

Coordinated Supervision of VIS

Activity Report 2012-2014

Secretariat of the VIS Supervision Coordination Group
European Data Protection Supervisor
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, 1000 Brussels
email: EDPS-VIS@edps.europa.eu

Table of Contents

1. Introduction and background.....	3
2. Organisation of coordinated supervision.....	4
2.1. Main principles.....	4
2.2. The supervision coordination meetings.....	4
3. 2012-2014: Issues discussed and achievements.....	6
3.1. Common framework for inspections.....	6
3.2. Use of ESPs for the processing of visa applications.....	7
3.3. Questionnaires.....	8
4. Members' Reports.....	8
4.1. Austria.....	8
4.2. Belgium.....	9
4.3. Bulgaria.....	10
4.4. Croatia.....	10
4.5. Cyprus.....	11
4.6. Czech Republic.....	12
4.7. Denmark.....	13
4.8. EDPS.....	13
4.9. Estonia.....	14
4.10. Finland.....	15
4.11. France.....	15
4.12. Germany.....	16
4.13. Greece.....	17
4.14. Hungary.....	17
4.15. Iceland.....	19
4.16. Italy.....	19
4.17. Latvia.....	20
4.18. Liechtenstein.....	21
4.19. Lithuania.....	21
4.20. Luxembourg.....	22
4.21. Malta.....	23
4.22. Netherlands.....	23
4.23. Norway.....	24
4.24. Poland.....	25
4.25. Portugal.....	25
4.26. Romania.....	26
4.27. Slovak Republic.....	27
4.28. Slovenia.....	27
4.29. Spain.....	28
4.30. Sweden.....	29
4.31. Switzerland.....	30
5. What to expect next.....	31

1. Introduction and background

The Visa Information System ('VIS') is a system for the exchange of visa data between Member States created by Council Decision 2004/512/EC of 8 June 2004¹ as completed by Regulation 2008/767/EC of 9 July 2008² ('VIS Regulation').

As stated in Article 2 of the VIS Regulation, the purpose of the VIS is to facilitate the visa application procedure, prevent visa shopping and fraud, facilitate border checks as well as identity checks within the territory of the Member States and to contribute to the prevention of threats to the internal security of the Member States. To this end, the VIS provides a central repository of data on all short-stay Schengen visas. This data can be accessed by authorities issuing visas, e.g. consulates of Member States (Article 15), by checkpoints at the Schengen border to verify the identity of visa holders (Article 18), as well as for the purpose of identifying third-country nationals apprehended within the Schengen Area with fraudulent or without documents (Article 19).

The VIS Regulation sets out which data shall be included in the database at the various stages of processing a visa (application, issuing, discontinuation of examination, refusal, annulment/revocation, extension, Articles 9-14). Apart from data on the visa application (such as planned travel itinerary, inviting persons etc.) it also includes a photograph of the applicant and fingerprints (Article 9 (5) and (6)).

The architecture mirrors that of Eurodac and other large-scale IT systems: a central unit ('central VIS') managed by the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice³ ('eu-LISA') (Article 26) and connected to national units in the Member States using sTesta. Article 32 sets out a list of mandatory security measures for the national units to implement; the national implementation shall also provide for audit trails (Article 34) and possibilities for a self-audit (Article 34).

The retention period is 5 years (Article 23), starting from the following points in time:

- the expiry of the visa, if one has been issued and/or extended;
- the date of the creation of the application file in the VIS, in case an application has been withdrawn, closed or discontinued;
- the date of the decision of the visa authority, if a visa has been refused, annulled or revoked.

At the end of this period, the data shall be automatically deleted. Data shall be deleted before the end of these periods if a data subject acquires the nationality of a Member State. Audit trails shall be deleted one year after the data to which they refer has been deleted, unless they are used in a data protection investigation (Article 34).

¹ Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS), OJ L 213, 15.06.2004, p. 5.

² Regulation 2008/767/EC of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, OJ L 218, 13.8.2008, p. 60.

³ The Commission was responsible for the operational management of the VIS for a transitional period until the establishment of a new permanent IT Agency, eu-LISA, which became fully operational in December 2012.

The VIS first became operational in October 2011. The system was rolled out on a regional basis and is to date implemented in and stores the data of 16 out of the 23 world regions set out in three Commission decisions⁴, which represents around 30% of the visa applications worldwide. Further roll outs are ongoing and foreseen in the remaining regions.

The VIS is currently used by 30 countries, i.e. all Schengen States, all four European Free Trade Association ('EFTA') member states - Iceland, Liechtenstein, Norway, and Switzerland - and Bulgaria, Croatia, Cyprus and Romania that are not yet part of the Schengen Area but nonetheless have a visa policy based on the Schengen acquis. Ireland and the United Kingdom do not take part in the VIS (recitals 28-29).

As established in the VIS Regulation, the lawfulness of the processing of personal data by the Member States shall be monitored by the national Data Protection Authorities ('DPAs') (Article 41) and the European Data Protection Supervisor ('EDPS') is in charge for checking the compliance of the Management Authority (Article 42). In order to ensure a coordinated supervision of the VIS and the national systems, as provided for in Article 43, the VIS Supervision Coordination Group ('VIS SCG') was established. In the 2012-2014 period, the VIS SCG was Chaired by Mr Peter Hustinx (EDPS), while the Vice-Chair was Ms Vanna Palumbo (Italian DPA). The present document reports on the activities of the Group for this period.

2. Organisation of coordinated supervision

2.1. Main principles

The cooperation took the form of meetings held on a regular basis with all DPAs in charge of supervising the VIS at national level and the EDPS, acting together as VIS Supervision Coordination Group. The main purpose of these meetings was to discuss common problems related to supervision and find common solutions or approaches whenever possible. According to Article 5 of the Group's rules of procedure, these meetings shall take place at least twice a year. In practice, two meetings are held per year. The Commission and eu-LISA are also invited to parts of the meetings in order to update the Group on new developments regarding the VIS.

2.2. The supervision coordination meetings

In the period 2012-2014, five supervision coordination meetings have taken place on the following dates:

- 21 November 2012;
- 11 April 2013;

⁴ Commission Decision 2010/49/EC of 30 November 2009 determining the first regions for the start of operations of the Visa Information System (VIS), OJ L 23, 27.01.2010, p. 62; Commission Implementing Decision (2012/274/EU) of 24 April 2012 determining the second set of regions for the start of operations of the Visa Information System (VIS), OJ L 134, 24.05.2012, p. 20; Commission Implementing Decision 2013/493/EU of 30 September 2013 determining the third and last set of regions for the start of operations of the Visa Information System (VIS), OJ L 268, 10.10.2013, p. 13.

- 16 October 2013;
- 7 May 2014;
- 29 October 2014.

The meetings were held in the EDPS premises in Brussels, usually back-to-back with the Eurodac and SIS II SCG meetings in order to reduce the financial, travel and administrative burdens and to ensure consistent, horizontal supervision policies of those large-scale IT systems where possible.

Typically, the first part of the meeting is devoted to a presentation by the European Commission and eu-LISA on the status of the VIS roll-out and other recent developments that impact data protection. This helps to ensure that the Group is always up-to-date on recent developments in order to ensure effective supervision. The second part is devoted to discussions between DPAs on issues that are in need of checking at national level or on new developments of interest for VIS supervisors.

The following paragraphs quickly recapitulate the topics discussed and actions taken at the five meetings. A more detailed description of selected actions will follow in section 3 of this report.

Meeting on 21 November 2012

During its first meeting, the new VIS SCG discussed its first drafts of the Rules of procedure and of the Working Programme for 2013-2014. The Commission gave a presentation on the state of play of the VIS roll-out, its position regarding data protection and the state of development and the involvement of the new IT agency. The EDPS presented a report on the follow-up of the Commission implementation plan regarding the 2011 inspection of the VIS central unit by the EDPS. The Group also shared relevant national experiences and the Swiss DPA gave a presentation on the inspections they had performed at the visa sections of Swiss representations in various countries.

Meeting on 11 April 2013

The Group adopted its Rules of Procedure and the Working Programme for 2013-2014. The Group discussed the status of Ireland and the United Kingdom and agreed to invite them as observers in future meetings. Eu-LISA updated the Group on the state of play of the VIS roll-out and answered questions asked by Group Members regarding the impact of the move to the IT agency on the VIS system. The Group also shared relevant national experiences, including on inspections.

Meeting on 16 October 2013

The Commission and eu-LISA updated the Group on the state of play of the VIS roll-out and other recent developments. The Group discussed the long term perspective of supervising the VIS and identified several issues to follow up, such as the list of authorities having access to the VIS, access to VIS data for law enforcement purposes and the exercise of data subjects' rights. A Subgroup was created in order to explore the data protection implications of the use of External Service Providers ('ESPs') by Member States for the processing of visa applications. The Group had a first discussion on the need to develop a common framework for inspections, the possibility of conducting joint investigations for countries that issue visas

together in several third countries, and on the feasibility of a similar format of inspections to be used in auditing other large-scale IT systems. Finally, the Members shared relevant information about national inspections in the different Member States.

Meeting on 7 May 2014

The Commission and eu-LISA updated the Group on the state of play of the VIS roll-out and other recent developments regarding the quality of the data in the system. The representative of the Spanish DPA presented a first input for a quality exercise at national level. The ESPs Subgroup presented a first analysis of technical and legal issues related to the use of ESPs for the processing of visa applications, including the question of jurisdiction, and reflected on the minimum conditions to be inserted in the contracts between Member States and subcontractors. The Group adopted three questionnaires respectively on the list of authorities having access to the VIS, on access to VIS data for law enforcement purposes and on the exercise of data subjects' rights. The Group also adopted a note on the way forward for a common framework for inspections. Finally, the Members shared relevant information about developments at national level, including inspections.

Meeting on 29 October 2014

The Commission and eu-LISA updated the Group on the state of play of the VIS roll-out and other recent developments regarding the quality of data in the system, the mechanism to keep track of such quality and how the envisaged Visa Code⁵ provisions on ESPs could have impact on the collection of fingerprints. The representative of the Spanish DPA gave a presentation on different aspects of data quality (e.g. the current status of the BMS quality assurance system, logs, ESPs). The Subgroup on subcontractors presented a note on the analysis of technical and legal issues related to the use of subcontractors for the processing of visa applications, including questions of jurisdiction. The Group took note of the first results of the three questionnaires circulated respectively on the list of authorities having access to the VIS, on access to VIS data for law enforcement purposes and on the exercise of data subjects' rights. The Fundamental Rights Agency invited to the meeting gave a presentation on a biometric project. Finally, the Members shared relevant information about developments at national level, including inspections.

3. 2012-2014: Issues discussed and achievements

3.1. Common framework for inspections

According to the VIS Work Programme for 2013-2014, the development of a possible common framework for inspections/audits - at least along main lines - has been foreseen as one of the main exercises to be started and carried out by the Group. Under the VIS Regulation, national DPAs shall carry out an audit of the data processing operations in the national systems in their Member State every four years; similarly, the EDPS shall audit the central unit every four years (Articles 41(2) and 42(2)). A coordinated preparation of these audits by the Group would allow for more effectiveness and harmonised results.

⁵ Regulation (EC) 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code), OJ L 243, 15.09.2009, p. 1.

The methodology agreed on by the Group in the Work Programme was to discuss the nature, scope and content of such a framework within the Group, while taking into account relevant experience with the Eurodac system in this context. The proposed common framework could include, as a minimum, a list of relevant questions that will have to be answered during the inspection, a procedure for exchanging relevant information and follow-up of inspections and deadlines that should be respected.

Taking into account the VIS features but also the similar work already existing for the Eurodac system, the VIS SCG Secretariat, along with the Vice-Chair and the DPA from Spain, prepared a first note on the possible way forward on a common framework for inspections, which was presented to the Group. This note suggests agreeing on a general outline, which is to be specified in stages, based on national experience and the Group's preference, and underlines that it would make much sense in that context to build on modules which are already in the making (such as focusing on subjects related to data security, consulates and subcontractors).

Eu-LISA also advised the Group on what issues should be looked at more closely (e.g. data quality and the availability of the network) and pointed out several reports (e.g. incident reports) that were made available to Member States and would be an interesting input for the Group.

3.2. Use of ESPs for the processing of visa applications

The collection and further processing of biometric data occupy a central place in the VIS system. The processing of such data poses specific challenges and creates risks which have to be addressed. In this context, the recourse to External Service Providers ('ESPs') for the collection of visa applications becomes more common as consulates of the Member States do not have the capacities to handle the collection of high volumes of applications in acceptable delays themselves. A Subgroup composed of representatives of the German, Italian, Maltese, Swiss and Swedish DPAs was established in order to explore the data protection implications of the use of ESPs by the Member States.

The Subgroup presented a first note on the analysis of technical and legal issues related to the use of subcontractors for the processing of visa applications. The note addresses the relevant legal basis for the cooperation with ESPs, the tasks that can be laid out to an ESP, the minimum requirements that should be included in contracts with ESPs (i.e. the existing requirements listed in Annex 10 of the Visa Code and suggestions of additional requirements), the supervision of ESPs' processing of personal data by Member States, or possibly by DPAs, and the enforcement of Member States' instructions in terms of data protection compliance. To conclude, the note recommends *inter alia* elaborating a model contract to facilitate contractual agreements between Member States and ESPs.

The ESPs Subgroup will continue to work on this subject and the VIS SCG will get in touch with the Commission, to which Member States have to submit contracts with ESPs upon conclusion, in order to check more closely these contracts. In parallel, the DPAs will start looking at national level on how such contracts are being used, which will allow the Subgroup to enrich its note with more empirical findings.

3.3. Questionnaires

One of the main risks of the VIS from a data protection perspective is that it is a much bigger database than Eurodac, with many more authorities having access to the system for specific purposes and quite often outside of EU territory (e.g. consular posts). According to its Work Programme for 2013-2014, the VIS SCG decided to further evaluate what is happening at national level by exploring, *inter alia*, which authorities have in fact access to the system, if there are any other authorities apart from those already mentioned in the lists of authorities having access to the VIS notified by Member States and how it is actually carried out. Therefore, two questionnaires containing basic questions with regard to these issues were circulated with the Group in summer 2014:

- 1) A questionnaire on authorities having access to the VIS addressed to DPAs;
- 2) A questionnaire on access to VIS data for purposes of law enforcement, which is split into two parts, one for the central access point(s) and one for the DPA.

The VIS SCG also decided to further investigate how data subjects' rights are implemented in practice. Therefore, a third questionnaire on data subjects' rights was circulated at the same time with the Group. Granting rights to data subjects is an important part of data protection law. Ensuring that data subjects can access, correct and contest data held about them increases the transparency of data processing for them, helps to uncover unlawful processing and increases data quality for lawful processing. These considerations are all the more relevant in a field such as visa applications, where compliance with the legal framework is especially important given the adverse consequences unlawful processing might have here.

The Secretariat collected and collated the replies received to those three questionnaires, based upon which a short synthesis note was prepared. The preliminary findings showed no major problems at national level but all contributions are needed in order to have a comprehensive view on these issues. This exercise is still ongoing and is to be finalised in 2015.

4. Members' Reports

4.1. Austria

- Overview: state of play and developments

There were no problems reported neither by the Ministry of Interior and the Ministry of Foreign affairs, nor by a data subject. The Austrian DPA is part of the VIS SCG. A VIS inspection is planned to be carried out by the Austrian DPA starting in September 2015 and including an onsite inspection of a consular office.

- Inspections

There was no inspection of the national VIS systems carried out by the Austrian DPA in the reporting period of 2012-2014.

- **Complaints**

There were no complaints filed with the Austrian DPA in the reporting period of 2012-2014.

- **Remarks**

/

4.2. Belgium

- **Overview: state of play and developments**

The Visa Code provides that consulates of Member States examine the visa requests for a transit or a short stay within the Schengen area. It also foresees the possibility to collaborate with an ESP. In this regard, the Federal Public Service Foreign Affairs in Belgium has addressed to the Belgian DPA a draft statement of work on the outsourcing of visa services for Belgian diplomatic and consular posts for opinion. The Belgian DPA issued its opinion n°57/2014 on 5 November 2014, which was published on the DPA's website (www.privacycommission.be).

- **Inspections**

The Belgian DPA has carried out an inspection in an embassy every year since 2012. The embassies of Casablanca and London were inspected respectively in 2013 and 2014 and several recommendations were issued.

The VIS SCG Work Programme 2015-2018 foresees the development of a common framework for inspections/audits as one of the main exercises to be carried out by the Group. The aim is to elaborate a common European approach for the compulsory audit of the VIS system, which has to be carried out every four years according to the VIS Regulation. The Belgian DPA has not performed this audit yet, *inter alia* because it waits for the elaboration of the abovementioned common framework. Nevertheless, the Belgian DPA has – on top of the embassy inspections mentioned above – carried out a first inspection of the national VIS system, including at the Federal Public Service Foreign Affairs and at the Federal Public Service Interior in Autumn 2014. Follow-up to this inspection is ongoing.

- **Complaints**

The Belgian DPA keeps statistics of all complaints but has not received complaints related to the VIS so far.

- **Remarks**

/

4.3. Bulgaria

- Overview: state of play and developments

Despite the full technical readiness and a successful evaluation, Bulgaria is not allowed to use the VIS due to the fact that the Council has not yet decide on the full implementation of the Schengen acquis and the lifting of controls at the internal borders with Bulgaria and Romania. In this context, Bulgaria continues to use a National Visa Information System ('NVIS') for visa issuances and related checks of third country nationals.

- Inspections

The Bulgarian DPA performs regular supervision of the activities of the NVIS. In March 2013, an inspection of the NVIS was conducted in order to check the implementation of the recommendations from the previous inspection performed in 2011, to assess the latest developments of the regulatory framework, the IT and other technical equipment of the system and to provide follow-up to possible complaints.

The inspection team concluded that the Bulgarian Ministry of Foreign Affairs, as the data controller of the NVIS, had taken the necessary steps to implement the recommendations of the Bulgarian DPA to review regularly, on a monthly basis, the log files of the access and other activities of the competent authorities in the NVIS. The Bulgarian DPA also used this occasion to present and discuss with the Ministry of Foreign Affairs the recently adopted Ordinance n°1 of 30 January 2013 on the minimum level of technical and organisational measures and the admissible type of personal data protection.

The Bulgarian DPA will continue the supervision of the NVIS in order to ensure full compliance with the relevant national and EU data protection rules. In 2015, it will perform inspections on the spot of three Bulgarian consular offices. Special attention will be paid to the role of ESPs in the process of visa issuance.

- Complaints

/

- Remarks

/

4.4. Croatia

- Overview: state of play and developments

On 21 March 2013, the Croatian Government adopted a Regulation on the Croatian Visa Information System ('CVIS'), which stipulates that the Croatian DPA independently monitors the lawfulness of data processing at least every four years in order to ensure that the control procedures of data processing are performed in accordance with the relevant international regulatory standards, and that the Croatian DPA will provide the necessary funds to perform those tasks.

End 2014, a joint coordination group was established with members from both the Croatian DPA and the Ministry of Foreign and European Affairs ('MFEA') to discuss the legal and technical implications for the protection of personal data in the VIS. The Croatian Personal Data Protection Act is *lex generalis* but the Regulation on the CVIS is considered as fundamental and relevant for the CVIS. It was also concluded that representatives of the Croatian DPA, in the context of educational activities entitled "Improving the Schengen skills and knowledge of the consular staff" organised by the MFEA, will maintain lectures related to the protection of personal data in general but also with regard to the protection of personal data in the context of CVIS, as it was done at the beginning of 2015.

- **Inspections**

In 2014, no direct controls in diplomatic missions and consular offices were performed by the Croatian DPA due to budgetary constraints. In 2015, control activities are planned to be performed as prescribed by the Regulation on the CVIS.

- **Complaints**

/

- **Remarks**

/

4.5. Cyprus

- **Overview: state of play and developments**

To date the VIS has been installed in 51 embassies, high commissions and points of entry (i.e. airports, ports and marinas). In Damascus (Syria) and Tripoli (Libya), the system is installed but not operable due to the suspension of those embassies' operations and functions. In Beijing, Teheran and Doha, the system is installed but not connected to the central VIS database at the Ministry of Foreign Affairs due to poor internet connection.

The installation of the VIS is planned in five District Police Migration Offices.

The VIS is currently used at national level for the issuance of visas that are valid within the territory of Cyprus. Concurrently every effort is made to comply with the EU requirements. Compliance with the central VIS is being tested through the pre-production and playground environments of EU using test data.

The main servers and databases of the system are located at the headquarters of the Ministry of Foreign Affairs. Each of the above points of issuance are equipped with stations, which are connected via secure VPNs - over the government network - dedicated to the system, in order to exchange data with the central servers. Data from the Cypress VIS to the central VIS and *vice versa* are exchanged through a secured network provided and supported by the EU.

- **Inspections**

/

- **Complaints**

/

- **Remarks**

/

4.6. Czech Republic

- **Overview: state of play and developments**

The Czech DPA actively participated in activities connected with the supervision of Schengen cooperation. As supervisory authority in Czech Republic, the Czech DPA ensured compliance with the relevant legislation, in particular for the protection of data subjects whose personal data are processed within the Schengen area.

- **Inspections**

Between 2012 and 2014, the Czech DPA performed series of inspections in Czech embassies in relation to the processing of personal data in the VIS. In 2014, the Czech DPA examined the activities of the Czech Ministry of Foreign Affairs, which is one of the data controllers. Although the Czech DPA did not uncover any breach of obligations under the Czech Data Protection Act by the Ministry of Foreign Affairs, it pointed out some problematic aspects with regard to the processing of personal data, such as the outsourcing of services to private companies.

In addition, the Czech DPA performed several inspections at consular departments of Czech embassies, namely in Kiev, Rabat, Belgrade, Moscow, Cairo, Istanbul and Astana.

- **Complaints**

The Czech DPA receives a great number of inquiries related to the visa policy of Czech Republic (precisely 66 in 2014), which rather fall within the scope of competences of the Czech Ministry of Foreign Affairs. Therefore, the Czech DPA clarified the division of powers in the visa sector, informed the ways to contact the Czech Ministry of Foreign Affairs and explained its supervisory competences.

The Czech DPA has not received relevant complaints related to data processing in the VIS from data subjects so far.

- **Remarks**

With regard to the activities of the Czech DPA between 2012 and 2014, it is necessary to highlight the relation between consular departments of Czech embassies and private outsourcing companies that act as data processors. Besides their other activities, these private companies receive applications for visas in the Schengen area, followed by the scanning of applicants' fingerprints, and deal with the subsequent distribution of personal data to embassies of Czech Republic. The Czech Ministry of Foreign Affairs is involved in this relation only in the Russian Federation. During an inspection conducted in 2014, the Czech DPA discovered that the cooperation with private companies will be further expanded in other countries. Since these companies act as data processors, the Ministry of Foreign Affairs is obliged to ensure strict compliance with the obligations arising from data protection law

and conclude contracts with them that include *inter alia* guarantees of technical and organizational measures to secure the personal data processed.

4.7. Denmark

- **Overview: state of play and developments**

/

- **Inspections**

The Danish DPA did not conduct direct inspections regarding the VIS. However the Danish DPA performed an inspection regarding the Schengen Information System ('SIS') at the Danish Embassy in Kiev on 6 March 2012 and the one in London on 30 September 2014. On this occasion, the Danish DPA found out that the embassies had a so-called "local restriction list" as part of the exchange of information in local Schengen cooperation. The list contains information on specific individual cases mentioning applicants' personal data. When a person applies for a visa, the applicant is compared to the local restriction list.

The Danish DPA asked the Danish Ministry of Justice whether the local restriction list falls within the scope of the Visa Code article 48(3), paragraph b. After discussing the local restriction list at a meeting of the Visa Committee on 12 November 2014 at the Commission, the Ministry answered that Member States cannot establish such local visa ban lists as it was never the intention of the Visa Code. Visas can only be refused on the basis of the refusal grounds set out in the Visa Code. A Member State who wants to impose a travel ban on a given person has to insert an alert in the SIS to that end. The Danish DPA will probably submit remarks to the Ministry of Foreign Affairs on that basis. However, where the VIS is operational, Member States have access to information on reasons for formal refusals, including information on the refusal ground (e.g. false or counterfeit travel document or false information). Therefore the need to exchange information on such specific cases will diminish.

- **Complaints**

The Danish DPA has not received complaints regarding personal data processing in the VIS during the reporting period.

- **Remarks**

/

4.8. EDPS

- **Overview: state of play and developments**

As the supervisory authority for eu-LISA, the EDPS was in contact with eu-LISA on a number of occasions, both on working and management levels.

Interactions with eu-LISA have increased since the establishment of the DPO function. The EDPS seeks to provide guidance where necessary, but also stresses the principle of accountability in its interactions with eu-LISA.

- **Inspections**

On 1 June 2012, the EDPS adopted the report of the security audit carried out under Article 42(2) of the VIS Regulation. The on-the-spot parts had been carried out before the reporting period, in July and November 2011 at the main site in Strasbourg (France) and at the backup site in Sankt Johann im Pongau (Austria). The report contained a number of recommendations and an implementation plan. Although a number of recommendations have been closed, follow-up was still ongoing at the end of 2014.

- **Complaints**

Given the role of the central system, complaints against the processing of personal data in the VIS will most likely be directed against processing under the responsibility of the Member States. Between 2012 and 2014, the EDPS has not received such complaints. If this were to happen, complainants would be referred to the relevant national DPA. Only complaints related to processing by the central unit would be relevant for the EDPS.

- **Remarks**

The EDPS has been invited to meetings of the VIS Advisory Group, but declined. The reason was that the Advisory Group takes decisions about the management of the VIS and that EDPS presence there could lead to conflicts of interest for the EDPS' supervisory role.

4.9. Estonia

- **Overview: state of play and developments**

The Estonian DPA had regular activities within the VIS SCG and a supervisory and consultative role at national level for authorities and public.

- **Inspections**

The Estonian DPA carried out several supervisory activities regarding data processing in visa issuance between 2012 and 2014.

The Estonian DPA carried out on-the-spot inspections at the Estonian consulate in Kiev (Ukraine), where it checked *inter alia* workflow, access rights, document management and ESPs. The outcome was that the VIS SCG should jointly analyze the question of ESPs and this process is currently ongoing.

One solution that the Estonian DPA and the Estonian Ministry of Foreign Affairs agreed on was the preparation of a questionnaire on personal data processing addressed to consulates. As the Ministry of Foreign Affairs regularly inspects all Estonian consulates, they also use this questionnaire. Reporting these results to the Estonian DPA allows planning inspection activities by risk assessment.

- **Complaints**

/

- **Remarks**

/

4.10. Finland

- **Overview: state of play and developments**

The national competent authority reported that the VIS functioned satisfactorily and that no major problems occurred. The Finnish DPA neither received any indication of shortcomings regarding data protection issues in the VIS.

- **Inspections**

The inspection of the VIS according to Article 41 of the VIS Regulation started in Autumn 2014 and is expected to be finished in early 2015.

- **Complaints**

The Finnish DPA has not received any complaints regarding data processing in the VIS.

- **Remarks**

/

4.11. France

- **Overview: state of play and developments**

The VIS is used for the examination of requests for short stay visas and decisions to refuse, extend, cancel or revoke a visa. It is also used to facilitate the verifications and identifications of visa applicants.

In France, the Ministry of Interior and the Ministry of Foreign Affairs and International Development share competences with regard to the common visa policy. Today, the VIS contains three data processing systems: the Global Virtual Network system of visas (RMV2), the VISABIO system and the VIS. These three systems have been interoperable since the VIS was launched at national level, through the NVIS exchange platform.

- **Inspections**

In 2012, several on-site inspections were carried out in order to check the compliance with the applicable French data protection act (Act 78-17 of January 6, 1978, as amended) of data processing set up by the Ministry of Foreign Affairs to deliver visas. A particular focus was put on the outsourcing of some of the missions normally carried out by the consular posts to subcontractors.

In 2015, on-site inspections were also carried out in order to check the compliance of data processed within the VIS with the VIS Regulation.

- **Complaints**

To date, the French DPA has not received any complaints concerning the VIS.

- **Remarks**

On the basis of these findings, comments were submitted by the French DPA to the aforementioned competent authorities on the faculty, for the consular posts, to outsource part of their activities to subcontractors and, in particular, the collection of visa applicants' biometric identifiers. These inspections allowed noticing that the vast majority of security measures (physical, logical and organizational) are effectively being implemented by the consular posts and the competent Ministries. The implementation of strict supervision and control measures (on site or remotely) on the contractor's activity was also found.

However, it remains necessary to take particular care of this specific modality of data collection and to maintain efforts aimed at improving the overall security.

Finally, a special attention should be given to the information provided for under Article 32 of Law No 78-17 of 6 January 1978 amended and to the articulation of responsibilities between the Ministry of Interior and the Ministry of Foreign Affairs and International development.

4.12. Germany

- **Overview: state of play and developments**

Germany has established the use of the VIS in embassies and consulates abroad according to the roll-out plan set up by the European Commission. It is not an early adopter in areas to be covered by a later roll-out phase.

Worldwide, German embassies and consulates examine about 2-2.5 million visa applications each year.

- **Inspections**

On-site inspections scheduled for 2015 were prepared in the reporting period.

A visit at the Federal Administration Office (Bundesverwaltungsamt - 'BVA'), which is in charge of running the national visa database and of providing the national interface to the Central Unit of the VIS on behalf of the Ministry of Foreign Affairs in Germany, was conducted in order to discuss the overall design of data flows in the process of handling visa applications and to gain an overview on the interaction of various databases.

- **Complaints**

A low number of access requests and complaints were lodged at the German DPA (federal). The access requests were forwarded to and answered by the BVA. The complaints proved not to be relevant with regard to data protection issues.

- **Remarks**

The subcontractor issue (ESP according to Article 43 of the Visa Code) was discussed with the Ministry of Foreign Affairs in Germany in order to maintain data protection friendly solutions and to stress the necessity of strong privacy safeguards. It appeared that there was an increasing demand for the use of ESPs, given the rising numbers of visa applications in specific countries.

Moreover, vis-à-vis the Federal Ministry of Interior different ways on how to (better) implement the provisions on advance deletion of VIS data according to Article 25 of the VIS Regulation were mentioned.

4.13. Greece

- **Overview: state of play and developments**

The Hellenic DPA is the supervising authority in relation to the operation of the national part of the VIS and the lawfulness of the relevant data processing, as provided by Article 41 of the VIS Regulation and (Hellenic) Law 2472/1997 on data protection.

- **Inspections**

The Hellenic DPA has not performed any inspection in the 2012-2014 reporting period of the national VIS at the Hellenic Ministry of Foreign Affairs, which is the data controller. Moreover, due to financial restraints no *in situ* audits were performed with regard to the Hellenic embassies and consular offices.

- **Complaints**

So far, the Hellenic DPA has not received any complaints regarding personal data processing in the VIS.

- **Remarks**

/

4.14. Hungary

- **Overview: state of play and developments**

The Hungarian DPA has taken part in the VIS SCG since its foundation on 1st January 2012. During the past two years the colleagues of the Hungarian DPA took an active part in the

meetings of the VIS SCG and contributed to the documents adopted by the SCG mainly by using their experience at national level.

- **Inspections**

The Hungarian DPA continued the inspection of foreign representations in relation to the use of the VIS database. It performed the inspection of the Embassy in Belgrade and Chisinau.

- **Complaints**

The Hungarian DPA handled several access requests to the VIS at national level. The main findings were shared with other Members of the VIS SCG.

- **Remarks**

The most important contributions of the Hungarian DPA were the followings in the past two years during the VIS SCG meetings.

In 2012, the Hungarian DPA reported about the supervision of the Hungarian foreign representations in Bregovo, Kiev and Moscow in the context of the inspection of the VIS national system.

In 2013, the Hungarian DPA suggested to the VIS SCG to build into its two years period programme the joint inspection of foreign representations and local consular cooperation from a data protection point of view. Furthermore, the Hungarian DPA suggested the overview of the question of access rights and of the legal basis and legality in the context of the access of national authorities to the central VIS system.

In 2014, the VIS CSG discussed the data protection issues of outsourcing the handling of visa applications, in particular the legal base, control, enforceability of obligations arising from contracts, data retention and applicable law. The Hungarian DPA pointed out during the debate that data protection must be ensured at European level by the contracting companies especially in countries where the law enforcement authorities can have access to every database and electronic register within the territory of the country for the purpose of combating terrorism and serious international crimes (US, India, China, Russia, etc). The Hungarian DPA furthermore urged for more consistency and precaution in the field of biometric data processing in the VIS as the concerns raised and shared among the group were significant. The Hungarian DPA among others suggested raising awareness on maintaining an adequate level of data quality.

The VIS SCG adopted the questionnaires on data subjects' rights and the one on access by law enforcement authorities. The Hungarian DPA urged that the VIS SCG should expand its joint inspection to the so-called Local Consular Cooperation because there is significant data processing going on and all Member States and representatives of the European Commission are taking part in it.

4.15. Iceland

- **Overview: state of play and developments**

The VIS system has been made accessible to Icelandic immigration authorities.

- **Inspections**

As of yet, the Icelandic DPA has not carried out inspections with regard to the VIS due to a lack of resources. However, the DPA is now in the process of gathering information from the relevant authorities asking for information on their processing of VIS data. When answers are received, the DPA will decide on the next steps, including whether an audit operation is needed.

- **Complaints**

No complaints have been received as of yet.

- **Remarks**

/

4.16. Italy

- **Overview: state of play and developments**

In Italy, the Ministry of Interior and the Ministry for Foreign Affairs share competences with regard to the establishment and use of the VIS. In particular the Ministry of Interior is responsible for access by immigration and asylum authorities under the VIS Regulation and for law enforcement authorities' access to the VIS under the Council Decision. Specific internal provisions have been adopted in implementing the VIS Regulation and Decision at national level, in order to clarify roles and responsibilities as regards the processing of personal data in the system. No specific resources were allocated to the Italian DPA for the supervision of the VIS (as well as SIS II and Eurodac).

Apparently the system is running as planned and no specific problems are reported either by the Ministry of Interior or the Ministry for Foreign affairs. No complaints have been received so far from data subjects.

The Italian DPA as part of the VIS SCG is conducting checks on access to the system and on the exercise of data subjects' rights. Particular attention is given to the role of ESPs, since the visa procedure relies largely on service providers.

An inspection on some consulates is planned to be carried out in 2015.

- **Inspections**

No inspections of the national VIS systems were carried out by the Italian DPA in the 2012-2014 reporting period.

- **Complaints**

The Italian DPA has not received any complaints related to data processing in the VIS so far.

In the past it did receive complaints/appeals against the refusal of visas, which actually fell within the scope of competences of the Ministry for Foreign Affairs. Therefore, the Italian DPA clarified the division of powers in the visa sector, informed on how to contact the Ministry for Foreign Affairs and explained its supervisory competences.

- **Remarks**

A possible overlap of procedures seems to exist when a visa is refused on the basis of a Schengen alert, since the rights of rectification, deletion etc. cannot be exercised in respect of the refusal and given that the data subject must lodge an appeal against the visa refusal before the competent administrative court in Italy (TAR of Latium) only.

4.17. Latvia

- **Overview: state of play and developments**

Within the time frame 2012-2014, the major development could be considered the achievement of the Latvian DPA (the Data State Inspectorate of Latvia) - finally receiving budgetary resources from the State budget for the supervision of the VIS (that budget was allocated on 1 January 2015 for the supervision of the SIS, the VIS and Eurodac). As up to then, there had been no budgetary resources allocated for this function. Thus, since 2015, the supervision of the VIS could be carried out in a more effective way.

There has been no major development regarding the legislation that concerns the VIS.

- **Inspections**

The supervision activities carried out regarding the VIS were related to the inspections carried out regarding the SIS. Up to now, no major problems were concluded during those inspections. However the need for public awareness and informative activities has been concluded. Therefore several informative meetings have taken place in order to inform the users of the VIS regarding the personal data protection principles.

- **Complaints**

There have been no complaints received regarding the VIS.

- **Remarks**

/

4.18. Liechtenstein

- Overview: state of play and developments

Liechtenstein joined the Schengen area in December 2011. The VIS Regulation has been implemented in 2011 into Liechtenstein law through a Visa-Information System-Ordinance⁶. The National Police has a limited access in order to verify the authenticity of visas. The competent authority, the Migration and Passport Office, only deals with a small amount of visa applications. The applications are gathered at the Swiss consulates and then forwarded to the Liechtenstein authorities. The vast amount of visa processing at the competent authority is visa extensions.

- Inspections

In connection with inspections and audits the DPA will stick to the inspections and audits coordinated by the VIS SCG. In this matter the Liechtenstein DPA forwarded three questionnaires regarding the access to VIS data, access of law enforcement authorities to VIS data and data subject's rights to the competent authority.

- Complaints

To date, no requests for information, deletion and correction were claimed neither at the Migration and Passport Office nor at the Liechtenstein DPA.

- Remarks

/

4.19. Lithuania

- Overview: state of play and developments

In 2014, the Lithuanian DPA, the State Data Protection Inspectorate, renewed established relations with competent institutions in order to exchange information on data protection aspects issuing visas. Meetings between the State Data Protection Inspectorate and representatives of competent institutions: Ministry of the Interior of the Republic of Lithuania, Information Technology and Communications Department under the Ministry of the Interior, the Migration Department under the Ministry of the Interior were organized. During the meetings, issues related to processing of personal data of persons submitting visa applications in the VIS, implementation of data subjects' rights (publishing or updating necessary information on websites of competent institutions) were discussed. In order to maintain close relations with competent institutions and continuous exchange of best practices, knowledge, necessary information the parties designated contact persons for VIS issues. Taking into account information collected, key aspects to ensure data protection compliance, the State Data Protection Inspectorate issued preventive inspections plan for 2015.

⁶ LGBI 152.206; Visa-Informationssystem-Verordnung.

- / - **Inspections**
- / - **Complaints**
- / - **Remarks**
- /

4.20. Luxembourg

- **Overview: state of play and developments**

The Luxembourgish data protection law provides for two supervisory authorities:

- one general DPA, namely the 'Commission nationale pour la protection des données' (or 'CNDP');
- one specific supervisory authority, which was set up by article 17 of the Luxembourgish data protection law and has exclusive competence to monitor and supervise the processing of personal data carried out by the Police force, the Customs authority, the Intelligence Service and the Army. This authority is made up of three members, namely the Attorney General or his deputy who acts as its chairman and two members of the Luxembourgish DPA.

As a consequence two different supervisory authorities are competent for the monitoring of the use of the VIS data. The general Luxembourgish DPA is competent for supervising the access to VIS data by the Ministry of Foreign and European Affairs, the embassies and the consulates, whereas the specific supervisory authority set up by Article 17 is competent for supervising the access to VIS data by the law enforcement authorities.

- **Inspections**

No formalized controls or audits have been carried out during the period covered by this Activity Report. Both supervisory authorities decided to wait for the common framework for inspections to be adopted by the VIS SCG in order to carry out an in depth audit. However both supervisory authorities have held regular meetings with the authorities having access to VIS data in order to check compliance of their use of data.

- **Complaints**

Nor the general Luxembourgish DPA neither the specific supervisory authority set up by Article 17 have received any complaints between 2012 and 2014 concerning VIS related matters.

- **Remarks**
- /

4.21. Malta

- Overview: state of play and developments

Malta is implementing the biometric part of the VIS in parallel with the EU. No specific problems were reported by the Ministry after the kick-start of the VIS and the quality of fingerprints in general was considered optimal. The system functionalities replicate more or less the central VIS. The concept for providing access to the different authorities follows the same standards. Different profiles, roles, and hierarchies may be created according to the powers and functions of the entity having access to the VIS in line with the VIS Regulation.

Although no specific laws were enacted to complement the VIS Regulation, its provisions are followed given that such Regulation is directly applicable. There has been a specific amendment in the Immigration Act in order to establish an independent appeal body in cases of visa refusals. The inclusion of an independent appeal body was a recommendation issued by the Maltese DPA as part of its prior-checking exercise carried out before the implementation of the VIS.

- Inspections

No inspections were carried out during the period under review. However, before the introduction of the new VIS, a prior-checking exercise was carried out. As part of this prior-checking exercise, two visits at the Ministry for Foreign Affairs were organised, with a view to assess the overall functioning of the VIS and in particular the biometric data capture. In addition, the Maltese DPA conducted an on-site inspection at two consular offices and at the air border control.

- Complaints

No complaints were received during the period under review.

- Remarks

/

4.22. Netherlands

- Overview: state of play and developments

In October 2015, the Dutch DPA expects the results from the NVIS audit as mentioned in Article 41(2) of the VIS regulation, which is carried out by the Ministry of Foreign Affairs.

A trial audit in order to prepare for the NVIS audit was initiated by the Ministry of Foreign Affairs in 2014.

- Inspections

In the reporting period 2012-2014, no inspection of the content of VIS data has been carried out by the Dutch DPA.

- **Complaints**

No complaints have been received in the reporting period of 2012-2014

- **Remarks**

/

4.23. Norway

- **Overview: state of play and developments**

Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code), as amended by Regulation (EU) No 154/2012 and Regulation (EU) No 610/2013 is incorporated into the Norwegian Immigration Regulation (FOR-2009-10-15-1286). This Regulation entered into force on the 1st of January 2010. The Norwegian Immigration Authority ('UDI') is the data controller for the national part of the system, NorVIS.

According to statistics provided by the UDI, 80 percent of all visa applications come from Russia, China, India, Thailand and the Philippines. From 2012 to 2013 there was a considerable increase in the number of Chinese and Russian applications. In the period from 2013 to 2014 there has been a notable decrease in applications from the same countries. The decrease in the Russian numbers may be explained by an amendment to the Immigration Regulation that entered into force in March 2014, laying down new exemptions from the general Visa obligations. The exemptions in question apply to Russians who reside in the area close to the Norwegian-Russian border (cf. Norway-Russia Border Treaty signed by the parties in Oslo on the 2nd of November 2010).

- **Inspections**

During the period, the Norwegian DPA has carried out one VIS-related inspection. The inspection took place at the Norwegian Embassy in Kiev, Ukraine, on the 10th of September 2013. The theme of the inspection was the Embassy's processing of personal data during its handling of visa applications from Ukrainian citizens. The DPA's main focus was on the Embassy's compliance with the relevant criteria laid down in the Personal Data Act and the national SIS Act, but the use of information from the NorVIS-system was also a part of the investigation. In the context of the inspection, the DPA also visited VFS Global, a company that has established a VISA Application Center on Ukrainian soil. The company has entered into a contract with the Embassy, assisting the Embassy in guiding Ukrainian citizens in the visa application process. Following the inspection, the DPA issued a report and a decision, ordering the UDI to make certain amendments to its internal control documentation.

- **Complaints**

The Norwegian DPA has received no complaints during the period.

- **Remarks**

We have no remarks as regards the period in question; however an inspection on the premises of the national data controller – UDI – is planned in 2015.

4.24. Poland

- **Overview: state of play and developments**

Between 2012 and 2014, the Polish DPA has undertaken a number of actions associated with the VIS; the Polish DPA carried out 22 inspections and conducted series of trainings on personal data protection for persons who have access to the VIS, in particular within law enforcement agencies and consulates.

- **Inspections**

The Polish DPA carried out nine inspections in 2012, nine in 2013 and four in 2014. The following authorities were controlled: the Central Technical Body of National Information within the Police, Border Guards units, Customs Service units, some voivods (i.e. provincial governors responsible for visa extensions), some consulates, the Office for Foreigners, the Head of Customs Service and the General Inspector of Treasury Control.

In general the results of the inspections were satisfactory, but in some cases the following shortcomings were found: incomplete documentation on data processing and access to the VIS by persons without valid authorization.

- **Complaints**

The Polish DPA has received one complaint with regard to the VIS in 2012, but none in 2013 and 2014.

- **Remarks**

Until now, no special problem concerning the VIS has occurred.

4.25. Portugal

- **Overview: state of play and developments**

Portugal is linked to the VIS since 2011. The fingerprint validation at the border control only started in early October 2014. There are two bodies linked to the VIS through a national gateway: the Aliens and Borders Office - SEF (which is also the data controller of the national part of the VIS) and the Ministry of Foreign Affairs. No access has been carried out yet for the purposes of articles 19 and 20 of the VIS Regulation.

Also, there are no law enforcement authorities linked to the VIS following Decision 2008/633/JHA of 23 June 2008.

The data controller provided specific training regarding the VIS to its inspectors posted in the border boxes.

- **Inspections**

The Portuguese DPA started in the second half of 2014 an audit of the VIS procedures, which is still ongoing as some of the verifications are conducted together with Schengen inspections.

- **Complaints**

The Portuguese DPA did not receive so far any complaint related to the VIS.

- **Remarks**

/

4.26. Romania

- **Overview: state of play and developments**

/

- **Inspections**

The Romanian DPA carried out 3 *ex officio* investigations to the diplomatic missions and consular offices in order to verify the conditions for observing the provisions of the national data protection law (Law no. 677/2001), including with regard to respect for the rights of data subjects and security measures. The investigations were made to diplomatic missions/consular offices established on the territory of certain EU Member States.

Within these investigations, the Romanian DPA took also into account the verification of the compliance with the conditions of processing personal data contained in the National Information System for Visas ('NISV') according to Law no. 271/2010 for setting up, organising and functioning of the National Information System for Visas and the participation of Romania to the Visas Information System and Regulation (EC) no. 810/2009 on establishing a Community Code on Visas.

The investigations were focused mainly on the following aspects: the notification of personal data processing to the DPA, the information to data subjects according to the provision of the national law on data protection, the purpose and quality of personal data processed, the compliance with the minimum security measures for processing the personal data, the data archiving. In the same time, verifications were carried out concerning the access to the premises of the consular posts, the organisation of the visas sections, the processing of the visa application forms, the compliance with security measures concerning the access to the NISV and protection of the rights of the data subjects.

With regard to the deficiencies, the Romanian DPA issued appropriate recommendations on the adequate information of data subjects (according to Article 12 of Law no. 677/2001), in all situations in which personal data is processed, the organisation of the premises in which

personal data is archived, the establishment and the observance of the limited retention period of the personal data, enabling the identification of the data subjects strictly for the period necessary to achieve the goals for which data is collected and further processed, as well as the periodic training of personnel. In the same time, recommendations have been made on securing access to consular bureaus, according to the conditions established by Law no. 271/2010 on NISV and Regulation (EC) no. 810/2009.

- **Complaints**

/

- **Remarks**

/

4.27. Slovak Republic

- **Overview: state of play and developments**

During the years 2012-2014, the national VIS was operated in routine performance without any fundamental changes in the application. Since 2011 the visa departments of each embassy/consulate have been connected to the central VIS in accordance with the timetable of the European Commission. In the present time, 16 regions are connected.

- **Inspections**

During the years 2012-2014, the Slovak DPA performed inspections of the VIS in embassies/consulates in Greece, Croatia, Bosnia Herzegovina, Macedonia, Serbia, Ukraine and Albania.

The only irregularities were found in the Slovak embassy in Croatia, where not all best practices related to entrance to area where personal data are processed were fulfilled.

- **Complaints**

There were no complaints in the above mentioned periods.

- **Remarks**

/

4.28. Slovenia

- **Overview: state of play and developments**

Slovenia's approach to the VIS is in accordance with the agreed roll-out scenario. The Slovenian Ministry of Foreign Affairs first connected with the VIS the Slovenian embassy in Cairo, then the embassy in Teheran (which is now closed), then followed the embassies in Tel Aviv, South America (Buenos Aires and Brasilia), North America (Washington, Ottawa and Cleveland) and finally in September 2014 all offices of the Western Balkan and Turkey (Sarajevo, Banja Luka, Belgrade, Skopje, Podgorica, Pristina, Tirana and Ankara).

Users of the VIS are the above mentioned representations and the Consular Department of the Slovenian Ministry of Foreign Affairs. In addition, the Police and border crossing points also have access to the VIS.

The national VIS database is called 'VIZIS' and is located at the Slovenian Ministry of Foreign Affairs. VIZIS contains information about visa applications (short stay visas and long stay visas). Slovenian users can only access VIS data through VIZIS.

- **Inspections**

In 2013 and 2014, the Slovenian DPA did not carry out any supervision activities for the VIS. In October 2011, the embassy in Cairo was inspected as well as national database of the VIS. The Slovenian DPA then decided to wait until the end of the connection to the VIS in the Western Balkan countries for its next supervision activities. Since then the Slovenian DPA has established a good cooperation with the Ministry of Foreign Affairs regarding the VIS. The available financial resources do not allow the Slovenian DPA frequent travels to third countries but one inspection on the VIS is planned for 2015.

- **Complaints**

The Slovenian DPA has not received any complaints.

- **Remarks**

The Slovenian DPA has not been informed of problems with the VIS database.

4.29. Spain

- **Overview: state of play and developments**

The Spanish DPA has included amongst its usual activities those related with the supervision of the VIS, in accordance with Article 41 of the Regulation 767/2008. In that sense, and from the purely national perspective, the Agency has been exercising its advisory role on legal and technical issues related with the deployment of the system, including the creation of files as well as the assessment of contractual clauses linked to the externalization of services involving personal data processing. The DPA has also exercised their investigative powers in response to individual complaints. From the international point of view, the Spanish DPA is actively involved in the activities of the Coordinated Supervision Group from the outset.

Rules related to the creation of the file National VIS data file were issued by order of the Ministry of Foreign Affairs and Cooperation dated January 4th 2011. The competent VIS authority in Spain is the General Directorate of Consular and Migratory Affairs.

- **Inspections**

The Spanish DPA has been carrying out a number of investigations in response to individual complaints related to the functioning of the VIS in Spain. In that sense, it is interesting to note the final decision of the procedure AP/00046/2013 establishing the existence of an

infringement of the Ministry of Foreign Affairs and Cooperation affecting the principle of quality of the personal data, set forth at article 4 of the Spanish Data Protection Act.

- **Complaints**

The Spanish DPA has received so far some individual complaints related to the VIS. Some of them are related to alerts included in the Schengen Information System (SIS II) leading to the refusal of a visa application. In other cases the claimant was interested in knowing the specific reasons why the application had been rejected when the refusal was based on Article 32(vi) of the Schengen Visa Code. The Agency has also received some complaints linked to the VIS that were actually outside of its competences.

- **Remarks**

The Spanish DPA will start in 2015 the inspection of the National VIS in accordance with Article 41(2) of the Regulation 767/2008.

4.30. Sweden

- **Overview: state of play and developments**

Swedish rules which were deemed necessary in order to supplement the VIS Regulation 767/2008 came into force in October 2011. This concerned e.g. rules on appointment of the national competent VIS authority and the national supervisory authority. The competent VIS authority in Sweden is Migrationsverket (the Migration Agency) and the national supervisory authority is Datainspektionen (the Swedish Data Protection Authority). Processing of personal data by the Migration Agency is regulated in specific legislation. As to processing of personal data in the VIS, this specific legislation includes a reference to the VIS Regulation.

- **Inspections**

The Swedish DPA has carried out two field inspections at the Migration Agency's office in order to see how the VIS is implemented. The first inspection was carried out in March 2012 and aimed at obtaining a first overview of the personal data processing in VIS. The second inspection was carried out in the beginning of 2015 and the case is still open. This inspection aimed at obtaining an updated view of the processing in VIS and some specific information about the communication of data between the diplomatic consulates and the Migration Agency. Apart from these inspections, we have also had some written consultation with the Migration Agency regarding the use of external service providers.

- **Complaints**

The Swedish DPA has so far only received one complaint regarding the VIS. The complaint concerned a Swedish embassy's consultation in accordance with article 21.3 c) and article 22 of the Visa Code. The case was closed with a remark on the information given to the applicant but no remarks were made as to the actual handling of the VIS.

- **Remarks**

The specific legislation for personal data processing by the Migration Agency is currently being reviewed but this will not affect the processing of data in VIS since this falls under the VIS Regulation and therefore is subject to EU rules with direct effect in the Member States.

4.31. Switzerland

- **Overview: state of play and developments**

At national level, the visa data were first collected in a subsystem of the central migration information system. In January 2014, this subsystem was replaced by a new and completely independent national visa system. The new system was demonstrated to the Swiss DPA before its entering into function. Specified Federal and Canton authorities may consult C-VIS data online.

In the period 2012-2014, Switzerland attended all coordinated supervision meetings and answered all questionnaires of the VIS SCG. During the first meeting of 21 November 2014, Switzerland made a short presentation of the controls the Swiss DPA made at four Swiss Consulates (Kiev in 2008, Cairo in 2009, Moscow in 2011 and Istanbul in 2010) concerning the Schengen-visa before the VIS rollout. Switzerland is also a member of the ESPs Subgroup.

In 2013, the Swiss DPA analysed the drafts of the new contracts with ESPs. The Swiss DPA asked for several minor amendments, which were adopted by the Ministry of Foreign Affairs. The contracts also contain the minimum requirements to be included according to Annex X of the visakodex.

- **Inspections**

In November 2013, the Swiss DPA inspected the Swiss consulate in Dubai. This control also included a control of the VIS, the log files, the biometrics (fingerprints) and of the externalisation. During the on the spot visit, the Swiss DPA was accompanied by the DPO of the Ministry of foreign affairs. As a result, the Swiss DPA asked for improvements concerning a secure transmission of the appointment-data, deletion of data, and a clause of deletion.

- **Complaints**

/

- **Remarks**

/

5. What to expect next

The VIS Work Programme 2015-2018 aims to ensure the follow-up to the activities started by the VIS SCG between 2012 and 2014, but also envisages other new issues to be explored. Therefore, the planned activities include the following:

- Reporting on the questionnaires circulated on checking the access to the VIS data and data subjects' rights;
- Reporting on the use of ESPs for the processing of visa applications;
- Developing a security audit framework;
- Checking how national authorities are ensuring training staff of authorities having a right to access the VIS on data security and data protection rules.

Besides the activities foreseen, the VIS SCG will work on a permanent basis on the follow-up of policy and legislative developments, any ongoing issues, exchange of experiences and mutual assistance.