. This section provides updates on the latest guidelines, training opportunities, and developments in the field. During 2024, the DPO published 25 articles on data protection, including a special newsletter in December featuring an End-of-Year Wish and a Key Takeaway from 2024:

'Building strong partnerships within and beyond the Agency ensures not only compliance but also innovation in addressing emerging challenges in data protection. Collaborative problem-solving amplifies our ability to protect individual rights while supporting operational excellence.'

3.2. Advice and Guidance

The DPO must be involved properly and in a timely manner in all issues relating to the protection of personal data to provide meaningful guidance (Article 44(1) of the EUDPR). Where the Agency ensured this obligation in 2024, the DPO was able to fulfil her mandate effectively.

The DPO provided one-on-one coaching sessions to staff members seeking advice and guidance to comply with their obligations as data controllers or processors under the EUDPR. In addition, the DPO issued formal recommendations, such as the guidance provided on 17 May 2024 following a consultation on the use of real biometric data within eu-LISA's testing environment.

As part of broader data protection efforts, the DPO contributed to policymaking at the European level by providing expert input to the European Commission, in close collaboration with eu-LISA's liaison office. This included consultations on Justice and Home Affairs (JHA)-related legislative proposals, such as those concerning the collection and transfer of Advance Passenger Information (API)¹⁰, as well as implementing acts related to the digitalisation of the visa procedure under Regulation (EU) 2023/2667¹¹. These contributions ensured that the initiatives align with data protection principles and compliance standards.

eu-LISA follows the principles of privacy by design and by default throughout the lifecycle of its large-scale IT systems. Data Protection Impact Assessments (DPIAs) are central to implementing these principles, supporting the operational management and development of these systems. In line with EDPS guidance¹² and WP29/EDPB guidelines on DPIAs¹³, the DPO has provided relevant advice and guidance to eu-LISA staff across all departments and its contractors, ensuring compliance with data protection regulation.

Furthermore, the team of the DPO has regularly contributed comments to ongoing and new DPIAs. The DPO has also been consulted by product owners seeking external support for data protection-related tasks. Feedback from the DPO emphasised the importance of engaging specialised support, such as certified data protection professionals with proven expertise, to effectively carry out consultancy tasks and ensure compliance with data protection requirements.

3.3. Records of Processing Activities as Controller

In compliance with Article 31(1) of the EUDPR, eu-LISA maintains records of processing activities under its responsibility. According to Article 4(3) of the eu-LISA DPO Implementing Rules, the DPO is responsible for maintaining a central register of records of processing activities as a controller.

Delegated data controllers within eu-LISA are required to document any new processing activity as a new record and notify the DPO to ensure the central register is updated accordingly. Similarly, when an existing processing activity undergoes changes, the data controller must update the associated documentation and notify the DPO of the change.

To facilitate these tasks and ensure compliance, the DPO has prepared step-by-step instructions and templates for documenting records of processing activities.

¹⁰ Proposal for a Regulation of the European Parliament and of the Council on the collection and transfer of advance passenger information (API) for enhancing and facilitating external border controls, amending Regulation (EU) 2019/817 and Regulation (EU) 2018/1726, and repealing Council Directive 2004/82/EC, COM(2022) 729 final, 13 December 2022; Proposal for a Regulation of the European Parliament and of the Council on the collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, and amending Regulation (EU) 2019/818, COM(2022) 731 final, 13 December 2022.

¹¹ Regulation (EU) 2023/2667 of the European Parliament and of the Council of 22 November 2023 amending Regulations (EC) No 767/2008, (EC) No 810/2009, and (EU) 2017/2226, Council Regulations (EC) No 693/2003 and (EC) No 694/2003, and the Convention implementing the Schengen Agreement, as regards the digitalisation of the visa procedure, OJ L 2667, 7.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2667/oj>.

¹² EDPS, **Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies**

¹³ Working Party Art. 29, **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01**

By the end of December 2024, the eu-LISA register of data processing activities included 142 ongoing records, seven of which were registered during 2024. This register is public, continuously updated, and accessible on the eu-LISA website.

3.4. Records of Processing Activities as Processor

Under Article 31(2) of the EUDPR, eu-LISA is required to maintain a record of all categories of processing activities carried out on behalf of one or more controllers. This register, centrally managed by the DPO, is public, continuously updated, and accessible on the eu-LISA website.

During 2024, no new records were notified to the DPO.

3.5. Personal Data Breach Register

Following obligations under Article 34(6) of the EUDPR, data controllers are required to document any personal data breaches. According to Article 4(3) of the eu-LISA DPO Implementing Rules, the DPO maintains a central register of records of data breaches.

During the reference period for this report, and following investigations, four data breaches were reported and documented by the data controller. The management and updating of the central register, a task delegated by the DPO to her team, demonstrated the value of collaborative efforts in addressing the Agency's data protection priorities. While the team's contributions were critical, challenges arose in ensuring accuracy and reporting, which underscored the need for enhanced oversight, areas for improvement, and implementing solutions. Under the DPO's guidance, the team engaged in targeted training and process enhancements, showcasing a shared commitment to ensuring compliance with the highest standards and maintaining the reliability of the breach management process over time.

3.6. Artificial Intelligence and Biometrics: Five Years of Collaborative Effort

One of the most significant milestones in 2024 was the culmination of five years of dedicated work on the Entry/Exit System (EES) and the shared Biometric Matching System (sBMS).



This effort, undertaken in close collaboration between the DPO, EES and sBMS colleagues, and key stakeholders, ensured compliance with rigorous data protection and ethical standards. The completion of the sBMS accuracy measurement exercise marked a defining moment in eu-LISA's commitment to ethical and compliant biometric systems.

In July 2024, the DPO of eu-LISA oversaw the sBMS annotation exercise, a critical part of the data preparation phase within the AI lifecycle. This involved the systematic analysis and categorisation of biometric data to identify potential inaccuracies, inconsistencies, or challenges in matching processes. Seven biometric experts from Italy, Greece, Spain, Hungary, and Frontex convened at eu-LISA's premises in Strasbourg to contribute to the creation of a ground truth database—a key component for accurately measuring the performance of the sBMS algorithm.



From the initial prior consultation with the EDPS to the development and implementation of measures, eu-LISA teams worked diligently with the DPO to:

- Mitigate bias in AI algorithms.
- Avoid discrimination.
- Ensure fair treatment of individuals, particularly based on an estimation of approximately 700 million third-country nationals (TCNs).

The EDPS was prior consulted on 28 July 2021 including the DPIAs of the EES, the sBMS and the related measures to mitigate the high risks (e.g., the accuracy measurement exercise). The **EDPS issued his first opinion on 4 November 2021**, providing recommendations for implementation by 4 February 2022 (three months after receiving the Opinion). A **second EDPS Opinion on 4 August 2022** granted approval for eu-LISA to proceed with the accuracy measurement.

eu-LISA continued working on the EDPS recommendations, submitting an updated package on 18 October 2023, which led to a EDPS follow-up opinion issued on 24 July 2024. This opinion required eu-LISA to submit a detailed report on the results of the accuracy measurement exercise, along with additional documentation to clarify aspects such as the distinction between matching scores and matching thresholds.

The DPO's leadership was crucial from the outset, providing a methodology and template for conducting DPIAs as early as 2019. Building on this foundation, the DPO guided the completion of the DPIAs for the EES, the sBMS, and the accuracy measurement exercise, ensuring alignment with EDPS recommendations. This work not only reinforced ethical compliance and safeguarded individual rights but also set a benchmark for data protection in biometric systems across the EU.

3.7. Change Management Process

The DPO of eu-LISA has been involved in the approval process of the Change Management procedure at the request of the Management Board. While this measure was intended to enhance oversight, the significant volume of changes has presented resource challenges, reducing the overall efficiency of the approach.

The Change Management procedure plays a critical role in ensuring that data protection risks associated with proposed changes are identified and addressed at an early stage. To improve its efficiency and effectiveness, the DPO strongly recommended revising the procedure to incorporate tools and checks to determine, for instance, whether a change is substantial enough to require a Data Protection Impact Assessment (DPIA) or a review of an existing DPIA.

To support these objectives, the DPO collaborated with the owner of the Change Management procedure. During 2022, the DPO designed and proposed a change threshold assessment, which underwent further refinement during the first months of 2023.

From April 2024 onwards, however, the DPO's involvement in the Change Management process was discontinued. This development raises concerns regarding the EDPS recommendation from the 2019 Eurodac audit (Recommendation 7), which stated:

“eu-LISA shall update and approve the Change Management Process to ensure that the Data Protection Officer is involved in the approval process when the change has an implication for the processing of personal data.”

This recommendation was successfully implemented and closed by Q2 2021, with the DPO's involvement documented in the SM9 system.

To ensure alignment with data protection obligations and assess the impact of the updated process, the DPO has requested a comprehensive report covering the following areas:

- A detailed description of the updated process, including how the Change Management procedure involves the DPO, criteria for DPO involvement, and documented management decisions (with approval dates and responsible parties).
- An evaluation of the EDPS recommendation regarding the DPO's involvement in the Change Management process.
- An analysis of risks to data subjects and the resulting impact on the Agency's compliance with its obligation to ensure a high level of data protection.
- The number of changes where the DPO function was not involved since the implementation of the update, with an estimation of how many should have required DPO assessment.
- The number of changes where the DPO function was involved since the update's implementation.

This evaluation aims to provide a thorough understanding of the updated Change Management process's implications and ensure alignment with the Agency's data protection obligations.

3.8. EDPS Supervision and Collaboration

3.8.1. Follow-up on the EDPS inspections and recommendations

Ensuring a high level of data protection is a core objective of the Agency. External audits on data protection compliance are key to achieving this goal, enhancing the Agency's reputation as a trustworthy IT partner. Integrating audit recommendations into eu-LISA's continuous improvement plan for the operational management of EU Large-Scale IT Systems significantly strengthens the effectiveness of this process.

3.8.1.1. *'Back-to-green' approach to the implementation of EDPS audit recommendations*

Since its introduction in 2019, the 'back-to-green' plan, led by the DPO and supported by her dedicated team, has been a cornerstone of DPO's efforts to ensure and monitor compliance with the data protection regulation, EUDPR. The team's ongoing commitment to monitoring and providing updates has been instrumental in sustaining progress. This proactive and strategic initiative, developed in agreement with the Executive Director, included quarterly actions such as internal follow-ups on the implementation status of EDPS audit recommendations and proactive updates to the EDPS. The objective was to complete all recommendations within the deadlines set by the EDPS and to address any exceptional cases promptly by providing justifications and revised timelines.

These efforts resulted in enhanced compliance across key areas, as evidenced by positive EDPS feedback and the successful closure of audit recommendations.

The 'back-to-green' goal was successfully achieved in 2023, marking a significant milestone in the Agency's compliance journey. However, sustaining this status proved challenging in 2024 due to limitations associated with the current organisational structure and resource distribution. Despite the DPO's repeated and proactive efforts to coordinate and facilitate the implementation of recommendations, challenges arose, including missed EDPS deadlines, incomplete or inaccurate information submissions, and delays in internal processes.

These challenges underscored the need for enhanced internal coordination, resource allocation, and streamlined processes to support the continuity of the 'back-to-green' initiative. The DPO, supported by her team, has consistently demonstrated a commitment to strengthening the Agency's compliance framework and has laid a strong foundation for measures that address these constraints, enabling the Agency to pursue renewed alignment with EDPS expectations in 2025.

3.8.1.2. 2022 audit on Eurodac, SISII and VIS

In October 2022, the EDPS conducted an inspection on Eurodac, SISII, and VIS. The final EDPS report, received in September 2023, contained 37 recommendations, all of which eu-LISA incorporated into an action plan. The DPO actively monitored the implementation progress and organised internal follow-ups with the responsible staff to ensure compliance.

Throughout 2024, on behalf of eu-LISA, the DPO liaised with the EDPS to provide proactive updates on the status of the recommendations. Notably, regarding Recommendation #33, quarterly reports on the status of the solution implementation were prepared and presented to the Advisory Group (AG) of Eurodac. These reports were also made simultaneously available to the EDPS by the DPO.



As a result of these efforts, the EDPS confirmed the closure of 21 out of the 37 recommendations in a follow-up letter issued in mid-October 2024. This achievement was made possible by the comprehensive documentation provided and the clarifications offered during the meeting on 19 September 2024 between the EDPS audit team and eu-LISA's responsible staff. The DPO played a main role in facilitating this activity.

The EDPS is scheduled to conduct an additional follow-up in 2025 to review the implementation of the remaining recommendations.

3.8.1.3. 2023 audit on SIS

In December 2023, EDPS conducted an inspection on the Schengen Information System (SIS) in accordance with relevant international auditing standards. The Draft EDPS Report was received on 6 May 2024. In line with Article 19(1)(hh) of eu-LISA Regulation, the Management Board of eu-LISA was required to adopt formal comments on the audit report before its final version was submitted to the European Parliament, the Council, the Commission, the Agency, and the national supervisory authorities.

To gather comprehensive feedback, an internal review of the draft report was conducted at staff level in May 2024, followed by an informal consultation with the SIS Advisory Group in June 2024. Subsequently, a consultation with the Management Board for comments took place during the same month. Upon completion of this process, the consolidated final comments were presented to the Management Board for formal adoption in July 2024. The Board formally adopted the comments on 31 July 2024, and these were submitted to the EDPS on 2 August 2024, fully meeting the EDPS's deadline of 5 August 2024. The entire process was led and coordinated by the DPO of eu-LISA.

The final EDPS report, received in September 2024, contained 22 recommendations with implementation deadlines ranging from 3 to 12 months following the adoption of the report on 19 September 2024. eu-LISA incorporated all the recommendations into an action plan. In a letter dated 20 September 2024, the EDPS requested an implementation plan outlining the measures and recommendations from the report to be submitted within three months of receiving the letter.



Despite repeated and proactive efforts by the DPO to coordinate the submission of the implementation plan, organisational constraints prevented its submission within the specified timeframe. These challenges underscored the need for improved internal coordination and execution processes. Nevertheless, the DPO continued to monitor the progress of implementation through quarterly follow-ups with relevant staff—a practice introduced in 2020 as an assurance tool for the Agency—laying a strong foundation for renewed progress in 2025.

Recognising the value of this practice, the DPO took proactive steps to ensure that quarterly meetings for the first quarter of 2025 were scheduled in advance, maintaining continuity and further strengthening the Agency's compliance framework.

In 2025, the EDPS is expected to conduct an additional follow-up activity to review the implementation of the recommendations, providing an opportunity for the Agency to demonstrate progress and alignment with compliance objectives.

3.8.2. 2024 Audit on VIS

Following an announcement letter dated 8 August 2024, the European Data Protection Supervisor (EDPS) conducted a new inspection of the Visa Information System (VIS) on 3 and 4 December 2024.

The purpose of the inspection was to verify on-the-spot compliance with the EUDPR and Regulation (EU) 767/2008. The audit focused on the following topics:



- Compliance with Article 33 of the EUDPR on security of processing, Article 11 of Regulation (EU) 2018/1726 as well as Articles 26, 29(2) and 32(3) of the Regulation (EU) 767/2008 on operational management and security measures to be adopted by eu-LISA.
- Compliance with Article 45(2) of the Regulation (EU) 767/2008 and related modifying Regulations on the measures necessary for the technical implementation of the central VIS.
- Compliance with Article 34 of the Regulation (EU) 767/2008 regarding the keeping of records of data processing operations in the central VIS (business logs) and the retention of these records.
- Compliance with Article 23 of Regulation (EU) 767/2008 regarding the retention period for data storage.



The DPO led the coordination of the inspection, serving as the primary liaison between the EDPS and eu-LISA during the second half of 2024. This involved organising meetings to prepare for the audit, both internally and externally, with EDPS auditors. The DPO also managed the collection of all documentation requested by the EDPS - before, during, and after the inspection - and facilitated the fulfilment of additional requests received prior to the on-site audit.

3.8.3. EDPS Survey on Data Protection Impact Assessments

In 2020, the EDPS conducted its first survey on DPIAs to gather insights into the practical approaches adopted by EUIs, the number of DPIAs conducted, and lessons learned up to that point. The DPO of eu-LISA contributed valuable insights and ensured the timely submission of eu-LISA's responses to the EDPS questionnaire.

Four years later, recognising the evolving landscape of processing activities and technologies, the EDPS launched a follow-up Survey on Data Protection Impact Assessments (DPIAs), based on Article 32 of the EUDPR. The survey, launched on 26 February 2024, specifically requested all Data Protection Officers (DPOs) of EU institutions, bodies, offices, and agencies (EUIs) to provide their inputs by 22 March 2024.

The request included a targeted questionnaire and required the submission of the last two DPIAs for which the controller decided not to consult the EDPS under Article 40(1). These submissions were to include references to the advice provided by the respective DPOs. The DPO of eu-LISA actively contributed to this initiative by submitting relevant and timely inputs, aligning with the EDPS's goal of identifying overarching patterns and notable exceptions in DPIA practices across EUIs.

3.8.4. Participation in the EDPS 20th Anniversary Celebrations

In 2024, the European Data Protection Supervisor (EDPS) celebrated its 20th anniversary, marking two decades of advancing privacy and data protection across the EU. The anniversary was commemorated throughout the year with a series of impactful events and initiatives aimed at promoting innovation and strengthening individuals' rights to privacy and data protection.

As part of the celebrations, the EDPS launched 20 initiatives in 2024, including concept papers on privacy and Artificial Intelligence (AI), a Data Protection Officer Certification Course for EU Institutions, Bodies, Offices, and Agencies (EUIs), and a pilot campaign to enhance privacy on EU institutions' websites. These efforts underscored the EDPS's commitment to fostering a more transparent and innovative approach to data protection.

On 20 June 2024, the DPO of eu-LISA honoured this milestone by attending the European Data Protection Summit in Brussels. The summit, themed "Rethinking Data in a Democratic Society," brought together privacy experts, technology specialists, policymakers, and other influential figures to reflect on the evolving role of data protection in democratic societies. The discussions recognised that, while data protection has made significant strides in the past two decades, challenges continue to grow, and its impact on democracies remains an area for further improvement.



The event emphasised the need for the data protection community to adapt to emerging technologies and societal changes, preparing for the next decade of developments. The EDPS reaffirmed its commitment to advancing the discipline, with the summit serving as a platform for exploring new approaches to bolster individuals' rights and strengthen the relationship between data protection and democracy.

The DPO of eu-LISA's participation in this significant event highlights the Agency's alignment with the EDPS' vision and its active role in contributing to robust data protection frameworks that safeguard democratic principles.

3.8.5. Supervision Coordination Groups for Eurodac and VIS and Coordinated Supervision Committee for SIS

In compliance with Article 5(1)(f) of the eu-LISA DPO Implementing Rules, the DPO, by invitation, represents eu-LISA at meetings of the Supervision Coordination Group (SCG) for Eurodac and VIS, as well as the Coordinated Supervision Committee (CSC) for SIS, within the framework of the European Data Protection Board (EDPB).

These groups and the committee, composed of representatives from National Data Protection Authorities and the EDPS, requested updates on the operational aspects of the three EU Large-Scale IT Systems. The updates addressed matters such as system performance, incidents, and data quality.

During the meetings held in July and December 2024, members were provided with the latest developments and issues affecting the processing of personal data, either through oral presentations or written updates. Due to scheduling constraints, subject-matter experts in VIS, SIS, and Eurodac offered valuable support to the DPO by providing updates to the respective supervisory groups on behalf of eu-LISA.

Collaboration across various areas of eu-LISA proved essential in delivering accurate and comprehensive information. The DPO extends gratitude for the exceptional cooperation and support from colleagues across the Agency.

3.9. JHAA DPO Network Meetings

As part of the 2024 eu-LISA Presidency of the Justice and Home Affairs Agencies Network (JHAAN), eu-LISA hosted the meetings of the JHAAN Working Group on Data Protection.



The first meeting, held on 18-19 April at eu-LISA Headquarters in Tallinn, Estonia, was conducted primarily in physical format and chaired by eu-LISA's DPO. Guest speakers from the Security Unit, the European Data Protection Supervisor (EDPS) Office,

and DG JUST-International Affairs and Data Flows contributed to discussions on:

- International transfers
- Artificial Intelligence and Data Protection
- Supporting IT Tools for the DPO function
- Cooperation between EDPS and JHAA DPOs
- Cybersecurity
- SaaS Questionnaire

As outcome of the meeting, members of the Working Group issued a Joint Opinion for the attention of the Heads of JHA Agencies and the EDPS, addressing the role of DPOs in Artificial Intelligence (AI). The Joint Opinion, which underscores the importance of maintaining the DPO as the single contact point with the EDPS for AI matters, was intended to be included in the JHAAN annual report and was discussed at the DPOs network meeting on 18 June in Brussels.

The second meeting, held online on 15 November, included participation from JHAA DPOs and the DPO of the European Public Prosecutor's Office (EPPO). The session, also chaired by eu-LISA's DPO, began with opening remarks from eu-LISA's Executive Director, who emphasised the Agency's strong commitment to data protection. Participant DPOs, and guest speakers from Europol's DPO Office and the EDPS Office addressed key topics, including:

- Artificial Intelligence and Data Protection
- Cooperation between the EDPS and JHAA DPOs
- Cybersecurity and cyber-attacks
- Data retention limits for administrative personal data

In line with the first meeting, participants provided updates on their agencies' data protection efforts, sharing insights into accomplishments, recent developments, and ongoing challenges.

3.10. EDPS - EUI DPO Network Meetings

In 2024, the DPO of eu-LISA actively participated in the 54th and 55th EDPS-EUI DPOs Network Meetings, which served as platform for sharing experiences and fostering compliance with EU data protection law.

The 54th EDPS-EUI DPOs Network Meeting was held on 18-19 June in Brussels, hosted by the European Economic and Social Committee and the European Committee of the Regions. The event featured interventions from EDPS speakers, including a welcome speech by Supervisor Wojciech Wiewiórowski, and covered key topics such as:

- The EDPS decision on MS365.
- Initiatives on website compliance scanning and a data breach notification awareness campaign.
- Updates on the Artificial Intelligence Act.
- Modalities of cooperation between the EDPS and the DPO network.
- Workshops on handling the right of access and on AI in data protection impact assessments.
- Recent case law on privacy and data protection.

Discussions among the EUI DPOs included the introduction of recently appointed DPOs, updates on the activities of existing working groups, and the creation of two new working groups focusing on the Position of the DPO and Artificial Intelligence. The new EDPS guidelines on generative AI were also presented, with specific attention given to the liaison officer/focal point function.

The 55th EDPS-EUI DPOs Network Meeting took place on 26-27 November in Luxembourg, hosted by the Court of Justice of the European Union (CJEU). The meeting began with an opening speech from the CJEU Registrar and included presentations by the First Advocate General and the CJEU's Data Protection Officer. The agenda covered topics such as:

- Storage limitations.
- DPIA survey results.
- Supervising AI through a data protection lens: the EDPS experience.
- Personal data breaches.
- Website awareness compliance campaign.
- Updates from the Technology & Privacy Unit.
- Recent case law on privacy and data protection.



Additionally, the CJEU presented on data protection in the context of judicial activities and a specific search engine, with further discussions on Artificial Intelligence held during the meeting.

These meetings provided highly valuable opportunities for DPOs to exchange views, share experiences, and address pressing data protection challenges. By building on each other's insights, the network fosters a collective approach to ensuring compliance with EU data protection law and advancing best practices across institutions.

3.11. Advancing Professional Expertise

The DPO of eu-LISA is committed to staying at the forefront of data protection and privacy developments.

The DPO ensures her professional expertise remains up to date by renewing her Data Protection Professional certification every two years and her ISO27001 Lead Implementer certification every three years. To further attest to her expertise and enhance her knowledge, in 2024, the DPO completed professional training on *Artificial Intelligence Governance* (IAPP) and obtained certification in *Artificial Intelligence and Data Protection* from the Spanish Professional Association of Privacy (APEP). Additionally, the DPO collaborated with external bodies, offering insights and contributing to discussions from a data protection perspective.

Continuous learning was further supported through regular review of EDPB and EDPS guidelines, academic publications, and landmark cases. Internally, the DPO, supported by her team, shared this knowledge through the Data Protection Officer intranet, awareness sessions, and weekly newsletters, ensuring that eu-LISA's operations uphold the highest data protection standards.

3.12. Professional Engagement in Data Protection Community Activities

In 2024, the DPO actively participated in key events, engaging with peers and experts to address emerging challenges and explore innovative solutions.

3.12.1. CPDP - Data Protection Day - 25 January 2024

Data Protection Day was celebrated globally in January 2024. On this occasion, the DPO of eu-LISA attended the CPDP - Data Protection Day event on 25 January 2024.

Organised by the Council of Europe (CoE), CPDP, and the European Data Protection Supervisor (EDPS), the event featured discussions and keynote speeches addressing critical aspects of safeguarding individuals' rights to privacy and data protection.



The conference focused on the latest developments and challenges in the data protection landscape, including:

- Global data flows
- Digital governance
- Regulating Artificial Intelligence (AI)
- Harmonising GDPR procedures



Additionally, the Permanent Representation of Poland and the Ministry of Digital Affairs, in partnership with the CoE, CPDP, and EDPS, hosted a complementary GDPR-focused event. The programme began with a keynote speech by Mr. Dariusz Standerski, Secretary of State in the Ministry of Digital Affairs, followed by a short debate on the future of privacy in electronic communications.

Participation in this outreach activity provided the DPO of eu-LISA with a valuable opportunity to engage with thought leaders, foster collaborations, and stay informed about the evolving dynamics of data protection and security. This engagement reflects eu-LISA's commitment to contributing to the ongoing dialogue on the future of data protection and its role in shaping secure digital ecosystems.

3.12.2. Internet Privacy Engineering Network Event

The DPO of eu-LISA attended the 2024 Internet Privacy Engineering Network (IPEN) event on 'Human Oversight of Automated Decision-Making' on 3 September. The event was hosted by the European Data Protection Supervisor (EDPS) and Karlstad University.



IPEN events bring together privacy experts and data protection engineers from public authorities, industry, academia, and civil society to address challenges and advancements in embedding data protection and privacy requirements into all phases of the engineering and development process.

The programme began with a keynote presentation titled "What We Expect Human Oversight to Be and What It Really Is." Subsequent expert panels explored critical topics, including "Human oversight in the GDPR and the AI Act", "Main challenges to effective human oversight" and "Creating conditions for more effective human oversight".

The event provided a valuable platform for exchanging expertise and best practices. The DPO of eu-LISA engaged in meaningful discussions with data protection engineers and other participants, contributing to a fruitful dialogue on the evolving challenges of human oversight in automated decision-making systems.

3.12.3. Annual Privacy Forum

The DPO of eu-LISA participated in the Annual Privacy Forum (APF), held on 4-5 September 2024 in Karlstad, Sweden. The event was jointly organised by ENISA, DG Connect, and Karlstad University, with the support of IMY (the Swedish Authority for Privacy Protection).

The growing value of personal data in the online world has been driven by the increasing integration of electronic products, services, and processes into daily life. However, limitations in the transparency, functionality, and interconnectivity of online and communication services pose significant risks, including the uncontrolled processing of personal data, lack of accountability, and exposure to diverse privacy threats.



The EU legal framework on personal data protection plays a crucial role in addressing these challenges by ensuring adequate control over data processing and providing a high level of protection. Yet, even the most robust legislative measures struggle to keep pace with the rapid evolution of technology and innovative business models, which continue to reshape how personal data is processed and privacy is safeguarded across the EU and beyond. Consequently, examining the origins of these threats and the stakes involved is of key importance.

Against this context, the APF programme addressed a wide range of topics, including consent management, emerging technologies and risks, threat modelling, privacy engineering, deploying GDPR, privacy technologies in practice, capacity building, data subject rights, data protection by design, and challenges in protecting personal data in the artificial intelligence era.

The forum provided a valuable platform for panellists and participants to exchange insights and perspectives. The participation of eu-LISA's DPO contributed significantly to the discussions, enriching the dialogue with practical expertise and forward-looking perspectives on privacy and data protection challenges.

3.13. Annual Survey

The annual survey, included in the eu-LISA Programming Document 2024, has faced delays in implementation over the years due to resource constraints and the prioritisation of other critical Agency operations. As a key activity for monitoring data protection compliance, the survey remains an essential tool in the DPO's efforts to ensure alignment with regulatory standards. While these priorities have addressed pressing needs, addressing the survey's implementation is essential to further strengthen the Agency's compliance framework and support its long-term objectives.

4. DPO Function

Article 44(2) of the EUDPR and Article 6 of the eu-LISA DPO Implementing Rules highlight the importance of providing the DPO with the necessary resources to effectively carry out her tasks and responsibilities.

In 2024, the DPO maximised the use of available resources to provide data protection guidance and support to the Agency. These efforts were strategically focused on high-priority areas, including the development and oversight of new and existing EU Large-Scale IT Systems, monitoring the implementation of EDPS audit recommendations, and coordinating new EDPS audits.

While resource limitations required careful prioritisation, the DPO successfully concentrated efforts on these critical areas, ensuring compliance with data protection standards and supporting the Agency's operational goals.

Expanding the DPO function would enable the continuation and enhancement of key activities, directly benefiting the Agency's objective of maintaining a high level of data protection. As the Agency's tasks and responsibilities grow, evolving the DPO function will be essential to effectively address current and future challenges.

