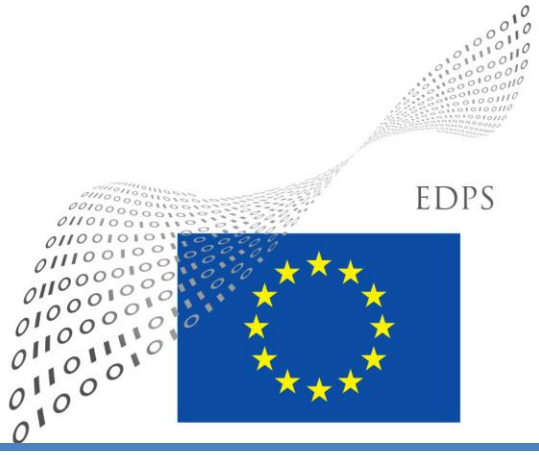
EUROPEAN DATA PROTECTION SUPERVISOR

Policy Paper

The EDPS as Supervisor of Large-Scale IT Systems and Member of Supervision Coordination Groups



December 2015

The European Data Protection Supervisor (EDPS) is an independent institution of the EU. The Supervisor is responsible under Article 41.2 of Regulation 45/2001 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies", and "…for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'.

The Supervisor and Assistant Supervisor were appointed in December 2014 with the specific remit of being more constructive and proactive, and they published in March 2015 a five-year strategy setting out how they intended to implement this remit, and to be accountable for doing so.

This paper outlines the EDPS' approach towards supervising large-scale IT systems and how the EDPS will cooperate with Member States' data protection authorities as a member of the Supervision Coordination Groups.

Executive Summary

The supervision of large-scale IT systems is becoming an increasingly bigger part of the EDPS' work. These systems, whose central units are provided by an EU institution, body or agency (EUI) and therefore are supervised by the EDPS, are used by the Member States, who have certain responsibilities in them as well and are supervised by the Member States' Data Protection Authorities (DPAs). Coordination of supervision activities on these two levels is important.

The Supervision Coordination Groups (SCGs) for the different systems serve to ensure this coordination. The EDPS is present in these groups in different roles: as a member (who may also be elected Chair) and as secretariat (working for the Chair, whether she/he is from the EDPS or from a national DPA).

It has therefore become necessary to define the role of the EDPS as member of the SCGs, distinct from the secretariat. At the same time, with the ramping up of eu-LISA's activities, EDPS' approach to consultations received from them and other management authorities needs to be defined explicitly. Similarly, EDPS' approach towards complaints, inspections and other supervision activities needs to defined, insofar as it deviates from standard procedures.

This policy paper therefore clarifies and documents the current approach as well as refining it for the future in order to provide close supervision of the management authorities of large-scale IT systems, as well as fruitful cooperation with Member State DPAs, respecting each other's mandates.

This document is closely linked to the EDPS Strategy for 2015-2019, notably action 6.2 on supervision coordination, action 8.3 on the accountability of IBOA and action 10.3 on promoting consistency in the supervision of large-scale IT systems.

TABLE OF CONTENTS

I. Contents

1 Introduction

This policy paper sets out the EDPS' approach regarding its roles as supervisor for the central units of large-scale IT systems and as member of the supervision coordination groups (SCGs) for these systems.

Explicitly defining the approach for these two roles is necessary because large-scale IT systems and SCGs are becoming an increasingly important part of the EDPS' work. While the EDPS has played this role for Eurodac and the CIS for a long time (since 2005 and 2009 respectively), these activities have grown dramatically in recent years: VIS 2011, SIS 2013 and IMI 2014. EES/RTP (and other possible "smart borders" initiatives) and other initiatives may well be added to this list in the future. At the same time, with the ramping up of eu-LISA's activities, our approach to consultations received from them and other management authorities needs to be defined explicitly.

We therefore clarify and document the current approach as well as refine it for the future in order to provide close supervision of the management authorities of large-scale IT systems, as well as fruitful cooperation with Member State DPAs, respecting each other's mandates.

This links clearly to the EDPS Strategy 2015-2019 (the Strategy): defining our approach on consultations will help to have management authorities embrace accountability (action point 8 of the Strategy); close cooperation with national DPAs in the SCGs will help to make sure that Europe speaks with one voice (action point 6 of the Strategy), and exchanging experience and coordinating supervision efforts will help to promote a mature conversation on security and privacy and show that supervision coordination procedures work, but can still be improved (action point 10).

Clearly defining our approach will also contribute to stable expectations on the part of the different parties (both supervised entities and fellow DPAs).

The remainder of this note will outline the legal regimes applicable to the different large-scale IT systems (including their commonalities and differences), explain how the EDPS will carry out its tasks as supervisor typically of the central systems with reference to different supervision activities and lay out the EDPS' approach to the SCGs (including matters such as level of representation, involvement in SCG activities, information sharing and relations with the Chairs).

The EDPS' role as secretariat for the SCGs is excluded from the scope of this document.[1]

[1] This role is distinct from the other two as supervisor of large-scale IT systems and member of the SCGs: the secretariat provides support to the SCGs acting under instructions from the respective Chairs, who may very well be from a national DPA.

2 Background on large-scale IT systems and the EDPS' role in them

This section will explain the legal bases, content and architecture of large-scale IT systems in whose supervision the EDPS plays a role and which have SCGs. While the provisions in the different texts are broadly similar, there are some differences, which will be explained as well.

2.1 SIS II

The second generation Schengen Information System (SIS II) is a large database which contains information on wanted or missing persons, persons under surveillance by the police and persons, not nationals of a Member State of the Schengen area, who are banned from entry into the Schengen territory, as well as information on stolen or missing vehicles and objects such as, in particular, identity papers, vehicle registration certificates and vehicle number plates. The main purpose of the database is to ensure a high level of security within the Schengen States in the absence of internal border checks, by allowing competent national authorities, such as police and border guards, to enter and consult alerts on persons and objects.

The system is established by Regulation (EC) 1987/2006 (SIS II Regulation) and Council Decision 2007/533/JHA (SIS II Decision).

Article 45 of the SIS II Regulation and Article 61 of the SIS II Decision state that the EDPS shall "check that personal data processing activities of the Management Authority are carried out in accordance with" the SIS II Regulation and Decision. Articles 46 and 47 of the Regulation on the duties and powers of the EDPS apply accordingly. According to Article 45(2) of the SIS II Regulation and Article 61(2) of the SIS II Decision, the EDPS shall ensure that a security audit of the central system is carried out at least every 4 years.[2]

Article 46 of the SIS II Regulation and Article 62 of the SIS II Decision establish the SIS II SCG, stating that there shall be at least two meetings per year; the SCG is meant to have its members "exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties of interpretation or application of this Regulation, study problems with the exercise of independent supervision or in the exercise of the rights of data subjects, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary." A report of activities shall be adopted every two years and be sent to European Parliament, the Council, the Commission and the management authority.

One specific procedure in the SIS, which does not exist for the other systems covered by this Paper, is the mediation procedure under Article 34(4) SIS Regulation and Article 49(4) SIS Decision: If one MS has reasons to believe that data introduced by another MS are factually incorrect or unlawfully stored, these two MS shall address the issue. If they are unable to reach an agreement within two months, the competent authority of the MS that did not issue the contentious alert shall submit the matter to the EDPS, who, jointly with the national DPAs concerned, shall act as a mediator. As of July 2015, the EDPS has not yet been contacted by national competent authorities for this procedure.

The management authority for SIS II is eu-LISA.

[2] A report of this audit shall be made available to the management authority, the Commission, the Council, the European Parliament and the national DPAs. Before the adoption of this report, the management authority shall be given an opportunity to comment.

2.2 VIS

The Visa Information System (VIS) is a large database which contains information, including photographs and fingerprint data, about applicants for short-stay visas in the Schengen Area. One of the main purposes of the database is to fight "visa shopping", i.e. the practice of making further visa applications to other EU Member States when a first application has been rejected.

The system was established by Council Decision 2004/512/EC, as completed by Regulation (EC) 767/2008 (VIS Regulation). Access for law-enforcement purposes is regulated in Council Decision 2008/633/JHA (VIS Decision).

The VIS Decision only regulates access to the VIS as established under the VIS Regulation for law-enforcement purposes, which is a subordinate purpose of the system; therefore, unlike the SIS II Regulation/Decision, it does not replicate the whole content of the legal text, but only addresses the specificities of this further use.

Article 42 of the VIS Regulation reaffirms the supervisory role of the EDPS using the same terms as the SIS II Regulation. According to Article 42(2) of the VIS Regulation, the EDPS shall ensure that a security audit of the central system is carried out at least every 4 years.[3] Again, the powers and duties of the EDPS established in Regulation (EC) 45/2001 apply accordingly.

The provisions on supervision coordination in Article 43 of the VIS Regulation are identical to those in the SIS II Regulation, except for the fact that the activity report shall include a chapter for each Member State, prepared by that Member State's DPA.

The management authority for VIS is eu-LISA.

2.3 Eurodac

Eurodac is a large database of fingerprints of applicants for asylum and irregular immigrants found within the EU. The database mainly helps the effective application of the Dublin Regulation on handling claims for asylum.

The system was initially established by Council Regulation (EC) 2725/2000 (old Eurodac Regulation). A new Eurodac Regulation, Regulation (EC) 603/2013 (new Eurodac Regulation), has become applicable on 20 July 2015. The new Eurodac Regulation notably adds law-enforcement access.

Article 31(1) of the new Eurodac Regulation states that the EDPS "shall ensure that all the personal data processing activities concerning Eurodac, in particular by the Agency, are carried out in accordance with Regulation (EC) No 45/2001 and this Regulation".[4] According to Article 31(2) of the new Eurodac Regulation, the EDPS shall ensure that a security audit of the central system is carried out at least every 3 years. A report of this audit shall be made available to the management authority, the Commission, the Council, the European

[3] A report of this audit shall be made available to the management authority, the Commission, the Council, the European Parliament and the national DPAs. Before the adoption of this report, the management authority shall be given an opportunity to comment.

[4] This provision is wider than the corresponding ones for the other large-scale IT systems. On the other hand, it has to be noted that Article 30, on the supervision by national DPAs, states that "lawfulness of the processing […] by the Member State in question, including their transmission to the Central System" shall be monitored by the relevant national DPAs. It appears that this different wording is due to historical reasons and copy & paste from the old Eurodac Regulation. The old Eurodac Regulation first created a Joint Supervisory authority with the same mandate, but also stated that it should be disbanded and replaced by the EDPS upon its establishment.

Parliament and the national DPAs. Before the adoption of this report, the management authority shall be given an opportunity to comment.

The provisions on supervision coordination are identical to those for SIS II: at least two meetings per year, and a joint activity report every two years.

The management authority for Eurodac is eu-LISA.

2.4 IMI

The Internal Market Information System (IMI) is a software application accessible via the Internet, developed and hosted by the European Commission, which aims at improving the functioning of the Single Market by facilitating administrative cooperation and mutual assistance between Member States. To this end, it provides a tool for the secure exchange of information that may include personal data.

The recognition of professional qualifications among different Member States is an example of the kind of questions that are dealt with in IMI.

The system in its current has been established by Regulation (EU) 1024/2012 (the IMI Regulation).[5]

Article 21 of the IMI Regulation establishes the rules on supervision coordination, stating that national DPAs and the EDPS shall "each acting within the scope of their respective competences, shall ensure coordinated supervision of IMI and its use by IMI actors". It does not establish a minimum number of meetings, stating that the EDPS "may" invite the national DPAs "as necessary" to discuss these matters; costs are to be borne by the EDPS.

A joint activity report is to be sent to the Council and the Commission at least every three years.

There is no periodic inspection obligation for IMI.

The Commission is controller for IMI, which is managed by DG GROW.

2.5 CIS

The Customs Information System ('CIS') is a database that aims at improving cooperation between the customs authorities of the EU Member States. To this end, it allows the exchange of information on customs investigations and to request other customs authorities to take specific actions.

The system was originally established under the CIS Convention of 1995. One particularity of the CIS is its double legal basis. Regulation (EC) 515/1997, as amended, is the legal basis for the former first pillar part of the CIS and Council Decision 2009/917/JHA establishes the former third pillar part of the CIS. The former first pillar part deals with cases such as customs fraud when importing agricultural products, while the former third pillar part deals e.g. with arms and drug trafficking.

The former first pillar part of the CIS has a SCG similar to the one for SIS II, while the former third pillar part still has a Joint Supervisory Authority (JSA) established under Article 25 of the CIS Decision. Article 26(3) of the CIS Decision establishes at least annual meeting between the EDPS and the CIS JSA, which are legally distinct from the SCG meetings.[6]

[5] The IMI Regulation replaced Commission Decision 2008/49/EC, the former legal basis for IMI.
[6] In the past, the CIS SCG meetings were implicitly treated to also be these meetings.

According to Article 26(1), the EDPS also has a role in supervising the former third pillar part of the CIS as regards "the activities of the Commission".

There are no periodic inspection obligations for the CIS, neither under the CIS Regulation nor under the CIS Decision.

The Commission is controller for CIS, which is run by OLAF, which not only hosts the system, but also has read access to it.

2.5.1 FIDE

The Customs Files Identification Database (FIDE) is an index of customs investigations in the different Member States. Its data fields are limited: name of the person/entity under investigation, subject area concerned, national reference number of the investigation, investigatory authority to contact for further information. The system can be searched via names only, allowing customs authorities in one MS to find out if the persons they are investigating are/have been also investigated in other MS.

Legally speaking FIDE is part of CIS. If no specific rules are defined, the rules for CIS apply accordingly (Article 41a of the CIS Regulation and Article 15 of the CIS Decision). As there are no specific rules on data protection supervision in Title Va of the CIS Regulation, the CIS SCG is also competent to discuss FIDE.

2.5.2 REX

The Registered Exporters System (REX) will be a database of registered exporters in third countries that qualify for preferential customs treatment. Norway and Switzerland grant similar preferential customs treatment to some third countries and will also make use of REX; Turkey may also start doing so in the future once it fulfils certain conditions.

Competent authorities in those third countries and in the Member States will send the registrations to the Commission, which will store them in a centralised database.

The legal bases for REX in that form are the amendments introduced in the Customs Code by Commission Implementing Regulation (EU) 2015/428.

Unlike for most of the other systems, there is no obligation for the EDPS to regularly organise meetings. In fact, the legal base for REX does not formally set up a SCG, but simply states that national DPAs and the EDPS shall work together, using similar wording as for SIS II (see Article 69c(8)).

REX as amended is scheduled to become operational on 1 January 2017. The Commission will be the controller and the system will be run by DG TAXUD.

2.6 European Database on Drug Precursors

The European database on drug precursors aims to control the trade in drug precursors (i.e. substances frequently used in the illicit manufacture of narcotic drugs and psychotropic substances). Operators using certain listed substances need to obtain a license/registration and need to register certain transactions with national competent authorities. It serves a number of purposes:

1) to facilitate reporting from Member States to the Commission - where possible in an aggregated and anonymised manner - of their measures to control drug precursors;

2) to create a European register of operators and users which have been granted a license or registration. This will include the name and contact information of the responsible contact point;

3) to enable operators to provide competent authorities with information about their transactions.

It is used by Member States authorities to report to the Commission, by licensed/registered operators to report transactions and by the Commission for monitoring purposes.

Its legal basis is Regulation (EC) 273/2004, as amended by Regulation (EU) 1258/2013. Personal data shall be included in the database only after the adoption of the delegated acts referred to in Articles 3(8) and 8(3) of this Regulation. Article 13b of Regulation 1258/2013 provides that the processing of personal data by the competent authorities in the MS shall be carried out in accordance with national laws/Directive 95/46/EC and under supervision of the supervisory authority of the MS; the processing of personal data by the Commission, including for the purpose of the European database, shall be carried out in accordance with Regulation 45/2001 and under supervision of the EDPS.

Unlike the other systems mentioned, the European database on drug precursors does not make specific mention of coordinated supervision; neither regular meetings nor regular inspections are mandatory.

The Commission is the controller for the European database on drug precursors which is managed by DG GROW.

3 The EDPS as Supervisor of the Central Systems

As explained in the preceding section, the EDPS is competent to supervise the central systems of the large-scale IT systems mentioned above. This section will explain how the EDPS will address its principal tasks as supervisory authority with reference to consultations, inspections, complaints and prior checks.

3.1 Consultations

According to Article 46(d) of the Regulation, the EDPS shall, either on its own initiative or on request "advise all [Union] institutions and bodies […] on all matters concerning the processing of personal data". Article 28(1) obliges EU institutions, bodies, offices and agencies of the Union ("EU Institutions", "EUIs") to inform the EDPS when drawing up administrative measures which relate to the processing of personal data. In line with the Policy Paper on Consultations in the field of Supervision and Enforcement, such requests for consultation should be channelled through the DPO of the relevant EUI.

In line with the accountability principle, controllers should pay proper attention to ensuring and documenting compliance with the Regulation; early internal consultation of the DPO can play a big part in achieving this. Internal advice by the DPO may often eliminate the need for further consultation of the EDPS. However, if a case is complex and/or novel, the EDPS should be consulted.

Given the nature of the activities of the management authorities, the questions submitted for consultation are likely to be at the border between technical and legal questions (e.g. up until which point operations by the management authorities on the central systems are covered by

their mandates to "maintain" the system). Answering such questions will require both technical and legal expertise, so cooperation between technical and legal experts is key.

Consultations in this field are often sensitive, as the activities of the management authorities (which the EDPS is consulted on) will often have an impact on Member States' interests (as users of the systems).

Replies to consultations that are relevant for the SCGs will be shared with the relevant SCG chair to assess further distribution to the relevant SCG.

3.2 Inspections

As explained above, there are regular inspection obligations in three of the systems. For SIS and VIS, it has to be ensured that an audit is carried out at least every four years, while for Eurodac, the obligation will be to have at least one audit every three years, starting from 20/07/15.

The EDPS will ensure that these audits happen by conducting them itself. In practical terms, this will result in inspections at eu-LISA (as management authority for SIS, VIS and Eurodac) almost every year, without prejudice to possible additional unplanned inspections. Inspections of one system may be combined with follow-up visits for systems that have been inspected before.

The scope of each inspection will be defined in accordance with the respective tasks of the management authority. This means e.g. that for SIS, the focus will be security and operational management, while the accuracy of the content is for Member States' DPAs to check. On the other hand, where EU IBOAs *use* a system, this use may be part of the inspection as well.

Inspections will be carried out in line with standard EDPS procedures as far as possible. Normally, EDPS inspection reports are not meant for sharing beyond the inspected EUIs. In standard EDPS inspection procedures, EUIs are requested to provide comments on the draft minutes of the inspection, but not on the final inspection report.

However, the legal bases for SIS, VIS and Eurodac establish that the management authority shall be given opportunity to comment before adoption of the report.[7] For SIS, VIS and Eurodac, the inspection obligations also mention that "a report" shall be made available to the management authority, the European Parliament, the Council, the Commission and national DPAs.

The current approach is to derogate from standard procedures in these two areas and to provide the full report for comments and to distribute it to the stakeholders mentioned above.

The EDPS will keep the relevant SCGs informed about inspections and share appropriate documentation.

3.3 Complaints

As explained in section 2 above, the actual use and filling of the systems is done by and under the responsibility of Member States. The EDPS is thus e.g. not competent to examine whether an alert of a specific person in the SIS is justified. This is a question for national DPAs and courts.

When receiving complaints for which it is not competent, the EDPS will refer the complainants to the relevant national authorities and supervisory authorities. Where it is not

[7] Articles 45(2) SIS Regulation, 61(2) SIS Decision, 42(2) VIS Regulation, 31(2) new Eurodac Regulation.

clear where to refer to, the designated EDPS member of the SCGs will liaise on working level with the relevant other members of the SCGs, taking confidentiality issues into account.

If a complaint is relevant for the central level (e.g. against a potential data breach that might have occurred on the central level or an alleged unlawful use of data by central unit) the EDPS may launch an investigation in accordance with standard procedures for complaints handling by the EDPS, in line with EDPS Rules of Procedure.[8] In such cases, the relevant SCGs will be kept informed in an appropriate way.

3.4 Prior Checks

IT systems with coordinated supervision do not necessarily fall under Article 27 of the Regulation. Given that the responsibilities are divided between the management authority and the Member States, it is an empirical question whether those parts for which the management authority is (co-)controller are subject to prior checking.

Where this is the case, prior checks are conducted in line with standard EDPS procedures.

3.5 Enforcement Measures

Where any of the supervision activities explained in this chapter require using enforcement measures, such as ordering rectification or imposing a ban, the EDPS will use its powers in accordance with its Policy Paper on Monitoring and Ensuring Compliance with Regulation (EC) 45/2001 (chapter 3). Again, the SCGs (via the chair) will be kept informed as relevant.

4 The EDPS as member of the SCGs

4.1 Role of the SCGs

As explained in chapter 2 above, the mandate of the SCGs is to "exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties of interpretation or application of this Regulation, study problems with the exercise of independent supervision or in the exercise of the rights of data subjects, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights".

It is therefore important to note how they differ from the former[9] and still existing[10] Joint Supervisory Authorities/Bodies (JSAs/JSBs). The JSAs/JSBs are/were collegiate supervisory authorities in their own right. For example, Eurojust is supervised by the Eurojust JSB *as a collective body*. SCGs, on the other hand, are *fora* for the different supervisory authorities *to cooperate and discuss*, but are not supervisory authorities in their own right: they cannot issue binding decisions.[11]

This means that while of course all members of the SCGs cooperate in order to arrive at a common understanding, the SCGs cannot override decisions taken by their members in the exercise of their supervisory powers regarding their sphere of competence; the standard wording on cooperation between DPAs and the EDPS "each acting within the scope of its respective competences" also stresses this point.

[8] See Articles 31 to 35 of the EDPS Rules of Procedure, OJ L 273/41, 15/10/2013
[9] Eurodac until 2004, SIS until April 2013
[10] Europol, Eurojust, CIS under the CIS Decision.
[11] Note the absence of any decision-making power in the legal bases of all SCGs.

4.2 Different Roles of EDPS in SCGs

EDPS staff is present at the SCGs in different roles:

1) As the secretariat, acting on instructions from the elected Chairs of the different SCGs. The secretariat prepares documents, takes minutes and ensures logistics for the meetings, including the reimbursement of travel expenses. It is provided by the Policy and Consultation Unit of the EDPS.[12] As mentioned in the introduction, this role is excluded from the scope of this document;

2) As a SCG member, representing the EDPS as supervisory authority of the central systems; members may also be elected Chair of the SCG. This role is provided by the Supervision and Enforcement Unit of the EDPS.[13]

A clear distinction between these roles is necessary to avoid misunderstandings by stakeholders and to clearly distribute responsibility in-house.

4.3 Representation in the SCGs

The EDPS as member of the SCGs will usually be represented on staff level.[14] A member of the Supervision and Enforcement unit will be designated as member of the SCGs. An ITP staff member will provide support on technical matters and will be designated as alternate member. Designations will be duly notified to the secretariats.

The EDPS as member may participate in subgroups established by SCGs where this could add value, including as rapporteur. For example, the EDPS actively participates in the Technical Experts subgroup of the SIS SCG and took the lead for one of its tasks (the so-called Data Security module of the Common Inspection framework).

4.4 Relationship with the SCG Chairs

The designated EDPS staff member will keep regular contact with the elected Chairs of the different SCGs, informing them about EDPS initiatives related to large-scale IT systems that may be relevant for the SCGs. The relevant secretariat will be kept in copy of all contacts with the SCG Chairs.

In these contacts, it will be made clear that they are interacting as the "EDPS as member" with the chair - the "EDPS as member" is not in a position to address e.g. how the SCG secretariat fulfils its tasks.

4.5 Information Sharing

The EDPS representatives in the SCGs follow an open and transparent approach towards the SCGs, sharing information as appropriate. Being transparent is important in order to build trust. On the other hand, each supervisory authority, including the EDPS, must remain able to exercise its powers independently. This means that sharing is strictly for information purposes only, unless indicated otherwise.

Examples of documents and activities that EDPS representative could share with the SCGs are:

[12] With support from the IT Policy sector where necessary.
[13] With support from the IT Policy sector where necessary.
[14] The representatives of Member States' DPAs present at the meeting tend to be by majority on staff level.

- Inspection reports (where not anyways mandated by legislation and unless inspected EUI objects), information on recommendations made and follow-up given;
- Replies to consultations that are also relevant for the SCGs;
- Information on complaints received (with relevant members);
- Other ongoing activities as deemed relevant (for information and/or input).

If in doubt whether a document is relevant for the whole group, the EDPS representative will share it with the Chair first, to obtain her/his views on wider distribution.

4.6 Joint Exercises

Joint exercises, such as coordinated inspections, are an important part of the activities of the SCGs.[15] Given that there is a difference between the tasks carried out by the authorities under supervision of national DPAs and by the management authorities under supervision of the EDPS, not all joint exercises will be relevant for the EDPS. For example, given that informing data subjects about alerts usually falls completely in the MS' competences, there would not be much need for an EDPS contribution here.

That being said, the EDPS will participate in such exercises where they are also relevant for the activities under its own supervision and will support the SCGs in their activities.

4.7 Cooperation on Specific Cases

There may be occasions where the EDPS and national DPAs will also need to cooperate on specific cases. Examples include information on referrals of complaints or the mediation procedures under Article 34(4) of the SIS II Regulation and Article 49(6) of the SIS II Decision.

5 Conclusion

The EDPS will participate as an active member in the SCGs, while respecting the mandates of national DPAs and exercising its own mandate in full independence. In the direct supervisory role of management authorities and controllers for large-scale IT systems, the EDPS will keep a close watch over the activities of the relevant EUIs.

[15] Schengen Evaluations, to which the EDPS may be invited as observer under Article 10(5) of Council Regulation 1053/2013 (OJ L 295, 6.11.2013, p. 27–37), are a related exercise, which, while not directly part of the SCG's activities, present a clear link to the use of VIS and SIS. For those exercises, the EDPS, where invited, will decide on a case-by-case basis whether to participate.