PUBLIC

To: the eu-LISA Management Board

From: Encarna Gimenez, Data Protection Officer (DPO)

Subject: DPO Annual Work Report - 2023

PUBLIC

DPO ANNUAL WORK REPORT 2023

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

www.eulisa.europa.eu

eu-LISA

Document Control Information

Settings	Value
Document Title:	DPO Annual Work Report – 2023
Document Author:	Data Protection Officer
Revision Status:	Final
Sensitivity:	Public
Issue Date:	06/03/2024

Summary of Changes:

Revision	Date	Created by	Short Description of Changes
[1]	19/12/2023	DP Expert	Initial version of the document created
[2]	25/01/2024	DP Expert	Updated based on DPO comments
[3]	06/03/2024	DPO	Review and creation of final version

Contents

Introduction

Article 2 of Regulation (EU) 2018/1726[1] ('eu-LISA Regulation') sets the objectives of the Agency. Explicitly, the Agency shall ensure a high level of data protection, in accordance with Union data protection law, including specific provisions for each EU Large-Scale IT System.

eu-LISA Data Protection Officer (DPO) is required to advise controllers and processors on fulfilling their obligations. Application of the provisions of Regulation (EU) 2018/1725[2] ('Regulation') is firstly ensured by the DPO of eu-LISA and, ultimately, by the supervisory role of the European Data Protection Supervisor (EDPS).

During 2023, eu-LISA DPO has dedicated efforts, on one hand, to ensure the smooth coordination of the EDPS inspection carried out in December on the Schengen Information System[3] (SIS[4]) and, on the other hand, to monitor the outstanding recommendations of previous EDPS audits and support with their implementation. For the latter, thanks to the committed and supportive work of the DPO of eu-LISA, management and staff in charge of implementing the EDPS audit recommendations became progressively engaged and positively collaborated. As a result, the Annual Report of 2023 features notable achievements of significant importance, including the first-ever full implementation of all recommendations coming from an EDPS audit, i.e., 2018 EDPS Audit on SISII, VIS and Eurodac, and the 'back-to-green' status of the EDPS audit recommendations. At the end of 2023, all recommendations were either on-track or expected to be completed within the deadline provided by EDPS.

Upon reception of the draft report of the EDPS inspection carried out in October 2022 on Eurodac[5], Visa Information System[6] (VIS) and Schengen Information System[7] (SIS II), the DPO led a comprehensive exercise to facilitate and support the formal adoption of comments by the Management Board of eu-LISA (MB) on this draft audit report in accordance with Article 19(1)(hh) of eu-LISA Regulation,

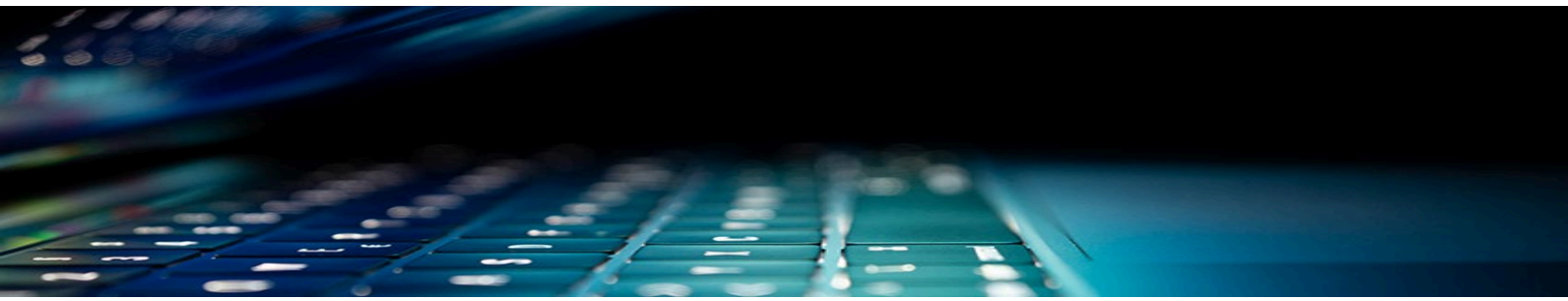
---

[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] **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.
[4] On 7 March 2023, SIS Recast entered into operation and the Schengen Information System is since then called SIS.
[5] **Regulation (EU) No 603/2013** of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.
[6] **Regulation (EC) No 767/2008** of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation).
[7] **Regulation (EC) No 1987/2006** of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II).

Additionally, the DPO of eu-LISA completed a revision of the methodology for carrying out data protection impact assessment (DPIAs) with the view to facilitate and support eu-LISA responsible personnel. To that extent, the DPO organised dedicated training and practical workshops on this specific topic. Moreover, general and specific data protection awareness sessions were delivered throughout the year, such as the ones targeting support agents.

Furthermore, the DPO also supported the Agency in its biggest data protection challenges, in particular, those deriving from the use of biometric matching technologies and measures to mitigate identified risks. Likewise, the entry into operation of the SIS in March 2023 was supported.

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.



1. Scope

Under Article 7(4) of the eu-LISA DPO Implementing Rules[8], the DPO shall submit to the Agency's Management Board an annual report on her activities and on the state of play as regards the data protection activities and compliance of the Agency.

This report presents the status of the data protection activities within the Agency and compiles the work performed by the DPO during the year 2023.

2. DPO Activities and Actions

The following sections detail by topic the state of play as regards the data protection activities and compliance of the Agency with the Regulation.

2.1. Awareness

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

On 27 January 2023, the DPO of eu-LISA provided to all staff an awareness training session in order to celebrate the European Data Protection Day. This session included the highlights and key concepts related to personal data processing with the aim to learn more about privacy notices, DPIAs, data breaches, controller-processor relationship and many other topics. The attendees were actively involved in different discussions and provided positive feedback at the end of the session. Around 100 participants joined the session.

On the same day, all eu-LISA personnel had the chance to take part in a Data Protection Quiz 2023. The quiz aimed at giving the participants the chance to self-assess their knowledge on the core principles of Regulation (EU) 2018/1725 and their practical implications while having fun and competing for a final prize. Fifty-three colleagues participated in this activity. The winner of the Data Protection Quiz 2023 answered all questions correctly in the first place, and was awarded with a special prize.

Additionally, in March the DPO organised four training sessions on "How to carry out a DPIA" with the aim to understand the key concepts and carry out DPIAs. what a DPIA is, when it is needed, which are the roles and responsibilities of the actors involved, which content a DPIA shall include, which actions should be taken based on conclusions. The event was open to all eu-LISA staff and up to 89 participants joined.

[8] 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.

Moreover, the methodology for carrying out data protection impact assessment (DPIAs) was also revised with the view to facilitate and support eu-LISA responsible staff. Based on this revision, two more practical DPIA workshops (each one split into two consecutive 2-hour training) took place in May. Up to 47 participants were involved step-by-step in the performance of a DPIA on a real case scenario. The systematic description of the data processing, the assessment of necessity and proportionality, the assessment of risks and the measures to mitigate such risks were some of the topics addressed during the training. The participants were continuously involved in an active discussion of the results of the ongoing DPIA.

Four additional data protection awareness sessions for support agents were delivered in July by the team of the DPO with the aim of providing an overview of the concepts of personal data and processing operation, the roles of controller and processor, and in particular how to deal with data breaches. Up to 15 support agents attended the sessions and it is available on-demand for all of those agents who were not able to attend in person. This training not only aimed to raise awareness on data protection, in particular on data breaches, but also closed one of the recommendations from the audit that the EDPS carried out in 2022.

Likewise, since March all eu-LISA staff can attend to the e-learning module on Data Protection available on iLearn. This online training – which specifically targets eu-LISA's newcomers - provides the fundamental knowledge on main data protection key concepts such as the main principles of data protection, roles in data protection activities, data breaches, international data transfers and so on. This e-learning module on data protection is part of the Onboarding Program of eu-LISA which is mandatory for all staff members and recommended for other personnel working for eu-LISA.

Furthermore, the DPO has provided one-on-one coaching sessions to specific staff members seeking for advice and guidance to comply with their obligations as data controllers and/or processors under the Regulation.

Likewise, in order to ease and optimize support for the data controllers and processors, the DPO Intranet was updated on a regular basis including templates, and step-by-step instructions.

In addition, other efforts to raise awareness across the Agency went to the internal weekly eu-LISA Newsletter, which is sent over to all eu-LISA staff members. This weekly newsletter includes a dedicated section on data protection that the DPO prepares. The purpose of this section is to update staff on the latest guidelines, available trainings, and recent developments in the field. During 2023, twenty-three articles on data protection were published in the weekly eu-LISA Newsletters, including a dedicated "special newsletter" in December.

2.2. Records of Processing Activities as Controller

In compliance with Article 31(1) of the Regulation, eu-LISA shall maintain records of processing activities under its responsibility. According to Article 4(3) of the eu-LISA DPO Implementing Rules, the DPO shall keep a central register of records of their processing activities as a controller.

Therefore, when delegated data controllers in eu-LISA want to start a new processing activity in eu-LISA, they document this processing activity as a new record and notify this new record to the DPO so the central register can be updated accordingly. In addition, when an existing processing activity changes in some way, the data controller needs to update the documentation associated to that record and notify the change to the DPO.

Step-by-step instructions and templates on how to document records of processing activities have been prepared by the DPO to facilitate the tasks and obligations of the data controller.

By the end of December 2023, the eu-LISA register of data processing activities included 134 records of on-going data processing activities. Ten of them were registered during 2022. This register is public, constantly updated and available from the eu-LISA website.

2.3. Records of Processing Activities as Processor

Under Article 31(2) of the Regulation, 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 is centrally managed by the DPO, is public, constantly updated and available from the eu-LISA website.

By the end of December 2023, the eu-LISA register of data processing activities – as processor included two records of on-going data processing activities. During 2023, the record for the 'Operational management of SIS II information system' was withdrawn and was replaced in March by a new record on SIS Recast.

2.4. Personal Data Breach Register

Following obligations stemming from article 34(6) of the Regulation (EU) 2018/1725, "*data controller shall document any personal data breaches*". According to Article 4(3) of the eu-LISA DPO Implementing Rules, the DPO will keep a central register of records of data breaches.

During the reference period for this report, and after investigation, eight data breaches were reported and documented by the data controller. The central register of data breaches is updated accordingly by DPO. The DPO also supported data controllers with the assessment in accordance with the EDPS guidelines on data breaches. Regard was also given to conditions set out in Articles 34 and 35 of the Regulation on notification to EDPS and communication to affected data subjects.

Reports of the data breaches were submitted to Executive Director and to EDPS when applicable.

2.5. Data Protection Impact Assessments (DPIAs)

Following its establishing regulation, eu-LISA is mandated to ensure a high level of data protection. Moreover, eu-LISA shall follow the principles of privacy by design and by default during the entire lifecycle of the development of the new large-scale IT systems.

DPIAs should not only be seen as an obligation for data controllers where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, but also a decision made by eu-LISA to achieve the above-mentioned objectives. The Agency may well decide to carry out DPIAs as a tool to generate knowledge and data protection culture, analyse or audit data processing activities, improve the global process management or control the level of risk accepted in each data processing activity in a systematic, methodical and documented way.

DPIAs shall be considered a 'live' document subject to regular review or re-assessment should the nature, scope, context or purpose of the processing change for any reason. Therefore, DPIAs will become a continuous practice in the activities of eu-LISA and therefore, it shall be adequately embedded in its processes.

In line with the EDPS guidance[9] and WP29/EDPB guidelines on DPIAs[10], the DPO has been supporting eu-LISA staff in Operation Department and its contractors with carrying out DPIAs, providing relevant advice and guidance.

At the end of July 2021, eu-LISA launched a Prior Consultation with EDPS concerning the high risks stemming from the use of biometric matching technologies in the Entry/Exit System (EES)[11], i.e., the shared Biometric Matching System (sBMS)[12], and the related mitigation measures. The package included DPIAs carried out by eu-LISA on EES, sBMS and the Accuracy Measures procedure. The EDPS Opinion - including his recommendations - was received on 4 November 2021. Since then, eu-LISA started the implementation of the EDPS recommendations.

Within the three months foreseen in the EDPS Opinion, eu-LISA provided the package with evidences of the implementation of the EDPS recommendations. eu-LISA DPO facilitated a staff-level meeting between eu-LISA and EDPS, and support the exchange of further views and clarifications between both organisations during June 2022.

On 4 August 2022, the EDPS issued a second Opinion deeming the majority of his recommendations as implemented, and providing further comments. During 2023, eu-LISA has continued working on implementing EDPS recommendations and comments. The EDPS was updated on the progress in October 2023.

The DPO has been regularly supporting EES and sBMS teams with their tasks throughout the different stages of the process and continue following up on the progress of this case.

The main DPIA of the Schengen Information System[13] (SIS Recast) and two of its appendixes covering specific one-time data processing activities were finalised in 2023. Moreover, other updates of the SIS DPIA were kicked-off during 2023 such as SIS Interoperability with ETIAS through the ESP and another one-time specific activities covering future evolutions of the system.

Furthermore, the DPO team has been regularly contributing with relevant comments to the DPIA of the Visa Information System (VIS)[14], and to other DPIAs concerning interoperability components.

---

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

[10] 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**

[11] **Regulation (EU) 2017/2226** of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011.

[12] **Regulation (EU) 2019/817** of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA and **Regulation (EU) 2019/818** of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816.

[13] **Regulation (EU) 2018/1860** on the use of the Schengen Information System for the return of illegally staying third-country nationals, **Regulation (EU) 2018/1861** on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks 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.

[14] **Regulation (EC) No 767/2008** of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation).

Throughout the progress of these DPIAs, support provided by DPO team included, but was not limited to, methodology, templates, relevant comments and guidance.

DPO has been also consulted by product owners with their requests for external support to carry out data protection related tasks. The feedback of DPO emphasised lessons learnt from previous experiences showing the high importance of counting with specialised support. In this respect, external contracted organisations shall offer and demonstrate sufficient guarantees to carry out DPIAs, for instance, by means of certified data protection professionals with appropriate knowledge and extensive expertise in this area.

2.5.1. Continuous improvement

DPIAs play a key role for eu-LISA to carry out their tasks and objectives in relation to the operational management and development of EU Large-Scale IT Systems. Therefore, analysis of experiences in this area and further development of the existing practices will have a real value and impact in the Agency.

With the mindset of continuous improvement, in 2023, the DPO continued undertaking a revision of the methodology in place for carrying out DPIAs. The goal was aiming to facilitate the responsible staff this task as much as possible. The project started in September 2022 and was completed by the end of March 2023.

A revised methodology and improved supporting templates are part of the outcomes. The final part of the project included the delivery of four training sessions about the concepts, requirements and revised methodology. This training was complemented with two additional workshops on how to conduct DPIAs of a practical case.

2.6. International Transfers

International transfers of personal data to countries outside the EU/EEA present some challenges from the data protection perspective.

On 4 June 2021, the European Commission adopted new standard contractual clauses (SCCs) for transfers to non-EU/EEA countries under the Regulation (EU) 2016/679[15] (General data protection regulation, GDPR), implementing the Decision (EU) 2021/914[16]. These SCCs may be used by eu-LISA as ad-hoc contractual clauses (subject to EDPS' authorization) in certain cases.

The DPO launched, in the second half of September 2022 and in December 2022, a new project to support and coach all those data controllers impacted by international transfers in eu-LISA, in particular, with the goal to review contracts in place, carry out transfers impact assessments (TIAs), and conclude new contractual clauses to ensure appropriate safeguards, as needed. For this project data controllers continued, during 2023, counting with the help of specialised external support.

On 10 July 2023[17], the European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework. The adequacy decision concludes that the United States ensures an adequate level of protection – compared to that of the EU - for personal data transferred from the EU to US companies participating in the EU-U.S. Data Privacy Framework.

[15] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A32016R0679
[16] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en
[17] https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

US companies can certify their participation in the EU-U.S. Data Privacy Framework by committing to comply with a detailed set of privacy obligations. This could include, for example, privacy principles such as purpose limitation, data minimisation and data retention, as well as specific obligations concerning data security and the sharing of data with third parties.

With the adoption of the adequacy decision, eu-LISA is able to transfer personal data to participating companies in the United States, without being subject to any further conditions or authorisations.

2.7. Change Management Process

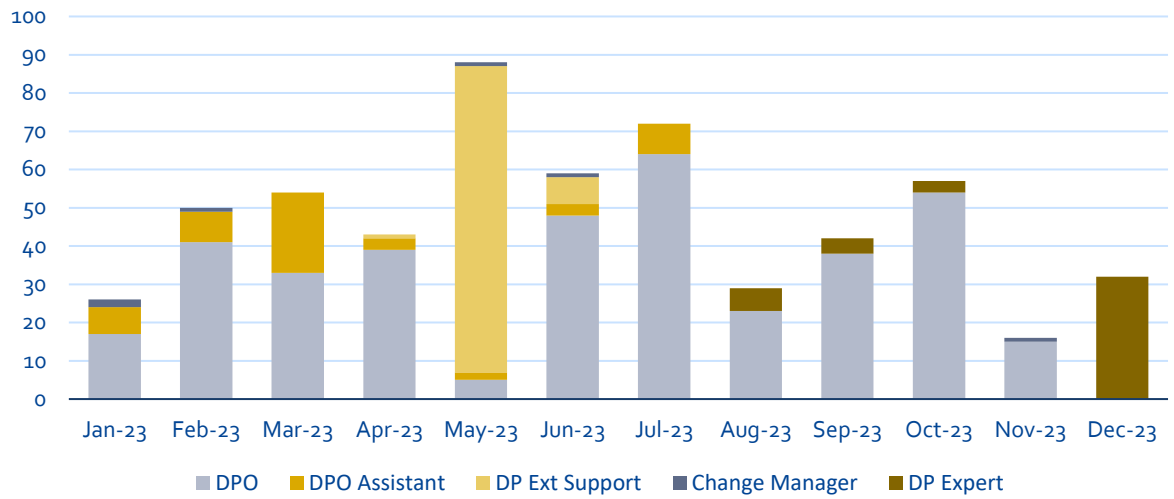
The DPO of eu-LISA is involved in the approval process of the Change Management procedure since the Management Board requested. Although this measure is very positive, the unbearable number of changes results in a disproportionate effort and makes this measure ineffective.

Change Management procedure shall ensure that the data protection risks associated to any proposed changes are detected at an early stage. Therefore, the DPO strongly recommended that the Change Management procedure is revised with the view to introduce a new efficient and effective approach. This new approach should integrate checks and tool to detect, for instance, if the change is substantial enough to trigger the need to carry out or to revisit an existing DPIA.

The owner of the Change Management procedure sought the advice of the DPO to address this task, and both are collaborating at this point. During 2022, a change threshold assessment has been designed and proposed by the DPO of eu-LISA to the owner of the Change Management procedure for his consideration and the discussions continued during the first months of 2023.

Along 2023, the number of changes assigned to DPO role reached 568, including changes not only for the development and operational management of the EU Large-Scale IT Systems (Figure 1) but also those changes related to the regular functioning and administration of eu-LISA. The Data Protection Assistant, who took over the position of Data Protection Expert from 1 August, assumed full responsibility for these tasks after her first three months of service in order to further support the DPO with her tasks and duties.

Figure 1 — 2023 - Number of changes assigned to DPO



2.8. EDPS Supervision and Collaboration

2.8.1. Follow-up on the EDPS inspections and recommendations

Ensuring a high level of data protection is one of the main objectives of the Agency. External audits on data protection compliance contribute to facilitate this goal and add value to the Agency's activities as a trustworthy IT partner. Including audit recommendations as part of the eu-LISA continuous improvement plan for the operational management of the EU Large-Scale IT Systems makes this process much more effective.

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

Soon after taking service in June 2019, an external audit was carried out by EDPS on eu-LISA premises. The DPO participated and, throughout this exercise, the DPO of eu-LISA noted some room for improvement in the Agency's approach to the implementation of EDPS audit recommendations for eu-LISA. Since then, and in order to ensure and monitor compliance with the data protection Regulation, the DPO of eu-LISA, at her own initiative and in agreement with the Executive Director of the Agency, introduced and led a 'back-to-green' plan including a set of actions on a quarterly basis. These actions included internal follow-ups on the status of the implementation of the EDPS audit recommendations with the responsible staff, and proactive updates to the EDPS. The expected outcome of the DPO 'back-to-green' plan was to have all EDPS audit recommendations implemented within the deadlines set by the Supervisor. In exceptional cases, where meeting deadlines would not be feasible, the EDPS would be immediately made aware including details on the reasons for that, expected new deadline and related risk.

The committed and supportive work of the DPO resulted in a progressive engagement and positive collaboration of all areas and staff in charge of implementing the EDPS audit recommendations. 2023 has become the year when the 'back-to-green' goal was finally achieved. By the end of 2023, and for the first time ever, none of the EDPS audit recommendations were overdue. By contrary, the EDPS audit recommendations were either already completed within the deadlines - set by the Supervisor -, or expected to be implemented within those deadlines.

2.8.1.2. 2018 audit on SISII[18] and VIS

In November 2018, the EDPS conducted an audit for the SISII and for the VIS in accordance with relevant international auditing standards. The purpose of the EDPS inspection was to check that the personal data processing activities of eu-LISA, as the Management Authority for both systems, are in accordance with the applicable data protection regulation.

The final EDPS report was received in April 2020 and contained 43 recommendations. eu-LISA transposed all of EDPS recommendations into an action plan. The DPO regularly monitored the progress of its implementation and, to this extent, organised quarterly follow-ups with responsible staff. In 2023, internal follow-up meetings took place in January, April and July. As outcome of the latter, eu-LISA considered all EDPS recommendations of this audit completed. The EDPS report of the 2022 audit on SISII, VIS and Eurodac from 25 October 2023 officially ratified and confirmed their closure. This features an accomplishment that holds significant importance. This achievement represents the fist-ever time when all recommendations of an EDPS audit are implemented, signifying a momentous occasion in the history of the Agency. This milestone serves as a reassurance of the commitment of eu-LISA to compliance with the Regulation and positively strengthens its reputation and credibility as a compliant trustworthy IT partner.

[18] **Regulation (EC) No 1987/2006** of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II).

To acknowledge the dedication and efforts of all those involved, on 26 September 2023, the DPO of eu-LISA invited all relevant internal stakeholders in the operational site of eu-LISA in Strasbourg to share a moment of reward for their significant contribution to closing all recommendations.

On behalf of eu-LISA, the DPO liaised with EDPS on a quarterly basis to proactively update on the status and final closure of the recommendations.

2.8.1.3. 2019 audit on Eurodac

At the beginning of December 2019, EDPS carried out an inspection on Eurodac system. The final report of the EDPS was received in March 2021 and contained 29 recommendations. eu-LISA transposed all of EDPS recommendations into an action plan. The DPO monitored the progress of its implementation and, to this extent, organised quarterly follow-ups with responsible staff. In 2023, internal follow-up meetings took place in February, April and July.

As outcome of the latter, eu-LISA considered 23 out of the 29 EDPS recommendations of this audit completed. The EDPS report of the 2022 audit on SISII, VIS and Eurodac from 25 September 2023 officially ratified and confirmed their closure. The remaining 6 recommendations have been embedded into the 2022 EDPS audit report on SISII, VIS and Eurodac with updated deadlines. For that reason, from now on, monitoring of these recommendations will be integrated within the regular follow-ups of the 2022 EDPS audit.

On behalf of eu-LISA, during 2023, the DPO liaised with EDPS every quarter to proactively update on the progress and status of the recommendations. In particular, regarding Recommendation #27, it is worth to mention that quarterly reports were prepared on the status of the solution implementation. Those reports were presented to Advisory Group (AG) of Eurodac and, in addition, the DPO of eu-LISA made them simultaneously available to EDPS.

2.8.1.4. 2022 audit on Eurodac, SISII and VIS

In October 2022, EDPS carried out an inspection on Eurodac, SISII and VIS in accordance with relevant international auditing standards. The Draft EDPS Report was received on 3 April 2023. In accordance with Article 19(1)(hh) of eu-LISA Regulation, the Management Board of eu-LISA shall adopt formal comments on this audit report before its final version is sent to the European Parliament, the Council, the Commission, the Agency, and the national supervisory authorities.

In order to collect relevant feedback, an internal revision of the draft report at staff level, and an informal consultation with the three Advisory Groups (SIS, VIS, Eurodac) were carried out in May 2023. Then, a consultation to the Management Board for comments followed. After its completion, the consolidated final comments were then sent to the Management Board for formal adoption in June 2023. The final comments to the EDPS draft audit report were formally adopted by the Management Board of eu-LISA during June 2023. Following such adoption, the formally adopted comments were sent to EDPS on 26 June 2023, in full compliance with the deadline provided by the EDPS to complete this exercise (28 June 2023). The full exercise was led and coordinated by the DPO of eu-LISA.

At this stage, the DPO was already liaising with the responsible staff in relation to the implementation of the EDPS recommendations included in the draft report. Specifically, the DPO organised two follow-ups on 7 July and 6 September with the operational teams, namely the Systems Operations Unit to further clarify the implementation of their recommendations.

The final report of the EDPS was received in September 2023 and contained 37 recommendations. Deadlines provided by EDPS for their implementation ranged from Q4 of 2023 up to Q2 of 2026, depending on the recommendation. eu-LISA transposed all of EDPS recommendations into an action plan. The DPO monitors the progress of its implementation and, to this extent, organises quarterly follow-ups with responsible staff. In 2023, the first kick-off meeting and internal follow-up took place in October.

On behalf of eu-LISA, the DPO also liaised with EDPS in October 2023 to proactively update on the progress and status of the recommendations.

2.8.1.5. 2023 audit on SIS

Following announcement letter of 29 September 2023, a new inspection was carried out by EDPS on the Schengen Information System on 5 and 6 December 2023.

It aimed to verify on-the-spot compliance with the Regulation, Regulation (EU) 2018/1861 and Regulation (EU) 2018/1862. The audit topics took into account:

- eu-LISA implementation of Regulations 2018/1861 and 2018/1862 on the responsibilities of eu-LISA in operational management regarding security, confidentiality, logs and data protection matters such as security incidents. In particular, Articles 15, 16, 17, 18 and 45 of the Regulation (EU) 2018/1861 and Articles 15, 16, 17, 42 and 60 of Regulation (EU) 2018/1862. For the purpose of the audit, in addition to the implementation of these articles, ISO 27001[19] and ISO 27002[20] international standards were applied.
- eu-LISA's implementation on Article 40 of Regulation (EU) 2018/1862 (alerts on unknown wanted persons), in particular which information is returned to users when queries include Article 40 data, which are the thresholds to determine the various results and how users feedback is handled and integrated by eu-LISA.
- eu-LISA implementation of Articles 33, 34 and 35 EUDPR regarding security and personal data breaches.

The DPO led the coordination of the inspection. The DPO acted as the liaison between EDPS and eu-LISA during second half of 2023, and will continue supporting this task in 2024. Furthermore, the DPO conducted meetings for the preparation of the audit both internally and externally between eu-LISA and EDPS auditors. Moreover, the DPO collected all documentation requested by EDPS– prior, during and after the inspection -, and facilitated fulfilment of additional requests received before the on-site audit took place.

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

Following the legal requirement of Article 5(1)(f) of the eu-LISA DPO Implementing Rules, by invitation of the Supervision Coordination Group (SCG) of Eurodac, VIS and SIS, the DPO represented eu-LISA at these meetings. In 2023, the SIS coordinated supervision passed to the Coordinated Supervision Committee (CSC) since 7 March, within the framework of the European Data Protection Board (EDPB).

The groups and committee, composed by representatives of the National Data Protection Authorities along with the EDPS, requested updated information regarding the three EU Large-Scale IT Systems on operational matters.

[19] ISO/IEC 27001 is the standard for information security management systems (ISMS).
[20] ISO/IEC 27002 is a supporting standard that guides how the information security controls can be implemented on Information security, cybersecurity and privacy protection.

During the meetings that were held in June and November 2023, members were informed, either orally or in writing, about the latest developments and issues of the systems that may impact the processing of personal data. The members were interested in how the systems were performing, related incidents and the quality of the data. Due to schedule constrains, the VIS Product Owner kindly supported the DPO and provided the update from eu-LISA in one of the meetings to the members of the SCG-VIS.

Colleagues from different areas of eu-LISA are key to provide the most accurate information. Therefore, the DPO would like to remark the excellent collaboration and support from all of them.

2.9. JHAA DPO Network Meetings

In 2023, meetings of the network of DPOs of the Justice and Home Affairs Agencies (JHAA) were chaired by the European Union Agency for Asylum (EUAA).

The DPO of eu-LISA attended the online meetings in April and December. During these meetings, the data protection provisions in the Regulation (EU) 2021/2303 ('EUAA Regulation'), an update on the new mandate of Eurojust, the use of Microsoft Cloud applications and work on Data Protection Impact Assessments were some of the topics addressed. Group discussions also focused on the 'lessons learnt' in view of the proposals for reform of the EU data protection rules and the independence of the DPO.

2.10. EDPS - EUI DPO Network Meetings

On 11 May 2023, the DPO took also part in the 52nd DPO Network meeting that was hosted by the European Union Intellectual Property Office (EUIPO) in Alicante (Spain). The meeting started with a welcome from the Executive Director of EUIPO. Then, an overview of the network of DPOs was presented and the new members were welcome. Discussions and presentations included updates on the impact of the new Eurojust mandate on data protection matters due to Ukraine war, EUIPO Intellectual Property Register in Blockchain, sharing experience on EDPS audits, two workshops on joint controllerships and records for DPO activities, and discussions and voting on the future of the network where the Chapter of the EUIs DPO Network was approved.

The following day, eu-LISA DPO attended 52nd EDPS-DPO Network meeting on 12 May 2023. The meeting started with a keynote speech from the EDPS, Wojciech Wiewiórowski. Discussions and presentations included updates from the from the Supervision & Enforcement Unit and from the Technology & Privacy Unit, recent case law on privacy and data protection, open forum for discussion between EDPS and DPOs and workshops on data transfers and Nextcloud.

eu-LISA DPO attended 53rd DPO Network meeting on 29 November 2023 that was hosted by the European Parliament in Strasbourg (France). The day started with an introduction of the recently appointed DPOs. The day continued with an update and discussion on EU-US Data Privacy Framework, an overview of the ECHR case-law on Data Protection, an update on the Artificial Intelligence Act, DPIAs and Data Protection Coordinator role.

The next day, the DPO of eu-LISA attended 53rd EDPS-DPO Network meeting on 30 November 2023. Discussions and presentations included but were not limited to relevant case law, data protection function and forum for discussion between EDPS and DPOs.

2.11. Annual Survey

Although this activity was part of the eu-LISA Programming Document 2023, the use of available resources has been allocated to provide data protection guidance and support to the Agency in regards to its highest priorities, mainly, the new and existing EU Large-Scale IT Systems. Therefore, this activity was put on hold.

3. DPO Function

Article 44 of the Regulation (EU) 2018/1725 and article 6 of the eu-LISA DPO Implementing Rules address the need to provide the DPO with the necessary resources to carry out his or her tasks and duties.

In light of the above, the DPO of eu-LISA has been supported by an intern, the Intern to the DPO, and a Data Protection Assistant (DPA) until the end of July. The latter began her service as a Data Protection Expert from August 2023 onwards. Additionally, the service counted with a Junior Administrative Support during 2023.

During the second part of 2023, the DPO has dedicated extensive working time to various selection processes, including the two vacant positions as Data Protection Assistant and the Intern to the DPO. The selected candidates are expected to join the team of the DPO from March 2024.

In 2023, the DPO made use of available resources to provide data protection guidance and support to the Agency - to the further extent possible - in regards to its highest priorities, mainly, the new and existing EU Large-Scale IT Systems, monitoring of implementation of EDPS audit recommendation and coordination of new EDPS audits. However, there are important activities that require action and support from the DPO which were put on hold due to the insufficient resources.

Granting an appropriate size of the DPO function directly and substantially benefits the Agency to achieve its objective of ensuring a high level of data protection. Subsequently, the function is expected to grow accordingly, and in line with the Agency’s important current and envisaged tasks and responsibilities.