

Coordinated Supervision Committee Report of Activities 2022-2024



Table of Contents

1. FOREWORD	3
2. THE ROLE OF THE CSC	4
2.1 CSC Mission	5
2.2 Tasks and duties	6
3. OVERVIEW	7
3.1 CSC Rules of Procedure	7
3.2 Organisation and working methods	7
3.3 Work programme	8
4. CROSS-CUTTING ACTIVITIES	10
4.1 Data subject rights	10
4.2 Interpretation and application of EU and national laws	10
4.3 Information exchange, joint audits and coordinated inspections	11
4.4 Preparing for future coordinated supervision	11
4.5 Supporting activities	12
4.5.1 <i>External dialogue</i>	12
4.5.2 <i>Reporting</i>	12
5. SPECIFIC ACTIVITIES	13
5.1 IMI	13
5.1.1 <i>Transparency obligations</i>	13
5.1.2 <i>Users' management</i>	13
5.1.3 <i>Compliance of data protection requirements in IMI</i>	14
5.2 EPPO	14
5.3 Eurojust	14
5.3.1 <i>Joint Investigation Teams</i>	14
5.3.2 <i>Counter Terrorism Register</i>	14
5.3.3 <i>Supervisory independence</i>	14
5.3.4 <i>Secure communication</i>	14
5.4 Europol	14
5.4.1 <i>Transition of supervision</i>	14
5.4.2 <i>Access guide</i>	15
5.4.3 <i>Report on minors</i>	15
5.4.4 <i>Improving cooperation on complaints</i>	15
5.4.6 <i>Information alerts</i>	15
5.5 SIS	15
5.5.1 <i>Transition of supervision</i>	15
5.5.2 <i>Access guide</i>	16
5.5.3 <i>SIS information campaign</i>	16
5.5.4 <i>Collection of statistics on data subject rights</i>	16
5.5.5 <i>SIS Article 36</i>	17
5.5.6 <i>SIS Article 40</i>	17
5.5.7 <i>Legal interpretation of provisions of the audit cycle</i>	17
5.5.8 <i>Commission Schengen evaluation</i>	17
5.5.9 <i>eu-LISA information sharing</i>	18
5.6 VIS	18

6. LOOKING AHEAD: CHALLENGES FOR 2024-2026	19
6.1 Preparation to onboard further existing and new EU-information systems	19
6.2 Enhanced internal organisation	20



1. FOREWORD

This 2022-2024 activity report summarises the work completed by the **Coordinated Supervision Committee (CSC)** from July 2022 to December 2024. During this period, it was possible to conclude some of the actions envisaged in the second CSC working programme, covering the same period, and other important coordinated activities were designed and structured or launched and are now running.

While Europol had just come under the purview of the CSC in June 2022, we also started in March 2023 to assume supervision of the upgraded Schengen Information System (SIS). This report thus shows the work carried out in relation to these two new major EU information systems, mostly on guidance addressed to individuals on the exercise of their rights. It should also be highlighted that the CSC committed to take on board the most relevant activities that were ongoing at the time of transfer of supervision bodies.

The CSC has been working hard to accommodate the large-scale European Union (EU) information technology (IT) systems that have already come under its purview and to prepare for the arrival of new systems and for the implementation of interoperability regulations.

Looking forward to the coming years, the CSC is ready to welcome more EU IT systems and EU bodies, offices or agencies within its purview. It will tackle the outstanding items in its current 2022-2024 work programme and develop our next programme of activities.

As the scope of the CSC's activities continues to grow, we will keep the organisation and operation of the committee under constant review to ensure

an effective and efficient supervision is delivered.

We will continue to assist national data protection authorities (DPAs) in their work, by providing further clarification on the interpretation of EU and national laws, stimulating the exchange of information and best practices, and providing support for joint audits and coordinated inspections. Taking advantage of its singular framework and holistic view, the CSC will ensure that the multiple data flows among systems and transversal interactions and sharing of information between EU agencies and bodies are properly monitored. To achieve that goal, the CSC will keep developing coordinated supervisory activities covering this new reality to guarantee a high level of data protection and the safeguard of fundamental rights.

Fanny Coudert

CSC Coordinator (July - December 2024)

Clara Guerra

CSC Coordinator (July 2022 - July 2024)

Sebastian Hümmeler

Deputy CSC Coordinator

Matej Sironic

Deputy CSC Coordinator



2. THE ROLE OF THE CSC

The Coordinated Supervision Committee (CSC) consists of representatives of the national data protection authorities (DPAs) of the EU-27 countries, plus Iceland, Liechtenstein, Norway and Switzerland (non-EU Members of the Schengen Area), and the European Data Protection Supervisor (EDPS).

The CSC was established in December 2019 to ensure the coordinated supervision of large-scale EU IT systems and of relevant EU bodies, offices and agencies, in accordance with Article 62 of Regulation (EU) 2018/1725¹ or with the specific EU legal act establishing the large-scale EU IT system or the EU body, office or agency. Regulation (EU) 2018/1725 provided for a single model of coordinated supervision for large-scale EU IT systems, EU bodies, offices and agencies within the framework of the European Data Protection Board (EDPB).

In March 2023, the Schengen Information System (SIS) came under the purview of the CSC making it the fifth EU IT system, body, office or agency under its supervision. This followed the entering into operation of the upgraded SIS on 7 March 2023 with enhanced data sharing and cooperation².

Currently, the EU IT systems, bodies, offices and agencies

falling within the scope of the CSC are the following:

- Internal Market Information System (IMI)
- European Union Agency for Criminal Justice Cooperation (Eurojust)
- European Union Agency for Law Enforcement Cooperation (Europol)
- The Schengen Information System (SIS)
- Visa Information System (VIS).

The CSC also provides a forum for cooperation in the context of the European Public Prosecutor Office (EPPO), the independent supranational prosecution body responsible for investigating, prosecuting and bringing to judgment crimes against the EU budget.

Further EU IT systems, bodies, offices and agencies are planned to come within the scope of the CSC in the near future. These are:

- Entry/Exit System (EES)
- The European Travel Information and Authorisation System (ETIAS)
- The European Criminal Records Information System on non-EU-nationals (ECRIS-TCN)
- European Asylum Dactyloscopy Database (EURODAC)

1. [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.](#)

2. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1505.

- Customs Information System (CIS-JHA)
- Prüm II³
- Interoperability of EES, ETIAS, ECRIS-TCN, EURODAC, Prüm II⁴, SIS, and VIS.

The CSC provides a horizontal approach to data protection supervisory activities anchored on the EDPB and enables an enhanced cooperation among DPAs and the coordination of enforcement actions at European⁵ and national levels. However, the CSC enjoys an autonomous functioning and positioning, pursuant to Article 37.2 of the EDPB Rules of Procedure⁶. The CSC has adopted its own rules of procedure and working methods⁷.

The EDPB Secretariat provides the Secretariat of the CSC and assists the CSC in the performance of its tasks. The CSC Secretariat offers analytical, administrative and logistical support including preparation of positions, and organising CSC meetings and communication between its members and with other institutions and the public.

The representatives of the national DPAs⁸ may participate in the activities of the CSC concerning a specific large-scale EU IT system or EU office, body or agency, only when their respective country applies the relevant EU legal act establishing the large-scale EU IT system or the EU office, body or agency.

2.1 CSC Mission

The central mission of the CSC is to ensure the coordinated supervision by DPAs of large-scale EU IT systems and of EU bodies, offices and agencies falling under its scope, in accordance with Article 62 of Regulation (EU) 2018/1725 or with the relevant EU legal act establishing the large-scale EU IT system or the EU body, office or agency.

For the EU IT systems, bodies, offices and agencies currently falling within the scope of the CSC, the specific mission objectives are as follows:

[The Internal Market Information System \(IMI\)](#) is a secure, multilingual online tool that facilitates the exchange of information between EU/EEA and national public authorities involved in the practical implementation of EU law and helps them to fulfil their cross-border administrative cooperation obligations in multiple Single

Market policy areas, including the General Data Protection Regulation (GDPR) and road transport, amongst others.

The CSC ensures coordination in the supervision of the processing of personal data in the IMI in accordance with Article 21 of Regulation (EU) No 1024/2012 (as modified by Article 38 of Regulation (EU) No 2018/1724).

The [European Union Agency for Criminal Justice Cooperation \(Eurojust\)](#) is based in the Hague and brings together national judicial authorities from EU Member States to fight serious organised cross-border crime.

The CSC ensures coordination in the supervision of the processing of operational personal data in the context of cooperation between the national members within Eurojust in accordance with Article 42.2 of Regulation (EU) No 1727/2018.

The [European Union Agency for Law Enforcement Cooperation \(Europol\)](#) is headquartered in The Hague and is an agency of the EU with a mandate to support and strengthen the action of EU Member States' law enforcement authorities and their cooperation in preventing and combating serious crime affecting two or more EU Member States, terrorism and forms of crime which affect a common interest covered by an EU policy.

The CSC ensures coordination in the supervision of the processing of personal data transmitted to and from Europol, and in any other issues requiring national involvement or raising questions on the implementation and application of the Europol Regulation, in accordance with Article 44.2 of Regulation (EU) 2016/794, as amended by Regulation (EU) 2022/991.

The [Schengen Information System \(SIS\)](#) allows information exchange for border management and for police and judicial cooperation in criminal matters in Europe⁹. A renewed SIS became fully operational in March 2023 with new alerts capabilities, upgraded data and other enhanced functionalities.

The CSC ensures coordination in the supervision of the processing of personal data in the SIS in accordance with Article 57 of Regulation (EU) No. 2018/1861, and Article 71 of Regulation (EU) No 2018/1862.

3. Article 59.3 of [Regulation \(EU\) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations \(EU\) 2018/1726, \(EU\) No 2019/817 and \(EU\) 2019/818 of the European Parliament and of the Council \(the Prüm II Regulation\)](#).

4. [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](#).

5. We refer to 'European', rather than 'EU', as the Member States of the European Free Trade Association (EFTA), namely Iceland, Liechtenstein, Norway and Switzerland, respectively apply the EU legal acts governing some of the EU IT systems covered by the CSC. As such Iceland, Liechtenstein and Norway (who are part of the [EEA Agreement](#)), participate in the CSC activities related to both the IMI and the SIS, and Switzerland participates in the CSC activities related to the SIS.

6. https://www.edpb.europa.eu/our-work-tools/our-documents/rules-procedure/rules-procedure-version-8_en.

7. https://www.edpb.europa.eu/our-work-tools/our-documents/rules-procedure/csc-rules-procedure_en.

8. https://www.edpb.europa.eu/csc/about-csc/members-coordinated-supervision-committee_en.

9. We refer to 'Europe', rather than the 'EU', as the SIS covers those EU Member States applying the Schengen acquis, plus Member States of the European Free Trade Association (EFTA), namely Iceland, Liechtenstein, Norway and Switzerland.

The [Visa Information System \(VIS\)](#) allows [Schengen States](#) to exchange visa data. It processes data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area. The system can perform biometric matching, primarily of fingerprints, for identification and verification purposes. The VIS was under the scope of the Visa Information System Supervision Coordination Group (VIS SCG)¹⁰ as set up by Regulation (EC) No 767/2008 to ensure a coordinated supervision in the area of personal data protection of the VIS information system. The VIS SCG was provided by the EDPS.

Regulation (EU) 2021/1134 amends with different application dates, among others, Regulation (EC) No 767/2008 (VIS Regulation). Among its amended provisions, Article 43(3) VIS Regulation mandates that the cooperation between the supervisory authorities and the EDPS shall take place within the framework of the European Data Protection Board. As a consequence, the coordinated supervision of the VIS is now to be carried out within the European Data Protection Board and its CSC.

The CSC also provides a forum for cooperation in the context of the [European Public Prosecutor's Office \(EPPO\)](#), an independent and decentralised prosecution office of the EU with the competence to investigate, prosecute and bring to judgment crimes against the EU budget, such as fraud, corruption or serious cross-border VAT fraud.

The CSC ensures coordination in the supervision of the processing of operational personal data in the context of cooperation between the national members within the EPPO in accordance with Article 87.3 of Regulation (EU) No 1939/2017.

2.2 Tasks and duties

Within its mission to ensure the coordinated supervision of large-scale EU IT systems and of EU bodies, offices and agencies, the CSC:

- Exchanges relevant information;
- Assists the DPAs in carrying out audits and inspections;
- Examines difficulties of interpretation or application of the EU legal act establishing the large-scale EU IT system or the EU office, body or agency under the scope of the CSC;
- Studies problems with the exercise of independent supervision or with the exercise of the rights of data subjects;
- Draws up harmonised proposals for solutions to issues; and
- Promotes awareness of data protection rights.

The CSC produces a report of its activities on coordinated supervision every two years that is provided to the EDPB for submission to the European Parliament, the Council, the European Commission and other relevant parties that

10. https://www.edps.europa.eu/data-protection/european-it-systems/visa-information-system_en



3. OVERVIEW

3.1 CSC Rules of Procedure

The [CSC's Rules of Procedure \(RoP\)](#) were adopted at its first meeting in 2019. During 2023, there were discussions for a possible revision of the RoP, and it was agreed that no amendments were needed at that time.

3.2 Organisation and working methods

The CSC elects a Coordinator and at least one Deputy Coordinator from among its members. The term of office for both Coordinators and Deputy Coordinators is two years.

In November 2022, the CSC re-elected Clara Guerra from the Portuguese DPA as CSC Coordinator. Sebastian Hümmeler from the German Federal DPA was re-elected in November 2023 as Deputy Coordinator. In view of the increasing number of EU IT systems coming under the purview of the CSC, and in order to prepare for a growing workload, in March 2024 the CSC elected, for the first time, a second Deputy Coordinator: Matej Sironič from the Slovenian DPA.

In July 2024 the CSC elected Fanny Coudert from the EDPS as its new Coordinator for a term of two years. She will lead the work of the CSC with the support of the two existing Deputy Coordinators.

The Coordinator convenes and chairs the meetings, acts

as a contact point in CSC matters, sets the draft agenda, and carries out all the tasks that have been assigned to them in the RoP. The Deputy Coordinators support the Coordinator in performing these tasks and in the absence of the Coordinator.

The Coordinator convenes and chairs the meetings, acts as a contact point in CSC matters, sets the draft agenda, and carries out all the tasks that have been assigned to them in the RoP. The Deputy Coordinators support the Coordinator in performing these tasks and in the absence of the Coordinator.

The CSC is mandated to meet at least twice a year and normally in-person meetings take place in Brussels, though where possible or necessary, such as during the COVID-19 pandemic, meetings are organised by way of videoconference¹¹.

In the last two years, coinciding with the end of the COVID-19 pandemic, in-person meetings have resumed and, as a consequence of increased CSC activity, the number of meetings per year has doubled. To keep a necessary flexibility in the CSC's way of working and being mindful of the limited budget allocated to the EDPB, including for CSC activities, a reasonable balance between in-person and remote/hybrid meeting formats has been achieved.

In addition, in 2024, the in-person meetings have been scheduled for one and a half days to allow adequate

11. In accordance, respectively, with Article 12.1 and Article 16.2 of the CSC Rules of Procedure.

discussion of all agenda items. From March 2023, meeting agendas were restructured to include data issues relating to borders, asylum and migration, after the entry into operation of the new SIS.

During the period covered by this report, from July 2022 to December 2024, twelve meetings of the CSC took place on:

- 6 July 2022 – 6th Meeting of the CSC in a hybrid format;
- 30 November 2022 – 7th Meeting of the CSC in a hybrid format;
- 22 March 2023 – 8th Meeting of the CSC in a hybrid format;
- 14 June 2023 – 9th Meeting of the CSC in an in-person format;
- 7 September 2023 – 10th Meeting of the CSC in a remote/online format;
- 29 November 2023 – 11th Meeting of the CSC in an in-person format;
- 19 - 20 March 2024 – 12th Meeting of the CSC in an in-person format;
- 29 May 2024 – 13th Meeting of the CSC in a remote/online format;
- 2-3 July 2024 – 14th Meeting of the CSC in an in-person format;
- 25 September 2024 – 15th Meeting of the CSC in a remote/online format;
- 6 November 2024 – 16th Meeting of the CSC in a remote/online format; and
- 10-11 December 2024 – 17th Meeting of the CSC in an in-person format.

Summaries of discussions at CSC meetings [can be viewed here](#).

Participation in CSC meetings can vary depending on which EU IT system, body, office or agency subject to CSC supervision, as well as the respective EU legal act, is to be discussed. In terms of the current EU IT systems, bodies and agencies supervised, participation is as follows:

- IMI: The EDPS and the national DPAs of the 27 EU Member States participate in activities in relation to IMI together with the national DPAs of Iceland, Liechtenstein, and Norway as their respective countries also apply the EU legal acts governing IMI;
- Eurojust: The EDPS and the national DPAs of the 27 EU Member States participate in activities in relation to Eurojust;
- EPPO: The EDPS and the national DPAs of the 23 EU Member States¹² that participate in activities in relation to the EPPO;
- Europol: The EDPS and the national DPAs of the 26 EU Member States that are part of Europol participate in activities in relation to Europol; and

- SIS: The EDPS and the national DPAs of the Schengen Member States (27 EU Member States with Cyprus joining the SIS in July 2023, plus Iceland, Norway, Liechtenstein and Switzerland) participate in activities in relation to SIS.
- VIS: The EDPS and the national DPAs of the Schengen Member States (27 EU Member States plus Iceland, Norway, Liechtenstein and Switzerland) participate in activities in relation to VIS.

An overview of the CSC members and their participation [can be found here](#).

3.3 Work programme

The [CSC's second work programme covering 2022-2024](#) was adopted on 6 July 2022. This ambitious programme was published just after Europol came under the CSC's purview. Within the context of the CSC, Europol joined Eurojust and the EPPO to form a trilogy of EU IT systems in a field where processing of personal data has a great impact on the rights of individuals. This reality requires constant and effective monitoring from DPAs to ensure that the level of interference with the fundamental rights to data protection and privacy, as provided for by the EU Charter of Fundamental Rights, is really necessary and proportionate to accomplish the important public interest of combatting serious and organised crime, including terrorism.

Building on previous experience of relevant supervisory bodies, the CSC has planned to intensify its supervisory activities in all EU IT systems within its remit, through coordinated targeted actions, based on enhanced cooperation and information exchange between the EDPS and the national DPAs to ensure effective results. This approach has turned out to be successful by enabling swifter verifications at national level with faster outcomes.

Over the 2022-2024 work programme period, new EU IT systems were expected to be set up, along with some components of the interoperability scheme, and existing EU IT systems were expected to be renewed with extended functions, such as the SIS and Europol information systems. The CSC therefore included in the work programme a transversal supervisory activity covering both Europol and SIS. However, delays in the implementation of the new EU IT systems (EES, ETIAS and VIS) and the consequential lack of use of the legal possibilities for new data processing meant that some of the programmed activities have been postponed.

The 2022-2024 work programme focused on data subjects' rights as a key-area of activity. The CSC planned to reinforce awareness raising and to provide more guidance to assist

12. [Commission Decision \(EU\) 2024/807 of 29 February 2024 confirming the participation of Poland in the enhanced cooperation on the establishment of the European Public Prosecutor's Office, OJ L, 29.2.2024](#) confirmed the participation of Poland in the EPPO and entered into force on the 20th day after its publication. Therefore, Poland became the 23rd Member State participating in the EPPO. The EPPO will be operational in Poland when the European Prosecutor for Poland is appointed by the Council of the European Union. This appointment was foreseen for July 2024.

individuals in navigating the network of EU IT systems, data controllers and different rules to exercise their rights. During these two years, the CSC took important steps in this regard.

The CSC also committed to improve its dialogue with stakeholders, in particular with NGOs, academia and researchers working in this field to promote debate on issues of common interest. That goal was accomplished with a first invitation to meet with some NGOs where a fruitful exchange of information, ideas and expectations took place.

The CSC is firmly committed to ensure that all individuals can enjoy an effective European area of freedom, security and justice.

In general, the main objectives of the work programme for this period were achieved with some activities being completed, while others were launched and are ongoing. A few activities were put on hold awaiting the implementation of new EU IT systems or the application of new functionalities that imply new types of data processing.



4. CROSS-CUTTING ACTIVITIES

In line with its biannual work programme, the CSC carried out its activities during the period July 2022 - December 2024 around the following four main axis:

1. Promote and facilitate the exercise of data subject rights;
2. Examine difficulties of interpretation or application of EU and national laws;
3. Exchange information and conduct joint audits or coordinated inspections; and
4. Prepare for the coordinated supervision of EU IT systems, bodies, offices and agencies that are planned to fall under the CSC's scope.

CSC specific activities relating to the EU IT systems, bodies, offices and agencies currently falling within its scope are described in Section 5 of this report.

The CSC has also worked on other activities that are not included in the work programme but that participating DPAs have brought to its attention, based on their relevance, urgency and/or unforeseen character.

4.1 Data subject rights

One of the main legal tasks of the CSC is to consider challenges related to the exercise of data subject rights, and to promote awareness of data protection rights. In this context, the CSC worked on two different plans and

carried out activities addressed to data controllers and to data subjects.

The CSC made recommendations to data controllers on the exercise of their data protection obligations, such as the information to be provided to data subjects and how they could handle the requests submitted by data subjects when exercising their rights.

The CSC also elaborated guidance to data subjects on their data protection rights. The CSC promoted updated guides on the exercise of data subjects' rights with respect to the new upgraded SIS and the Europol information systems.

Finally, the CSC members exchanged information on best practice on data subject's rights.

4.2 Interpretation and application of EU and national laws

The CSC is a significant forum for discussion where DPAs can exchange information on national experiences, practices and legal provisions, in particular whenever there are difficulties of interpretation or application of EU and national laws. In the past two years, DPAs discussed several issues, such as supervision challenges in the field of police and judicial cooperation. Other significant topics were the applicable legal framework for Schengen data processing, in particular when data subjects' rights are at stake, and the issues emerging from simultaneous requests for access in different Member States vis-à-vis the SIS or the interpretation of Article 47 of the Europol Regulation.

The CSC has also started to discuss the full extension of the SIS obligation for DPAs to carry out an audit every four years using international auditing standards. The interpretation of this legal provision is very relevant, since similar articles are provided in other EU legal instruments.

4.3 Information exchange, joint audits and coordinated inspections

The sharing of information among DPAs on data processing at European and national levels, and especially in those areas that could present higher risks to individual rights, such as in the area of law enforcement of criminal matters, is of paramount importance. This information sharing not only improves supervisory activities at national and European levels, but also streamlines the work of the CSC when designing joint coordinated inspections.

The information provided by the EDPS with regard to various central EU IT systems, in particular prior opinions on certain data processing activities associated with new projects and inspection reports, has been of utmost relevance for national DPAs to better understand data processing operations at EU level. This information is based on the data collected and transmitted by Member States and further queried and consulted by Member States, and enables national DPAs to conduct their own national inspections in a more targeted way. This exchange has also allowed the EDPS to gather important feedback from the national DPAs on the reality of operations at the Member State level.

This exchange of information has been a basis for mutual assistance in conducting audits, including contributing to the subjects that are inspected at central EU level. This has included the participation of some national DPAs in EU-level inspection teams during the current reporting period, for example in the Europol annual inspection. This collaboration has also helped to promote best practice on the engagement of competent authorities both at EU and national levels.

Lastly, the work of the CSC in preparing the joint inspection actions has benefitted immensely from the close cooperation and assistance between the EDPS and the national DPAs, which has allowed the achievement of a more effective coordinated supervision based on a dynamic interaction between the national and the European levels and the ability to follow data flows across systems.

4.4 Preparing for future coordinated supervision

During this reporting period, two EU large-scale IT systems were brought under the scope of the CSC: the upgraded SIS entering into operation in March 2023 and the VIS.

The CSC followed closely the development of the new EU IT systems, including the components of the interoperability

structure, as well as the envisaged entry into operation of the revised EU IT systems. Despite the consecutive schedules advanced for the implementation of these new or enhanced EU IT-systems, the dates of entry into operation have been continuously postponed, in particular with respect to the EES and the ETIAS and, consequently, the upgraded VIS.

Within that context, the CSC invited the European Commission (DG HOME) to make a presentation to its members on the latest progress and their connection with the overall interoperability system and on the information campaign in preparation for the launch of the EES.

As a consequence, some of the CSC's planned activities have not been carried out yet, as they depend on progresses in the deployment of the new EU IT systems. Nevertheless, the CSC has undertaken other activities in preparation for future deployment specifically of the entry into operation of EES and ETIAS.

Since such EU IT-systems are being implemented at national level, competent authorities need advice and guidance in terms of data protection issues. Hence, the CSC considered it imperative to exchange information amongst DPAs to establish an appropriate monitoring of the situation from the outset and facilitate the provision of advice and guidance where needed.

Within this context, the EDPB representatives in the ETIAS Fundamental Rights Guidance Board (EFRGB) also provided information to CSC members on the discussions held at that level related to data protection issues.

More recently, some issues have arisen in the interpretation and application of the ETIAS Regulation related to the exercise of data subjects' rights, as well as the data controllers' obligations to carry out a data protection impact assessment and to provide information to data subjects. Frontex requested the CSC to step in and coordinate actions across these issues, in close cooperation with Frontex, to ensure the establishment of a common approach at national level. The CSC and its members also participated in data protection working groups organised by Frontex to provide support and receive relevant information.

Rapid progress on the technical and organisational implementation of the ETIAS at central and national level with open data protection issues still in place, significantly reduces the likelihood that changes may be implemented that are necessary to safeguard the fundamental right to protection of personal data and others such as the right to non-discrimination. Therefore, the CSC addressed a letter to the European Commission to inform them about the open data protection issues and highlight the urgency required to solve them.

The CSC has also been a forum for exchange of information, experiences and ideas. One of the most significant issues on the table during the reporting period was the preparation

and internal organisation of the national DPAs' work to perform their roles in the near future as the number of EU IT systems under their supervision continually increases. This is a significant challenge for the national DPAs, the EDPS and the CSC.

One of the key elements of the preparation for the new EU IT systems falling within the scope of the CSC has been organisational issues within the Committee itself. The CSC has discussed how to improve its working methods, namely the organisation of its meetings, including how they are structured with respect to different subject matters and membership rights depending on which countries participate in the supervision of which EU IT system and/or body, office or agency, and ensuring enough time is provided for adequate debate of complex issues and activities.

Another issue is the allocation of resources by DPAs to the work of the CSC that must be balanced with the fulfilment of their competing tasks at national and EU levels. This matter has been intensely discussed during the past two years. Issues highlighted include a lack of human, financial and technical resources to supervise so many information systems at national and EU levels, with the added challenges of enabling effective supervision of all the interactions between the systems and their respective data flows and data processing operations.

In particular, the CSC discussed this important matter based on the results of studies commissioned by some DPAs on supervision requirements, inspection challenges and resources requirements. In September 2023, in an informal initiative outside of the CSC, a workshop took place, promoted by the Dutch DPA, to share views and projects on these subjects. A follow-up workshop took place on 7 March 2024.

4.5 Supporting activities

A significant role for the CSC is to be a privileged platform for cooperation and mutual assistance among national DPAs and the EDPS in performing inspections, as well as to promote a closer engagement between the European and national levels. During this reporting period, national DPAs instigated numerous requests for exchange of information on specific problems identified at national level within the CSC, which fed discussions held between CSC members.

4.5.1 External dialogue

The CSC fosters dialogue and engagement with stakeholders, in particular with civil society. As such, representatives of two selected NGOs (EDRI, Access Now) joined a dedicated part of the CSC's November 2023 meeting for an initial session.

Specifically, these NGOs presented their ongoing activities and developments in CSC-related matters. The CSC members and these NGOs also exchanged on potential synergies, always respecting the CSC's obligations and

independence. The input from these NGOs at the meeting was substantial, very useful, and was seen as a successful start to widening and institutionalising substantive dialogue with stakeholders.

The opening of a dialogue with NGOs active in data protection and in contact with data subjects is important. In the law enforcement area, the number of complaints and instances of direct interaction with the DPAs is quite low, unlike for GDPR matters. Individuals, both EU citizens and third country nationals, tend to not contact DPAs in relation to police or judicial matters. Therefore, DPAs have less knowledge of possible data infringements.

Engagement with organisations who work in the field and have meaningful interventions with individuals as data subjects is a very useful source of information for the work of CSC that can help the committee better prepare and target its supervisory activities.

4.5.2 Reporting

The CSC Coordinator reports to the EDPB on the CSC activities at least twice a year, in accordance with Article 4.2 of the CSC Rules of Procedure. Therefore, every six months, the CSC Coordinator has provided an update at the EDPB plenary on the coordinated supervision actions during the previous semester. During this reporting period, five reports were presented to the EDPB at the July 2022, January 2023, July 2023, January 2024 and July 2024 EDPB plenary meetings.



5. SPECIFIC ACTIVITIES

This section describes the specific activities undertaken by the CSC during this reporting period with respect to the EU IT systems, bodies, offices or agencies currently under its supervision.

5.1 IMI

5.1.1 Transparency obligations

The CSC has worked on a set of recommendations on IMI transparency obligations for data controllers. The [final recommendation document](#) was adopted at the CSC meeting in March 2024 and published in April 2024.

The EU internal market rules give individuals and businesses the right to move freely within the European Economic Area (EEA) for work, study, or other purposes. The recommendations address data controllers within authorities that are involved in the cooperation procedures for applying these rules, via the IMI, and are required to exchange information with competent authorities in other Member States, and therefore to process personal data in a manner that complies with Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR).

Under the GDPR, transparency obligations play a key role in ensuring the rights of data subjects in relation to the processing of their personal data. The CSC's recommendations are intended to assist data controllers in complying with the GDPR's data protection provisions on the information to be provided to data subjects, in relation to the data processing their competent authority carried

out when using the IMI.

The recommendations briefly describe what information must be given to data subjects, and when and how this information must be provided under the GDPR in combination with Regulation (EU) No 1024/2012 (the IMI Regulation).

The IMI Regulation determines that a competent authority using the IMI, being a data controller, should ensure that data subjects are informed as soon as possible about the processing of their personal data in the system, and of the identity and contact details of the data controller and of its representative, if any. They must also be informed of their individual rights and how they can exercise them. These information duties must be complied with in accordance with Articles 13 and 14 of the GDPR.

5.1.2 Users' management

The CSC had an initial exchange on a supervisory action on how national competent authorities exercise their obligations concerning IMI and the management of users' access to the system. The CSC has discussed the format of such a coordinated activity starting with a fact-finding exercise and then, based on the results of that exercise, the possible development of a joint guidance document and/or enforcement at national level.

5.1.3 Compliance of data protection requirements in IMI

The CSC invited representatives of the European Commission to present their initiative with IMI national contact points in Member States and relevant competent authorities to enhance compliance of data protection requirements in IMI.

5.2 EPPO

During the reporting period, the CSC has been monitoring the implementation of European Delegated Prosecutors' offices at Member States level, including specific relevant national laws and the interplay between the EPPO case management system at national level and national databases, which are respectively supervised by the EDPS and by the national DPAs.

To assess this interplay and the actual conditions under which the European Delegated Prosecutors work at national level and apply national law while inserting data in the EPPO case files, the CSC promoted a joint activity involving the EDPS and national DPAs to make operational visits to European Delegated Prosecutors' offices in each Member State, on a rotating basis.

The Portuguese DPA volunteered to participate in this activity, together with the EDPS. For that purpose, a working arrangement was signed in December 2022. In 2023, the Portuguese DPA and the EDPS, each acting within their own competence, examined the integration of systems and relations between EPPO case files, the EPPO case system, and the national source databases at the local European Delegated Prosecutors' office. This joint visit with the EDPS at national level was the first of its kind and will serve as a pilot for future coordinated activities.

5.3 Eurojust

5.3.1 Joint Investigation Teams

The CSC has surveyed the participation of third country authorities in Joint Investigation Teams (JIT) supported within the scope of Eurojust, in view of the lack of data protection clauses in JIT agreements. The CSC survey found that in the great majority of the cases, the third country involved either held an adequacy decision or had signed a cooperation agreement with Eurojust and/or Europol. Following an exchange with Eurojust, the CSC was informed that Eurojust is drafting a model clause to insert in the JIT agreement. The CSC will continue to monitor the situation at national level.

5.3.2 Counter Terrorism Register

The CSC has taken up the subject of data quality issues related to data inserted in the Eurojust Counter-Terrorism Register (CTR).

A drafting team set up in 2023 prepared a questionnaire to facilitate fact-finding at national level on the reasons why the personal data processed in the CTR is not kept up to date. The outdated information in the CTR, available to all Member States, could represent a major negative impact on a data subjects' rights and freedoms. This coordinated action was launched at the end of May 2024.

5.3.3 Supervisory independence

The CSC has also started to gather information from its members on their assessment, based on relevant national law provisions, regarding the DPAs' independence, powers and legal tasks in relation to police and judicial cooperation in criminal matters. The specific focus of the investigation is to assess any impact on the supervision of Eurojust (and Europol) at national level.

5.3.4 Secure communication

Over the past two years, an activity related to the issue of secure communication channels for exchanges between Member States and Eurojust has been ongoing. For a couple of Member States, the situation was improved after the intervention of national DPAs, but was finally concluded at central level, following recommendations by the EDPS.

5.4 Europol

5.4.1 Transition of supervision

The CSC has ensured the smooth transition of supervision from the Europol Cooperation Board (ECB). This has included the transfer of ongoing activities and assessing new possibilities for cooperation and exchange of information between DPAs and law enforcement authorities.

This work has included following closely the implementation from June 2022 of the new legal framework that followed the amendments to Regulation (EU) 2016/794 (the Europol Regulation)¹³. In particular, the CSC has focused on the determination of the purposes of data processing by the national competent authorities and by Europol.

The CSC is looking to address the so-called 'big data challenge' in close cooperation with the EDPS and national DPAs, either by checking compliance with national law when data is transmitted to Europol or compliance with the Europol Regulation when data is further processed by

13. [Regulation \(EU\) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation \(EU\) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation.](#)

Europol. Special attention has been given to processing of data without data subject categorisation.

5.4.2 Access guide

In July 2023, the CSC published '[Europol's information systems - a guide for exercising data subjects' rights: the right of access, rectification, erasure and restriction](#)'. The content of the Guide was provided by Member States and compiled by the CSC.

Individuals whose personal data are collected, held or otherwise processed by Europol are entitled to rights regarding their personal data, namely the right of access, rights to rectification, erasure or restriction of the data, and the right to have the legality of transfer of their personal data verified by a national DPA or, where applicable, by the EDPS. The CSC guide describes how those rights can be exercised.

The guide is divided into three sections: a description of the data categories and exchange of personal data between Member States and Europol; a summary of the rights granted to individuals whose personal data are processed in Europol's IT systems; and a description of the procedure for exercising the right of access in each of the countries concerned.

The Guide also lists contact points for the relevant body to which requests for access, rectification and/or erasure should be addressed in each Member State, together with the contact details of the national DPAs and of the EDPS. Finally, as annexes, model letters are provided that can be used to file requests to the relevant national competent authority where that authority does not require a specific standard form.

5.4.3 Report on minors

Following the 2022 Audit Report of the EDPS on Europol's processing of personal data of minors under 15 years old provided to Europol by third countries and international organisations¹⁴, in 2023 the CSC undertook a coordinated activity on Europol with respect to the transmission by Member States of data on minors as suspects. Almost all concerned national DPAs conducted verifications at the national level to assess the lawfulness of such data transmission to Europol and provided feedback to the CSC.

The CSC is currently collecting the key-findings to draft a joint report on the exercise.

5.4.4 Improving cooperation on complaints

The CSC has set up an activity to determine internal procedures (including data flows, deadlines, interpretation of the extent of checks, and identification of scenarios) for cooperation between the EDPS and national DPAs to handle complaints under Article 47 of the Europol Regulation.

The main aim of the activity is to enhance cooperation between EDPS and national DPAs, make the complaints process more efficient and shorten as much as possible the deadlines to reply to data subjects. Most of the complaints received are connected to the exercise of data subjects' rights.

A brief guidance note for cooperation on the implementation of Article 47 complaints, including specific steps, procedures and deadlines, is being developed.

5.4.5 Information alerts

The CSC is monitoring the implementation of the provisions on 'information alerts' inserted in the new SIS by Member States, either at EU level (Europol) or national level (SIS). This includes checking that the periodic reporting mechanism is in place. This will be the first cross-system supervisory activity within the scope of the CSC activities.

However, the criteria for information alerts relating to the SIS Regulation were still to be established by the Europol Management Board, so this CSC activity has not yet been launched.

5.5 SIS

5.5.1 Transition of supervision

During this reporting period, the upgraded SIS, which came into operation in March 2023, was brought under the scope of CSC.

The transition of coordinated supervision from the SIS II Supervision Coordination Group (SCG)¹⁵ to the CSC was successful and seamless. The SIS II SCG itself had taken over from the Schengen Joint Supervisory Authority (JSA)¹⁶ when the second-generation SIS (SIS II) entered into force on 9 June 2013.

The CSC decided to take stock of the most relevant ongoing activities of the SIS II SCG, such as the coordinated inspections on the alerts regarding discreet and specific checks under Article 36 of the SIS II Decision and the updated Guide for the exercise of data subjects' rights.

14. https://www.edps.europa.eu/data-protection/our-work/publications/audits/2023-09-06-audit-report-europol_en.

15. https://www.edps.europa.eu/data-protection/european-it-systems/schengen-information-system_en.

16. https://www.edps.europa.eu/data-protection/our-work/publications/scg-documents/archived-website-former-schengen-joint_en.

The SIS has a special legal regime¹⁷ with respect to reporting that requires annual reporting of coordinating activities, rather than biannual reporting as is the norm for other EU IT systems, bodies offices or agencies under the scope of the CSC.

2023 is the first (partial) year that SIS has been under the scope of CSC and coincides with the biannual reporting of CSC activities. Therefore, the 2023 and 2024 CSC Reports on SIS Coordinated Activities are included as part of this document.

The annual assessment of SIS statistics provided by Member States on data subject rights (see 5.5.4 below) is a new reporting activity and should be considered as a stand-alone document. This document/report is being finalised at the time of publication of this report.

Next year CSC will produce a report dedicated to CSC coordinated activities in 2025 with respect to SIS and an assessment of 2024 SIS statistics.

5.5.2 Access guide

In April 2023, the CSC published '[The Schengen Information System - a guide for exercising data subjects' rights: the right of access, rectification and erasure](#)'. This guide had been compiled by the SIS II SCG. It was then reviewed and adopted by the CSC.

Within the SIS, any individual is guaranteed the right of access to their own data, the right to rectification of inaccurate data and the right to the erasure of unlawfully stored data.

The 2023 guide outlines those rights and describes how they can be exercised. It takes into account the recent changes brought by the current SIS legal framework and the revision of the EU data protection framework, as the SIS Regulations now refer to the exercise of some rights as laid down under Regulation (EU) 2016/679 - the General Data Protection Regulation (GDPR)¹⁸, and Directive (EU) 2016/680 - the Law Enforcement Directive (LED)¹⁹.

The guide has three sections: a description of the SIS; a description of the rights granted to the individuals whose

data are processed within the SIS; and a description of the procedure for exercising these rights in each of the Schengen State countries concerned, together with contact details for the competent national authorities.

Annexes to the guide give three model letters to be used by applicants to request access, and to rectify or erase their personal data in cases where the national competent authority does not require a specific standard form.

5.5.3 SIS information campaign

The CSC engaged strongly with the European Commission for the information campaign around the new SIS, in particular in coordinating implementation at national level. A link to the CSC website for the Guide for exercising the right of access was included in the Commission's digital leaflet²⁰ and general presentation²¹ on the renewed SIS.

5.5.4 Collection of statistics on data subject rights

As previewed under 5.5.1 above, the CSC is tasked with developing and drafting an annual report from information provided by Member States to submit to the EDPB on the exercise of data subjects' rights, on court proceedings, and on mutual recognition of final decisions. This assessment is to be included in the joint report of activities regarding the SIS pursuant to Article 54.3 of Regulation (EU) 2018/1861 and Article 68.3 of Regulation (EU) 2018/1862.

The format of the template for use by Member States to report on data subject rights related to the SIS regulations is set out in Commission Implementing Decision (EU) 2022/2206²².

2023 is the first year for which CSC will publish a report on these SIS statistics.

In 2023, the CSC adopted a model letter for national DPAs to send to Member State competent authorities for SIS to raise awareness on the new obligation to collect statistics on data subjects' rights. The letter includes information on the obligations and court proceedings, the template laid down by the Commission's Implementing Decision indicating the statistics to be provided and details of where to transmit the statistics collected (i.e., the CSC

17. Obligations under Article 54.3 of [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 Article 68.3 of [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](#).

18. [Regulation \(EU\) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC \(General Data Protection Regulation\)](#).

19. [Directive \(EU\) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA](#)

20. [The Schengen Information System guaranteeing freedom, security and justice \(Guide\)](#).

21. [The Schengen Information System guaranteeing freedom, security and justice \(Presentation\)](#).

22. [Commission Implementing Decision \(EU\) 2022/2206 of 11 November 2022 laying down the reporting template for the annual reports to the European Data Protection Board by Member States on the exercise of the rights of data subjects related to the Schengen Information System](#).

Secretariat).

5.5.5 SIS Article 36

During 2019, the SIS II Supervision Coordination Group (SCG) was informed of reports of an increase in Article 36²³ alerts in the SIS. These alerts relate to discreet surveillance, which are generated and used without the knowledge of the individual concerned.

This increase was confirmed, and the SCG agreed to conduct a coordinated activity, which would involve a short questionnaire and onsite checks. The purpose of this exercise would be twofold: to gather more specific information and statistics about the use of Article 36 alerts by competent authorities; and to enable the national DPAs to assess the legality and the conditions under which such alerts are inserted and maintained in SIS II.

A short questionnaire was developed by the SCG to gather specific information and statistics about the use of Article 36 alerts by Member States. A checklist for national DPAs to use during onsite inspections was also developed.

However, with the advent of the COVID-19 pandemic in 2020 few DPAs were able to conduct inspections before they stopped for almost two years. In 2022 and 2023 the DPAs resumed this activity.

This work, initiated under the SCG, was transferred to the CSC. The CSC members have reported on their supervision actions and the findings have been assessed by CSC. A report was published in October 2024²⁴ drawing conclusions on the level of compliance, identifying any issues, and providing a set of recommendations with regard to the documentation of the alerts, their quality, the time limits and retention period, as well as substantive and technical issues.

5.5.6 SIS Article 40

SIS Article 40²⁵ alerts enable Member States to enter data, such as partial fingerprints, on unknown wanted persons. Such alerts should only be entered into SIS when there is a very high probability that they belong to the perpetrator of a terrorist act or other serious crime. From the outset of its supervision, the CSC has monitored the statistics on these alerts since this is a new alert in the SIS within the new capabilities of the system.

In the first three months of operation, only 14 alerts by two Member States were introduced to the system. The concerned Member States were advised in case they

wished to verify the alerts or check for further information.

The CSC members also exchanged information related to the interpretation of Article 40 and on the existence of national provisions or internal policies establishing criteria or providing guidance to ascertain the requirement of very high probability that the latent fingerprint belongs to a perpetrator.

The CSC continues to monitor Article 40 alerts and reviewed the statistics after one full year of operation of the new SIS at the May 2024 meeting. The number of alerts was low and involved only a very few Member States. The low alert level means that a coordinated activity is not required currently, but the DPAs of the Member States can query specific instances at national level to obtain insights on how the alerts are being applied.

The CSC will continue monitoring statistics on the creation of these alerts.

5.5.7 Legal interpretation of provisions of the audit cycle

During 2023, the CSC has started to work on the legal interpretation of Articles 55.2 and 56.2 of SIS Regulation (EU) 2018/1861 and Articles 69.2 and 70.2 of SIS Regulation (EU) 2018/1862 concerning the audit cycle, the extent and comprehensiveness of audit, and the use of international auditing standards. This is an ongoing activity that was inherited by the CSC from the SIS SCG.

This issue is important for all DPAs because the obligation to carry out an audit at regular intervals falls upon the EDPS and national DPAs. Similar audit provisions exist in other legal instruments (for example, EES, ETIAS, interoperability, VIS, etc.), so the outcome of this CSC legal assessment is key to establishing the precise methodology and frequency of the audits that the DPAs should perform for other EU IT systems.

Following preliminary discussion in CSC, a draft proposal for a common approach is being prepared for further consideration in the committee.

5.5.8 Commission Schengen Evaluation

The European Commission, represented by officials from DG JUST and DG HOME, made a presentation to the CSC at their September 2023 meeting. The new SIS was described along with the existing tools that were available to support Member States to implement the system.

The presentation covered the new Schengen Evaluation

23. Article 36 of [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](#).

24. https://www.edpb.europa.eu/our-work-tools/our-documents/csc-documents/report-article-36-alerts-schengen-information-system_en

25. Article 40 [ibid](#).

Framework (SCHEVAL)²⁶. Issues raised during the presentation included the composition of the SCHEVAL pool of experts, training, exchange of relevant information, thematic evaluations, and the security accreditation of experts. The CSC has continued to cooperate with the Commission through training of data protection experts and the organisation of evaluation exercises for training purposes. appendix.

In the July 2024 CSC meeting the European Commission presented the Schengen Scoreboard, the KOEL platform set up to facilitate exchange of communication among the Member States and the Commission and some additional issues including an exchange on the experience from recent SCHEVAL evaluations conducted under the new methodology, the inspection plan for the next few years and the state of play of implementation of EES/ETIAS into SCHEVAL.

5.5.9 eu-LISA information sharing

The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) was established to provide a long-term solution for the operational management of large-scale EU IT systems, which are essential instruments in the implementation of the asylum, border management and migration policies of the EU.

The CSC promotes regular contact, sharing of information and queries with the eu-LISA's Data Protection Officer (DPO), and considers this an extremely useful part of its supervisory activities enabling it to detect emerging issues and better shape its supervisory activities.

The CSC invited the eu-LISA's DPO to present the status of the new SIS after its first three months of operation, and the Committee aims at further enhancing the cooperation and bilateral exchange on the latest statistics trends. The eu-LISA's DPO reported at the CSC May and July 2024 meeting including extensive information on the first year of entry into operation of the new SIS.

5.6 VIS

During this reporting period, the VIS, was brought under the scope of CSC. The transition of coordinated supervision from the VIS Supervision Coordination Group (SCG)²⁷ to the CSC was successful and seamless.

Currently, the VIS is undergoing a revision, including to enable its integration into the interoperability architecture. The revised VIS is planned to be ready to enter into operation in autumn 2026.

Next year CSC will produce a report dedicated to CSC coordinated activities in 2024 with respect to VIS, and VIS statistics for the period 2022-2024 will be included as an

26. https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-area/schengen-evaluation-and-monitoring_en.

27. https://www.edps.europa.eu/data-protection/european-it-systems/schengen-information-system_en



6. LOOKING AHEAD: CHALLENGES FOR 2024-2026

The CSC will continue to work on the pending actions of its defined 2022-2024 work programme and will develop its next work programme for 2024-2026. With the potential onboarding of several additional EU IT systems and an increased focus on interoperability between IT systems, the workload of the committee will considerably increase.

6.1 Preparation to onboard further existing and new EU-information systems

A number of existing and new EU IT systems are expected to fall within the remit of the CSC over the next few years.

The **Customs Information System (CIS)** is a computer system centralising customs information with the aim of preventing, investigating and prosecuting breaches of Community customs or agricultural legislation. The CIS is composed of a central database accessible through terminals in each Member State.

The CIS is currently under the scope of the Customs Information System Supervision Coordination Group (CIS SCG)²⁸ as set up by Regulation (EC) No 766/2008 to ensure a coordinated supervision in the area of personal data protection of the CIS information system. The EDPS currently provides the secretariat and organisation of meeting for the CIS SCG.

Supervision of relevant CIS activities previously under the scope of the Customs Joint Supervisory Authority were

transferred to CSC in the first half of 2024.

The **Entry-Exit System (EES)** was expected to be launched in November 2024, but its entry into operation have been further postponed. It is a new automated IT system that will replace the physical stamping of passports when entering the EU and other Schengen countries. All EU Member States, except Cyprus and Ireland, and all four EFTA countries (Iceland, Liechtenstein, Norway and Switzerland) will take part. The system will record all entries to and exits from participating European countries with collection of personal data including passport information, facial images and fingerprints.

The **European Travel Information and Authorisation System (ETIAS)** is scheduled to follow shortly afterwards and will be a new entry requirement for visa-exempt nationals travelling to 30 European countries (the EES countries plus Cyprus). An ETIAS authorisation will be linked to the traveller's passport and will be valid for up to three years or until the passport expires. The CSC is already preparing to assume its role as a forum for coordinated supervision in regards of ETIAS.

The **Prüm II Regulation** on automated data exchange for police cooperation was adopted in March 2024. It revises the existing Prüm framework and includes provisions on the automated exchange of DNA profiles, dactyloscopic data, facial images, police records and vehicle registration

28. https://www.edps.europa.eu/data-protection/supervision-coordination/customs-information-systems_en.

data. It also contains new technical infrastructure and extends its participants to include Europol. The CSC is preparing to assume its role as a forum for coordinated supervision in regard to Prüm II.

Further systems – namely, the [European Criminal Records Information System on Third-Country Nationals \(ECRIS-TCN\)](#) and the [European Asylum Dactyloscopy Database \(Eurodac\)](#) will also fall within the remit of the committee along with the continuing coordinated supervision of elements of the interoperability framework.

6.2 Enhanced internal organisation

The CSC currently actively contributes to the coordinated supervision of five EU IT systems, bodies, offices and agencies. In addition, in the near future, the CSC will cover the EES, ETIAS and parts of CIS activities.

With the number of EU IT systems, bodies, offices and agencies under its purview more than doubling, the CSC will need to adapt, which will require much more resources from the EU budget authorities, as it provides the CSC Secretariat. In addition, national DPAs will need to allocate substantially more resources, not only to supervise the data controllers under their purview, but also to support the work required to coordinate supervision at EU/CSC-level.

Going forward, the CSC will be organising more meetings. To ensure an efficient and resourceful coordinated supervision into the future, it will be essential that national DPAs and the EDPS support the work of the CSC, including by ensuring the availability of staff to engage actively within the committee, act as rapporteurs, and lead specific activities, in order to maintain the ability of the CSC to effectively fulfil its legal obligations.

CONTACT DETAILS

Postal adress
Rue Wiertz 60, B-1047 Brussels

Office adress
Rue Montoyer 30, B-1000 Brussels