Council of the European Union: COMMISSION STAFF WORKING DOCUMENT Evaluation of the implementation of Regulation (EC) No 767/2008 of the European Parliament and Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) / REFIT Evaluation Accompanying ST 13530 2016 ADD 2

European Union News

November 29, 2016 Tuesday

Length: 66913 words

Dateline: New York

Body

Brussels: Council of the European Union has issued the ***following*** document:

13530/16 ADD 2 JdSS/cr

DGD 1 A EN

Council of the European Union Brussels, 21 October 2016 (OR. en) 13530/16 ADD 2 ***VISA*** 329 FRONT 391 COMIX 689 COVER NOTE From: Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director date of receipt: 18 October 2016 To: Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union No. Cion doc.: SWD(2016) 328 final Subject: COMMISSION STAFF WORKING DOCUMENT Evaluation of the implementation of Regulation (EC) No 767/2008 of the European Parliament and Council concerning the ***Visa*** Information System (VIS) and the exchange of data between Member States on short-stay ***visas*** (VIS Regulation) / REFIT Evaluation Accompanying the document REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the ***Visa*** Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the ***visa*** application procedure/REFIT Evaluation

Delegations will find attached document SWD(2016) 328 final.

Encl.: SWD(2016) 328 final

EN EN

EUROPEAN COMMISSION Brussels, 14.10.2016 SWD(2016) 328 final COMMISSION STAFF WORKING DOCUMENT Evaluation of the implementation of Regulation (EC) No 767/2008 of the European Parliament and Council concerning the ***Visa*** Information System (VIS) and the exchange of data between Member States on short-stay ***visas*** (VIS Regulation) / REFIT Evaluation Accompanying the document REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the ***Visa*** Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the ***visa*** application procedure/REFIT Evaluation {COM(2016) 655 final} {SWD(2016) 327 final}

2

TABLE OF CONTENTS

3

INTRODUCTION

Purpose of the evaluation

In August 2014, the Commission launched an overall evaluation of the VIS Regulation1 and of the VIS founding Decision2. The evaluation also looked at how the VIS is used for the purpose of law enforcement access and the use of biometrics in the ***visa*** application procedure.

The purpose of the evaluation was to analyse the performance of the VIS as a system, how the VIS Regulation has been implemented in practice, the extent to which the VIS has achieved its policy objectives, and whether the VIS Regulation remains fit for purpose in terms of effectiveness, efficiency, relevance, coherence and added value for the EU ***visa*** policy.

This was the first time the VIS Regulation was evaluated since it entered into force in 2011.

The evaluation was part of the Commission's REFIT programme, which underlined the importance of assessing the relevance of the VIS Regulation for its stakeholders, whether its underlying rationale remains valid and the impact of the system on the various policies it has

1 Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the ***Visa*** Information System (VIS) and the exchange of data between Member States on short-stay ***visas*** (VIS Regulation) OJ L 218, 13.8.2008, p. 60.

2 Council Decision No 512/2004 establishing the ***Visa*** Information System (VIS) OJ L 213, 15.06.2004, p. 5.

supported (***visa***, border management, migration management, asylum, law enforcement) and on the data subjects (third-country nationals obliged to obtain a Schengen ***visa***).

Scope of the evaluation

Article 50(4) of the VIS Regulation requires the Commission to produce a report on the overall evaluation of the VIS three years after it was brought into operation and every four years thereafter. The evaluation should examine the results achieved against objectives and assess:

• the continuing validity of the underlying rationale;

• the application of the VIS Regulation;

• the security of the VIS;

• the use made of the provisions on the communication of data to third countries or international organisations referred to in Article 31;

• any implications for future operations.

Article 50(5) of the VIS Regulation requires the Commission to produce a report on the technical progress made regarding the use of fingerprints at external borders and its implications for the duration of searches at borders, including whether the duration of these searches entails excessive waiting time at border crossing points.

Furthermore, in order to ensure the regular monitoring and evaluation of the system put in place by the VIS Regulation, Article 57(3) of the ***Visa*** Code3 requires the Commission to present, three years after the VIS is brought into operation and every four years thereafter, a report on the implementation of the VIS-related provisions of the ***Visa*** Code (i.e. Articles 13, 17 and 40-44). Thus, the assessment of how Member States implement the provisions on the use of biometrics in the ***visa*** application procedure and organise procedures relating to applications, including their practical cooperation, is relevant for and should be considered part of the overall VIS evaluation covering the VIS Regulation and the VIS Founding Decision.

However, a distinction should be made between:

a) the overall evaluation of the implementation of the ***Visa*** Code, covered by the 'Commission Staff Working Document (SWD(2014) 101 final) on the Evaluation of the Implementation of the ***Visa*** Code', published in April 2014; and

b) the report to the European Parliament and to the Council referred to in Articles 57(3) and (4) of the ***Visa*** Code, covered by the evaluation detailed in this Commission Staff Working Document.

The objective of b) is to verify and monitor:

• the implementation of the provisions concerning the collection and use of biometric identifiers;

3 Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on ***Visas***, OJ L 243, 15.9.2009, p. 1.

12

• the suitability of the International Civil Aviation Organisation (ICAO) standard chosen;

• compliance with data protection rules in ***visa*** application procedures;

• Member States' experience of cooperation with external service providers, in particular as regards the collection of biometric data;

• the implementation of the 59-month rule for the copying of fingerprints; and

• the organisation of application procedures.

As required under Article 57(4) of the ***Visa*** Code, the report on the implementation of the provisions on collecting and using biometric identifiers also had to address the issue of whether the fingerprints of children under the age of 12 were sufficiently reliable for identification and verification purposes, and how fingerprints evolve with age.

Finally, Article 17(4) of the Decision on the law enforcement access to the VIS ('the VIS Law Enforcement Access (LEA) Decision4') requires the Commission to produce an overall evaluation of the VIS.

This evaluation is complementary to the evaluation of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) which was carried out by the Commission in close consultation with the Management Board of eu-LISA, as required under Article 31(1) of the eu-LISA founding Regulation.5 The eu-LISA evaluation examined the way and extent to which the Agency effectively contributes to the operational management of large-scale IT systems in the area of freedom, security and justice, including the VIS, and fulfils its tasks laid down in its founding Regulation. It also assessed the Agency's role in the Union strategy aimed at achieving a coordinated, cost-effective and coherent IT environment at Union level that is to be established in the coming years. The eu-LISA evaluation was completed in March 20166 and, based on its findings, the Commission, after consulting the eu-LISA Management Board, will issue recommendations regarding possible changes to the eu-LISA founding Regulation to bring it further in line with the Union strategy. The Commission will then forward its recommendations, together with the opinion of the Management Board, to the European Parliament, the Council and the European Data Protection Supervisor.

4 Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the ***Visa*** Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218, 13.8.2008, p. 129.

5 Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 286, p. 1 of 1.11.2011.

6 "Independent external evaluation of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice - eu-LISA", ISBN: 978-92-79-58236-3, Catalogue number, DR-01-16-464-EN-N.

2. BACKGROUND TO THE VIS REGULATORY FRAMEWORK

Baseline

When establishing an area of freedom, security and justice, the European Union committed to ensuring the free movement of people and a high level of security. In this context, the EU has prioritised the development and establishment of the VIS as a system for exchanging ***visa*** data between Member States.

Before the VIS was put in place in 2011, around 12 million Schengen ***visas*** were issued every year by the 25 countries of the Schengen area, and numbers were growing (see graph below).

The Seville European Council of 21 and 22 June 2002 considered the establishment of a common identification system for ***visa*** data a top priority and called for its introduction as soon as possible. In response to this request, the Commission presented a feasibility study in May 2003. The Council welcomed the study and invited the Commission to continue its preparatory work to develop the VIS. The Thessaloniki European Council of 19 and 20 June 2003 deemed that guidelines should be drawn up for planning the development of the VIS. A legal basis permitting establishment of the VIS and engaging the necessary financial means was also to be adopted.

According to the common ***visa*** policy developed ***following*** the Schengen Agreement of 1985, uniform short-stay ***visas*** were to be issued to third-country nationals, allowing them to travel freely throughout the Schengen area. The common ***visa*** policy also harmonised the criteria and conditions for issuing a Schengen ***visa*** in a uniform format. Citizens from 134 countries were required to apply for a ***visa*** ***before*** entering Schengen states.7

However, information from the ***visa*** application was routinely held only by the Member State which issued the ***visa***, making it difficult to implement a common ***visa*** policy. If a bona fide traveller8 applied for a Schengen ***visa*** again, but to the authorities of another Member State, the record of his or her past ***visa*** application was not readily ***available*** to the consular

7 This number has since decreased with the number of ***visa*** waiver agreements concluded by the EU with third countries. On 1 June 2016, people from 104 countries were still required to obtain a Schengen ***visa***, according to Annex I to Regulation (EC) No 539/2001 listing the third countries whose nationals must be in possession of ***visas*** when crossing the external borders and those whose nationals are exempt from that requirement.

8 The term ‘bona fide traveller’ is used to refer to third-country nationals who travel to the Schengen States for leisure or business, have not nor intend to breach their ***visa*** and other immigration requirements, and do not constitute a threat to internal security.

0

2

4

6

8

10

12

14

16

18

20

2007

2008

2009

2010

2011

2012

2013

2014

2015

Millions

Schengen ***visas*** applied for

Schengen ***visas*** issued

* A, LTV and C ***visas*** considered

15

authorities of that Member State. Some important ***visa*** data were exchanged, but the exchange was partial, inefficient and time consuming.

As shown in the impact assessment leading to the establishment of the VIS9, the system for delivering, monitoring and verifying ***visas*** was struggling to cope with such big numbers. A sizeable proportion of people tried to obtain a Schengen ***visa*** on dubious grounds. It was not always easy to prevent fraud and abuse, and the application process was often cumbersome for those legitimately seeking a short-stay ***visa*** for travel within the EU.

Member States also had difficulties in ascertaining whether a ***visa*** applicant was using a false identity to obtain a Schengen ***visa***. Statistics showed high levels of travel document fraud.

Another phenomenon developing at that time was '***visa*** shopping', i.e. bypassing the criteria for determining which Member State is responsible for examining the ***visa*** application. If one Member State refused to issue a Schengen ***visa***, the same applicant could apply to another Member State for a ***visa***, even from within the same country of application. This is because there was no formal information system for authorities to check whether the applicant had applied and been refused, or had previously failed to pursue a Schengen ***visa*** application, or indeed whether a ***visa*** had been granted to the individual in the past.

In 2001, around 360,000 people illegally present in the EU were apprehended. In the same year around 390,000 people illegally present in the EU were removed and around 1.2 million non-EU citizens were refused entry10. Statistics indicated that overstayers were the biggest category of illegal immigrants.

In addition, there were problems with the subsequent implementation of the Dublin II Regulation, which determines which Member State is responsible for examining an asylum claim. One of the criteria for establishing responsibility is that the Member State issuing the ***visa*** is also responsible for examining the asylum claim. At that time, Member States did not have an efficient means of checking whether an asylum seeker had been issued a ***visa*** by another Member State.

On 8 June 2004, the Council adopted Council Decision 2004/512/EC establishing the ***Visa*** Information System (VIS).11 This constituted the legal basis defining the architecture of the VIS and giving the Commission the mandate to develop the VIS at technical level. The national infrastructures had to be adapted and/or developed by the Member States. A comprehensive legal framework was needed to further develop and establish the VIS.

9 Commission Staff Working Document, Annex to the Proposal for a Regulation to the European Parliament and to the Council concerning the ***Visa*** Information System (VIS) and the exchange of data between Member States on short stay-***visas*** — extended impact assessment COM(2004) 835 final – SEC(2004) 1628, p. 5.

10 Idem, p. 6.

11 Referred to in footnote 2 above.

Given the potentially significant impact of action in this field, the Commission carried out an extended impact assessment12 to ensure that economic and social impacts could be taken into account as early as possible in the process. This impact assessment was presented in 2004, accompanying the proposal for a Regulation to the European Parliament and to the Council concerning the ***Visa*** Information System (VIS) and the exchange of data between Member States on short-stay ***visas***.

It assessed various policy options:

• no VIS;

• an entry-exit system' similar to the US-VISIT;

• VIS without biometrics;

• VIS with biometrics.

The option of VIS with biometrics was chosen because it had the potential to bring the most substantial improvements in most domains.

The VIS Regulation was adopted in 2008. It sets out the purpose, functionalities and responsibilities of the VIS, as well as rules for setting up and maintaining the system. The Regulation also stipulates the procedures and

conditions for exchanging data on short-stay ***visa*** applications between Member States to strengthen the examination of such applications and the related decisions.

The VIS central system was developed by the Commission and handed over to eu-LISA as of December 2012, according to the legal basis setting up this Agency.13

Law enforcement access to the VIS

In March 2005, the Council adopted conclusions stating that 'in order to achieve fully the aim of improving internal security and the fight against terrorism', Member State authorities responsible for internal security should be guaranteed access to the VIS, 'in the course of their duties in relation to the prevention, detection and investigation of criminal offences, including terrorist acts and threats', 'subject to strict compliance with the rules governing the protection of personal data'.

Consequently, the VIS LEA Decision was adopted in June 2008.

12 See footnote 9.

13 See footnote 5 above. For the Commission's specific role in the VIS see section in Annex 2 'Detailed explanation of the initiative'.

17

The VIS and the ***visa*** application procedure

In 2009, the Regulation establishing a common ***Visa*** Code was adopted as a 'recast' and consolidated all legal acts governing the conditions and procedures for issuing short-stay ***visas*** (i.e. ***visas*** for intended stays of no ***more*** than 90 days in any 180 days).

The ***Visa*** Code provided, among other things, for measures to improve consular organisation and cooperation (partly in view of the roll-out of the VIS14). Consequently, VIS-related rules on collecting biometric identifiers and on facilitating the ***visa*** application procedure, including through forms of cooperation among Member States, were included in the ***Visa*** Code.

2.1. Objectives of the VIS

The VIS was set up to:

• improve the implementation of the common ***visa*** policy;

• ensure smooth consular cooperation and the consultations between central consular authorities to prevent threats to internal security and '***visa*** shopping';

• facilitate the ***visa*** application procedure, the fight against fraud and checks both at external border checkpoints and within the Member States,

• help identify and return illegal immigrants; and

• facilitate application of the Dublin Regulation.15

By improving the assessment of ***visa*** applications, including the consultation between central authorities and the verification and identification of applicants at consulates and at border checkpoints, the VIS helps strengthen the internal security of the Member States. It also helps combat terrorism which, along with the fight against illegal immigration, constitutes a cross-cutting objective and basic criterion for the common ***visa*** policy.

The VIS should also benefit bona fide travellers by improving the procedures for issuing ***visas*** and for checks including in terms of simplification and administrative burden reduction of procedures for identity checks and identity verification procedures.

14 Originally the VIS was to become operational in 2007. This is why the Commission chose to present a separate legal proposal which:

- established the standards for the biometric identifiers to be collected;

- provided for a series of options for the practical organisation of Member States' diplomatic missions and consular posts for the enrolment of biometric data from ***visa*** applicants;

- laid down a legal framework for Member States' cooperation with external service providers.

The content of the adopted Regulation (OJ L 131, 28.5.2009, p. 1) was inserted into and adapted to the structure of the ***Visa*** Code adopted in July 2009.

15 Initially the 'Dublin II Regulation', Regulation (EC) No 343/2003, repealed and replaced by the 'Dublin III Regulation', Regulation (EU) No 604/2013, OJ L 180, 29.6.2013, p. 31.

18

2.2. Description of the VIS and its functions16

The VIS founding Decision

This Decision sets up the VIS as a system for exchanging data between the Member States, enabling national authorities to enter and update ***visa*** data and to consult those data electronically. According to the Decision, the system was to consist of a central information system, an interface in each Member State and a communication infrastructure.

The measures necessary to develop the central system, the national interfaces and the communication infrastructure were to be adopted by the Commission in accordance with the comitology procedure,17 assisted by the SIS (Schengen Information System) II committee.18

The VIS Regulation

16 For detailed information see Annex 2.

17 The procedure referred to in Decision 1999/468/EC.

18 Set up by Article 5(1) of Council Regulation (EC) No 2424/2001 (OJ L 328, 13.12.2001, p. 4).

19

The first chapter of the VIS Regulation lays down the object of the act, definitions, the purpose of the VIS, the categories of data and general rules on access and on procedures and protocols for the exchange of ***visa*** data.

The second chapter details the obligations on ***visa*** authorities and the procedures they must use for entering data. It also specifies which data must be entered when registering an application and the data to be added when a ***visa*** is issued, refused, annulled, revoked or extended.

The third chapter details the conditions and procedures for the use of data for the specific purposes of the VIS, namely data for:

• examining applications, including the consultation between central authorities;

• checks on ***visas***;

• identification and return purposes;

• determining responsibility for ***visa*** applications;

• determining responsibility for asylum applications;

• examining asylum applications; and

• reporting and statistics.

The authorities which should have access to the VIS vary according to the specific purposes.

The fourth chapter lays down rules on retaining and amending the data recorded in the VIS.

The fifth chapter specifies who is responsible for the VIS, including for the operational management of the VIS, for the use of data and data security, and rules on liability, records and penalties.

The sixth chapter deals with the rights of the data subject and the role of the national supervisory authorities and the Independent Supervisory Authority.

The final chapter covers the implementation approach, the start of transmission, comitology, the evaluation, the entry into force and applicability of the VIS Regulation.

The VIS LEA Decision

The LEA Decision provides the legal basis under which Member State authorities responsible for internal security and the European Police Office (Europol) may access and consult the VIS for the purposes of preventing, detecting

and investigating terrorist offences. The Decision also lays down the conditions under which they may do so and the types of crime and the offences in respect of which Europol is competent to act pursuant to Article 2 of the Europol Convention (i.e. 'serious criminal offences').

The provisions of the ***Visa*** Code on the functioning of the VIS

The rules governing the collection and use of biometric identifiers and the forms of cooperation for the collection of ***visa*** applications are provided in the ***Visa*** Code.

20

2.3. Scope

The VIS Regulation covers the exchange of data on short-stay ***visas*** between Member States 'which have abolished checks at their internal borders'.19 As such, it constitutes a development of Schengen legislation on the common ***visa*** policy and is subject to specific legal rules as regards the Member States' participation in the VIS. Not all EU Member States are part of the VIS, but the VIS does include the four Schengen associated countries: Iceland, Liechtenstein, Norway and Switzerland.

Denmark:

Pursuant to Protocol No 22 on the position of Denmark annexed to the Treaty on European Union and the Treaty establishing a European Community, Denmark does not participate in the adoption of the Regulation and is therefore not bound by it or subject to its application.

However, Article 4 of Protocol No 22 does apply. This is because the Regulation is an act which aims to build upon Schengen legislation in accordance with the provisions of Title V of Part Three of the Treaty on the Functioning of the European Union. In line with this Article, Denmark notified the Council and the Commission within six months after the adoption of the VIS Regulation of its intention to implement it in national law. Consequently, at present, Denmark applies the VIS Regulation and participates fully in the exchange of data on the basis of this Regulation.

United Kingdom and Ireland:

According to Articles 4 and 5 of Protocol No 21 integrating Schengen legislation into the framework of European Union and Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland,20 and Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen acquis,21 the United Kingdom and Ireland are not taking part in the adoption of the Regulation and are not bound by it or subject to its application.

Bulgaria, Croatia, Cyprus and Romania (Member States not yet fully applying Schengen legislation):

The VIS builds on the Schengen acquis or otherwise is related to it within the meaning of the relevant provisions of each country's Act of Accession. However, the VIS Regulation will only apply in these Member States once the relevant Council decisions on the full application of the Schengen acquis to these countries have been passed.

19 Point 2 of the Annex to the Council Conclusions of 19.2.2004.

20 OJ L 131, 1.6.2000, p. 43.

21 OJ L 64, 7.3.2002, p. 20.

21

Iceland, Liechtenstein, Norway and Switzerland (Schengen associated countries):

This Regulation builds on the Schengen acquis within the meaning of the respective Association Agreements22 concluded with the Schengen associated countries, and the procedures laid down in these Agreements are applicable.

3. EVALUATION CRITERIA AND QUESTIONS

The evaluation of the Regulation was undertaken on the basis of the ***following*** evaluation criteria and questions:

• Effectiveness:

o Has the Regulation been effective in meeting the defined objectives?

o Did it facilitate the ***visa*** application procedure?

o Has it prevented the bypassing of the criteria for determining which Member State is responsible for examining the application?

o Did it facilitate the fight against fraud?

o Did it facilitate checks at external border crossing points and within the territory of the Member States by simplification and administrative burden reduction?

o Did it help with the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States?

o Did it facilitate the application of the ‘Dublin III Regulation’?

o Did it contribute to the prevention of threats to the internal security of the Member States?

o What effects did the Regulation have on third-country nationals under Schengen ***visa*** obligation?

• Efficiency:

22 Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latter’s association with the implementation, application and development of the Schengen acquis; OJ L 176, 10.7.1999, p. 31.

Council Decision 2008/146/EC of 28 January 2008 on the conclusion, on behalf of the European Union, of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation’s association with the implementation, application and development of the Schengen acquis; OJ L 53, 27.2.2008, p.1.

Council Decision 2011/350/EU of 7 March 2011 on the conclusion, on behalf of the European Union of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis, relating to the abolition of checks at internal borders and movement of persons; OJ L 160, 18.6.2011, p. 19.

22

o Has the Regulation delivered its results efficiently in terms of the resources used?

o Does it create or reduce administrative burdens?

o What are the main costs and benefits of the Regulation for (i) the Schengen states and (ii) third-country nationals under a ***visa*** obligation?

o Overall, did the benefits of setting up the VIS outweigh its costs?

• Utility: To what extent did the effects of VIS correspond with the needs, problems and issues to be addressed?

• Relevance: Are the objectives of the Regulation still relevant today?

• EU added value and sustainability:

o What is the ongoing added value of EU legislation in this field?

o Is the Regulation still fit for purpose and will it meet its objectives in the future?

o What would happen if the Regulation were to be withdrawn and Member States were free to adjust their national regulatory frameworks?

• Acceptability: To what extent do Schengen states' administrations and third-country nationals accept the VIS?

• Coherence: To what extent are positive/negative spill-overs into other policy areas (migration, trade/tourism, external relations, security) being maximised/minimised?

4. METHOD AND CONSULTATION

The evaluation assessed the performance of the VIS Regulation, i.e. whether it has achieved its objectives, whether it is efficient, coherent, relevant and has an added value at EU level.

The implementation of the system was assessed based on a broad consultation process based on targeted consultations, which included the 22 EU Member States that are Schengen members, the four Schengen associated countries, as well as the principal agencies involved — eu-LISA and Europol. Although not directly consulted for the purpose of this evaluation, Frontex data contained in various annual reports were also used.

The objectives of the consultation process were to collect concrete evidence on the functioning of the VIS and to enable an assessment of the VIS's possible future.

The evaluation criteria and questions focused on both quantitative and qualitative aspects.

23

The process was carried out internally by the Commission. An inter-service steering group23 was set up to oversee the process.

The data collection phase consisted of gathering primary and secondary data relevant to the consultation process. It covered data related to the functioning of the VIS from its entry into operation in September 2011 until December 2015.

A number of different data collection tools were used to collect data from a wide variety of stakeholder groups. These included:

• an extensive documentary review;

• an e-survey for the Member States and eu-LISA;

• direct observation of the VIS Management Board and VIS Advisory Group meetings; and

• observations of the competent working groups in the Council (the ***Visa*** working party, Friends of VIS, VISION).

Third-country nationals and governments of countries under ***visa*** obligation were consulted indirectly via national authorities.

Considering that several ministries and national authorities are involved in implementing and applying VIS-related policy in the Member States, and since this varies according to national legislation, information regarding the evaluation was channelled through the Permanent Representations of the Member States. In addition, information was disseminated through the ***Visa*** working party, the Friends of VIS group in the Council, as well as through the eu-LISA's VIS Advisory Group.

The evaluation questions were also incorporated into an e-survey (see Annex 5).

The consultation process started in May 2015. Initially planned to last until December 2015, it was extended to mid-February 2016 to allow ***more*** Member States to contribute.

However, consultations with Member States were not the only source used in this evaluation; it is also based on the Commission's regular monitoring of the correct implementation of EU legislation. This includes:

• the evaluations under the SCHEVAL system24;

• information from petitions addressed to the European Parliament;

• the questions raised by Members of the European Parliament;

• complaints and questions from private people.

23 The Secretariat General of the Commission, the Legal Service, DG JUST and the European External Action Service were part of the Inter-service steering group.

24 Schengen Evaluation Mechanism, established by the Council Regulation (EU) No 1053/2013 to verify the application of Schengen legislation. Initiated in 2015, the Mechanism had been used to monitor application of the common ***visa*** policy in six Member States (Austria, Belgium, Germany, the Netherlands, Luxembourg and Italy) by the time this report was drafted (first quarter 2016). Two consulates were visited for each Member State, thus resulting in 12 consulates visited worldwide.

24

Answers to the queries of the European Migration Network25 on this matter were also taken into account.

The viewss of third countries' authorities and nationals were taken into account in several ways: from opinions expressed in bilateral official contacts with the European Union/the Commission and the Member States and from the practice experienced by national authorities when implementing the VIS. Views on the implementation of the VIS Regulation have also been exchanged in the Joint Committees set up under the various ***Visa*** Facilitation Agreements26 between the EU and a number of third countries, as well as in the ACP-EU ***Visa*** Sub-group set up under the ACP/EU Dialogue on Migration and Development.

Information gathered within the local Schengen cooperation — in place in all locations where Schengen ***visa***-issuing consulates of the Member States are present — also provided feedback on the functioning of the VIS.

On data protection issues, the Commission used input from the 'Coordinated Supervision of VIS Activity Report 2012-2014' of the VIS Supervision Coordination Group. The report is to be produced every two years by the European Data Protection Supervisor in cooperation with the national supervisory authorities/data protection authorities of each Member State.27 The Commission also drew on the European Data Protection Supervisor's audits of the Management Authority's (eu-LISA) personal data processing activities, which it must carry out every four years.28

16 EU Member States (Austria, Belgium, the Czech Republic, Estonia, France, Germany, Greece, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Sweden and Slovakia) and three Schengen associated countries (Iceland, Norway and Switzerland) contributed to the evaluation (as there are 26 Schengen Member States, this gave a 76 % response rate).

eu-LISA contributed substantially to this evaluation and provided quantitative data on all requested items. It should be borne in mind that the statistics provided by eu-LISA cover all the Schengen Member States using the VIS system (unless specifically mentioned otherwise), and thus make up for the lack of quantitative data by the Member States who did not reply or did not reply in full to the questionnaires.

Europol did not reply to the consultation, given that it has not yet established a connection with the VIS and thus has not been using the system.

25 Established by Council Decision 2008/381/EC, *http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/european_migration_network/index_en.htm*.

26 ***Visa*** facilitation agreements have been concluded with Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Cape Verde, FYROM, Georgia, Moldova, Montenegro, the Russian Federation, Serbia and Ukraine.

27 Article 43(4) of the VIS Regulation.

28 Article 42(2) of the VIS Regulation.

25

Limitations — robustness of findings

The Commission was called on to deliver an evaluation three years after the VIS began operating. This deadline took into account the political objective of achieving the full VIS roll-out within two years of it starting to operate.

However, by 11 October 2014 (i.e. three years after it started operating) the VIS had been rolled out in only 16 of the 25 world regions, while regions with the highest number of Schengen ***visa*** applications (covering countries such as Belarus, China, India, Russia and Ukraine) were not yet covered by the VIS. As a result, less than half of the ***visas*** issued (and thus ***visa*** holders' fingerprints) were stored in the VIS at the end of 2014. Due to the delay in the roll-out, information was insufficient for an in-depth evaluation at that time.

The VIS worldwide roll-out was finalised in November 2015. In February 2016, the system became operational at the Schengen border crossing points.

The data gathered and the ensuing analysis had to take into account this gradual deployment. Therefore, while this evaluation took into account data relating to four years of functioning of the VIS, the relevance of the data is sometimes limited by the recent experience with the system in most regions of the world (regions covering 70 % of the VIS volume only started using VIS in the last year ***before*** the evaluation, while over 50 % of VIS volume is in regions where VIS was only deployed 3-4 months ***before*** the end of the evaluation).

Member States indicated in their contributions that the recent and sometimes limited experience with the VIS narrowed their assessment given that the worldwide roll-out had barely finished by the time the evaluation was carried out. While this aspect has no impact on the findings or conclusions of this evaluation, which remain valid, it must be taken into account that a longer lifespan of a system of this complexity would naturally trigger a higher likelihood of problems arising from its functioning (e.g. when the volume of the database reaches its upper limits, this could have consequences on its efficiency, which cannot be measured at this point in time).

On law enforcement access, a full evaluation on the basis of the VIS Decision was initially planned as part of the overall assessment of the VIS. However, during the data collection period Europol informed the Commission that no access had yet been established to the VIS and hence no experience could be reported. Member States' feedback also pointed overwhelmingly to little or no use, by December 2015, of the VIS for law enforcement purposes (16 Member States had used the VIS for law enforcement purposes, and most of them started doing so in the last months of 2015). Consequently, the information on the limited use of the system for law enforcement fed into this overall evaluation report, but did not provide enough basis for a stand-alone dedicated report.

The input on data protection provided by the European Data Protection Supervisor and the national data protection authorities which could be used for this evaluation did not go beyond

26

2014 (the year the national data protection authorities last evaluated the lawfulness of the Member States' processing of personal data in the VIS; this information was communicated to the Commission for this evaluation) and the 2012 audit of the Central VIS carried out by the European Data Protection Supervisor. By the time of publishing this evaluation, the report on the 2016 audit of the VIS had not yet been published. Moreover, a report by the VIS Supervision Coordination Group on access to the VIS and the exercise of data subjects' rights was not yet public and could not be quoted in this report.

5. IMPLEMENTATION STATE OF PLAY (RESULTS)

The VIS founding Decision was adopted in June 2004 and became applicable 20 days ***following*** its publication in the Official Journal. The VIS Regulation, setting out the detailed functionalities and responsibilities for the operation of the VIS was adopted in July 2008 and became applicable 20 days ***following*** its publication in the Official Journal.

In conformity with the VIS founding Decision, the Commission, assisted by the SIS II committee,29 was responsible for developing the Central VIS, the national interface in each Member State and the communication infrastructure between the Central VIS and the national interfaces. Thus, the Commission was mandated to develop and carry out the entire implementation process from the first stages of planning in 200430 until the operational responsibility was transferred to eu-LISA.31

At national level, Member States developed or adapted their national infrastructure on ***visas*** in order to accommodate the VIS.

The VIS project was divided into three phases:

1. Phase 1 (detailed design) delivered all the documents necessary to fully describe the VIS from a technical perspective and was closed in 2006.

2. Phase 2 (development, testing and deployment) took place in 2007.

3. During phase 3 (migration and integration) Member States connected their national systems to the VIS central database.

The VIS did not start operating on the same date in all Schengen states' consulates worldwide. The VIS has been progressively deployed, region by region, in the order determined by the Commission on the basis of three criteria in the VIS Regulation:

29 The comitology framework for both the SIS II and VIS projects in the development phase, set up by virtue of Article 5(1) of Regulation (EC) No 2424/2001 (OJ L 328, 13.12.2001, p. 4).

30 According to Article 2 of the VIS founding Decision (see footnote 5).

31 According to the eu-LISA founding Regulation (see footnote 8).

27

• the risk of irregular immigration;

• the threats to the internal security of the Schengen states;

• the feasibility of collecting biometrics from all locations in the region.

The Commission consequently adopted in November 2009 an Implementing Decision determining the first three regions for the VIS consular roll-out.32 Furthermore, for each geographical region, the Commission adopted a Decision setting the date for the 'go-live' of the VIS in that particular region (although the date could sometimes coincide for several regions). Such decisions were adopted in each case after all Member States had notified their legal and technical readiness to collect and transmit data to the VIS from that particular region.

The VIS first started operating in all Schengen states' ***visa***-issuing consulates in North Africa in October 2011, in the Near East in May 2012, and then in the Gulf region in October 2012.

On 24 April 2012, the Commission adopted an Implementing Decision determining the second set of regions for the start of operations33: West and Central Africa (start of operations in March 2013); East and Southern Africa (June 2013); South America (September 2013); Central Asia, Southeast Asia and the occupied Palestinian territory (November 2013).

On 30 September 2013, the Commission adopted an Implementing Decision setting the sequence of the VIS roll-out in the remaining regions of the world:34 Central America, North America, the Caribbean, Australasia (May 2014), the Western Balkans and Turkey (September 2014), the eastern neighbouring countries (June 2015), Russia (September 2015), China/Japan and neighbouring countries (October 2015), India/Pakistan and neighbouring countries (November 2015), the European 'microstates', the UK and Ireland, the other EU Member States (November 2015).

The Schengen border crossing points are included in the first roll-out Decision as a separate region for the VIS roll-out, to cover the use of the VIS to issue ***visas*** at the border. The decision to deploy the VIS at Schengen border crossing points for this purpose was made in order to avoid the roll-out in the geographical regions being circumvented by third-country nationals of these regions lodging their applications at the external borders. In practice, due to the low figures of ***visa*** applications at borders (around 0.7 % in 2015, i.e. 102 110 out of 14 410 502 worldwide), the Schengen border crossing points were the last 'region' where the VIS was rolled out, in February 2016.

Schengen states have had the possibility to start using the VIS, with or without collecting ***visa*** applicants' fingerprints, in any location ahead of the general roll-out, provided that they first notified the Commission. 19 Member States notified the Commission that they would roll out the VIS in various locations, without fingerprints, as ***follows***:

32 Commission Decision 2010/49/EC of 30 November 2009, OJ L 23, 27.1.2010, p. 62.

33 Commission implementing Decision 2012/274/EU of 24 April 2012, OJ L 134, 25.5.2012.

34 Commission implementing Decision 2013/493/EU of 30 September 2013, OJ L 268, 10.10.2013, p. 13.

• Belgium, Estonia and Switzerland notified that they would use the VIS ahead of the general roll-out in all their consulates;

• Switzerland, Germany, Finland, Iceland, the Netherlands, Poland, Portugal, Slovenia and Slovakia notified that they would start VIS operations at external border crossing points without fingerprints;

• Austria, Denmark, Hungary, Italy, Liechtenstein, Lithuania, Malta and Sweden notified that they would roll out the VIS at various specific locations.

On 1 December 2012, eu-LISA started operations and took over the operational management of the VIS from the Commission, in line with the VIS Regulation.

Monitoring the development of the system

Several structures were put in place to monitor the development and implementation of the VIS.

A 'Friends of VIS' informal group was established by the French Presidency of the Council of the European Union in 2008 to ***follow*** up on how the Member States were developing national VIS projects, to provide a link between ministerial and expert levels and ensure that Member States made the necessary arrangements to guarantee that their ***visa*** authorities (or another Member State on their behalf) collect and transmit the ***visa*** application data to the VIS, according to the regional roll-out. The group had its final meeting on 7 April 2016 ***following*** the end of the worldwide roll-out of the VIS and thus completing its mandate.

The Change Management Board was established in March 2008 as an informal sub-group of the Schengen Information System and ***Visa*** Information System committee ('the SISVIS Committee') to maintain stable specifications and to give advice about any change requests brought forward that affect the technical specifications of the VIS.

The Test Advisory Group was also established as an informal sub-group of the SISVIS Committee for the purpose of discussing and agreeing all testing-related issues (preparation, execution and evaluation) with Member States.

The VIS Advisory Group, an integral part of eu-LISA's management's structure, assists the Management Board on topics of a rather technical nature, including security, and contributes to the preparation of various documents such as the multi-annual work programme and the annual work programme. The VIS Advisory Group is also consulted on the annual activity report35 of eu-LISA in particular.

35 In accordance with Article 12(1)(k) of Regulation (EU) No 1077/2011.

29

In accordance with Article 6 of the VIS founding Decision, between 2004 and 2011 the Commission submitted eight progress reports to the Council and the European Parliament on the development of the VIS.36

6. EVALUATION OF VIS ACCORDING TO THE EVALUATION CRITERIA

6.1. Effectiveness

6.1.1. Facilitation of the ***visa*** application procedure37

The sizeable majority of contributing Member States concurred in that the introduction of the VIS facilitated the ***visa*** application procedure: 61 % of them consider that VIS had a slightly positive impact on the procedure, while 11 % consider this impact strongly positive. 16 % of the responding Member States considered that the VIS had no

impact on the ***visa*** application procedure, and 11 % consider this impact to be negative (5.5 % consider it strongly negative and 5.5 % slightly negative).

All responding Member States concur that the procedure was made slower and lengthier by the introduction of the VIS because it obliges them to carry out biometric capture and

36 See Commission staff working papers on the development of the ***Visa*** Information System, SEC(2005) 339, SEC(2006) 610, SEC(2007) 833, and the Reports from the Commission to the Council and the European Parliament on the development of the ***Visa*** Information System — COM(2008) 714 final, COM(2009) 473 final, COM(2010) 588 final, COM(2011) 346 final, COM(2012) 376 final.

37 For detailed analysis and reporting see also Section 3.1 of Annex 2.

1 MS

1 MS

3 MS

11 MS

2 MS

VIS impact on the ***visa*** application procedure

Strong negative impact

Slightly negative impact

No impact

Slightly positive impact

Strong positive impact

* 1 MS did not answer this question

30

maintain biometric equipment38. Consequently, it is ***more*** cumbersome for applicants as well. At the same time, Member States consider the procedures for entering and using the VIS data sufficient and effective for the purpose of further processing the application. However, all responding Member States agree that the VIS has also made the procedure ***more*** secure in terms of due diligence and that applicants are better protected against identity theft.

Moreover, those who consider the impact of the VIS positive emphasise how it has facilitated the decision-making process, which was simplified by setting-up a common system to store and exchange data between Member States on applications and related decisions39. The ***visa*** history of the applicants is now easily ***available*** to ***visa***

authorities throughout the Schengen area, and centralised in a single database which can be easily accessed and answers a search in a matter of seconds.40

Eu-LISA statistics from the system show that from 1 August to 15 October 2015 the average time taken to complete an examination procedure (from the moment a ***visa*** application is admitted and until a ***visa*** is issued41) was four days. Most Member States take on average five days to complete the procedure, though experiences vary, ranging from within the same day for one Member State to 13 days for another Member State. With the ***Visa*** Code requirement that applications be decided on within 15 calendar days, the average time of five days currently taken by the Member States to complete this procedure indicates that the VIS has helped reduce the overall length of the ***visa*** application procedure.

Some Member States consider that the impact of the VIS cannot be fully evaluated at this point because the VIS does not currently contain enough data about applicants and their ***visa*** history to simplify the ***visa*** procedure. When the VIS contains ***more*** information, ***more*** elements will be ***available*** for analysis and this will further simplify the ***visa*** procedure.

6.1.2. Preventing applicants from bypassing the criteria for determining which Member State is responsible for examining the application

The prevailing view among the contributing Member States (63.2 %) was that the introduction of the VIS had no impact on preventing applicants from bypassing the criteria for determining the Member State responsible for examining their ***visa*** application. Only 31.5 % of the responding Member States considered that the VIS had a positive impact, either slightly positive (21 %) or strongly positive (10.5 %). However, none of the responding Member States considered that the introduction of the VIS had worsened the situation.

38 See details in Section 1.1. Facilitation of the ***visa*** application procedure in Annex 2.

39 See also Sections 1.1 and 2.1 of Annex 2.

40 See also Section 6.1.4 below.

41 Data on the length of ***visa*** processing-related operations towards VIS is extracted directly from the VIS technical records (logs). The date/time of the start and the end of the ***visa*** application procedure per Member State is then compared. The average response per Member State is calculated by comparing when the Member State created the application file and when it registered the ***visa*** decision (i.e. ***visa*** sticker) in the VIS.

The advantage given by the possibility to check previous applications (especially recently rejected ones) in the VIS is considered rather marginal. The history of applications helps determine the main destination, which is very useful in cases where the applicant uses a new (blank) passport for a new application. However, the criteria for determining the Member State responsible ***follow*** from the information citing the main destination for the visit as provided in the application form, rather than from the history of applications. Moreover, a previous rejection does not necessarily call for a rejection of the current application, nor does it imply that the current application should not be handled by a given consulate.

Responding Member States underlined that in order for the system to work satisfactorily it is extremely important that all Member States perform the searches and the linking of individual files in the VIS central system correctly and that the biometrics taken are of sufficient quality.

6.1.3. Facilitating the fight against fraud42

A substantial majority of the responding Member States — 89 % — agreed that the introduction of the VIS facilitated the fight against ***visa*** fraud (50 % found this impact slightly positive, while 39 % found it strongly positive). 11 % considered that the VIS has had no impact on ***visa*** fraud. Notably, no Member State seems to consider that the VIS would in any way have facilitated fraud.43

42 See also Sections 3.2.1, 3.2.2, and 3.2.3 of Annex 2 and Section 1 of Annex 3.

43 See also Section 1.3 of Annex 3.

12 MS

4 MS

2 MS

VIS impact on preventing the bypassing of the criteria for the determination of the Member State responsible for examining the application

Strong negative impact

Slightly negative impact

No impact

Slightly positive impact

Strong positive impact

* 1 MS did not answer this question

32

Due to their nature and function, ***visas*** are checked mainly on entry to the Schengen zone at border crossing points. Thus, detections at border crossing points are the main indicators of ***visa*** fraud. Frontex's 'Annual Risk Analysis 2016' reports a constant decline in the number of fraudulent ***visas*** detected at external borders between 2012 and 2015, from over 1 800 false ***visas*** detected in 2012, to around 1 500 in 2013, 1 100 in 2014 and 776 in 2015 (a 32 % decline on the previous year).

The main VIS feature contributing to the fight against fraud is the storage of fingerprints in the VIS. When a new ***visa*** application is lodged, the system provides a secure link to the identity of the applicant through biometrics and no look-alike fraud is possible.

Thus, a major turning point in the identification of fraudulent ***visas*** at borders was the obligation, as of October 2014, for border authorities to check ***visa*** holders by using fingerprints (checking the ***visa*** sticker number was sufficient ***before***). This made it virtually impossible for a person to cross the border using a forged or falsified ***visa*** sticker, as the system would immediately identify that the person was not registered with such a ***visa*** sticker number.

The Frontex Annual Risk Analysis 2016 also showed that there was an increase in detections of false ***visas*** at borders in the period immediately ***following*** the introduction of the VIS checks at borders (2012). The VIS checks also constituted a deterrent, in the longer run, to the use of false ***visas*** to enter the EU territory.

However, the effectiveness of the check relies on the requirement that the correct searches are made, that files are systematically linked, and that the biometrics taken are of sufficient quality.

2 MS

9 MS

7 MS

VIS impact on the fight against ***visa*** fraud

Strong negative impact

Slightly negative impact

No impact

Slightly positive impact

Strong positive impact

* 1 MS did not answer this question

33

In addition, VIS cannot prevent fraud with documents/false passports presented during application. The obligation to check the ***visas*** using fingerprints reduces the possibility for fraudsters to cross the border using fraudulent ***visa*** stickers. A possible knock-on effect could have been a shift from the use of fraudulent ***visa*** stickers towards the use of ***visas*** obtained under false pretence in consulates (at the time of applying for a ***visa***), and thus an increase in the likelihood of fraud with other types of documents (such as travel documents). To prevent this, consulates have to be sure about the identity of the applicant ***before*** taking the fingerprints.

6.1.4. Facilitating checks at external border crossing points and within the territory of the Member States44

A vast majority of the responding Member States (73.5 %) considered that the introduction of the VIS facilitates the checks both at external border crossing points and within the territory of the Member States. 52 % considered the VIS to have a slight positive effect in this sense and 21 % considered that the VIS had a strongly positive effect. 16 % of the responding Member States considered that the VIS had no impact on these checks at external border crossing points and within the territory, and 5 % consider that the impact was slightly negative.

The three main positive impacts of the VIS are:

44 See also Section 3.2.1 of –Annex 2.

2 MS

1 MS

13 MS

1 MS

VIS impact on checks at Schengen border crossing points and within the territory

Strong negative impact

Slightly negative impact

No impact

Slightly positive impact

Strong positive impact

* 2 MS did not answer this question

34

• the fact that it has improved the quality of the ***visa*** checks (thanks to the use of centralised data making it possible to verify within seconds the identity of the ***visa*** holder and the authenticity of the ***visa***, including when issued by another Member State);

• the increase in the information accessible to relevant authorities (by allowing access to the ***visa*** history and information input by 26 states);

• its contribution to detecting and fighting the use of fraudulent documents (made useless by a system carrying identity checks based on fingerprints).

A turning point in performing checks at borders using the VIS45 was, as in the case of fraud detections, the obligation as of October 2014 to carry out these checks using fingerprints. While slightly adding to the length of the border check procedure, the comparison using fingerprints greatly facilitates the procedure by providing an irrefutable element to the decision regarding whether someone fulfils the conditions necessary to cross the external border.

As regards the rapidity of the system, data logs indicate that, even with fingerprints, the VIS enables border checks to be performed within seconds, as evidenced in the table below (source eu-LISA).

The few responding Member States who did not notice any impact or considered that the system has had a slightly negative impact were mainly concerned about the increased time required for border checks. The low quality of the fingerprints and the missing information in the VIS files were also mentioned as issues faced at external border crossing points. According to one Member State, the evaluation was also negatively impacted by the difficulty in evaluating the system ***before*** the roll-out was fully completed, meaning the VIS may be viewed ***more*** positively in the future.

The evaluation of technical progress on the use of fingerprints at external borders46 found that, overall, Member States have made progress on the use of fingerprints at external borders. Outside the first months of running the new system, Member States have experienced very few technical problems with the technology used and only infrequent administrative impediments in checking fingerprints at external borders. Cases where multiple scans were needed to collect fingerprints of sufficient quality and attempts at spoofing have been reported

45 For further details see also Annex 4 on the technical progress made regarding the use of fingerprints at external borders as well as Sections 1.4 and 3.2.1 of Annex 2.

46 See Annex 4.

1st Line with FP1st Line without FP2nd Line with FP2nd Line without FPAvg time (s)Avg time (s)Avg time (s)Avg time (s)1.360.3113.780.28VIS Border business statistics : 01/10/2015 - 31/12/2015

35

as sporadic. Situations where capturing devices and the VIS are unavailable are managed using appropriate alternative procedures.

6.1.5. Assisting in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States47

A vast majority of responding Member States — 78 % — were of the opinion that the introduction of the VIS helped them identify people who do not, or no longer, fulfil the conditions for entry to or stay or residence in the territory of the Member States. 50 % consider this impact slightly positive, while 28 % consider that the VIS had a strongly positive impact. 17 % of the responding Member States consider that the VIS had no impact on the identification of these persons and 5.5 % consider the impact of the VIS to have been slightly negative.

Most Member States consider that the VIS gives them the possibility to assess in an unambiguous and timely manner whether a person fulfils the conditions for entry to or stay in the territory of the Member States. One Member State insisted on the positive impact of fingerprints on the ability to identify someone who has no identity or travel document. The main concerns of the few Member States who consider that the system has no, or a slightly negative, impact on the identification of these people referred to the length of the identification procedure, although some Member States have already noticed an improvement in that respect. The fact that the police lack equipment for identification during checks within the territory was also raised48.

47 See also Section 3.2.3 of Annex 2.

48 See also Section 1.5 Annex 2.

1 MS

3 MS

9 MS

5 MS

VIS impact on the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States

Strong negative impact

Slightly negative impact

No impact

Slightly positive impact

Strong positive impact

* 1 MS did not answer this question

36

6.1.6. Facilitating the application of Regulation (EC) No 343/2003 (as replaced by Regulation 604/2013, the ‘Dublin III Regulation’)

The majority of the responding Member States — 63 % — consider that the introduction of the VIS supported the application of the Dublin Regulation by determining the Member State responsible for examining an asylum application where a ***visa*** has been issued by a Member State to the asylum applicant. Almost 31.5 % consider the impact of the VIS to have been slightly positive, and 31.5 % consider it strongly positive. Almost 26.5 % of the responding Member States consider that the introduction of the VIS had no impact on the Dublin procedure and 11 % did not provide any answer. None of the respondents found this impact to be negative.

The VIS was used for asylum purposes by 12 Schengen Member States in nearly 400 000 cases between November 2011 and end December 2015 to help determine the Member State responsible under the Dublin Regulation. Since October 2011 it has been used by 15 Member States in 1 384 988 cases to support the examination of asylum applications. The vast majority of those VIS searches were carried out by four Member States. Feedback from Member States shows that VIS data provide evidence for determining the Member State responsible and facilitate take charge requests. The data are also used to assess the identity and credibility of applicants when examining an asylum application.

In a questionnaire carried out by the Commission in April 2015 on the use of the VIS for asylum purposes, the 11 Member States who had used the VIS for Dublin purposes at that time stated that they experienced little or no difficulties in obtaining acceptances to transfer requests based on VIS-hits. This shows that the VIS is overall well accepted by Member States as an instrument of proof in the Dublin procedure.

5 MS

6 MS

6 MS

VIS impact on the application of the Dublin Procedure

Strong negative impact

Slightly negative impact

No impact

Slightly positive impact

Strong positive impact

* 2 MS did not answer this question

37

6.1.7. Contributing to the prevention of threats to the internal security of any of the Member States49

Almost half of the responding Member States — 47 % — considered that the introduction of the VIS had a positive impact on preventing threats to the internal security of the Member States. For 42 % this impact was slightly positive and for 5 % it was strongly positive. For 10.5 % of the respondents the introduction of the VIS had a limited impact and for 16 % no impact. 26 % of the respondents did not rate the contribution of the VIS to the prevention of security threats.

The mitigated response can be due to the fact that access to the VIS data by law enforcement authorities is recent (the VIS LEA Decision became applicable in September 2013) and very fragmented among the countries using the VIS. Of 26 Member States, eight never accessed the VIS for this purpose. However, the use of VIS for law enforcement purposes has recently been increasing.

6.1.8. Ensuring appropriate protection of data subjects in the ***visa*** application process50

The rights of data subjects are an important part of data protection law. Ensuring that data subjects can access, rectify and erase data held about them increases the transparency of data

49 On the basis of Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the ***Visa*** Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences. For detailed information on the evaluation of this Decision see section 1.7 of Annex 2.

50 For details see section 3.6. of Annex 2.

38

processing for them, helps to uncover unlawful processing and increases data quality for lawful processing.

The evaluation found that only a very limited (a few dozens51) requests were ever made by ***visa*** applicants to access their VIS data, and hardly any one to correct or erase such data. All Member States have in place procedures to request access to data, most of them allowing direct requests to the VIS data controller52. During the period under evaluation, there has been no there has been no reported situation in which a request to correct or

delete data was refused and which led to actions or complaints ***before*** the national competent authorities, and therefore, no case either when Member States should have exercised their duties to assist and advise the person concerned in proceedings ***before*** a court or competent authority

The lawfulness of the processing of personal data by Member States is monitored by the national data protection authorities (DPAs), while the European Data Protection Supervisor (EDPS) is responsible for supervising the management authority (eu-LISA), mainly through inspections and audits53.

DPAs monitoring showed that the relevant staff members of the competent authorities dealing with the VIS have a satisfactory level of awareness regarding their obligation to safeguard data subjects' rights. Training covering data subjects' rights is provided to the relevant staff in some Member States. The VIS SCG54 noted the absence or very low number of requests made by data subjects to exercise their rights of access, correction or deletion of their personal data stored in the VIS. This could be due to data subjects not being aware of their data protection rights, but also to the lack of information about the way to exercise them (e.g. to whom data subjects should address their requests). In this sense, the EDPS invited national DPAs to carry out quality controls regarding the information provided to data subjects by diplomatic missions, consular posts and ESPs.

In its almost three years of operation, eu-LISA has not received any complaint related to data protection. The EDPS has performed inspections on the spot to monitor the lawfulness of the processing of personal data and performed two security audits of the VIS central system to date (in 2011 and 201555).

6.2. Efficiency

The roll-out of the VIS was initially planned to take three years, but in fact it took over four years to be fully rolled out worldwide. However, given the magnitude of the project and its

51 For details see section 3.6.2 of Annex 2.

52 In accordance with Article 41(4) of the VIS Regulation and with Article 2(d) of Directive 95/46/EC.

53 Required every four years on the basis of Article 41(2) of the VIS Regulation.

54 The VIS Supervisory Coordination Group established by the EDPS on the basis of Article 43 of the VIS Regulation.

55 For findings and ***follow*** up to these inspections see section 3.6.6.2 of Annex 2.

unique nature, the delay was not considerable or of a length that would create any negative consequences for the ***visa*** examination processes. On the contrary, the set up and launch of the VIS brought a gradual benefit compared with the baseline situation where there was no centralised system enabling Member States to compare national data and trace back applicants' ***visa*** history.

As regards the main financial costs for developing the system, the 2004 VIS impact assessment56 estimated that the one-off investment costs for the EU would be around EUR 93 million and EUR 186 million for all the Member States. As regards operational costs, the annual costs for the EU were estimated at between EUR 14-16 million, while the costs for the Member States' national systems were estimated at around EUR 49 million.

In reality, the cost of setting up the VIS57 totalled nearly EUR 151 million spread over a period of six years from 2005 to 2011. The cost breaks down as ***follows***:

• Development contract (without fingerprints) — EUR 39.9 million (25 %)

• Development contract (with fingerprints) — EUR 37.4 million (23 %)

• Technical assistance — EUR 9.4 million (6 %)

• Network infrastructure (including Member States' connection) — EUR 46.2 million (29 %)

• Site preparation — EUR 4.7 million (9 %)

• Other, including security — EUR 13.1 million (8 %)

56 See footnote 8.

57 See also Section 3.5 of Annex 2.

Quantifying the costs incurred by the Member States to set up national systems is ***more*** complicated due mainly to the way in which systems are organised at national level. Most often the national systems were not built from zero, rather existing systems were upgraded and adapted to enable them to connect with the VIS. Since the verification and identification of third-country nationals were shifted to the Central VIS system, in certain cases the VIS helped enforce synergies at European level, hence limiting costs at national level.

Depending on their consular network and the level of equipment used, the costs incurred by Member States in setting up the system vary between EUR 1-2 million and EUR 30 million.58 A total high-level rough estimate of Member States' expenditure is approximately EUR 600 million, including maintenance costs for the first years.

It is not easy to calculate the financial benefits of setting up the VIS given that it is a non-profit instrument. Moreover, its benefits (listed below) are unquantifiable:

58 For detailed national expenses see Tables 15 and 16 in Section 3.5 of Annex 2.

• the contribution to enforcing a common Schengen ***visa*** policy and consular cooperation and providing an easily ***available*** and secure means of consultation between central ***visa*** authorities;

• the possibility to identify any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence in the territory of the Member States;

• the facilitation of the application of criteria and mechanisms for determining the Member State responsible for examining an asylum application;

• the contribution to preventing, detecting and investigating serious criminal offences.

These benefits are of societal value in terms of enhancing internal security, fighting irregular migration and preventing, detecting and investigating terrorist offences and other serious crime.

The areas where Member States have acknowledged greatest impact are:

• prevention of '***visa*** shopping':

• the facilitation of checks at external border crossing points and within the territory of the Member States;

• the fight against fraud.

The reliability of fingerprint-based identifications means ***visa*** shopping is no longer reported as a significant phenomenon during the ***visa*** application procedure. Similarly, the reliability of fingerprint-based verifications at borders deters travellers from crossing the borders with forged ***visa*** stickers. In the context of growing international migration pressure, this favourable trend is particularly noteworthy, although not financially quantifiable.

The impact assessment for the 2014 recast of the ***Visa*** Code59 showed that it is rather difficult, if not impossible, to have specific statistics on ***visa*** revenues, although some Member States have estimates of the revenues generated from ***visa*** fees.

However, modelling and approximation could be developed, taking into account that the ***visa*** fee charged by the Schengen states under the ***Visa*** Code is set at EUR 60 per application and that by end February 2016 nearly 23 million applications are stored in the VIS. This means that ***more*** than EUR 1 380 million was collected by Member States for processing these applications.60

At the same time, it must be taken into account that the revenues thus obtained do not only cover the costs of connecting to the VIS. Several other elements contribute to the overall cost of processing a Schengen ***visa***, including the use of staff, usually (expatriate) civil servants,

59 Commission Staff Working Document accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council on the Union Code on ***Visas*** (***Visa*** Code) (recast), SWD(2014) 68.

60 A rough estimate of EUR 60/application was applied. However, it can be reasonably assumed that some of these applications must have been collected in third countries subject to ***visa*** facilitation agreements i.e. in countries where the ***visa*** fee was reduced to EUR 35/application and the fee applicable to certain categories (children under 12, pensioners etc.) is waived. Given that the percentage of these categories in the total number of ***visa*** applications is unknown, the overall estimate of EUR 1 380 million should be treated as an estimate only.

who need to be extensively trained, and other various inventories (such as ***visa*** stickers, stamps and paperwork). Some Member States even argued that there is not always a direct link between consulates' work and ***visa*** revenues because revenues go straight to either the Ministry of Foreign Affairs budget or the Treasury.61

On the other hand, the calculation above leaves out the service fee applied by the external service providers. The fee, which can reach EUR 30 per application, covers the administrative cost of collecting ***visa*** data (including biometrics) and all other front office relations with the applicants. Using external service providers (which is common practice in most locations throughout the world62) relieved Member States of a heavy administrative burden in terms of handling the ***visa*** application procedure. It can therefore reasonably be deduced that a large share of the ***visa*** revenues could be used to develop the national VIS.

Comparing these figures shows that the financial costs of setting the system would be largely exceeded by the fees charged for the ***visa*** applications stored in the system. In this respect, we could assume that the costs of setting up the system have, by and large, already been amortised by the Member States.

The operational costs, i.e. the contractual expenses necessary for the Managing Authority to monitor and adapt the VIS, ranged from EUR 5 million to slightly ***more*** than EUR 24 million between 2011 and 2015. These operation costs must be compared with the annual costs for the EU, which were estimated at between EUR 14 and 16 million in the 2004 impact assessment. After the first two years, the expense increases mirrored the capacity upgrade of the VIS needed to enable it to match the growing ***visa*** issuing activity resulting from the worldwide roll-out. Overall, ***visa*** issuing activity increased significantly between 2004 and 2014. For example, the number of applications for uniform short-stay Schengen ***visas*** increased by 48 % between 2009 and 2012.63 The operational costs include the development of new technical features to adapt to changes such as the replacement of the Schengen Consultation Network by a specific consultation mechanism streamlining exchanges between Member States.64

61 Section 2.3.1.3 of SWD(2014)68 — footnote 47, Impact Assessment accompanying the ***Visa*** Code proposal for a Regulation.

62 For details see Section 2.2 of Annex 3.

63 Source: Overview of Schengen ***visa*** statistics 2009-2012 (*http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-**visas**/**visa**-policy/docs/overview_of_schengen_**visa**_statistics_en.pdf*).

64 See Articles 46 and 16 of the VIS Regulation ((EC) No 767/2008).

Figure 1: VIS operating costs (2011-2015)

To conclude, the main benefits of setting up the VIS are in operational and policy terms. Although unquantifiable, the policy benefits clearly justify the costs, especially given that developing the system was a one-off event which will continue to produce benefits for a long time, far beyond that needed for the system to be amortised.

6.3. Utility

The Member States' contributions to the evaluation showed that the VIS fully addresses the needs, problems and issues which it was set up to tackle. Member States need a system that facilitates the ***visa*** application procedure, the fight against fraud and checks at external borders or within the territory. They need a system that enables them to quickly and reliably identify people who may otherwise not have appropriate identification documents or may have false ones, in order to ascertain their right to be or to remain on the territory.

The VIS provides all these services in a quick and reliable manner and is therefore a useful tool in improving the management of the external borders of the Schengen Area. The Member States which used the VIS for asylum purposes confirmed that it could be used not only to support application of the Dublin Regulation (between October 2011 and November 2015, nearly 400 000 searches in the VIS were carried out for this purpose), but also to examine individual asylum applications to identify and check the credibility of applicants.65 Between October 2011 when the VIS began operating, and November 2015, nearly 1.5 million searches had been carried out for this purpose.

65 See Sections 3.2.4 and 3.2.5 of Annex 2 for details.

6.4. Relevance

6.4.1. Assessment of the continuing validity of the VIS as an instrument for supporting the implementation of the common EU ***visa*** policy

All responding Member States consider the VIS as essential for the good functioning of the common ***visa*** policy and that it supports the common area of free movement. The system has further streamlined and harmonised the ***visa*** application procedure, albeit rendering it lengthier and ***more*** cumbersome. It has minimised fraud and ***visa*** shopping and enhanced the global security features of ***visa*** procedures. It facilitates and encourages communication between Member States.

By introducing increased transparency in the ***visa*** process, especially by linking applications, the VIS is an incentive for Member States to seek common practice when assessing applications, thus leading to ***more*** harmonised procedures. The VIS has also made cooperation between the Member States both easier and quicker. The biometric identifiers are reliable and immediately ***available***. This gives consulates and central ***visa*** authorities the information they need to check whether the applicant in question has previously been issued with a ***visa***.

The VIS is useful both in consulates and centrally to analyse how the common rules are applied and to receive early indications of the level of abuse of ***visas*** issued in specific locations (e.g. ***visas*** used for other purposes than those declared, for example to access the EU territory for asylum or work purposes). Although exact figures on the level of abuse of Schengen ***visas*** in the form of overstaying cannot be currently collected, the future entry/exit system (Entry/Exit System EES66) will address this issue, as it will be able to systematically and reliably identify ‘overstayers’ and periodically produce a list of people who have overstayed. At the same time, some Member States indicated that regional disparities exist in the way the VIS obligations are implemented, for example when applying the exemptions from the rule to enrol biometrics, depending on the economic and diplomatic opportunities that exist in each region. While Member States need to take measures to correct such uneven application of the common rules on ***visas***, the scope of these cases remains limited and does not call into question the validity of the VIS as an instrument supporting the implementation of the common EU ***visa*** policy.

The VIS also has the potential to make the ***visa*** process and its end result ***more*** predictable for ***visa*** applicants, regardless of which Member State assessed the application. The possibility for the Member States to conduct searches against the VIS offers bona fide travellers a simplified procedure when applying for a ***visa***.

66 See Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external

borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011, COM(2016) 194 final.

45

If the VIS search on asylum applicants is done properly, it should lead to a ***more*** effective and uniform practice of providing evidence for determining the Member State responsible for examining an asylum application. It should also help check the identity and credibility of asylum seekers.

However, Member States also underlined the need to make better use of the information held in the VIS: firstly, by making ***more*** use of its under-exploited functionalities, for example for asylum, return or law enforcement purposes, and secondly by developing it and integrating it with the EES67 and improving data quality68 (including alphanumeric data), which is essential to obtain full and reliable information for the queries in the VIS. ***More*** detailed information on the reasons for refusing69 or withdrawing70 an application and on revoking or annulling ***visas*** would be welcomed.

Another suggestion from the Member States contributing to this evaluation is that eu-LISA's mandate needs to be extended to allow it to access the VIS for data analysis (trends) and biometrics quality reporting. The current legal basis confining the right to access the VIS data for the purpose of statistics exclusively to the Member States (with the exception of statistics on logs related to processing operations) is sub-optimal, in that it does not ensure a centralised way of reporting.71 This limitation is further aggravated by the fact that the eu-LISA founding Regulation does not explicitly provide a basis for eu-LISA to deliver statistics on data quality, despite these being key to ensuring the VIS functions properly. Sharing statistics on the basis of the VIS data would also provide evidence of any need to change the common ***visa*** policy.

6.4.2. Assessment of the continuing validity of the VIS for performing biometric matching, primarily of fingerprints, for identification and verification purposes

Member States consider the VIS an essential tool in detecting identity theft and ***visa*** shopping and that biometric checks are key to an efficient VIS. Biometric matching is considered the cornerstone of the common identification and verification procedure. A biometric Schengen ***visa*** means identity theft is no longer an option for those attempting to cross the EU border fraudulently, as the fingerprint check would immediately expose the fraudster. The VIS works by dissuasion and its applications in the ***visa***, asylum, migration and return policies are very much appreciated by practitioners.

67 The interconnectivity with EES is already provided for in the Proposal for the EES Regulation (see footnote 63).

68 For ***more*** details and analysis on data quality see Sections 1.3 and 2.2.5 of Annex 3, and Sections 3.2.1 and 3.4.11 of Annex 2.

69 Article 12(2) of the VIS Regulation.

70 Article 10(2) of the VIS Regulation.

71 For further details on reporting and statistics see Section 3.1.4 of Annex 2.

46

The biometric match provides a strong means of identification and prevents the misuse of applications and fraudulent behaviour.

The VIS helps identify third-country nationals who are staying irregularly and is a very useful tool for return purposes. As regards asylum, the VIS is a fast and reliable source of information to establish whether an asylum applicant has been granted a ***visa*** and check the identity of an asylum applicant and the identification document the person in question has submitted for his/her ***visa*** application.

At the same time, many Member States emphasised the need to do ***more*** about the quality of the biometric data.72 Though rare, cases of 100 % biometric match of two different people have been observed in practice by national authorities, resulting from low quality of fingerprints. Bad quality fingerprints discourage Member States from carrying out border checks against the VIS. For example, the asylum authorities reported some cases where there was no match in the VIS despite the fact that the asylum applicant had applied for a ***visa***. In some cases the authorities found the applicant in VIS via an alphanumeric search, but the fingerprints search did not find the person in the VIS.

On the other hand, the system is performing very well in terms of keeping files. Thus, between October and December 2015, 97.2 % of the NIST73 files in the VIS were complete (i.e. they contained all 10 fingerprints). Only 0.23 % of facial images and 2.64 % of fingerprints required were missing out of the 20.5 million applications.74

In order to address these issues at the most appropriate level, Member States recommended that eu-LISA's legal basis should be supplemented to give it the mandate to assist them in improving the quality of biometrics.

Some Member States suggested adding in the VIS the possibility to automatically check against other databases, in particular the SIS, and the upcoming EES,75 in order to increase the efficiency of searches.

6.5. Acceptability

The VIS was set up at the request of the Member States. It did not raise acceptability issues from the national authorities dealing with it. However, the evaluation has showed that some of its functions are not used by the Member States to the level required. For example, despite frequent calls at political level for better use of the VIS, monitoring of usage in the past few years showed that the VIS is not fully used for asylum purposes, or not as frequently as it

72 For ***more*** details on this please see Sections 1.1, 1.3 of Annex 3.

73 Standardised file containing fingerprint information. The name comes from the National Institute of Standards and Technology (NIST) which is a measurement standards laboratory, also known as a National Metrological Institute, which is a non-regulatory agency of the United States Department of Commerce.

74 Source: eu-LISA.

75 Interoperability between VIS and the future EES is already provided for in the 'smart borders' proposals (footnote 48).

should be by all Member States.76 By December 2015 the VIS had been used only by 12 Member States to determine the Member State responsible under the Dublin Regulation, and by 15 Member States to support the examination of asylum applications. By March 2015 only one in two ***visas*** were checked against the VIS at the external border crossing points.

Some resistance to the deployment of the VIS was met in certain third countries (Russia, Ukraine, the Gulf countries). This was expressed either at the highest political level or at individual level, usually by applicants resisting fingerprinting. The reason for the negative perception is mainly related to the taking of fingerprints, which is sometimes perceived in certain societies as linked to a criminal record, while other concerns were also highlighted (e.g. the requirement of personal appearance resulting in travels of long distances to nearest consular services to lodge ***visa*** applications or in complaints by travel agencies that have been in many places important intermediaries in ***visa*** application processes). Concerns expressed at the highest political level (as with Ukraine) led to delays in the roll-out of the VIS.

However, none of these concerns lead to long-term rejection. To alleviate the possible negative impact of the procedure at individual level and make the system ***more*** acceptable, the level of discretion of the procedure was increased, mainly by setting up individual booths in the consulates and ***visa*** application centres of certain countries. Additionally, the Member States checked on their consular presence in third countries to facilitate opportunities for fingerprint-taking, and information sessions were organised with the relevant stakeholders to ensure that accurate factual information was being shared in the public domain with the ***visa*** applicants.

6.6. Coherence with other EU policies

Current trends show that the VIS is becoming ***more*** consistent with other EU policies in the field of home affairs. Member States have made very little use so far of the provisions in Article 31 of the VIS Regulation (relating to communication of data to third countries or international organisations to prove the identity of third-country nationals for the purpose of return). However, the recent enhanced political focus on return policy, collaboration with countries of origin and renewed focus on the transit of irregular migrants will only increase the use of the VIS, allowing it to properly identify people in a return procedure.

The evaluation also showed that while access to the VIS for law enforcement purposes77 currently remains quite fragmented and limited among the Member States,78 the high level of satisfaction and real or expected benefits from VIS access indicate that the number of users and requests should only increase in the future.

76 See section 1.6 of Annex 2.

77 For details see Chapter IV of Annex 2.

78 As revealed by the evaluation, 8 out of 26 Member States never accessed the VIS for this purpose and out of the 18 using the system, eight have regularly done so. One single Member State generated ***more*** than half of all the requests.

The reports received from the local Schengen cooperation in third countries, as well as statistics gathered ***following*** the roll-out of the VIS in any given location, indicated that the VIS has had no negative impact on the

amount of ***visa*** applications. Introduction of the VIS did not cause a drop in tourism or business travel to the Member States.

6.7. EU added value

A return to a state of affairs in which national systems are used to ensure the security of the external borders, fight irregular migration or assist in the fight against terrorism and other serious crimes does not seem to be an option this point in time. The added value of the EU legislation in this field is only increasing. The recent calls by the Council of Ministers of the EU in the field of justice and home affairs to ***step*** up checks at external borders including by 'carrying out a systematic registration, including fingerprinting, of third-country nationals illegally entering the Schengen area, whether migrants or applicants for international protection, and performing systematic security checks by using relevant databases, in particular SIS II, Interpol databases, VIS and national police databases, with the support of Frontex and Europol (…)'79 are a strong appeal to ***more*** systematic and wider use of the VIS and to making it ***more*** interoperable with existing and possibly new EU databases.

Member States also confirmed that the VIS is an important tool that supports asylum authorities in determining the Member State responsible and in examining asylum applications.

7. CONCLUSIONS

The findings of this evaluation allow for a clear assessment of the key evaluation criteria and questions, especially given the abundance of quantitative and qualitative data. This clear assessment is possible despite certain limitations in the degree of response of the stakeholders.

The VIS seems to have been effective in achieving its main objective, namely to facilitate the ***visa*** application procedure. The costs of setting up the VIS were reasonable and in certain cases the VIS contributed to enforcing synergies at European level, hence limiting costs at national level. The Regulation created only a limited administrative burden, which was outweighed by the gains brought by the system in terms of simplifying the ***visa*** procedure. At the same time, the VIS creates benefits in operational terms by facilitating checks at external borders, combating ***visa*** fraud and enabling the rapid identification of people who may not or no longer fulfil the conditions for entry or stay in the territory of the Member States. It also supports asylum authorities by providing relevant information for determining the Member

79 Conclusions of the Council of the EU and of the Member States meeting within the Council on Counter-Terrorism on Strengthening controls of external borders, 20.11.2015.

State responsible and for examining asylum applications. Thus, overall, the VIS is efficient in general terms of costs and benefits.

However, the Member States need to do ***more*** to implement the VIS in order to reap the full benefits of the VIS. In this respect, the use of the VIS for the purpose of checks at external borders or within the territory, and for asylum, return or law enforcement purposes, needs to be enhanced and/or intensified.

The objectives of the VIS Regulation remain relevant and the Regulation continues to be important for the area of free movement. Recent developments mean the relevance of the VIS can only increase in the future.

Member States need to improve their practical implementation of the LEA Decision. The results of the evaluation demonstrate that urgent action is needed in some Member States to bring the national measures into line with the provisions of the Decision. Specific attention should be focused on the recording of access operations and on training authorised staff.

The VIS is coherent with other policies in the field of migration and borders and with international relations. Its added value is consolidation. Given the general political objective of increased cooperation between Member States in the field of migration and borders and in ***stepping*** up controls at external borders, including through increased interoperability between the systems, it now appears hard to imagine that a system such as the VIS be withdrawn.

On this basis, it can be concluded that the VIS is fit for purpose. It is recommended that the VIS regulatory framework be further developed in the ways described in these conclusions to respond to new challenges in ***visa***, border and security policies.

50

Annex 1: Procedural information concerning the process to prepare the evaluation

In August 2014, the Commission launched an evaluation of the VIS Regulation.

The evaluation is part of the Commission's Agenda Planning (2016/HOME/004) and Work Programme (COM(2014) 910 final — Annex 3).

The process developed in four phases:

phase I — Inception: August 2014-March 2015;

phase II — Data collection: May 2015-February 2016;

phase III — Exploitation: February-March 2016;

phase IV — Completion of Commission internal procedures and final adoption: April-September 2016.

An inter-service group steering group was set up at the launch of the evaluation to oversee the process. The Secretariat-General, the Legal Service, DG JUST and the European External Action Service participated in the group. The group met twice during the evaluation process (16 April 2015 and 15 April 2016).

The evaluation was performed internally. Hard data to support the assessment have been relatively easy to find. The main contributors were Member State authorities in charge of ***visa*** policy and those managing the VIS.

The evaluation criteria and questions were assessed both quantitatively and qualitatively.

51

Annex 2: Summary of findings on the implementation of the ***Visa*** Information System (VIS) Regulation based on Member States and eu-LISA reporting

I. RESULTS ACHIEVED AGAINST OBJECTIVES

1.1 Facilitation of the ***visa*** application procedure

The overwhelming majority of Member States that responded to [a questionnaire on implementation of the ***Visa*** Information System (VIS) agree that the introduction of the ***Visa*** Information System facilitated the ***visa*** application procedure: 60 % consider the VIS to have had a slightly positive impact on the procedure, while 11 % consider this impact strongly positive. 16 % of the responding Member States consider that the VIS had no impact on the ***visa*** application procedure, and 10 % consider the impact to be negative (5 % consider it strongly negative and 5 % slightly negative).

All responding Member States agree that the procedure was made slower and lengthier by the introduction of the VIS, because it requires biometric capture and the maintenance of the biometric equipment, and consequently ***more*** cumbersome for applicants as well. All Member States agree that the VIS has also made the procedure ***more*** secure in terms of due diligence and that applicants are better protected against identity theft.

However, those who consider the impact of the VIS positive emphasise that it has simplified decision making, by streamlining the exchange of data between Member States on applications and related decisions. Applicants' ***visa*** history is now easily ***available***.

Statistics from the eu-LISA system show that from 1 August to 15 October 2015 the average time taken to complete an examination procedure (from the moment of accepting the ***visa*** application until a ***visa*** was issued) was around 4 days. Most Member States take an average of 5 days to complete the procedure, but the range is wide: from less than a day (0 days) for one Member State to 13 days for another.

Some Member States consider that the impact of the VIS cannot, at this point, be fully evaluated, because it does not currently contain enough data about applicants and their ***visa*** history to simplify the ***visa*** procedure. When the VIS contains ***more*** information, ***more*** analysis will be possible and this will simplify the procedure.

1.2 Preventing bypassing of the criteria for determining the Member State responsible for examining the application

The prevailing view among the contributing Member States (63 %) was that the introduction of the VIS had no impact on preventing the bypassing of the criteria80 for determining the

80 Possibly due to the relative recent experience of ***visa*** applicants with the VIS, in particular in regions of the world with high migratory risks, the system has not had a large impact on preventing the applicants from

Member State responsible for examining ***visa*** applications. Only 31.5 % of the responding Member States considered that the VIS had a positive impact, either slightly positive (21 %) or strongly positive (10.5 %). However, none of the responding Member States thought the situation had worsened with the introduction of the VIS.

There is considered to be little advantage in checking the VIS for previous applications (especially recently rejected applications). The history of applications helps determine the main destination, which is very useful in cases where

the applicant uses a new (blank) passport for a new application. The criteria for determining the Member State responsible ***follow*** from the information provided in the application form, where the main destination for the visit is given. Previous rejection does not necessarily mean the current application will be rejected, nor is it grounds for the current application not to be handled by a given consulate.

A well-coordinated LSC remains an essential tool to fight ***visa*** shopping.

Member States that replied stressed that for the system to work satisfactorily it is extremely important that all Member States perform searches and linking of individual files in the VIS correctly and that the biometrics taken are of sufficient quality.

1.3 Facilitating the fight against fraud

The overwhelming majority of responding Member States — 84.2 % — agreed that the introduction of the VIS facilitated the fight against ***visa*** fraud, 42 % found this impact slightly positive, while 42.2 % found it strongly positive. 10.5 % consider that the VIS has had no impact on ***visa*** fraud. No Member State seems to consider that the VIS might, in any way, have facilitated fraud.

The main feature contributing to the fight against fraud are the fingerprints stored in VIS. The system thus provides a secure link to the identity of the applicant through biometrics and no 'look-alike fraud' is possible. However, this requires searches made on the basis of fingerprints, systematic linking of files, and biometrics of sufficient quality.

VIS is not intended to prevent fraud with documents/false passports presented as part of an application; to tackle this problem, when examining a ***visa*** application, ***visa*** authorities should use SIS II and Interpol's Stolen and Lost Travel Documents database. Consulates must be sure of the applicant's identity ***before*** taking fingerprints.

1.4 Facilitating checks at external border crossing points and within the territory of the Member States

The vast majority of the responding Member States (73.5 %) consider the introduction of the VIS to have facilitated checks at external border crossing points and within the territory of the Member States, 52.3 % considering the VIS to have a slight positive effect in this sense and 21.2 % considering the VIS to have a strong positive effect. 15.9 % of the responding Member States consider that the VIS had no impact on these checks at external border

continuing to attempt to bypass the criteria for determining the Member State responsible for examining a ***visa*** application.

53

crossing points and within the territory, and 5.3 % consider that the impact was slightly negative.

The main positive impacts relate to the enhancement of the quality of the ***visa*** checks, the increase in the amount of information accessible to relevant authorities and the VIS' contribution to the detection of and fight against fraudulent documents. The few responding Member States who did not notice any impact or consider the system to have had a slightly negative impact are mainly concerned about the increased time required for border checks. Poor-quality fingerprints and missing information in the VIS files were also mentioned as issues faced at external border crossing points. According to one Member State, the evaluation was also negatively impacted by the

difficulty of evaluating the system ***before*** the roll-out was completed and an increase in positive appreciation may therefore be expected in the future.

1.5 Assisting in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States

An overwhelming number of responding Member States — 78.9 % — were of the opinion that the introduction of the VIS helped with the identification of persons who do not, or no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States. 63 % consider this impact slightly positive, while 15.9 % consider that the VIS had a strong positive impact. 5.3 % of the responding Member States consider that the VIS had no impact on the identification of these persons and 5.3 % consider the impact of the VIS to have been slightly negative.

Most Member States consider that the VIS gives them the possibility to assess in an unambiguous way and in a timely manner if a person fulfils the conditions for entry to or stay in the territory of the Member States. One Member State stressed its positive impact on identifying a person who has no identity or travel document, thanks to access to fingerprints. The main concerns of the few Member States who consider that the system has had no impact or a slightly negative one on identifying people referred to the lengthy procedures mentioned above, though some Member States have already noticed improvement in that aspect. The lack of police equipment for identification during checks within the territory was also raised.

1.6 Facilitating the application of Regulation (EC) No 343/2003 (as replaced by Regulation 604/2013, the 'Dublin III Regulation')

The vast majority of the responding Member States — 63 % — consider that the introduction of the VIS supported the application of the Dublin Regulation to determine the Member State responsible for examining an asylum application. Almost 31.5 % consider the impact of the VIS to have been slightly positive, and 31.5 % consider it strongly positive. Almost 26.5 % consider that the introduction of the VIS had no impact on the Dublin procedure and 11 % did not answer. None of the respondents found this impact to be negative.

For asylum purposes, the VIS has been used by 12 Schengen Member States in 399 991 cases since October 2011 to help determine the Member State responsible under the Dublin

54

Regulation and by 15 Member States in 1 384 988 cases since October 2011 to support the examination of asylum applications. The vast majority of these VIS searches were carried out by four Member States. Feedback from Member States shows that VIS data yield evidence for determining the Member State responsible and facilitate 'take charge' requests. They also help with assessing the identity and credibility of applicants when an asylum application is being examined.

1.7 Contributing to the prevention of threats to the internal security of any of the Member States (on the basis of Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the ***Visa*** Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences)

For almost half of the responding Member States — 47.3 % — the introduction of the VIS had a positive impact on prevention of threats to the internal security of the Member States. For 42 % this impact was slightly positive and for 5.3 % it was strongly positive. For 10.5 % of respondents the introduction of the VIS had a limited impact and for 15.9 % no impact. 26.3 % of respondents did not rate its contribution to the prevention of security threats.

II. ASSESSMENT OF THE CONTINUING VALIDITY OF THE UNDERLYING RATIONALE FOR THE SYSTEM

2.1 Assessment of the continuing validity of the VIS as an instrument for supporting the implementation of the common EU ***visa*** policy

All responding Member States consider the VIS essential for the good functioning of the common ***visa*** policy and for supporting the common area of free movement. It has led to ***more*** streamlining and harmonisation of the ***visa*** application procedure, albeit rendering it lengthier and ***more*** cumbersome. It has minimised fraud and ***visa*** shopping, and enhanced the global security features of ***visa*** procedures. It facilitates and encourages communication between Member States.

By introducing increased transparency in the ***visa*** process, especially by linking applications, VIS seems to be an incentive for Member States to seek common practice when assessing applications, and so leads to ***more*** harmonised procedures. Using the VIS has also made cooperation between the Member States in individual cases both easier and quicker. Biometric identifiers are both reliable and immediately ***available***. This gives the consulates and the central ***visa*** authorities the information they need to determine whether the applicant in question has previously been issued with a ***visa***.

The VIS is useful both for consulates and centrally to analyse how the common rules are applied and to obtain early indications of the level of abuse of issued ***visas*** in specific locations. However, there are regional disparities in the way VIS obligations are implemented, for example when applying the exemptions from the rule to enrol biometrics.

The VIS has the potential to make the ***visa*** process and its end result ***more*** predictable for ***visa*** applicants, too, regardless of which Member State assessed the application. Allowing Member States to conduct searches in the VIS is a tool well suited to offering bona fide travellers a simplified procedure when applying for a ***visa***.

55

Where the VIS consultation on asylum applicants is properly done, it should lead to ***more*** uniform practice in assessing ***visa*** applications with a potential for asylum.

Member States also underlined the need to expand the use of VIS information and improve data quality (including alphanumeric data), which is essential to obtain full and reliable information for queries in the VIS. ***More*** detailed information on the reasons for rejection / withdrawal of an application and on revocation / annulation of a ***visa*** would be welcomed.

Some Member States suggested that the mandate given to eu-LISA needs to be extended in order to allow it to access the VIS for data analysis (trends) and for reporting on biometrics quality, in particular compiling statistics. Sharing statistics on hits in the VIS among Member States and with the EU bodies concerned would also provide information and the hard evidence needed to identify and support any change to the common ***visa*** policy.

Also, the VIS should be developed and unified with the Schengen entry/exit system. In addition, it could be the background to the e-***visa*** or EU travel authorisation system.

Member States indicated that a limitation of the assessment was imposed by the very recent and rather limited nature of the experience with the VIS, given that the worldwide roll-out had barely finished by the time the evaluation was carried out.

2.2 Assessment of the continuing validity of the VIS for performing biometric matching, primarily of fingerprints, for identification and verification purposes

Member States find the VIS an essential tool in the detection of identity theft and ***visa*** shopping and the biometric check as the key element that renders the VIS efficient. Biometric matching is considered the cornerstone of the common identification and verification procedure. Its applications in the ***visa***, asylum, migration and return policies are very much appreciated by practitioners.

The biometric match provides a strong means of identification and prevents the misuse of applications and fraudulent behaviour.

It helps to identify non-EU nationals who are staying irregularly and is a very useful tool for return purposes. As regards asylum, the VIS is a fast and reliable source of information to establish whether the asylum applicant has been granted a ***visa***, the identity of the asylum applicant and the identification document the person in question submitted for the ***visa*** application. In some cases there is no match in the VIS although the asylum applicant has applied for a ***visa***. Some authorities signalled that they have, in some cases, found the applicant in the VIS via an alphanumeric search, although the fingerprints search had not resulted in identifying the person in the VIS.

At the same time, many Member States emphasised the need to do ***more*** on data quality. Though rare, cases of a fingerprint-based match between two different persons have been found, resulting from poor-quality fingerprints. In some cases, poor-quality fingerprints discourage Member States from carrying out border checks using the VIS. eu-Lisa should be given a mandate to assist Member States in improving the quality of biometrics, e.g. with the delivery of fingerprint software kits.

Some Member States suggested adding a function in the VIS allowing an automatic check against other databases, such as the SIS or Eurodac.

Some Member States proposed that information on D-***visas***, including biometrics, should also be recorded in the VIS.

56

To make VIS searches ***more*** efficient for law enforcement purposes, the possibility of searching with latent fingerprints was suggested to be included in the law.

57

III. THE APPLICATION OF THE VIS REGULATION

3.1 Entry and use of data by ***visa*** authorities

3.1.1 Use of the procedures for entering data upon application

With one exception, responding Member States consider the current procedures provided in Article 8 of the VIS Regulation for entering data upon application, ***visa*** issuance, discontinuation, refusal, revocation, or extension are sufficient and effective for the purpose of further processing of the application, provided they are correctly ***followed*** and that all data are ***available***.

Long waiting times are sometimes reported when entering data and ***before*** receiving confirmation from the VIS of the identity of the applicant. It is unclear whether this is due to low system capacity, delays in communication between national systems and the VIS, or a break in transfer between the consular posts and the Member State's national system.

On Article 8(5) of the Regulation, which lays down rules on marking data which cannot be provided for legal or factual reasons, a further distinction was suggested in the second category between: (a) fingerprint(s) not in fact provided for technical reasons; (b) fingerprint(s) not provided because of permanent disability; and (c) fingerprint(s) not provided because of a temporary disability.

The Member State that considered the current rules as insufficient mentioned that the applicant cannot fill in all the information, only fragments. An example is given of a person travelling through three countries, when the application form only allows one hotel to be entered. It could be misleading for the consul examining a future application to compare the information from the passport (i.e. border-check stamps) and in the VIS application file, which only shows one country, i.e. the first country of entry.

Ten out of the 19 responding Member States reported having experienced various problems when entering data in the VIS. The most common problem arises because not all Member States seem to ***follow*** the same pattern for entering data. Also, some entries seem to be incorrect, incomplete or misleading. In rare cases, the applications sent contained the fingerprints or photograph of another person.

With very rare exceptions, all respondents reported having systematically checked for the existence of previous applications when entering data on admission and systematically linking them to earlier applications. Files are created for each applicant travelling in a group and systematically linked to those of the other applicants in the same group. However, problems were reported in the event of long system response times or of work overload, when the linking fails.

58

However, eu-LISA figures for October to December 2015 indicate great discrepancies between Member States in terms of the rates of operations linked to previous applications by the same person as a percentage of total applications made — from 0 % for one Member State (i.e. every applicant is a new one to the system) to 55.65 % for another Member State (i.e. over half of the applicants are already recorded in the system). Most often this rate is around 20 % to 24 %. It is, however, difficult to draw a conclusion on this basis, as the rate of linked applications may indeed vary significantly in practice. However, a general conclusion could be drawn, as the probability of only new applicants showing up at the consulate seems rather low. Thus, rates close to 0 % may indicate that there is no systematic linking; the service might not be technically implemented in the national information system.

As regards the use of 'grouping' operations for persons travelling in the same group, eu-LISA data reflecting entries between October and December 2015 show the same wide discrepancy between Member States' performance.

Thus, rates vary from as low as 0 % in two Member States to almost 62 % in one Member State. Five Member States have rates below 1 % (including the two that have 0 %), 1 Member State between 1 % and 2 %, 5 Member States between 2 % and 6 %, 1 Member State 7 %, 8 Member States between 10 % and 20 %, 2 Member States between 20 % and 30 %, 1 Member State around 32 %, 1 Member State 44 % and 1 Member State 62 %.

These figures seem supported by similar findings during the field visits part of SCHEVAL monitoring. For example, the consulate of one Member State was found not to systematically check against the VIS for previous applications lodged by the same person, nor to link them to the new application. This practice is not compliant with Article 8(2) of the VIS Regulation, or with Article 21(2) of the ***Visa*** Code.

In five instances, the Member States' consulates were found not to systematically link the applications of persons travelling together in a group when entering data in the VIS. This practice does not comply with Article 8(4).

In all these cases, recommendations had been addressed to the Member State monitored, to remedy the problems identified.

3.1.2 Use of the data to be entered

Most responding Member States (10) declared having experienced no problem when entering data into the VIS according to Article 9 to 14 of the VIS Regulation, i.e. on applications, ***visa*** issuance, discontinuation of an application, refusal, revocation or ***visa*** extension. Two responding Member States provided no reply or no statistics on this particular issue. Six Member States reported limited problems, including occasional inability to upload alphanumeric identification information about the applicant or biometric data or to register the ***visa*** sticker. Sometimes long delays are experienced in communication between the VIS and

the consulate, and it is unclear whether this is due to delays between the national system and the VIS, or to low capacity of the VIS database.81

Where particular data are not required to be provided for legal reasons or cannot in fact be provided, the specific data field in the VIS should be marked with 'N/A', in accordance with the legal basis. None of the responding Member States could provide figures on the use of the 'N/A' entry, as they are not collecting statistics on it.

When asked whether they systematically collect and enter in the VIS all information set out in Article 9 of the VIS Regulation, 11 Member States said yes, 3 said no, and 5 did not reply. Only one Member State provided some examples of difficulties preventing it from systematically entering the Article 9 data into the VIS. Such difficulties relate to the 'address' field during the registration of the applications, depending on the particularities of each country. Details of persons and companies issuing an invitation are sometimes not filled in the application form, so cannot be entered in the VIS. The lack of such data has to do with the training of the authorised consular staff and of the external service providers (ESPs). Another piece of information typically omitted by applicants in the application is the names of the parents.

Comprehensive statistics (see below) on filling-in of the Article 9 and Article 10 fields extracted from the VIS show, however, that only 'date of birth', 'intended date of departure', 'latest ***visa*** sticker number', 'latest ***visa*** type decision date', first name and surname, and the travel document number, type and validity are always filled in. By April 2015, around 70 % of some fields, such as '***visa*** type requested', 'occupation, employer name', and 'host organisation or host person', were being filled in, while the figure for 'place of residence, country' was around 80 %. This information is required to be systematically entered in the VIS, and 'n/a' filled in if it is not applicable, under Article 8

of the VIS Regulation. Its use becomes all the ***more*** relevant if there is prior consultation under Article 22 of the ***Visa*** Code, because a search using any fields in which data is missing yields no results and means the person being checked will not be found. The fields highlighted in red in the graphs below are often used as search criteria by Member States in prior consultation.

81 The reference to the low capacity of the system was made by the Member States; however, we note that capacity has been increased several times and is currently seven times ***more*** than what is needed for the VIS to function with its current parameters.

60

Figure 1. Fields to be entered in VIS, in line with Article 9

Source: eu-LISA

Figure 2. Fields to be entered in VIS, in line with Article 10

Source: eu-LISA

In addition to the missing fields relating to Article 9 and 10 of the VIS Regulation, some inconsistencies and a lack of common practice were identified particularly in relation to filling

61

in the ‘nationality at birth’ field and information concerning applicants with ***more*** than one current nationality.

For ‘nationality at birth’, monitoring (based on eu-LISA data taken from the VIS) showed that this field is currently filled-in in two different ways: some Member States use the historical name of the country (at the time of the applicant’s birth) and some the current name (e.g. ‘Soviet Union’ versus ‘Turkmenistan’). Either option is legitimate, but in practice this discrepancy leads to difficulties in identifying the ***visa*** applicant and even to security problems if search operations then fail. The matter has been discussed at various levels with the Member States and eu-LISA and as a result a recommendation was made that the nationality stated in the travel document should be used in such cases.

For applicants with ***more*** than one current nationality, the issue arose from a request by some Member States to have all current nationalities entered in the VIS, as they consider such information relevant to prior consultation under Article 22 of the ***Visa*** Code. So they asked for the VIS interface to be extended to allow this. To keep practice in line with the Regulation and prevent any inconsistency in applying the law (i.e. different Member States carrying out prior consultations based on different criteria), a recommendation was made that Member States carry out prior consultations only on the basis of the nationality stated in the travel document presented when applying for the ***visa***, into which a ***visa*** sticker will be inserted if a ***visa*** is granted.

Visa applicants must state whether fingerprints have been previously collected. It is possible they may make an error, either in stating that fingerprints have previously been collected, although they are subsequently not found in the VIS, or by stating that fingerprints have not previously been collected, although they are then found in the VIS. Most responding Member States could not provide quantitative data or evidence of such occurrences. A very few Member States provided figures showing very little occurrence of the former case (mostly below 1 %), and a rather

more frequent occurrence of the latter (over 7 % or 'often'). This suggests a rather cautious approach by applicants, consulates and ESPs in practice, i.e. people avoid taking the risk of having to come back to give fingerprints at a later date, and so have a tendency to give fingerprints even if it is likely that biometrics have already been entered in the system up to 59 months previously.

Schengen evaluation visits showed that decisions to revoke ***visas*** are not systematically entered into the VIS by two Member States. This practice is not compliant with Article 13 of the VIS Regulation (and Article 34(8) of the ***Visa*** Code) and therefore relevant recommendations have been addressed to these Member States.

3.1.3 Use of the VIS to examine applications

All responding Member States except one said they systematically consult the VIS when examining the ***visa*** application. One Member State said that in urgent cases checks on the history of applications can be overlooked, although in such cases a check against the records of the local consular post is required.

62

One responding Member State does not consult the VIS if a ***visa*** application is made in circumstances that do not raise doubts to its validity or authenticity. If the application is subject to prior consultation under Article 22 of the ***Visa*** Code or in cases of domestic consultation, sufficient data is usually provided by their own consular posts without having to consult the VIS. For this purpose, the VIS was used as confirmation of an applicant's identity and of whether the application was lodged in the proper consulate (representation cases).

Seven out of nineteen responding Member States (almost 40 % of respondents) experienced problems to various extents when consulting the VIS with the purpose of examining applications. These problems relate to errors in linking the applications, incomplete (missing data fields) or erroneous data, including poor-quality biometrics, long response times for consultations, and the existence of open 'junk' cases in VIS, which generate mistaken alerts relating to ***visa*** shopping. It was felt the information entered into the VIS about previous rejections could be ***more*** extensive.

3.1.4 Use of the data for reporting and statistics

In all responding Member States except one, the competent ***visa*** authorities have access to consult all the data provided for in Article 17 of the VIS Regulation for the purpose of reporting and statistics. Three of them declared they had allowed access to consult these data for purposes other than reporting or statistics, for example for monitoring the work of the consular authorities or for the purposes set out in Article 6(1) of the VIS Regulation, i.e. entering, amending, deleting or consulting data.

NB: The term 'solely' used in Article 17 seems to create a certain confusion in interpretation, as many respondents understood it as a limitation of the ***visa*** authorities' access to data. However, the word 'solely' refers to the purpose of reporting and statistics and does not affect the core competences of the ***visa*** authorities which, under Article 6, should have access to the data recorded in the VIS for the purpose of amending, deleting and consulting it.

This evaluation has shown that, although there is a clear legal provision on collecting statistics on the VIS, most Member States do not make full use of it. So the response rate to many of the quantitative questions addressed to the Member States was quite low and most answers referred to eu-LISA as the most appropriate source of

information on VIS statistics, as the entity that manages the central database where all the aggregated data can be found.

For example, when asked to provide information on the number of cases in which applicants were exempted from fingerprinting because fingerprinting was physically impossible, pursuant to Article 17(12) to (14) of the VIS Regulation, only 7 out of the 19 responding Member States provided any information; the others provided no reply or reported that they collect no such data.

As for data on the number of cases in which the applicant was exempted from fingerprinting by virtue of their status as heads of state or government, members of a national government, accompanying spouses or members of an official delegation, pursuant to Article 17(13) of the

63

VIS Regulation, again only 4 (SE, SK, EL, PT) out of 19 responding Member States provided some.

None of the responding Member States (including the four that provided data on the previous issue), was able to provide data on cases in which the applicant was not exempted from fingerprinting despite their status as heads of state or government, members of national governments, accompanying spouses or members of official delegation, despite this issue being intrinsically related to the previous one.

3.2 Access to data by other authorities

3.2.1 Use of the data for verification at external border crossing points

The vast majority of the responding Member States (12 out of 19) limit access to the VIS at external border crossing points to border authorities, while in 5 Member States access is open to other law enforcement bodies (such as customs services, immigration services, or federal police82) in accordance with their national responsibilities for border controls. However, all authorities given access to the VIS for checks at the external borders were properly notified to the Commission in accordance with Article 6(3) of the VIS Regulation and a consolidated list for the Member States has been published in the Official Journal.83

In terms of the number of checks, although only 5 Member States were in a position to provide data on the percentage of ***visa*** holders whose ***visa*** is recorded in the VIS and who have been checked against the VIS at external border crossing points, the average percentage is very encouraging, at 96.5 %.

A big majority (73.7 %) of the responding Member States confirmed that the obligation to check the identity of the ***visa*** holder and the authenticity of the ***visa*** sticker at the border by searching on the number of the ***visa*** sticker in combination with fingerprints was introduced from October 2014. Very little information is, however, ***available*** on whether this obligation is systematically met (5 out of 19 Member States said yes, one said no, while the remaining 13 did not give further details).

82 Some Member States do not have a specific ‘border guard’: the work is done by the ‘police’.

83 An updated list is in course of publication at the time of drafting this report. The last update was in 2014: OJ C 106, 9.4.2014.

Figure 3. Comparison of ***visas*** issued between January and November 2015 and ***visas*** checked at the borders up to 1 March 2016

Source eu-LISA

On average, less than 1 in 2 ***visas*** are checked.

Intended Border of First EntryIssued VisasVias not checkedGlobal Check RateAUSTRIA142,39762,00656.46%BELGIUM173,696114,21034.25%CZECH REPUBLIC109,40628,93773.55%DENMARK48,68721,96554.89%ESTONIA85,40210,13788.13%FINLAND534,889168,03668.58%FRANCE1,873,0451,277,18731.81%GERMANY1,057,534668,58236.78%GREECE536,962297,555344.59%HUNGARY31,6375,16583.67%ICELAND4,4723,38824.24%ITALY677,081506,55425.19%LATVIA39,0827,18281.62%LIECHTENSTEIN923759.78%LITHUANIA209,64024,07088.52%LUXEMBOURG2,0521,26538.35%MALTA15,1174,71268.83%NETHERLANDS228,968107,21053.18%NORWAY30,0157,57174.78%NOT APPLICABLE10910.00%POLAND877,183136,46784.44%PORTUGAL221,82490,60559.15%SLOVAKIA20,4902,31947.21%SLOVENIA17,6638,65850.98%SPAIN768,702556,23627.64%SWEDEN65,36212,74380.50%SWITZERLAND320,090216,27232.43%[EMPTY]344,188114,46466.74%8,435,6864,453,54047.21%***Visas*** issued from 01/01/2015 - 30/11/2015 (Per Intended Border of First Entry)

65

Figure 4. Average time for processing ***visa*** checks at MS' borders

Source eu-LISA

However, according to the statistics provided by eu-LISA, checks based on fingerprints as a percentage of total checks on ***visa*** holders against the VIS at external borders steadily increased, from 0.55 % in October 2011 (first data ***available***) to almost 23 % in November 2015. Interestingly, this number stood at only 3.22 % in September 2014, the month ***before*** most of the Member States started to implement the requirement to check the identity of the ***visa*** holder and the authenticity of the ***visa*** sticker at the border by searching on the number of the ***visa*** sticker in combination with fingerprints.

It would be impossible to reach 100 %, because of cases where it is legally or physically impossible to record the fingerprints in the VIS, and the limitations of the calculation method (which assumes that all ***visa*** holders will cross the border at least once within three months of

Member State1st Linewith FP1st Linewithout FP2nd Linewith FP2nd Linewithout FPAustria1.130.158.150.14Belgium1.290.246.200.18Denmark1.520.474.890.33Estonia1.620.409.390.45Finland1.230.274.530.33France1.260.3311.490.20Germany1.300.278.030.27Greece1.530.316.600.48Hungary1.160.1126.580.11Iceland1.390.35N/AN/AItaly1.410.1825.250.20Latvia1.930.3910.950.39Liechtenstein0.000.000.000.00Lithuania1.550.8619.210.17Luxembourg1.230.23N/A0.33Malta0.690.485.200.27Netherlands1.430.186.930.17Norway1.590.385.340.27Poland1.290.248.470.17Portugal1.310.346.420.23Slovakia1.430.1510.680.24Slovenia1.230.15N/A0.13Spain1.370.316.610.31Sweden1.740.3714.450.33Switzerland1.260.245.990.34The Czech republic1.280.147.250.13VIS Border average processing time (seconds)

66

the date of application84 and does not take into account the proportion of multiple entry ***visas***). But still, the low number of checks based on fingerprints, as a percentage of all checks on ***visa*** holders against the VIS at external borders, has raised concern about whether the VIS Regulation is being properly implemented. The issue has been constantly under the attention of the Commission and considerable work has been done with the Member States to raise awareness of the need to properly and fully apply the law.85

The current rise in fingerprint (FP-based) checks shown in the Figure 5 below is, in that respect, encouraging (up 19.24 % between October and November 2015).

Figure 5. Comparison between total number of checks and checks based on fingerprints

Source: eu-LISA

The main difficulties linked to using the VIS for checks at external border crossing points are reported to be poor-quality fingerprints (see the graph below on fingerprint quality); missing data, especially in regions where it is newly rolled-out (see the graph below on missing facial images, for example), the fact that some fingerprints have been switched and are therefore not linked to the right person, and the length of the process.

84 Article 9 of the ***Visa*** Code: ‘Applications shall be lodged no ***more*** than three months ***before*** the start of the intended visit’.

85 This has been discussed especially at various meetings of the Frontiers and ***Visa*** working parties and the VIS Advisory Group.

Figure 6. % of applications with poor quality fingerprints

Source: eu-LISA

* 0-FTE feature: as from the end of 2014 fingerprints are accepted by the VIS irrespective of their quality. This measure requested by some Member States and agreed upon by the VIS Advisory Group, means fingerprints are ***more*** often ***available*** for border checks. In the vast majority of cases, fingerprints originally rejected by the VIS were of sufficient quality for border checks. A side-effect of this measure is a slight decrease in fingerprint identification accuracy at consular posts, in examining ***visa*** applications and in second-line checks at borders. This slight decrease is offset by additional checks by the end-user on the facial image ***available*** in the VIS. This measure does not exempt consulates from attempting to collect fingerprints of the highest quality, in particular by using a software kit embedded locally in the fingerprint capture devices and by signalling potentially poor quality in real time.

Figure 7. % of cases in which facial image is not ***available*** in VIS

Implementation of the 0-FTE feature as from October 2014*

Source: eu-LISA

In 9 out of the 12 responding Member States, if data quality is unsatisfactory the border guards contact the Member State which issued the ***visa*** (either the consular post or the central ***visa*** unit). In the other 3, the border guards proceed to a second-line check. When asked to suggest options for solving cases of insufficient data quality at borders, Member States suggested a 24/7 centralised call centre or contact point and/or a quality check mechanism to be used when data are entered in the VIS.

3.2.2 Use of the data for verification within the territory

According to the data provided by eu-LISA (see Figure 8), the use of VIS data for checks within the territory varies greatly between Member States. Only half made use of VIS data for that purpose and in ***more*** than 61 % of cases searches were not carried out systematically but only for certain non-EU nationals. In addition, in 2015, ***more*** than 60 % of searches were made by the same Member State.

Figure 8: Monthly usage (by Member State) of services supporting verification of personal data within Schengen territory (Article 19 of the VIS Regulation)

Source: eu-LISA

Among the authorities with access to the VIS, most Member States referred to the police and the border guards; four to immigration services, and three to asylum services. One Member State provided direct access not only to border services and the police, but also to the customs service and local government, while indirect access was also given to courts, the prosecutor's office, the internal security agency, the foreign intelligence agency, the central anticorruption

69

bureau, the tax control authorities, and the government protection bureau, plus military intelligence, counter-intelligence services and the police.

The dates as of which verification had been carried out ranged between November 2011 and June 2015. Approximately 42 % of the responding Member States conducted verification only for certain non-EU nationals, while only 26 % did it systematically in combination with the fingerprints. The others provided no reply.

As regards the number of cases in which the VIS was used for the purpose of verification within the territory, only 1 Member State provided a number; most respondents gave no reply or replied that no statistics were ***available***. Asked for the number of cases in which a person was identified staying irregularly, only 2 Member States provided figures, one of which previously claimed to have used VIS for the purpose of verification in 0 cases. 21 % of respondents stated that their authorities responsible for carrying out checks within the territory have experienced difficulties in meeting their obligation to verify the identity of ***visa*** holders.

16 out of the 19 responding Member States (84 %) affirmed the utility of the VIS for identifying persons who may not or may no longer fulfil the conditions of stay or residence on the territory of the Member State.

3.2.3 Use of the data for identification

Use of VIS data for identification, either at external border crossing points or within the territory, was recorded in almost all Member States (92 %) between October 2011 and November 2015 but to widely varying degrees (see Figure 9 below).

70

Figure 9. Monthly usage of VIS (by Member State) for identification purposes, within the territory and at the borders

Source: eu-LISA

Approximately 84 % of responding Member States confirmed that their authorities make use of the VIS to identify persons who may not, or may no longer, fulfil the conditions for stay or residence on the territory of the Member States.

With regard to questions about the percentage of checks in which the VIS helped to ascertain that the person had a ***visa*** which was no longer valid and the percentage of searches which could not be made using fingerprints, half of the respondents indicated 0 cases, while the others gave no reply or replied that no statistics were ***available***. One Member State replied that most of these checks are made with the information written on the sticker and if necessary counter-checked with the VIS.

In cases where a search with fingerprints could not be made, those few Member States who provided an answer use the photo and other alphanumeric data entered in the VIS and compare them with the travel document: e.g. the name, passport number, ***visa*** sticker number, and date of birth. Otherwise they have to ask partner states' embassies for information.

Only 26 % of the responding Member States have experienced difficulties in carrying out the obligation to verify the identity of ***visa*** holders at external border crossing points, such as the lack of response of the central system.

To sum up, Member States are far from using the full potential of the VIS for return purposes. Unfortunately, the ***available*** information does not shed light on the reasons for this situation (whether the cause is the lack of internal coordination, practical or legal obstacles, lack of awareness or lack of fingerprint capturing devices on the spot).

3.2.4 Use of the data for determining responsibility for asylum applications

One of the criteria for determining responsibility for examining an application for international protection is whether the applicant is in possession of a ***visa*** issued by a Member State,86 and if so, whether the ***visa*** has expired (and when) and whether the ***visa*** was issued on behalf of another Member State. To help determine which Member State is responsible, Article 21 of the VIS Regulation allows the competent asylum authorities to search in the VIS.

86 Article 12 of the 'Dublin III' Regulation (EU) 604/2013/ Article 9 of Regulation (EC) 343/2003.

71

Figure 10. Monthly usage of VIS (by Member State) for the purpose of determining the Member State responsible for deciding on an asylum application. Source: eu-LISA

72

The eu-LISA statistics (see Figure 10 above) suggest that in a total of 399 991 cases, VIS searches were carried out for this purpose by 12 Member States between November 2011 and November 2015 inclusive. Total monthly VIS searches for this purpose increased from 496 in February 2012 to 11 778 in September 2014 and, after a slight fall, rose rapidly again from 15 954 in July 2015 to 44 173 in November 2015, with a peak in October 2015 (56 437).

The vast majority of these searches were made by only two Member States, with 269 387 and 96 638 searches respectively. At the other end of the spectrum, one Member State searched the VIS once in the second half of 2014 and once again in November 2015; another Member State searched only in very sporadic cases, and another Member State in a single case.

Member States' replies suggest that the VIS data was used to provide evidence for determining the Member State responsible not only when a search was carried out for this purpose under Article 21 of the Regulation, but also when a search was carried out under Article 22 in the context of examining the application.

Member States' replies show some inconsistencies with the eu-LISA statistics. Only seven of the Member States that searched the VIS according to those statistics to determine the Member State responsible (partly) replied to the relevant sections of the questionnaire. On the other hand, seven Member States submitted some observations even though, according to the eu-LISA statistics, they do not yet use the VIS or use it only for examining asylum applications. Eight Member States, including four for which the statistics show no searches under Article 21 of the VIS Regulation, stated that they had given their competent asylum authorities access to search the VIS using the applicant's fingerprints under Article 21. One Member State had given access to search with alphanumeric data only. In one of those Member States, all officials of the competent asylum authorities have access to the VIS for this purpose; in the other Member States access is only given to certain categories of officials.

Member States' experience shows that the VIS helps in determining the Member State responsible and the procedures for 'take charge' requests based on the evidence of the ***visa*** information. Examples of the most relevant situations where the use of the VIS significantly contributed: providing evidence solving or clarifying cases of responsibility for the examination of applications for international protection, where applicants were not in possession of the relevant travel or identity documents, in the absence of a Eurodac hit or of a credible statement about their itinerary, or for establishing the age of the applicant or the responsibility of a Member State on whose behalf the ***visa*** has been issued. One Member State reported that in 2014 almost 500 out of 1 100 'take charge' requests on the basis of the ***visa*** criteria were based on a VIS hit. Another Member State, which does not use the VIS regularly for determining Member State responsibility, noted that the number of incoming 'take charge' requests based on VIS hits has increased considerably. One Member State reported that in 2015 (up to 17 November) 705 'take charge' requests had been accepted by other Member States based on evidence from the VIS and 59 requests had been refused on the basis of evidence from the VIS.

73

Of those Member States who gave an overall rating as regards the use of the VIS for asylum purposes, eight see a strong positive impact of the use of the VIS on the application of the asylum policy. The use of the VIS significantly intensified in the last months of the reporting period, although, according to the eu-LISA statistics, one of those Member States did not use the VIS for asylum purposes at all. Four Member States (one of which did not use the VIS for asylum purposes) see a slightly positive impact. One other Member State that searches the VIS to determine the Member responsible and three other Member States that did not use the VIS for asylum purposes see no VIS impact on the application of the Dublin Regulation.

As regards refusals of a 'take charge' request, some requested Member States considered the VIS hit not enough proof of entry into the territory, particularly if the ***visa*** had expired, or also required submission of a passport with an entry stamp. They also considered the VIS hit to be insufficient proof in cases where the ***visa*** had expired no ***more*** than six months ***before*** the application for asylum was made.

3.2.5 Use of the data for examining the application for asylum

Article 22 of the VIS Regulation provides that the competent asylum authorities may search in the VIS for the purposes of examining an application for international protection.

74

Figure 11. Monthly usage (by Member State) of VIS for the purposes of examining an asylum application. Source: eu-LISA

69

The eu-LISA statistics (see Figure 11 above) indicate that in total approximately 1.4 million VIS searches were carried out for this purpose by 16 Schengen Member States between October 2011 and November 2015. Total monthly VIS searches for this purpose increased from 284 in October 2011 to 121 151 in October 2015 and 109 459 in November 2015.

The vast majority of the searches under Article 22 of the VIS Regulation were carried out by only four Member States, which made 551 830, 477 068, 118 408 and 104 136 searches respectively.

Four Member States used VIS data for this purpose only in sporadic cases, i.e. for 138, 39, 9, and 2 cases respectively.

According to the figures submitted by the responding Member States, which do not always match the eu-LISA statistics, seven Member States have given their competent asylum authorities access to search the VIS using an applicant's fingerprints for the purposes of examining the asylum application, and one Member State allows searches with alphanumeric data only. In one Member State all of the authorities' officials have access to the VIS for this purpose; in one other Member State access is only granted to certain categories of officials.

Member States' experience confirms the utility of VIS data for examining an application for international protection, in particular for assessing applicants' credibility (taking into account other information), for identifying applicants who have few or no travel or identity documents, and for identifying the applicant's country of origin. In two Member States, the VIS was checked when examining 99 % and 94 % of all applications.

3.3 Retention period, amendment and deletion of data

Under Article 23 of the VIS Regulation, each application file should be stored in the VIS for a maximum of five years, without affecting the deletion provisions in Articles 24 and 25 or record keeping as referred to in Article 34. The VIS became operational on 11 October 2011 and thus the end of the retention period will start applying as of 11 October 2016. It is therefore not possible, at the time of this evaluation, to assess whether the retention period has been properly applied. No statistics are ***available*** on this topic.

As regards the amendment of data, as provided for in Article 24 of the VIS Regulation, eu-LISA reporting shows that the 'update application' operation is used to delete individual data (in order to correct the application data) and to make other small data corrections. Often Member States use the operation 'update application' to insert data to complete the uploading of the application. From a technical point of view, it is therefore not possible to distinguish whether the 'update application' operation is used to insert new data (the practice referred to) or merely to correct data already inserted. To cover those cases, the creation of another operation (CorrectApplication) could be proposed.

70

An overview of data modification after issuing the ***visa*** between the VIS' entry into operations in October 2011 and November 2015 is presented in Figure 12 below. The general trend shows a net decrease over time of the 'update' application (from almost 40 % at the launch of the system in October 2011 to 3 % in November 2015), and of the 'biometric' deletion of data (which fell from 2 % to 0 % in a matter of few months ***following*** the launch of the system).

VIS application modifications performed after issuing the ***visa***

Month

Applications

Application UPDATE

UPDATE %

Application DELETE

Biometric DELETE

Bio. DELETE %

2011/10

71 829

28 250

39 %

0

1 310

2 %

2011/11

99 630

26 192

26 %

0

1 168

1 %

2011/12

122 000

26 847

22 %

0

1 091

1 %

2012/01

105 296

16 697

16 %

0

872

1 %

2012/02

107 473

37 629

35 %

0

497

0 %

2012/03

127 209

24 146

19 %

0

395

0 %

2012/04

129 087

26 652

21 %

0

251

0 %

2012/05

160 710

59 055

37 %

0

303

0 %

2012/06

176 362

28 634

16 %

0

206

0 %

2012/07

162 937

28 204

17 %

0

185

0 %

2012/08

136 599

27 748

20 %

0

185

0 %

2012/09

137 867

24 622

18 %

0

117

0 %

2012/10

185 371

23 873

13 %

0

250

0 %

2012/11

177 174

23 667

13 %

0

339

0 %

2012/12

169 636

19 347

11 %

0

329

0 %

2013/01

172 057

21 131

12 %

0

208

0 %

2013/02

179 243

25 159

14 %

0

226

0 %

2013/03

221 191

52 266

24 %

0

793

0 %

2013/04

270 919

67 516

25 %

0

783

0 %

2013/05

323 769

84 164

26 %

0

1 375

0 %

2013/06

373 006

93 767

25 %

0

1 166

0 %

2013/07

419 396

97 843

23 %

0

925

0 %

2013/08

304 802

72 109

24 %

0

374

0 %

2013/09

320 758

31 910

10 %

0

488

0 %

2013/10

285 155

30 773

11 %

2

375

0 %

2013/11

297 820

28 820

10 %

0

318

0 %

2013/12

279 715

23 018

8 %

0

377

0 %

2014/01

284 113

24 259

9 %

0

468

0 %

2014/02

339 112

28 322

8 %

0

341

0 %

2014/03

446 240

40 123

9 %

0

482

0 %

2014/04

470 531

40 215

9 %

0

691

0 %

2014/05

543 981

44 275

8 %

0

827

0 %

2014/06

606 463

53 952

9 %

0

771

0 %

2014/07

583 842

51 123

9 %

0

769

0 %

2014/08

467 195

44 245

9 %

0

462

0 %

2014/09

472 511

44 415

9 %

0

550

0 %

2014/10

458 416

37 459

8 %

1

425

0 %

2014/11

434 002

34 127

8 %

0

389

0 %

2014/12

407 549

27 805

7 %

0

306

0 %

2015/01

380 073

26 950

7 %

0

503

0 %

2015/02

434 085

30 058

7 %

1

525

0 %

71

2015/03

586 598

37 266

6 %

0

767

0 %

2015/04

648 574

42 804

7 %

0

579

0 %

2015/05

773 489

65 049

8 %

0

676

0 %

2015/06

972 834

89 995

9 %

0

670

0 %

2015/07

1 022 585

74 564

7 %

0

867

0 %

2015/08

871 390

53 130

6 %

0

733

0 %

2015/09

829 825

104 354

13 %

0

1 159

0 %

2015/10

891 202

68 246

8 %

2

2 476

0 %

2015/11

979 596

34 277

3 %

0

1 205

0 %

Figure 12. VIS application modifications performed after issuing the ***visa***

Source: eu-LISA

Most Member States provided no information as regards data deleted or amended. The few that did so (5 out of 19 Member States) noted that incorrect data is usually corrected. In such cases, the procedure is that the Member State that finds the incorrect data sends a VIS Mail message to the ***visa*** authority of the Member State responsible, asking it to correct the data in the VIS. If a consulate/embassy receives such a request, it will send it to the national competent authority to check and if necessary to correct or delete the data. If ***visa*** data entered by another Member State is incorrect or breaches the VIS Regulation, that Member State is informed through a VIS Mail message.

Very few cases of data deletion under Article 25 of the VIS Regulation (Advance data deletion) have been recorded to date (as shown by the eu-LISA statistics above) and they are normally situations where a person obtains citizenship. However, although incorrect, one Member State also reported the practice of deleting a ***visa*** application and creating a new one if an error is found.

Another practice identified, when the wrong dossier is selected in the VIS, is to cancel the electronic application and enter a new one in the system. In such cases, there is no need for any kind of correction or deletion of data in the VIS.

3.4 VIS operation and responsibilities

3.4.1 State of play of the VIS roll-out

The Commission took the decision to launch the VIS in accordance with the legal basis, when the conditions under Article 48(1) (a), (b) and (c) were met, i.e. once:

• the implementation of the central VIS, national interfaces and the communication infrastructure between them was finalised, according to Article 45(2);

• comprehensive testing of the VIS had been carried out; and

• Member States validated the technical arrangements and notified them to the Commission.

72

Consequently, Commission Implementing Decision 2011/636/EU set the date of 11 October 2011 as the date on which the VIS would start operations.

The VIS was deployed region by region, until all Schengen countries' consulates across the world were connected. The Commission decisions on the sequence of the VIS' geographical roll were adopted based on criteria set out in the VIS Regulation (risk of irregular immigration, threats to the internal security of Schengen countries, technical feasibility of collecting biometrics). There were three decisions that addressed this:

1) Commission Decision 2010/49/EC of 30 November 2009 determining the first three regions for the start of operations of the ***Visa*** Information System (North Africa, and most of the Middle East);

2) Commission implementing Decision 2012/274/EU of 24 April 2012 determining the second set of regions for the start of operations of the VIS (eight regions in Africa, the Americas, Central and South-East Asia, the Caribbean and Australasia); and

3) Commission implementing Decision 2013/493/EU of 30 September 2013 determining the third and last set of (12) regions for the start of operations of the VIS (the Eastern Partnership countries, Russia, China/Japan and neighbouring countries, India/Pakistan and neighbouring countries, the European 'microstates', the UK/Ireland, the other EU Member States).

The Commission then adopted implementing decisions to determine the date from which the VIS was to start operations in each of the regions set out in the Decisions listed above. It adopted 15 such decisions between September 2011 and February 2016 (these are listed in Annex 6).

The start of operations meant that consulates started collecting fingerprints and digital photos from ***visa*** applicants and that the applicants' data were stored in the VIS. Once in the system, the data can be consulted by all ***visa***-issuing authorities of the Schengen Member States, and is counter-checked by border authorities when a ***visa*** holder enters the Schengen area.

The global roll-out was initially scheduled to last three years from the launch of the VIS (by October 2014), but was delayed until the end of November 2015. Schengen Border Crossing Points (SBCPs) were defined in the first roll-out Decision as a separate region for the VIS roll-out, to make it possible to use the VIS to issue ***visas*** at borders, but it was decided to first roll out to the regions covered by the second and third Decisions and to leave SBCPs for last. The technical preparations that Member States had to carry out as a prerequisite to the VIS roll-out in the SBCPs meant that it was only possible to roll out in this region on 29 February 2016.

Schengen countries have had the possibility to start using the VIS, with or without collecting ***visa*** applicants' fingerprints, ahead of the general roll-out, provided they notified the Commission first. Nineteen Member States used this possibility in various locations, two used it for all their consulates worldwide since October 2011, and twelve Member States used it for

73

the SBCPs. The Member States who chose to roll out the VIS ahead of its general deployment did so without collecting fingerprints, in order to maintain the coordinated character of the roll-out and to avoid creating an uneven playing field between consulates present in a certain location.

Member States encountered no major problems since the VIS entered into operations. Most reported issues were of limited severity and related to the quality of biometrics, in particular in certain regions at the beginning of the roll-out, where climatic conditions lead to poor fingerprint quality. During the roll-out (when ***visa*** stickers were marked as 'VIS 0' and 'VIS'), some ***visa*** stickers were issued with a 'VIS' mark even though fingerprints were not collected.

3.4.2 Operational management of the VIS

From the first stages of planning in 2004, the Commission took responsibility for the development and entire implementation process of the VIS. The operational management of the VIS was delegated to the French Administration (C.SIS) for the first year of operation (between going live on 11 October 2011 and 30 November 2012), based on a contract of services. On 1 December 2012, eu-LISA ('also the Agency') started operations and took over the operational management of the VIS, in line with the VIS Regulation.

Supervision activities taken over by the sTESTA87 network include: the review of operational and project reports; verifying the reports' correlation with the eu-LISA's records and investigating discrepancies; and participation in regular operational meetings with the network provider, Orange Business Services (OBS). The Eu-LISA took over coordination from the Commission and restructured communication between sTESTA and Member States so that it is always involved in communication between them if any part of the VIS site is affected. On eu-LISA's side, supervision and coordination activities are carried out by the Network Infrastructure Sector. The security officer in charge of the sTESTA network is involved in: the change management process, where eu-LISA reviews and approves all change requests that might affect the security of the sTESTA infrastructure; the review of monthly security reports; approval of the generation of smart cards used for the TAPs and related administrative tasks; the biweekly DG HOME SOC88 operations meetings.

The eu-LISA develops and implements comprehensive governance and operational frameworks based on best practice and current industry standards. It ensures efficient and cost-effective system management by continuously monitoring and developing operational processes. It is gradually applying IT service management based on ITIL best practice. The

87 The sTESTA network service — i.e. the secured Trans-European Services for Telematics between Administrations — is a European network for exchanging data between various public administrations. The network uses internet protocols to ensure universal reach, but is operated separately from the internet. It provides guaranteed performance and high levels of security and has connections with all EU institutions and national networks.

88 Service Operation Centre.

following ITSM processes have already been defined and put into practice: the incident management process, problem management process, request fulfilment management process, access management process, change management process, configuration management process, release and deployment management process, test management process, service-level management process, and service catalogue management process. The VIS is continuously monitored and a technical team is on-site 24/7.

eu-LISA has increased the capacity and performance of the VIS by implementing infrastructure- and software-focused improvements in the VIS and the BMS89. Projects finalised include new flow control measures at VIS level, the VIS middleware, server and database upgrades, and introduction of a ***more*** modern and efficient alphanumeric search engine. eu-LISA is now developing a new test environment, exploiting the benefits of virtualisation and examining possibilities related to an active-active central unit to backup central unit (CU-BCU) connection.

eu-LISA staff are bound by the obligation of confidentiality under the Staff Regulation, internal security rules and individual responsibilities included in their security clearance briefing. sTESTA staff are bound by the obligation to hold valid security clearance (SOC staff and field engineers) and the related obligation of confidentiality. A background screening is carried out for each staff member, and a confidentiality clause is included as a contractual obligation.

The evaluation carried out by the Commission in 201590 concluded that the eu-LISA had overall achieved its objective of effectively ensuring the operational management of the three IT systems entrusted to it.91 The evaluation found that eu-LISA successfully fulfilled the tasks entrusted to it in its establishing Regulation and under the service-level agreements (SLAs) in place. It correctly developed the systems, and met the requirements stemming from security, data protection and industry best practices. It also put in place the resources and organisational framework needed to cope with tasks related to the development of the systems under its responsibility (ITILv3, Prince2, ISO2700x).

Nevertheless, the evaluation also identified areas for improvement, the most important of which are discussed below:

− Although eu-LISA made commendable progress on implementing ITILv3 best practices, there is still work to be done. For instance, the evaluation identified the need to strengthen the monitoring of implemented IT process performance and to extend the scope of performance indicators, which are currently limited to business performance.

89 Biometric Matching System, a component of the VIS specialised in fingerprint-based services such as authentication, identification and quality assessment.

90 Independent external evaluation of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice - eu-LISA Final Evaluation Report, PDF/Volume_01, catalogue number DR-01-16-464-EN-N, ISBN 978-92-79-58236-3, doi 10.2837/76935.

91 The VIS, the SIS II and EURODAC.

75

− There is a risk to business continuity, linked to the absence of a unique and transversal Disaster Recovery Plan and Business Continuity Plan covering all three systems (e.g. for staff, facilities, resources, etc.). This should be addressed.

− On capacity management, the evaluation identified a need (e.g. VIS Evolution Case Study) for eu-LISA to put in place a review process that would make it possible to regularly review system capacity needs with Member States. This should be based on the statistics generated from the systems and a prospective exercise.

− On IT security, the evaluation identified a need to hire a cross-functional architecture management person, to be in charge of validating infrastructure choices, selecting the application technology and implementation at a transversal level, across systems.

− On data protection, the evaluation identified a need to ensure that appropriate data protection clauses are included in agreements with external contractors. Moreover, it identified existing concerns about the production of data quality and data analysis reports. The extent to which eu-LISA can access the databases to produce these reports is unclear since the current legal framework does not provide for an explicit mandate, especially regarding data analysis reports (i.e. reports analysing data added to the systems by Member States). There is a need to further clarify this issue in a future update to or reform of the current legal framework.

In its meeting of 15-16 March 2016, the eu-LISA's Management Board took due note of these recommendations and committed to adopting an action plan to address them by March 2017.

3.4.3 Use of the VIS for consultation and requests for documents (VISION, VIS Mail 2)

The VIS Mail Communication Mechanism ('VIS Mail Mechanism') is based on Article 16 of the VIS Regulation, and aims to provide a standard way of exchanging business and administrative messages via the VIS. Personal data sent via this mechanism must be used solely for the consultation of central ***visa*** authorities and consular cooperation.

Since the VIS started operations, VIS Mail 1 has been ***available*** for sending information related to consular cooperation, requests for supporting documents, and advance data deletion.

Since 20 January 2016, VIS Mail 2 has replaced the Schengen Consultation Network as per Article 46 of the VIS Regulation (and as agreed by the ***Visa***/VISION92 Working Party in May 2015). From this date onwards, all new requests have been sent via the VIS infrastructure using the VIS Mail Mechanism.

VIS Mail 2 is used for consultations and to send information between Member States, based on Articles 8, 22, and 31 of the ***Visa*** Code. A Member State is able to send a message with a VIS application number and indicate the Member State to which the message is addressed. The recipient Member State(s) can send its (their) response via the VIS Mail Mechanism

92 Reference: 9074/15 ***VISA*** 194 SIRIS 38 COMIX 236.

quoting the same VIS application number. All data related to the applicant concerned is then ***available*** in the VIS.

In October 2015, OBS handed over the VIS Mail infrastructure to eu-LISA, and it has since been responsible for the operational management of VIS Mail exchanges, its network infrastructure, and the provision of VIS Mail statistics.

eu-LISA identified a need for close coordination, proper communication, alignment and close ***follow***-up of actions in order to ensure a successful transition. It set up the Transition Board, an informal group managing all preparatory actions, risks, prerequisites and procedures for the transition from VISION to VIS Mail 2. In cooperation with Member States, eu-LISA also drafted Transition Guidelines.

In order to facilitate Member States' preparations, eu-LISA also updated the VIS Mail Operational Guide and the VIS Mail global campaign 'test design description' document. The global testing phase lasted from September 2015 until mid-December 2015. At the end of this phase, all Member States formally declared their readiness to comply with the Council's conclusions.

eu-LISA reported that usage of VIS Mail 1 has been limited. This could be explained by technical reasons, Member State(s) not meeting specifications, or the system's limited business coverage and thus limited interest for end-users.

As identified by the European Data Protection Supervisor (EDPS) and indicated in the Commission's implementing decision adopting VIS Mail specifications, the VIS itself could be used for the direct exchange of well-structured messages, instead of relying on a separate VIS Mail Mechanism based on SMTP. Compared to using SMTP, this approach would be ***more*** reliable and would be implemented using the same logic as for already existing exchange mechanisms used by Member States cooperating through the VIS. If this option is legally endorsed, eu-LISA could include it in a future VIS release.

3.4.4 Communication infrastructure

The Commission's work relating to the communication infrastructure between the central system and national interfaces started with the preparation and publication of tendering specifications for the sTESTA framework contract. After this contract was signed in September 2006, DG HOME signed a specific contract for the VIS on 18 December 2007. The network components were subsequently implemented in each Member State and in the central domain, both on the main and the backup sites. Since the VIS started operations in 2011, the contract includes operations and monitoring activities related to the VIS network.

The 2008-2010 budget for developing the communication infrastructure rose to slightly above EUR 20 million, and the annual operational budgetary ranges varied slightly between 2011

77

and 2015, around EUR 8.5-8.7 million. This is for the 26 Member States connected to the VIS and the 493 preparing to connect.

After a new framework contract was signed with T-Systems in 2013, a new contract with OBS was negotiated and signed in August 2014, and is still in force.

The contracts are for the delivery, monitoring and maintenance of one local national interface (referred to as LNI, terminal access point or network access point) for each Member State that connects with the secure communication network. The local national interface contains the encryption devices dedicated to the VIS.

The contracts also allow for the delivery, monitoring and maintenance of an optional backup local national interface ('BLNI') which has the same contents and function as an LNI. A BLNI connects the backup national system to the VIS on other premises of the national authority in charge of the national system, generally located in another area of the city or in another city.

The specific configuration of the LNI and BLNI, e.g. the bandwidth, precise physical location, etc., are agreed with each individual Member State.

The network services are specifically delivered for the VIS, as the VIS network remains separated from any other network at central level — this could change in the future for reasons of cost-effectiveness. Hence, Member States can use the LNI and BLNI exclusively for the purposes laid down in the EU legislation applicable to the VIS.

The contractual agreements applicable to the VIS provide for an encrypted, virtual, private network dedicated to VIS data exchange between Member States as well as between Member States and eu-LISA, which is responsible for the operational management of the VIS.

Under EU legislation related to the VIS, the VIS architecture makes use of centralised services, which are accessible from the different Member States. For resiliency purposes, these centralised services are duplicated in two locations namely Strasbourg, France, which hosts the principal central unit and St Johann im Pongau, Austria, which hosts the backup central unit. Note that, for reliability and cost-efficiency purposes, the distinction between the central- and the backup unit may be lifted in the future.

The principal and backup central units are accessible from the different Member States via the LNI and BLNI, which connect national systems to the VIS. Each central unit can be accessed by either the LNI or the BLNI.

The connection between the principal and the backup central unit makes it possible to continuously synchronise them, so that if there is a switch-over or failover, Member States

93 Croatia, Bulgaria, Romania and Cyprus, although not yet full Schengen members (i.e. their VIS sites are not yet live), have already had their sites ready so that they can test their applications in view of future use.

78

can still work on an up-to-date alternate unit. There is currently nothing to stop this connection being used for new architecture and technology in the future.

As ***visa***-issuing and border-check activities vary from one Member States to another, the bandwidth needed for the LNI and the optional BLNI is specific to each of them. The communication infrastructure offers site connection bandwidths adapted to the expected traffic load, and has increased the bandwidth in some cases as a result of capacity management observations.

The network guarantees sufficient minimum upload and download speeds for each connection and supports the total bandwidth size of the network access points. eu-LISA assesses the monthly reports, which include information on line utilisation (to assess whether there may be issues of capacity bandwidth or peaks), round trip delay (maximum and 95 %), and packet loss (average and 95 %). These metrics help assess the needed bandwidth in coordination with the Member States.

IPv4 Layer 3 connectivity is provided without any traffic filtering so anything that uses IPs may pass through the network filters (applied by eu-LISA at central level). Protocols such as HTTP, FTP, NTP, SMTP94 are supported. Only the SAN95 replication protocols that are IP-oriented and capable of operating over WAN networks are supported. Proprietary java-to-java connection protocols of BEA WebLogic work if they are used over TCP/IP.

All IP addresses used on the sTESTA network are dedicated to this network and for VIS purposes only. Each Member State's LNI or BLNI uses unique allocated subnet for production and pre-production and dedicated subnet for VIS Mail traffic (production and pre-production).

Up to now, no Member State has requested IPv6. However, the network access points and backbone are IPv6 compliant. If such a request is made, a study and testing would need to be carried out first.

Some Members States are able to fully utilise the provided bandwidth for brief moments of time only. CU and BCU are not the bottlenecks, however. It is the connectivity with Member States that briefly saturates during peak times. This only happened in 2015 and, after the eu-LISA assessed the situation, new bandwidth was ordered for some sites.

The communication infrastructure complies with the minimum set of technical specifications set out in the Annex to Decision 2008/602/EC of 17 June 2008. The contract is governed by a service-level agreement which determines availability, thresholds for round trip delay (both maximum and 95 %, measured both towards CU and BCU), and packet loss (both average and 95 %, measured both towards CU and BCU). These measurements result in a weighted value. Penalties are applied if the value falls under the threshold.

94 Hypertext transfer protocol, file transfer protocol, network time protocol, simple mail transfer protocol.

95 Storage area network.

79

The maximum transit delay or round trip delay is contractually defined as 200 miliseconds (ms) for production and the same for pre-production. The 95 % network round trip delay is calculated based on real usage; on the production network, it is below 150 ms for all Members States except Malta, which is slightly above at 153 ms. However, the actual measured values remain well below this threshold (lately below 100 ms) . The threshold contractually defined for 95 % network packet loss is at the level of 0.01 % (10-4) and average network packet loss at the level of 0.005 %. Each access point has its own specific value and each is measured and reported on separately.

There are two paths between the CU and the BCU; one is over EuroDomain and one is over a dedicated point-to-point connection. The contractual 95% network round trip delay threshold for the path over EuroDomain is 48 ms for production. The 95 % network round trip delay threshold for the path over point-to-point is 14 ms for production. In 2015, the average maximum round trip delay was around 14 ms and the average 95 % round trip delay was 11.5 ms, which is far better than the target.

The communication infrastructure offers high availability. The backbone is fully resilient; there are multiple paths between the points of presence (POPs) and also between countries. There are always two customer edge routers in each terminal access point (TAP) connected to two different provider edge (PE) routers. Each of the PE router is located in different POPs, which are physically in different locations. If possible, dual entrance to the building is used, along with different connections to the building and different cable tracing inside it. On the production branch of the TAP there is level 1 resiliency and all critical devices (crypto devices, firewalls and switches) are in resilient setup on production. All generic services are operated by eu-LISA and located in the CU/BCU, except for the NTP service, which is located in Brussels on the contractor's premises. The connection between the LNI and the BLNI falls under the responsibility of the Member States. The contractor provides one of the failover mechanisms to switch between the LNI and BLNI, and this is usually operated manually by Member States.

sTESTA monitoring relies on a Service Operation Centre located in Bratislava. Specific monitoring tools are ***available*** to eu-LISA for the operational management of the Central VIS (CS-VIS). This makes it possible to analyse incidents quickly, and to quickly assess whether or not the issue lies at network level between the CS-VIS and the LNIs.

Generic services are also offered through, for example, mail relay and NTP. The mail relay protocol is used by VIS Mail and the NTP protocol allows Member States to synchronise their time on the central server.

Contracts include an SLA which is based on the 99.99 % availability for production sites. Penalties are applied whenever availability drops, up to the full monthly cost of running each site.

80

In terms of security services, no VIS-related information circulates on the communication infrastructure without encryption. The VIS network is ensured by a virtual private network managed by the network provider. SINA encryption boxes are remotely administered and monitored. 3DES 128 bits and AES 192 bits are used on encryptors. In order to guarantee that no one, not even the network provider, can have access to the information exchanged on the network, a supplementary level of encryption will be added to the currently existing VPN. Encryption and decryption will be ensured by crypto boxes located in the terminal access points, and their key will be under the eu-LISA responsibility. This is planned to take place once the migration to TESTA-ng is completed.

All infrastructure under the responsibility of the Commission and eu-LISA is monitored and if there is a threat the security level is raised either automatically or manually. It could be escalated to a ‘security incident’, and these are reported on weekly and monthly. If there is a critical incident, a full incident report should be prepared.

A redundant helpdesk and support structure is established by the network provider. It remains in permanent contact with eu-LISA. eu-LISA also has some of the network provider's monitoring tools in its premises.

The EuroDomain network infrastructure is dedicated and is separated from other networks by an air gap. In common interconnection points like SOCs and on the Brussels premises, the communities are separated by firewalls and encryptors. At the backbone level, each community has its own IP VPN. This prevents data from leaking into other systems or networks. However, Members States are responsible for their part of the network and Commission and eu-LISA cannot ensure that Members States' networks do not interconnect.

3.4.5 Relationship between the VIS and national systems

Under Article 28 of the VIS Regulation, how national authorities provide access to the VIS varies based on their internal organisation. Member States can decide on this themselves.

A consolidated list of national authorities was first published in the Official Journal of the European Union on 17 March 201296, with two subsequent updated consolidated lists published in April 201497 and May 2016,98 respectively.

The management and arrangements for VIS access of duly authorised staff of the competent national authorities also depend on Member States’ internal organisation.

In general, a system of role-based individual access is set up by the national authorities and formal authorisation is needed in order to grant such access. A personal account or individual certificate to log into the VIS is provided, when necessary and in accordance with the relevant legislation.

96 OJ 2012/ C 79/04.

97 OJ 2014/C 106/04.

98 OJ 2016/C 187/04.

81

Duly authorised staff may only consult the VIS when they need to do so in order to carry out their work. Member States report that they usually provide access to specific staff members of consulates, national authorities, asylum authorities and law enforcement authorities (‘LEAs’). One Member State reported that its procedure for granting access is controlled by its cybersecurity department.

3.4.6 Technical incidents caused by the VIS or national systems

Incidents resulting in long response times or downtime have been experienced by 9 Member States (out of the responding 19). These happened both in national and central parts of the VIS.

In these cases, applications could not be registered in the VIS or the VIS did not reply to requests sent by the national system. However, such incidents were only sporadic.

The way in which technical incidents are handled varies between Member States. Two Member States reported having developed a specific functionality in its national system to register failed applications at a later time (i.e. data queuing). Usually, a single point of contact (SPoC) is set up in each Member State according to eu-LISA's VIS Operational Manual. The single point of contact is ***available*** to monitor the functioning of the national system and to liaise with the Agency’s central helpdesk in case of an incident at national or central level. An escalation procedure is activated if necessary.

10 Member States reported having an emergency plan in place for situations where it is impossible for users to search in the SIS II due to a problem with a national system or network inaccessibility. 4 Member States reported having no such plan and 5 Member States did not reply. Although this is not directly related to the VIS, it impacts ***visa***-related activities.

The Agency’s annual survey measured customer99 satisfaction with how incidents were managed and their ***follow***-up.

99 In this context, the ‘customer’ is SPoC technical staff in contact with the Agency for supervision and incident management.

Numeric values range:

1 (minimum, very dissatisfied)

5 (maximum, very satisfied)

82

Figure 13. Overall level of customer satisfaction based on the answers provided by Member States.

The responses showed that the Agency is meeting customer expectations and properly addressing the areas of improvement identified in the preceding reports. Please see in Figure 13 and 14 the main results of the report issued in 2015 and covering 2014.100

Figure 14. Overall level of customer satisfaction based on the answers provided by 17 Member States

Source: eu-LISA

Some observations about Member States' satisfaction with VIS services can be made based on the Agency's annual survey, as ***follows***:

1. 88.25 % of Member States indicated that they are satisfied or very satisfied with the services received.

2. The score given to the Service Manager Tool (SM7) is the survey's lowest score and shows that Member States are insufficiently satisfied with it.

3. The VIS areas that need improvement are:

• the overall SPoC experience;

• the completeness of the information provided when closing an interaction;

• the Service Manager Tool and User Guide.

4. Member States are especially satisfied with the ***available*** technical documentation, which they consider sufficient and clear.

5. Other comments received concern various aspects of the VIS, for example:

• Member States' requests not being properly understood by the helpdesk, and responses received not being related to the question asked;

• occasional misunderstandings when sharing information.

100 Document 2015-110, Customer Satisfaction Survey — eu-LISA 2014 services.

The ***following*** recommendations can be made for the VIS services:

• improve the Service Manager Tool to meet customer expectations

• put in place mechanisms to ensure the quality of answers provided in the interactions, in terms of completeness, relevance and clarity.

3.4.7 Training activities for authorised staff

Member States provided information on training activities for staff authorised to process data stored in the VIS and for staff of the national authorities that have access to the VIS.

Some Member States train staff ***before*** they start working with the VIS, and some provide annual training. Others trained their staff only with the roll-out of the VIS. All training courses addressed software functionality, security and authorisation issues, as well as data protection and security.

In some Member States, staff members have access to e-learning education, handbooks and routines on the intranet; these also address security and authorisation issues and data protection.

One Member State reported that the ***following*** subjects were also covered by the training:

• detection and prevention of trafficking in human beings, and illegal immigration as an integral part of the investigation procedure for ***visa*** applications;

• specificities related to the ‘EU nationals and their family members’ category;

• issues relating to the fundamental rights of the applicants.

The Commission’s evaluation of the Agency, carried out in 2015, concluded that since its establishment the Agency has made commendable efforts to develop robust training activities in line with the needs of national authorities, both technical and practical. The training strategy is further developed annually, via the National Contact Points.

The evaluation also found that further alignment with technical needs was necessary, particularly in terms of improving training courses’ technical content. This gap in technical content could have been caused by stakeholders’ passive participation in the development of the training strategy, despite the Agency’s efforts to keep them engaged (e.g. the Advisory Group and NCP members).

3.4.8 Responsibility for using data and keeping it in national files

Most responding Member States never keep data retrieved from the VIS in national files. One responding Member State stated that only technical logs, not data, are kept in national files, for an average duration of one year (see section on Keeping of records below). One Member State reported that the data page summarising the applicant’s basic information is kept in the national file (entry/exit date, decision) when the applicant lodges an application with this Member State. However, this falls outside the remit of this topic, which concerns only the

84

retention at national level of information taken from the VIS and not retention of information collected during the ***visa*** application process, which naturally remains under national ownership. 4 Member States did not reply.

Incidents related to non-compliance with provisions related to keeping data in national files under Article 30(1) of the VIS Regulation

No specific information was provided by Member States on any incidents related to non-compliance with provisions related to keeping data in national files under Article 30(1) of the VIS Regulation.

No incident of unauthorised access to VIS data was reported.

3.4.9 Member States' liability towards the VIS

17 Member States stated that they have never failed to comply with their obligations and thus caused damage to the VIS. 2 Member States did not reply. The Agency confirmed that it is not aware of any such cases.

Consequently, no Member State reported having claimed for compensation against another Member State's failure to comply with its obligations and thus causing damage to the VIS.

3.4.10 Keeping of records

Information recorded when a data processing operation is carried out within the VIS (logging) varies depending on the Member State.

11 Member States reported that they collect and keep records of authorised staff members entering data into the VIS. 2 Member States did not specify and 6 did not reply. It is therefore difficult to assess the extent of Member States' compliance with their obligation to keep records of all data processing operations within the VIS under Article 34 of the VIS Regulation.

All responding Member States confirmed that they keep a record of all transactions and their details, notably the ***visa*** application number and ***visa*** sticker number (when ***available***), search criteria, etc.

Legal provisions require that the records collected both at central and at national level must show the purpose of access, the date and time, the type of data sent, the type of data used for interrogation, and the name of the staff member entering or retrieving the data.

At central level, it is only possible to access the VIS to consult records for the purpose of data protection, monitoring of the admissibility of data processing (only services fit for purpose are usable by a specific end-user profile), and to ensure data security. These records are protected by access control measures (username, profile and password) to prevent unauthorised access and are deleted after one year after the retention period applicable to the ***visa*** applicant and ***visa*** application data.

85

3.4.11 Self-monitoring and penalties

The VIS Regulation requires Member States to ensure that each staff member entitled to access VIS data takes the necessary measures to comply with the VIS Regulation and cooperate, where necessary, with the national supervisory authority, i.e. the data protection authority (DPA).

All responding Member States have in place a supervision system for data processing. Access is controlled via access controls (e.g. through individual accounts, accessed with an ID and password, usually accessible only to back office national officials based on authorisation principles, i.e. not to local staff) and monitored via logging (i.e. every action is logged so that every file manipulation can be linked to an account).

All responding Member States declared having in place security routines according to which only duly authorised staff members have access to the VIS system/data. Staff access to personal data is restricted, based on access control rights. Access to the data is granted only to staff who need it to carry out their tasks. The data are encrypted

before transfer from the consulates to headquarters and back. Security measures are usually set out in the security documentation which details access, technical and object-oriented security rules.

The answers received show that Member States have put in place routines to make sure that data processing is in compliance with the VIS Regulation and the ***Visa*** Code. The law provides for administrative and criminal sanctions for breaches of personal data processing rules. However, there is some uncertainty about the interpretation of the 'self-monitoring' provision in the VIS Regulation. The answers provided by some respondents indicate that by self-monitoring they mean the monitoring carried out by DPAs and not by the national authority designated as controller under Article 2(d) of the Data Protection Directive.101

Self-monitoring performed by national authorities since the entry into operation of the VIS shows that obligations related to authorised access and keeping adequate and accurate information records have been met. No penalties have been reported.

Irregularities most often encountered during monitoring relate to data quality problems, for example when the correct reasons for exemption from fingerprinting are not consistently specified (either 'not legally applicable' or 'not factually applicable'), when several applications of the same applicant are not linked, or when applications are linked erroneously.

Some Member States mentioned that self-monitoring resulted in a series of improvements in national procedures and the overall improvement of data quality. Improvements were seen in areas such as: application reviews and audits (architecture management board); application monitoring and consistency of workflows; regular network security checks; review of

101 Directive 95/46/EC.

authorities' and users' access rights; regular training (Article 28(5) VIS Regulation); and updating of the security screening level.

3.5 The costs of setting up and operating the VIS

The impact assessment102 for the VIS projected the ***following*** costs to set up and run the system:

The ***following*** is an overview of the financial costs incurred to set up and run the VIS, including the investment and operational costs of the communication infrastructure between the national interface and the national system:

Expenses

VIS setting-up

Expenses 2005-2011 (€ m)

Development contract (without fingerprints)

39.9

Development contract (fingerprints)

37.4

Technical assistance

9.4

Network infrastructure (including Member State connection)

46.2

Site preparation

4.7

Other including security

13.1

Total

150.7

The two pie charts below (Figures 15 and 16) indicate the same expenses in both full amounts and as a percentage of the total.

102 Commission Staff Working Document, Annex to the Proposal for a Regulation to the European Parliament and to the Council concerning the ***Visa*** Information System (VIS) and the exchange of data between Member States on short-stay ***visas*** — COM(2004)835 final.

VIS with biometrics

One-off investment costs (€ m)

Annual operational costs (€ m)

Costs for the Community

93

14-16

Costs for the Member States (national systems)

186

49

Total costs

246-256

55-57

87

Figure 15. VIS expenses in full amounts (€)

Figure 16. VIS expenses in percentages (%)

As to the cost of setting up the national systems, the calculation is ***more*** complex because the source of the funding was both national and EU (External Border Fund for the period 2007-2013). The External Border Fund contribution to setting up and run the VIS at national level during the period was about EUR 140 million for the 21 Member States that benefited from such funding. However, individual expenditure varies greatly among Member States, from almost EUR 40 million in the case of France (the Member State with the largest consular network) to around EUR 10 million for Belgium, Italy or Germany and over EUR 16 million for Switzerland, to less than EUR 1 million in Slovakia and around EUR 300 000 by Malta and Iceland.

88

No

Member

State

Total

2007

2008

2009

2010

2011

2012

2013

2007-

2013

1

AT

596

-

620

629

153

226

-

2 224

2

BE

1 490

1 088

1 426

2 064

1 609

1 100

2 032

10 809

3

BG

-

-

-

2 907

464

1 127

-

4 498

4

CH

-

-

-

7 486

3 707

5 293

-

16 486

5

CZ

-

-

127

1 531

2 434

363

-

4 455

6

CY

-

-

219

-

894

786

-

1 899

7

DE

-

1 661

2 806

1 161

2 237

1 592

1 203

10 660

8

DK

753

1 134

1 576

-

232

1 634

-

5 329

9

ES

-

2 568

741

1 300

747

921

1 161

7 438

10

FI

-

614

930

410

1 666

2 215

1 998

7 833

11

FR

10 154

3 758

2 544

6 085

5 380

2 731

7 620

38 272

12

HU

-

1 152

271

707

1 854

-

-

3 984

13

IT

1 900

1 359

1 399

1 580

1 626

2 229

-

10 093

14

IS

-

-

-

89

134

65

-

288

15

MT

223

-

-

-

-

128

-

351

16

NL

96

502

2 977

-

1 758

840

-

6 173

17

NO

-

-

-

607

711

-

1 146

2 464

18

PL

-

1 681

-

-

-

-

-

1 681

19

SE

-

1 633

-

455

205

222

-

2 515

20

SI

-

-

-

-

497

688

-

1 185

21

SK

121

383

-

117

178

128

-

927

Total

139 564

Figure 17. Expenses for setting up National VIS (N-VIS)

Source: European Commission, EBF VIS-related expenditure 2007-2013 (in thousands of euros).

The full costs for setting up and running the national ***visa*** information system (N-VIS) in each Member State are actually higher. Only 8 of the 19 responding Member States could provide any figures (or approximation) regarding these costs. However, they give an idea of the financial requirements.

1. Sweden estimates that the national VIS-related system had a total cost of EUR 14 m.

2. For Switzerland, the development costs amounted to EUR 31 m. The operational costs were EUR 12 m, and the biometric enrolment infrastructure and operational costs were EUR 12 m.

3. For the Netherlands, the investments made by the Dutch Ministry of Foreign Affairs were estimated to be around EUR 2 m. Operational costs were minimal and shared between the Dutch partners, since all use a centralised point of communication with the VIS. No figures are ***available*** for other authorities.

89

4. For Lithuania, the financial costs incurred by the implementation of the N-VIS development project during the period 2013-2015 were about EUR 1.2 m.

5. For Poland, infrastructure costs were EUR 1.7 m. The communication and maintenance costs for the VIS could not be estimated, as the SIS II and the VIS share the same communication infrastructure. The annual cost of the contractor who delivers some extra maintenance services for both SIS II and VIS was EUR 0.4 m.

6. In Malta, the maintenance costs for the national system were EUR 0.23 m. Other costs related to connectivity. However, it is difficult to quantify them given that the same connection is used by other services that the embassies and consulates provide.

7. For Norway, the costs for setting up and running the national system were estimated at approximately EUR 30 m.

8. France estimated direct investment costs to be around EUR 12 m from 2014 to 2018, the year of delivery of the final release. The peak would be in 2015 and 2016 for major developments for the front and back offices. A contribution of up to EUR 7 m from EU funds has been sought, thus reducing the actual cost for France to EUR 5 m.

Figure 18: VIS operating costs (2011-2015)

The VIS was handed over to eu-LISA on 1 December 2012. Applicable as from 2013, the Agency's budget for Title 3 (i.e. relating to the system's operation) is set out in Error! Reference source not found.. For 2011 and 2012, the expenses relate to the operational management entrusted to the French authorities. The increase in appropriations over the years relates to necessary investments to adapt the system's capacity to the gradual roll-out of the VIS. On entering into operation, the VIS capacity was 60 000 requests an hour on a database capacity of 40 million applications. In the first half of 2016, the system is able to cope with 450 000 requests an hour from a database of 60 million records. Until further notice, this is sufficient until 2018 for Member State activities related to ***visa***-issuing and border checks.

In the same period, the biometric matching system capacity was also significantly increased. This was to cope with Member State fingerprint identifications in all consular posts and for

authentications for all border crossing points, in particular ***following*** the systematic use of the fingerprint as from October 2014.

These figures exclude staff, infrastructure and logistics costs applicable for eu-LISA's seat in Tallinn and the operational site in Strasbourg. Although having identified certain possibilities for improvement, the eu-LISA evaluation carried out in 2015 concluded that the VIS, as one of the three large-scale IT systems in the Justice and Home Affairs area entrusted to eu-LISA, has been operated effectively. The evaluation found that the VIS developments have been effectively ensured by the Agency. The evaluation found that 81 % of the VIS Advisory Group members strongly agreed or agreed that continuity and uninterrupted services were ***available***. Although some respondents could not provide their opinion on this matter, there was no perception among the VIS Advisory Group members of any disagreement on continuity and uninterrupted services.

3.6 Data protection in the ***visa*** application procedure related to the VIS

3.6.1. Right of information

Article 37 of the VIS Regulation requires Member States to inform ***visa*** applicants of their rights related to data protection. From the consultation carried out with Member States, it is unclear whether all of them have put in place the necessary measures to ensure that this information is systematically made ***available*** to all ***visa*** applicants.

Five of the eighteen responding Member States did not provide any input regarding this subject, and one advised that the process is still being implemented.

Most respondents, however, confirmed that appropriate measures are in place to inform applicants. Various means are used to ensure that data subjects are informed of their rights and of the way in which they can request a copy of their stored personal data. This information is mainly provided in the ***visa*** application form, sometimes with an additional cover letter, which needs to be signed ***before*** the application is submitted. There are various other means of providing the information:

• information fliers, in particular one drafted by the European Commission '***Visa*** Information System (VIS), Improving Schengen ***visa*** procedures';

• information posted on the websites of ***visa*** authorities, DPAs, consulate homepages or external service providers; and

• additional information provided by ESPs upon application.

Particular attention seems to be given to informing applicants of their rights concerning their biometric data and the rights of access, rectification and erasure related to it.

91

3.6.2. Access, rectification and erasure of data

When it comes to requests received from applicants to access their VIS data, most responding Member States advised that they had not received any such request, and one Member State reported that it does not keep account of such requests. One Member State received one request (which turned out to be groundless), one received six requests, one received eight requests, and one received 22 requests.

As regards requests to correct VIS data, only one of the responding Member States reported having received two such requests, while none of the others received any. During the reporting period, only one received a request to erase the data.

The procedures in place to request access to data vary, though usually they provide that data subjects can submit their requests directly to the VIS data controller. National DPAs can also receive such requests and can provide information on the applicable procedure and contact details of the data controller. Under the responsible authority, the matter is referred to the data protection officer (DPO), who would then directly treat the requests for access, rectification or erasure.

As regards the period for answering a request to access or rectify data, all responding Member States declared that they respect the one-month deadline in processing the request (where applicable).

Member State procedures provide that when the right to access data, or to correct or delete such data, is refused by the authorities of a Member State, a decision in this respect is to be issued by the competent authority of that Member State. Such decisions are subject to an appeal ***before*** an administrative court (e.g. Switzerland, Lithuania) or else the person has the right to submit a complaint to the data protection authorities (e.g. Poland, Iceland).

According to the reported information, there has been no situation in Member States during the reporting period in which a request to correct or delete data was refused and which led to actions or complaints ***before*** the national competent authorities.

As regards information on requests for which another Member State was responsible, most contributing Member States reported that no such requests were received. Only one Member State advised having received one request concerning data for which another Member State was responsible. The request was forwarded to the responsible Member State via VIS Mail.

As regards complaints related to personal data recorded in the VIS, two of the responding Member States received one each and one Member State received 16. None of the others received any such complaints, while one Member State advised that it does not keep any record of such complaints.

92

3.6.3. Member States cooperation on data protection

As regards cooperation with other Member States to ensure an individual's right of access, correction and deletion of VIS data as provided for under Article 39 of the VIS Regulation, responding Member States reported they do not have any special provisions in law or established practice for this. This is mainly because cases that would require cooperation between several Member States do not usually occur in practice.

However, specific international cooperation on these matters is carried out either at the level of local Schengen cooperation (i.e. through the consular posts of other Schengen states in a certain location) or of the national data protection supervisors, through the VIS Supervisory Group (SCG VIS) founded on the basis of Article 43 of the VIS Regulation — which meets regularly in Brussels.

3.6.4. Remedies on data protection

According to Article 40 of the VIS Regulation, data subjects have the right to bring an action or complaint ***before*** the competent authorities or courts of a Member State when their right to access VIS data related to them is refused.

As reported under the previous point, there has been no situation in the Member States during the reporting period in which a request to correct or delete data was refused. Consequently, to date, no action has been brought ***before*** a competent authority or court on this ground. Therefore, there was no case when Member States should have exercised their duties to assist and advise the person concerned in proceedings ***before*** a court or competent authority.

3.6.5. Liability towards individuals

The Commission has received no information and no evidence regarding cases of individuals or Member States who suffered damage as a result of a processing operation incompatible with the VIS Regulation. Nor is it aware of cases where a person or Member State has made a complaint claiming damage suffered as a result of a processing operation incompatible with the VIS Regulation.

3.6.6. Supervision by the national supervisory authority (DPA) and EDPS

3.6.6.1 Supervision by the EDPS of the central VIS

According to Article 41 of the VIS Regulation, the lawfulness of the processing of personal data by Member States is monitored by the national data protection authorities (DPAs). The European Data Protection Supervisor (EDPS) is responsible for supervising the management authority (eu-LISA), as provided for under Article 42 of the VIS Regulation.

The VIS Supervisory Coordination Group (hereafter VIS SCG) was established in order to ensure a coordinated supervision of the VIS and national systems, as provided for under Article 43 of the VIS Regulation. Cooperation takes the form of meetings held on a regular

93

basis with all DPAs in charge of supervising the VIS at national level and the EDPS, acting together as the VIS SCG. The main purpose of these meetings is to discuss common problems related to supervision and to find common solutions or approaches whenever possible. On average, two meetings are held each year. The Commission and eu-LISA are also invited to parts of the meeting to update the group on new developments regarding the VIS.

Since the entry into operation of the VIS and until the date of publication of this report, eight supervision coordination meetings have taken place: in November 2012, April and October 2013, May and October 2014, March and October 2015, and April 2016.

The meeting typically consists of two parts: firstly, the VIS SCG is updated by the European Commission and eu-LISA on the status of the VIS roll-out and other developments with a potential data protection impact; and secondly, DPAs discuss issues that are in need of checking at national level or new developments of interest for VIS supervisors.

3.6.6.2 CS-VIS's compliance with data protection rules

From a data protection perspective, Member States are responsible for personal data in the VIS, while eu-LISA acts as a data processor with regard to the central ***visa*** information system (CS-VIS). Therefore, there is a sharing of tasks: eu-LISA operates the CS-VIS and Member States provide for the NI-VIS. The responsibility of eu-LISA as the management authority for the CS-VIS and data processor is to ensure that the CS-VIS is operated in accordance with the requirements, including those related to data protection, of the VIS Regulation. This is in particular as regards the security of the system, the network and the national interfaces, to ensure that only authorised staff have access to data processed in the VIS for the purposes of the performance of tasks specific to this authority. As regards eu-LISA, the protection of personal data related to individuals processed by CS-VIS is monitored by the eu-LISA DPO and supervised by the European Data Protection Supervisor (EDPS). Member States have the obligation to ensure that personal data are lawfully processed (collected, transmitted to the VIS and accessed) and that they are accurate when transmitted to the VIS and kept up to date.

The data protection obligation is central to the system's risk assessment. VIS data (e.g. the applicant data and application data) and VIS logs (see the section on 'Keeping of records') are rated as the most sensitive assets to be protected, thus covered by all technical and organisational security controls described in the VIS Security Plan. The VIS data benefit from the highest level of security controls. The processing of VIS data is limited to what is necessary and proportionate for carrying out the tasks. Personal data of applicants are kept in the VIS for five years. Personal data is never passed to second or third-level support (i.e. never to anyone except eu-LISA staff). Personal data can be provided by Member States as data controllers when and as far as necessary in case of technical investigations ***following*** incidents. To this end, specific protected communication channels and procedures are in place.

94

For its part, eu-LISA reported one incident where a Member State did not use the proper channel to communicate issues with the VIS. This resulted in emails containing personal data of VIS applicants being delivered to personal mailboxes of the operations team and the application team. This incident was reported by security to the eu-LISA data protection officer who contacted the Member State in question and requested the removal of emails with personal data. In mid-2014, a communication was sent to all Member States requesting them to use the proper secure channels to communicate incidents, as per the operator's manual.

Authorised Agency staff have access to personal data as far as necessary for technical purposes and for the fulfilment of an agency's obligations under Article 50 of the VIS Regulation (i.e. monitoring the functioning of the VIS against objectives relating to output, cost-effectiveness, security and quality of services).

In its almost three years of operation, eu-LISA has not received any complaint related to data protection.

The EDPS has performed inspections on the spot to monitor the lawfulness of the processing of personal data. The EDPS uses monitoring tools for self-auditing in accordance with Article 34(1) of the VIS Regulation.

As the supervisory authority responsible for ensuring that the personal data processing activities of the ***visa*** information system management authority are carried out in accordance with the VIS Regulation, the EDPS has to date performed two security audits of the VIS central system, as required under Article 42(2) of the VIS Regulation.

The first EDPS audit of the CS-VIS took place in November 2011, when the management authority of the VIS was still the European Commission. In June 2012, the findings were sent to the European Parliament, the Council, the European Commission and the national data protection supervisory authorities.

The 2012 audit assessed whether the infrastructure, personnel, organisation and technologies complied with the security requirements provided for in the applicable legislation and particularly in Commission Decision 260/2010 on the security plan for the operation of the VIS.

On this occasion, the EDPS found that the absence of a security policy made it impossible to assess the security measures in place. Instead, the audit's findings and recommendations were based on the requirements provided for in Commission Decision 260/2010 on the security plan for the operation of the VIS and on the assessment of the mandatory areas defined in the BSI103 IS methodology (information security quick audit).

In the course of this first audit, the EDPS did not find any critical security weakness that would justify imposing a temporary ban on processing data, under the terms of Article

103 British Standards Institution.

95

47(1)(f) of Regulation 45/2001. However, in order to address the issues identified, the EDPS requested the Commission to put in place an implementation plan to address all these recommendations and also to consider the additional actions that could be needed to adapt the current system to the requirements of the security policy (once properly established).

The EDPS made a series of recommendations, among the most important being the need to put in place a proper security policy, to assess and plan the training needs of the operational staff, and to set an adequate business continuity plan.

The second EDPS audit took place in 2015. It focused on the central VIS database and the biometric matching system. The fieldwork was carried out on 23-24 September 2015 at the eu-LISA premises in Strasbourg, France, and was preceded by a pre-visit documentation review. The report with the EDPS findings and final recommendations was not published by the time of publishing this report and therefore could not be taken into account.

One of the objectives of the September 2015 inspection was to ***follow*** up on the 2012 audit. At the time of the inspection, 15 of the 24 recommendations made by the EDPS in the 2012 report were considered closed. The remaining open recommendations were included in the ***follow***-up to the 2015 inspection.

3.6.6.3 Supervision by DPAs of the national authorities having access to the VIS

National supervisory authorities (DPAs) monitor by various means the lawfulness of the processing of personal data stored in the VIS at national level. The main and most often used tool is through undertaking an inspection — covering the VIS and the log-files and activities of the ESPs — either of the national ***visa*** authority or of consulates to whom Member States delegate the ***visa*** application collection. DPAs also carry out other tasks:

• giving opinions on new national legal proposals concerning the national ***visa*** information system;

• ruling in cases of dispute concerning the processing of personal data;

• providing data protection training of the staff responsible in national authorities; and

• carrying out audits of the national system.

Of the 18 Member States that responded to the Commission consultation on this point, eight reported that an audit of the national VIS data processing operations (required every four years on the basis of Article 41(2) of the VIS Regulation) had been carried out, four reported that such an audit had not taken place, and six did not provide any answer.

The Joint Activity Report 2012-2014 of the VIS SCG (see above), which summarises the contributions of national DPAs, reported that inspections had been carried out in 14 Member

96

States ,104 and no inspections had been carried out in the reporting period in 11 Member States105 (although investigations had been carried out on the basis of complaints received). One national DPA (Lithuania) provided no information on inspections. With four exceptions (several complaints in the Czech Republic and Spain, and one each for Poland and Slovenia), no national DPA reported having received complaints from anyone regarding the data processed in the VIS, or the complaints received turned out to be irrelevant from a data protection perspective. One national DPA (Hungary) reported having received an access to data request.

Some inconsistencies are apparent between the information provided by Member States in response to the questionnaire for the VIS evaluation and that provided in the Joint Activity Report. The inconsistencies concern whether an audit took place or not, and as regards the content of that audit. Most national contributions in the Joint

Activity Report seem to refer to inspections of the consular posts carried out by DPAs, as opposed to audits of the national VIS in the Member State itself. While the latter are relevant for the overall assessment of compliance with data protection rules, they are not equivalent to an audit of the national VIS under the terms of Article 41(2) of the VIS Regulation. Only two national DPAs (Netherlands, Portugal) reported that they had carried out such an audit of the national system. The remaining reports referred rather to on-site inspections of consulates in non-EU countries.

To ensure that only authorised users access the VIS and that such access complies with purposes legally provided for, national competent authorities have put in place various measures to grant access, exclusively based on legal grounds. Only authorised personnel have access to the VIS personal data. Various audit and verification measures are in place for the individual competent authorities. Risk assessments are in place for personal data processing operations. Every account is logged so that every operation can be traced. Technical measures are also in place, such as encryption of communication lines. Regular audits are carried out and training is provided for the personnel responsible for VIS data processing in the various authorities.

As part of its 2013-2014 work programme, the VIS SCG evaluated the legality of data processing by the national authorities having access to the VIS. In this respect, three questionnaires were circulated within the Group in summer 2014, relating to the ***following***:

1) authorities having access to the VIS addressed to DPAs;

2) access to VIS data for the purposes of law enforcement, split into two parts — one for the central access point(s) and one for the DPA; and

3) how data subjects' rights are implemented in practice.

104 Belgium, Czech Republic, Estonia, Finland, France, Germany, Hungary, Norway, Poland, Portugal, Slovakia, Slovenia, Sweden, Switzerland.

105 Austria, Denmark, Greece, Iceland, Italy, Liechtenstein, Latvia, Luxembourg, Malta, the Netherlands, Spain.

97

Although the results of the questionnaires were not public by the time the present staff working document was finalised, the VIS SCG communicated several main conclusions to the Commission. The VIS SCG welcomed the progress achieved so far on issues as important as access to the VIS and data subjects' rights. It encouraged Member States to go further to ensure compliance with the legal framework of the VIS in every detail. In this respect, the report found that there is room for improvement in certain respects.

In particular as regards law enforcement authorities, the group recommended that Member States ensure that access is restricted to the operational units that need to use VIS data under the terms of Article 3(6) of Council Decision 2008/633/JHA.

With regard to data subjects' rights, the VIS SCG monitoring showed that, according to the assessment by Member States, the relevant staff members of the competent authorities dealing with the VIS have a satisfactory level of awareness regarding their obligation to safeguard data subjects' rights. Training covering data subjects' rights is provided to the relevant staff in some Member States.

The VIS SCG noted the absence or very low number of requests made by data subjects to exercise their rights of access, correction or deletion of their personal data stored in the VIS. The group assumes that the phenomenon is due to data subjects not being aware of their data protection rights, but also to the lack of information about the way

to exercise them (e.g. to whom data subjects should address their requests). In this sense, the EDPS invited national DPAs to carry out quality controls regarding the information provided to data subjects by diplomatic missions, consular posts and ESPs.

As regards the procedures in place to answer requests by data subjects to access, correct or delete their personal data stored in the system, the group encouraged Member States to better define the expression 'without delay' in Article 38 of the VIS Regulation and to adopt uniform maximum time limits for replying in writing to such requests.

Finally, the VIS SCG found that there was a lack of statistics, in most Member States, on the exercise of data subjects' rights of access, correction and deletion, and on the cases in which those requests were denied. It invited Member States to find a common approach to keep such statistics.

3.6.7. Data protection supervision of external service providers (ESPs)

The EDPS and national DPAs have taken particular interest in the activities of ESPs. In its Joint Activity Report 2012-2014, the EDPS refers to a subgroup composed of representatives of the German, Italian, Maltese, Swiss and Swedish DPAs. This was set up to explore the data protection implications of the use of ESPs by Member States.

The subgroup presented a first note on the analysis of technical and legal issues related to the use of service providers for the collection of ***visa*** applications. The note addresses the relevant legal basis for cooperation with ESPs, the tasks that can be delegated to an ESP, the minimum

98

requirements to be included in contracts (see above), supervision by Member States or DPAs of the processing of personal data by ESPs, and the enforcement by Member States of instructions in terms of data protection compliance.

In its conclusions, the note recommends to draw up a model contract to facilitate contractual agreements between Member States and ESPs. In the future, the subgroup intends to check these contracts ***more*** closely. In parallel, national DPAs plan on looking at how such contracts are being used.

The EDPS looked into how data subjects' rights are implemented in practice. It analysed extensively the issue of data protection by ESPs. The final results of the EDPS inquiries into data subjects' rights were not ***available*** at the date of publication of the present evaluation and could not be taken into account for the present evaluation.

IV. THE APPLICATION OF THE VIS DECISION

4.1 Access to data by designated law enforcement authorities

Access to the VIS data by law enforcement authorities is recent and very fragmented among the countries using the VIS. Of 26 Member States, eight never accessed the VIS for this purpose and one Member State alone generated 54 % of all requests. However, the statistics provided by eu-LISA show that the use of VIS for law enforcement purposes has recently been increasing. The recent and limited use of the system explains the low quantity and quality of replies to the questionnaire and its limited analytical value.

Regarding alphanumeric searches, up to the end of 2015, 26 629 accesses to VIS for law enforcement purposes had been requested. These requests originated from 18 of the 26 countries that use the system. However, only

eight Member States can be considered as regular users, having used the system for ***more*** than one year and requested access for a substantial number of cases (***more*** than 400 requests). Of the 10 remaining countries, eight request access very rarely (1 to 82 requests, some likely submitted for testing purposes) and two started to use the system only during the second half of 2015 but they have already generated several hundred requests.

Compared with alphanumeric searches, the number of fingerprint-based searches is very low. Only 49 such searches had been requested by the end of 2015, originating from seven Member States, and some of them were probably testing the system. Only two Member States accounted for the majority of requests but still in low numbers (16 and 21 requests). The use of fingerprint-based searches was marginal in the five remaining Member States (1 to 5 requests).

99

The number of requests to access the VIS for law enforcement purposes is presented in Figures 19 and 20 below.

Figure 19. Quarterly usage of VIS by Member State for law enforcement purposes (total number of searches)

Source: eu-LISA

Figure 20. Quarterly usage of VIS by Member State for law enforcement purposes (fingerprint based searches)

Source: eu-LISA

The numbers provided by eu-LISA do not enable a clear trend in the use of VIS to be detected. Among eight regular users of the system, five of them recorded a decline in the number of requests. The number of requests for the three remaining regular users is increasing over time.

Six responding Member States provided statistics on the number of requested searches in VIS. It is noticeable that these statistics do not correspond to the statistics provided by eu-LISA, since the numbers provided by the respondents are always lower then these registered by eu-LISA. For two reporting Member States, the difference between both sets of data is very high, with the respondents providing information about only 1 % to 5 % of the total number of searches registered by eu-LISA.

The overall perception of the effectiveness and usefulness of the VIS as an instrument to support the prevention, detection and investigation of terrorist offences and other serious criminal offences is clearly positive. Ten of the 19 responding countries consider that

100

access to VIS by law enforcement authorities is or could be beneficial in this context. No respondent expressed a contrary opinion.

4.2 Procedures for access to the VIS by designated authorities

The first ***step*** in the implementation of Decision 2008/633/JHA is in principle the designation of the central access point through which access is executed, and the competent law enforcement authorities that are authorised to access VIS data.

Moreover the Decision requires Member States to keep a list of the designated competent law enforcement authorities. This list, and any subsequent amendments, should be notified to the Commission and the General

Secretariat of the Council. Sixteen of the 19 responding countries designated a central access point to VIS. However, only 14 of them indicated that they had designated the relevant competent authorities. Ten of them had drafted their list and notified it to the Commission and the General Secretariat of the Council. Two of the responding countries, one of which is a regular user of VIS data for law enforcement purposes, acknowledged that the relevant authorities had not been designated. One respondent reported that even if the designation had been made, the list of the competent authorities had not been drafted and notified. Reasons are not provided for not designating the central access point and the competent authorities or, if they are designated, for not drawing up the list. All 15 respondents that replied to this question acknowledged that the Decision is clear as regards the authorities and central access points that may be designated to access VIS data.

All the responding Member States consider that the central access point is easily accessible for the designated authorities.

In an exceptional case of urgency, the central access point may process the request immediately and only verify after the fact whether all the conditions for access were fulfilled under Article 4(2) of the Decision. Member States reported 52 such urgent requests and all of them were justified by the ex post verification.

The awareness of law enforcement authorities on the possibility of getting access to VIS for law enforcement purposes appears to be sufficient in 13 Member States. However, in two Member States, the competent authorities are not fully aware of this possibility.

Few recipients provided general remarks on access to VIS for law enforcement purposes. Three Member States reported that the access procedure is adequate or sufficient. One Member State considered that the conditions for access are set at a high level, which prohibits the use of VIS to prevent, investigate or detect less serious offences. Only one example of a standard and of an urgent reasoned request to access the VIS was provided. This does not enable any conclusions to be drawn on the quality and lawfulness of the requests.

4.3 Conditions for access by designated authorities

Only two respondents provided a description of the conditions for access to the VIS data by competent authorities. In both cases, the designated authorities must use a specific form to

request access to the VIS. In one case, the designated criminal investigation authority sends to the public prosecutor's office a request with reasons for querying VIS. The public prosecutor determines if the conditions are met. If so, it orders the criminal investigation authority to send the written request with the written verification of the public prosecutor to the national access point. In the second case, verification of whether the conditions of access are fulfilled is carried out by the central access point.

All 14 States that replied did not report any case of requests to access to VIS that did not meet the conditions for access as referred to in Article 5 of the Decision.

4.4 Conditions for access by designated authorities of Member States not participating in the VIS

No Member State reported any requests for access to the VIS by designated authorities of Member States in respect of which Regulation (EC) 767/2008 had not yet been put into effect.

4.5 Access to the VIS by Europol

Europol is not yet connected to the VIS.

4.6 Data protection by law enforcement authorities

4.6.1 Protection of personal data in the process of access by designated authorities under the VIS Decision

The data protection and data security training for the staff of the authorities that have access to VIS is clearly insufficient. While such training is compulsory for all staff having access to VIS, only five Member States replied that they provide such training. Of these, three of them use VIS only exceptionally. A brief description of the training was provided by three respondents and they appear to cover data security and data protection issues. It seems that the training is not specific to VIS but is part of general training provided to law enforcement staff.

Regarding the supervision of the processing of personal data pursuant to the VIS Decision, seven respondents indicated that the competent data protection authority had undertaken an audit. However, only three of these process VIS data for law enforcement purposes in any significant manner. Under Article 8(6), data protection audits must be carried out at least every four years, which leaves the Member States some time to implement this provision.

Three respondents reported that the audits did not identify any irregularities. Instead, in one country, the data protection authority discovered violations of data protection rules: incomplete documentation on data processing activities and access to VIS by one or ***more*** persons without authorisation. The relevant law enforcement authorities were ordered to remedy this situation.

No complaints were reported from anyone concerned by the processing of their VIS data.

102

4.6.2 Keeping of VIS data in national files

Nine Member States replied that they do not keep any data originating from VIS in national files. On the contrary, three acknowledged that such data are indeed kept in national files. In two countries, the data are kept in a specific file related to the individual criminal investigation in which VIS data were processed.

4.6.3 Access, correction and deletion of data related to them by persons concerned

No respondent reported the existence of request for access, correction or deletion of the data obtained from VIS for law enforcement purposes. Three Member States reported that they would process such requests in line with the relevant national law and provided examples and content of the applicable provisions. In all three cases, the legislation regulating access to police files would apply.

4.6.4 Keeping of records on the processing operations resulting from accessing VIS data

The keeping of records on processing operations from accessing VIS data is an essential element to enable the supervision and enforcement of the lawfulness of data access. It is also necessary to ensure data integrity and data security. Specific and detailed records of access operations are therefore required under Article 16 of the Decision. The replies to the questionnaire suggest that the Member States do not fully comply with their obligations in this respect.

Only four Member States reported that access to VIS is fully recorded in line with Article 16. Moreover, one other Member State informed that the recording is done but only partially: only the request for access, and no other processing operation, is recorded.

Only one Member State provided information about the number of records kept. These numbers are inconsistent and significantly lower compared with the number of access requests registered by eu-LISA.

In this context, the difference in the numbers of search requests to VIS provided, on the one hand, by national authorities and, on the other, by EU-LISA, also indicates weaknesses in recording at national level (see above 'Access to data by designated law enforcement authorities').

Regarding the security of the records, five respondents briefly described the security measures in place. They emphasised, in particular, the fact that records are accessible to a limited number of people — subject an identification protocol — and protected by encryption and/or physical protections.

4.6.5 Member States' liability in case of damage to persons

No Member State provided information on liability for unlawful or incompatible processing of data.

103

eu-LISA is not aware of any damage arising from any illegal processing of data by Member States.

V. THE SECURITY OF THE VIS106

According to eu-LISA, the VIS complies strictly with the VIS Regulation in terms of data protection and information security. Since its creation, eu-LISA has had a security sector in place answering directly to the eu-LISA Executive Director, with both a system security officer and a local security officer as provided for under the legal basis. In a first phase, the existing VIS security policy and controls have been maintained and translated into the new context of the Agency.

A new Agency security framework is being developed with the purpose of implementing a Security and Continuity Management System based on the ISO 27001, 27002 and 22301 international standards and taking into account the Commission Decisions in this respect107.

The risk mitigation strategy covers all security layers: physical, personnel, network, operating system, application and data. The communication infrastructure is based on a non-routable, logically private closed group network, provides a strong encryption mechanism, and is further protected by firewalls.

The central VIS is an isolated, controlled and secure environment. The operational and administrative access to the system is managed in accordance with the principles of segregation of duties and least-required privileges. All activities and communication in VIS are controlled, monitored and logged. The system's access configuration enforces that only a limited group of eu-LISA staff administrators are able to gain access to the VIS data if it is required for technical maintenance (Article 50(2)).

VI. THE USE MADE OF THE PROVISIONS REFERRED TO IN ARTICLE 31 AND IMPLICATIONS FOR FUTURE OPERATIONS

Communication of data to non-EU countries or international organisations

Only 3 out of the 19 responding Member States declared they communicated VIS data to non-EU countries or international organisations for the purpose of return.

106 Data security taking into account Commission Decision 2010/260/EU of 4 May 2010 on the Security Plan for the operation of the ***Visa*** Information System.

107 Commission Decision (EU, Euratom) 2015/443 on Security in the Commission of 13 March 2015, Commission Decision (EU, Euratom) 2015/444 on the security rules for protecting EU classified information of 13 March 2015, and Commission Decision C(2006) 3602 concerning the security of information systems used by the European Commission of 16 August 2006.

104

Only one Member State identified the authority communicating VIS data to non-EU countries/international organisations for the purpose of return, i.e. the national immigration police.

No information was provided on the number of cases in which Member States communicated VIS data to non-EU countries or international organisations for the purpose of return, or in which a person could be successfully returned or at least acquire a travel document by using these data. Only one Member State replied to the question on the main purpose for which the data were provided: the purpose was identification of the applicant and facilitating return of an applicant with a rejected residence permit.

No transfer of data to a non-EU country or to an international organisation for the purpose of the prevention, detection and investigation of terrorist offences and of other serious criminal offences was reported by the responding Member States.

Complementary to the VIS evaluation survey, a European Migration Network ad hoc query was launched on 18 March 2016 on the subject of Member States' experiences with the use of the VIS for return purposes. Twenty-four Member States provided replies by 29 April 2016, including four that do not have access to VIS as they do not — or do not fully — implement the Schengen acquis.

Member State experiences have been limited due to the fact that not all immigration services already have access to the system. It is also in part because queries based only on fingerprints, which would enable identification of undocumented irregular migrants, are not yet ***available***.

Nevertheless, 14 Member States acknowledge using VIS data to identify people and to facilitate the issuance of emergency travel documents by consulates of the countries of origin. However, experience with the use of the data obtained from VIS are mixed due to the fact that non-EU countries often do not accept such data as prima facie evidence of nationality. Acquiring a copy of the passport (which would be a much stronger evidence base) from the Member State consulate that issued the ***visa*** is in turn very difficult: some consulates refuse to provide such a copy or the files are destroyed as a result of the two-year limitation on the retention of documentation. Two Member States suggested that the availability of a scan of the passport (in particular of the data page) in the VIS would substantially help speed up the return process and ***more*** returns could be carried out on the EU travel document together with a copy of the passport.

105

Annex 3: Summary of findings on the implementation of VIS-related provisions of the ***Visa*** Code, based on Member States' and eu-LISA reporting, Local Sschengen Cooperation and Schengen evaluations

I COLLECTION AND USE OF BIOMETRIC IDENTIFIERS

1.1. Implementation of the obligation to collect biometric identifiers

In order to make it possible to fully examine ***visa*** applications, where physically and legally possible Member States should capture and record each ***visa*** applicant's 10 fingerprints in a way that produces results of an adequate quality.

When asked whether they have experienced any technical or administrative difficulties in implementing the obligation to collect an applicant's biometric identifiers, 17 % of the responding Member States declared having experienced no such difficulty, 61 % declared having experienced some sort of problems in time, and 22 % provided no answer.

Some of the reasons given for these difficulties were technical, e.g. the slow connection between the fingerprint-capturing device and the computer, the system being slow when copying fingerprints from previous applications, or interference from other electronics. However, most difficulties were linked to the quality of the applicants' fingerprints, due to parameters such as climate, age, and dust. Also, people who perform hard manual labour or work with chemicals have fingerprints that are difficult to capture. Finally, some consulates had to deal with self-acclaimed VIP applicants protesting strongly against having their fingerprints taken.

Where the quality of fingerprints was so low that the fingerprints could not be recorded in the system, consulates generally asked the applicant to come back a second time.

Responding Member States stated that technology used to be ***more*** of a problem when the VIS was first introduced and that now problems due to the technology used have become rare.

For the obligation to record all of a person's 10 fingerprints when they apply for a ***visa***, eu-LISA statistics indicate that the percentage of applications that included fingerprints consistently increased over time, from 62 % in the fourth quarter 2011 to 91 % in the fourth quarter of 2015. It should be taken into account that it was during this period that the VIS was gradually rolled out worldwide and that some Member States chose to introduce it in certain regions or locations ahead of the general rollout. Such rollouts took place without registration of applicants' biometric data, thus artificially increasing the percentage of missing fingerprints in the system, when in reality the recording of biometric data was not yet legally required in these regions.

106

Figure 1. Applications where fingerprints were not attached

97.3 % of NIST files108 in the VIS from August 2015 to October 2015 include all 10 fingerprints, which is a clear improvement compared to previous reporting periods. The analysis of the statistics also revealed that Member States often encode incorrectly the reason for not recording fingerprints by not setting the right combination of the two indicators fingerprints not required for legal reason and fingerprints physically impossible to collect.

Eu-LISA statistics show that the percentage of records of facial image missing from the VIS decreased from almost 2.4 % in October 2011 when the VIS was first rolled out to 0.02 % in June 2015. This low level was maintained for seven months in 2015, after which an increase of approximately 0.12 % was recorded in October 2015. The table below (Figure 2) shows the monthly evolution of the percentage of missing photographs in the VIS109 since the first rollout and until October 2015.

108 Standardised files containing fingerprint information. The National Institute of Standards and Technology (NIST) is a measurement standards laboratory, also known as a National Metrological Institute (NMI), which is a non-regulatory agency of the United States Department of Commerce.

109 Source: eu-LISA.

107

Figure 2. Applications where a facial image was not included- monthly evolution

As regards the distribution of missing facial image per rollout region, the figures are very low as well, usually around 0.03 %-0.06 % per region, with the exception of Australasia (0.17 %) and Schengen Member States (1.68 %).

1.2. Implementation of the technical requirements for collecting biometric identifiers, including the use of appropriate standards

8 out of the 19 responding Member States collect the applicant's facial image directly at the consular post and 11 Member States scan applicants' printed photos from the travel document.

9 Member States encountered difficulties when electronically collecting a photograph or when adding it to the VIS. These were mainly because the photos provided by the applicants did not comply with rules on quality, colour parameters or dimensions. For photos taken at the consular post, the reported difficulties were caused by the morphology of the applicant's face (regional particularism, very young children).

The Schengen monitoring and evaluation mechanism ('SCHEVAL') found that for one Member States the photo quality standards in practiced at national level were incompatible with those in the CS-VIS .

7 Member States reported situations in which biometric identifiers could not be collected according to the International Civil Aviation Organisation ('ICAO') technical requirements because of the unusual features of some categories of applicants' fingerprints (e.g. photographing very young children, fingerprinting manual labourers or elderly people, etc.), wrong user handling or software problems (and lack of IT support).

108

Language barriers have also been reported to be a challenge when communicating information to the applicant on what they need to do for their fingerprints to be captured correctly.

It should be noted that the system requires 10 good-quality fingerprints, which in some cases may be difficult to obtain, may require several attempts and may therefore be time consuming.

One Member State noticed a discrepancy between the definition of 'good quality' in its national system and that in the CS-VIS.

One Member State mentioned the lack of a harmonised procedure for collecting biometrics across Member States as an impediment to operational cooperation between Member States in the field. Each Member State has developed its own software, and there are often incompatibilities with software used by other Member States.

According to eu-LISA, the current tools and practices used to collect biometrics should be replaced by common standards and best practices so as to increase the overall quality and efficiency of both fingerprints and photographs. Furthermore, the capacity to monitor performance centrally and provide feedback should be

increased. The central certification of equipment used should be considered. Introducing anti-spoofing standards should also be considered. Higher resolution (1000dpi) images should be accepted, for example, to allow the use of extended feature sets.

1.3. Quality of data collected

Statistics on the quality of data collected with the application for the reporting period from October 2011 to October 2015 show a continuous improvement (see Figure 3 below). Although the initial levels of insufficient quality fingerprinting (i.e. missing fingerprints or poor quality of one or ***more*** of the 10 fingerprints taken) were around 6 -7 % in the first months after the VIS entry into operations of the system, with a peak of almost 9 % in December 2011, they decreased to almost 3 % by October 2014.

The introduction of the '0-FTE' measure110 (zero failure-to-enrol, i.e. no fingerprint set is refused by the central system for insufficient data quality) in October 2014 made sure that all fingerprints were recorded in the subsequent period. This made it possible for border guards to perform fingerprint-based authentication for all ***visa*** holders whose fingerprints are stored in the VIS. One potential negative effect concerns the accuracy of fingerprint-based identification, needed particularly for new ***visa*** applicants. However, Member States have not reported any problems of this kind so far. Moreover, the introduction of the '0-FTE' measure did not have a detrimental effect on the overall fingerprint quality: despite the fact that the VIS now accepts all fingerprints irrespective of their quality, consulates still aim to collect the best quality fingerprints possible.

110 This measure had been requested by Member States already ***before*** the VIS was introduced, though its implementation was delayed because priority was given to other technical changes in the VIS.

109

Figure 3. Percentage of applications with poor quality fingerprints

Source: eu-LISA.

1.3.1. Statistical data for cases in which fingerprints could factually not be provided

The Commission requested that Member States provide information on cases in which fingerprints could factually not be collected, as well as the percentages that these figures represent in the total number of cases in which fingerprints were taken. Only 4 out of the 19 responding Member States provided any data on this and the data submitted was not reliable enough for the Commission to be able to draw any conclusions.

According to the information provided by eu-LISA, between April 2011 and April 2015 the percentage of cases recorded in the VIS in which fingerprints could not be collected because they were factually not ***available*** (i.e. persons for whom fingerprinting is physically impossible steadily decreased. Therefore, while the total number of applications recorded in the system increased four-fold during this period, the number of fingerprints missing because they could factually not be collected remained stable, with the exception of some peaks in February 2014 and February-March 2015, which are not related to the new regional rollouts. In April 2015 (latest period reported on by eu-LISA), the number of applications with fingerprints not attached because factually impossible represented approximately 8.6 % of the total number of applications.

Implementation of the 0-FTE feature as from October 2014*

110

Figure 4. Cases in which fingerprints could factually not be provided

Source: eu-LISA

1.3.2. Information/statistical data on cases in which fingerprints were not required for legal reasons

Only 4 out of the 19 responding Member States provided data on cases in which the applicant was exempt from fingerprinting due to their age (<12 years), which makes the overall aggregated data unreliable. For these four Member States who contributed data, the number of cases evolved as ***follows***: 125 cases in 2011; 2570 cases in 2012; 17726 cases in 2013; 28791 cases in 2014; and 44338 cases in 2015.

Only 4 of the 19 responding Member States provided data on cases in which the applicant was exempt from fingerprinting due to their status as Head of State or Government, member of a national government, accompanying spouse, or member of an official delegation. Although these data are inconclusive due to the very low response rate, they show a dramatic increase in such cases over time. This could be due to practitioners in the national ***visa*** authorities being ***more*** aware of the applicable legal provisions or to the sheer increase in the number of VIS entries because of the system's increased geographical coverage over time: 29 cases in 2011; 100 cases in 2012; 292 cases in 2013; 948 cases in 2014; and 1753 cases in 2015.

None of the responding Member States provided information on cases in which the applicant was not exempt from fingerprinting despite their status. Eight Member States reported zero such cases, while the others stated that they do not compile statistics on this.

According to eu-LISA, between April 2011 and April 2015 the proportion of cases recorded in the VIS in which fingerprints could not be collected because they were legally not required steadily decreased. The evolution ***follows*** the same pattern as for cases in which fingerprints

0

500.000

1.000.000

1.500.000

2.000.000

2.500.000

3.000.000

Fingerprints not attached, not ***available***

Total Applications

No fingerprints attached

Fingerprints not ***available***

111

could factually not be provided, showing the same relative peak in February 2014 and reaching about 8.7 % of total applications in April 2015.

Figure 5. Cases in which fingerprints were not required for legal reasons

Source: eu-LISA

1.3.3. Comparison between the number of cases in which fingerprints could factually not be provided or were legally not required and the number of cases in which fingerprints were taken

In the fourth quarter 2011, the cases in which fingerprints were not attached represented about one-third of the total number of applications (due in part to the fact that two Member States started using the VIS worldwide on 11 October 2011 without recording fingerprints), and in the fourth quarter 2015 they represented about one-tenth of the total number of applications. At the same time, although at the beginning of the reporting period the number of cases in which fingerprints could physically not be collected represented about half of the number of cases in which the fingerprints were not attached, towards the end of the period these two figures were almost equal. This means that there were very few applications in which fingerprints were not attached because they were legally not required.111

111 The statistics presented must, however, be considered with caution. If the legal definitions are correctly applied, the sum of the number of cases in which fingerprints were not ***available*** and the number of cases in which fingerprints were not required should equal the total number of cases in which fingerprints were not attached . However, according to the below table (Figure 6) extracted from the VIS, it appears that the number of fingerprints not ***available*** often equals the number of fingerprints not required, and sometimes these have values similar to the number of fingerprints not included. Such cases are not possible in reality. The fact that they appear in the system indicates inconsistencies in the way Member States encode the reason for not including fingerprints and shows that the legal and physical reasons are in practice often confused (probably because in reality a lack of fingerprints for physical reasons is also a legally justified reason for not providing the fingerprints).

112

Quarter

Total applications

Fingerprints

not included

Fingerprints not ***available***

Fingerprints not required

2011/4

297 347

112 033

61 471

61 883

2012/1

342 891

107 902

53 257

52 380

2012/2

469 678

161 541

84 056

85 773

2012/3

440 869

135 755

82 856

79 893

2012/4

537 221

141 710

95 380

98 470

2013/1

577 404

126 201

85 327

83 937

2013/2

976 141

230 519

177 215

173 865

2013/3

1 052 918

210 721

182 805

176 757

2013/4

869 094

157 045

142 474

83 388

2014/1

1 075 996

207 274

192 918

128 237

2014/2

1 629 464

379 134

358 525

290 101

2014/3

1 535 298

312 487

296 383

243 461

2014/4

1 305 966

203 518

196 110

148 642

2015/1

1 408 616

214 190

205 628

164 685

2015/2

2 405 285

658 768

641 176

393 709

2015/3

2 734 616

594 626

567 708

345 871

2015/4

1 882 977

177 936

162 316

164 279

Figure 6. Cases in which fingerprints could factually not be provided or were legally not required compared with the total number of applications

Source: eu-LISA

1.4. Cases of ***visa*** refusal where a person could not physically provide fingerprints

The quantitative information provided by Member States to eu-LISA112 is presented in the table below (figure 7). The trend recorded from September 2013 until September 2015 indicates a slow general increase of the relative proportion of cases in which a ***visa*** was refused when it was physically impossible to collect fingerprints in the total number of ***visas*** refused. The relative proportion varies from less than 7 % in September 2013, with a peak of

112 For the fields ‘Registered applications’, ‘Registered applications with fingerprints’, ‘Registered applications without fingerprints’, ‘Registered applications without fingerprints — legal’ and ‘Registered applications without fingerprints — physical’, the figures are missing data from two Member States. The latter field is missing data from a third Member State as well. However, for the field ‘Refused ***visas*** — fingerprints could not be provided factually", the figures include data from all Member States.

113

almost 14 % in July 2014, to around 11 % in September 2015. The overall annual percentage of these cases during the reported period was around 11 %, with a small decrease in 2015 (10.8 %).

Period

Registered applications

Registered applications with fingerprints

Registered applications without fingerprints

Registered applications without fingerprints — legal

Registered applications without fingerprints — physical

Refused ***visas***

Refused ***visas*** — physically impossible to collect fingerprints

% Refused ***visas*** — physically impossible to collect fingerprints

Sep-13

282.357

243.176

37.317

33.576

3.987

39.825

2.748

6.9 %

Oct-13

261.023

217.755

47.375

37.224

10.389

39.967

3.111

7.8 %

Nov-13

274.325

224.587

48.228

20.425

27.954

37.045

2.963

8 %

Dec-13

253.587

206.289

45.623

20.865

25.066

41.003

3.519

8.6 %

2013 TOT

1.071.292

891.807

178.543

112.090

67.396

157.840

12.341

7.8 %

Jan-14

256.407

217.927

36.640

20.029

16.739

37.032

3.369

9.1 %

Feb-14

301.098

248.983

50.293

29.361

21.104

36.810

3.658

9.9 %

Mar-14

407.480

318.429

87.026

59.273

28.282

42.287

4.305

10.2 %

Apr-14

426.318

326.854

101.681

76.312

25.412

41.110

4.605

11.2 %

May-14

496.852

377.841

116.372

92.949

23.078

41.941

4.973

11.9 %

Jun-14

553.543

420.163

129.563

103.115

26.192

45.147

5.932

13.1 %

Jul-14

516.634

391.408

121.287

97.653

23.435

47.340

6.562

13.9 %

Aug-14

423.187

340.867

80.636

62.973

17.485

44.113

5.795

13.1 %

Sep-14

427.270

349.495

76.108

57.640

17.809

47.299

5.349

11.3 %

Oct-14

405.009

341.623

62.252

42.107

19.862

48.785

4.609

9.4 %

Nov-14

392.517

328.362

62.875

45.869

16.727

50.312

4.354

8.7 %

Dec-14

359.310

296.847

61.153

44.298

16.464

53.247

5.447

10.2 %

2014 TOT

4.965.625

3.958.799

985.886

731.579

252.589

535.423

58.958

11 %

Jan-15

348.036

298.470

48.278

37.492

10.281

43.609

3.777

8.7 %

Feb-15

398.423

338.297

58.676

44.162

13.704

46.155

4.010

8.7 %

Mar-15

540.597

441.753

97.032

70.799

25.144

52.385

4.627

8.8 %

Apr-15

589.168

451.261

136.274

88.322

46.628

51.022

4.596

9 %

May-15

705.258

490.383

213.408

104.016

107.911

51.156

5.557

10.9 %

Jun-15

848.153

590.236

255.043

124.891

127.530

62.689

8.067

12.9 %

Jul-15

954.344

672.888

280.324

117.872

160.656

63.108

8.501

13.5 %

Aug-15

782.190

609.364

170.795

86.957

82.039

65.307

7.687

11.8 %

114

Sep-15

739.759

617.926

120.832

71.162

47.408

63.674

7.096

11.1 %

2015 TOT

5.905.928

4.510.578

1.380.662

745.673

621.301

499.105

53.918

10.8 %

Total

11.942.845

9.361.184

2.545.091

1.589.342

941.286

1.192.368

125.217

10.5 %

Figure 7. Cases of ***visa*** refusal where a person could not physically provide fingerprints

Source: eu-LISA

The information provided by the responding Member States shows that the few cases in which a ***visa*** was refused to a person whose fingerprints could physically not be collected were not linked to the physical impossibility of collecting fingerprints, but rather to one of the grounds for refusal set out in the ***Visa*** Code. These included an absence of proof of sufficient means of subsistence, situations where the purpose of travel was not clear or justified, and no proof of return to the point of origin after the end of travel.

1.5. Implementation of the 59-month rule for copying fingerprints

Figure 8. Statistics of fingerprints copied in VIS, per Member States

Source: eu-LISA

Statistical data on situations in which fingerprints were collected again ***before*** the end of the 59-month period were not ***available***. However, most Member States admit that this takes place in practice, and evaluation teams confirmed this on two occasions during SCHEVAL monitoring missions (in two different Member States).

The reported reasons for repeated collection are related to doubts regarding the identity of the person, the poor quality of the first collection, difficulties in finding the first file in the system

MS

Applications

% Copy

MS

Applications

% Copy

Austria

49,397

0.79%

Lithuania

96,323

5.98%

Belgiu

44,527

11.77%

Luxembourg

2,04

6.46%

Denmark

19,510

10.56%

Malta

6,45

0.00%

Estonia

31,341

3.48%

Netherlands

105,63

5.80%

Finland

140,99

1.88%

Norwa

18,912

2.47%

France

607,71

7.98%

Poland

257,50

11.35%

Germany

389,23

11.39%

Portugal

39,739

30.80%

Greec

64,506

16.95%

Slovakia

17,995

2.88%

Hungary

57,181

2.25%

Slovenia

5,20

8.52%

Icelan

510

2.94%

Spain

265,34

8.98%

Italy

321,46

5.04%

Sweden

30,298

7.32%

Latvia

36,440

5.05%

Switzerland

78,996

9.07%

Liechtenstein

0

N/A

The Czech republic

96,058

0.00%

Total

2,783,32

8.00%

VIS usage of CopyBiometric operation October-December 2015

115

due to different country codes used by different Member States, or simply the fact that applicants are often themselves uncertain of whether or not they already gave their fingerprints and volunteer to give them (again) when they apply for a ***visa***. This last situation occurs frequently due to the widespread use of external service providers (ESP) for collecting applications and biometrics, as these do not have access to the VIS and thus cannot check whether the applicant's fingerprints have already been taken.

Except for very small Member States with limited consular networks, cases with a 0% occurance of the 'copyBiometric' operation would suggest that the service has not been technically implemented or that there is a serious lack of awareness among consular staff as regards the rule on copying biometrics.

1.6. Suitability of the chosen International Civil Aviation Organisation standard

The technical requirements for the ***visa*** photograph must be set in accordance with the standards set out by the International Civil Aviation Organisation (ICAO) in document 9303 Part 1, 6th edition. All Member States and the eu-LISA confirmed that the current ICAO standards for photographs are most suitable for ***visa***-related activities. One Member State, however, noted that there are no requirements for the recording procedure.

If automated facial image recognition were to be used in the VIS (1:1 operation), all photographs would at least need to comply with ICAO standards. As the ICAO standards set a number of conditions which would not be sufficient in case of a search (1:n operation — see for example the Entry Exit System currently under discussion, where a search should combine four fingerprints with a photograph), a minimum photograph quality would need to be set and enforced.

Fingerprints must be taken in accordance with ICAO standards and Commission Decision 2006/648/EC of 22 September 2006 laying down the technical specifications on the standards for biometric features related to the development of the ***Visa*** Information System. Most of the responding Member States (13) declared that the current standards are most suitable for ***visa***-related activities.

116

II ORGANISATION OF APPLICATION-RELATED PROCEDURES

2.1 Operational cooperation between Member States

In order to facilitate the ***visa*** application procedure, the ***Visa*** Code provides for several forms of cooperation, such as limited representation, co-location, common application centres, recourse to honorary consuls, and cooperation with ESPs, taking into account data protection requirements.

The impact assessment accompanying the 2014 Commission proposal to amend the ***Visa*** Code113 identified insufficient geographical coverage in ***visa*** processing as one of the major problems in the development of a common ***visa*** policy, leading to costly and lengthy application processes for applicants in many third countries.

Since then the situation has slightly improved as the number of representation arrangements between Member States is steadily growing (also indirectly, due to the lifting of the ***visa*** requirement for a number of third countries in 2015), making it the most widespread means of cooperation and of expanding consular coverage. Access to consulates/ESPs can be challenging in countries where all or most of the Member States are present in the capital and where many applicants need to travel long distances to reach them. Finally, there are still eight third countries114 whose nationals are subject to a ***visa*** requirement obligation and in which no Member State is present for the purpose of collecting/processing ***visa*** applications.

Despite improvements in geographical coverage, to date there are still around 500 ‘blank spots’ in the table of consular presence/representation,115 where Member States are neither present nor represented in the capital. Full presence/representation is only ensured in approximately 25 locations worldwide116.

Most responding Member States described the quality of operational cooperation between Member States as good or satisfactory. Examples of good cooperation include exchanges of information/lessons learned prior to VIS roll-out in a certain region, with Member States that were already outsourcing parts of the ***visa*** process. During audit

missions, Member States include meetings with other Member States to exchange information and harmonise procedures. If a Member State temporarily cannot process ***visa*** applications due to technical

113 Doc COM(2014) 164 final and SWD(2014) 68 final.

114 Belize, Gambia, Guyana, Liberia, Maldives, Papua New Guinea, Sierra Leone, Swaziland.

115 A full table with Member States' consular presence is published on the DG HOME website at *http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/borders-and-**visa**s/**visa**-policy/index_en.htm*.

116 Annex 28 to the ***Visa*** Code Handbook (last revision:15.01.2016): Algeria: Algiers; Azerbaijan: Baku; China: Beijing, Shanghai; Egypt: Cairo; Georgia: Tbilisi; Ghana: Accra; India: New Delhi; Indonesia: Jakarta; Israel: Tel Aviv; Japan: Tokyo; Jordan: Amman; Russian Federation: Moscow, St. Petersburg; Saudi Arabia: Riyadh; Serbia: Belgrade; Sri Lanka: Colombo; Thailand: Bangkok; Turkey: Ankara; Ukraine: Kiev; UK: London; USA: Washington; Vietnam: Hanoi.

117

problems, other Member States may ensure back up, taking in ***visa*** applications on behalf of the Member State in need. However, the number of ***visas*** issued manually for technical reasons remains high for some Member States and a spot check carried out in 2014 revealed that data on manual applications were not entered in the VIS. Unfortunately, the Commission was not in a position to carry out a comprehensive study of this phenomenon because of lack of access to data in the VIS.

The temporary dysfunction of the N-VIS in one Member State in December 2015 was an example of how Member States cooperate in crisis situations and showed the importance of support provided by other Member States in such situations. The dysfunction started on 10 December 2015 and the normal situation was fully restored only on 6 January 2016. Technical failures in the national system prevented the Member State's consulates from sending data to the VIS. The Member State concerned immediately stopped issuing ***visas***, while other Member States' representations in the various locations ***stepped*** in to handle urgent applications. There was regular communication with eu-LISA and other Member States throughout, and situation reports were submitted. When the normal situation was restored, the concerned Member State's authorities immediately carried out an assessment of the event's impact on the VIS, and established its causes and consequences. The results were presented to the relevant bodies (such as the Friends of VIS Working Party in the Council and the VIS Advisory Group).

There are currently no co-locations or common application centres (CACs) as defined by the ***Visa*** Code, although the Commission has promoted the setting up CACs in the past. The 2014 Commission Report on the ***Visa*** Code already identified this as a major issue and the situation has not changed since. The impact assessment for the 2014 Commission proposal to revise the ***Visa*** Code identified several reasons for this situation, one of a legislative nature: Article 41 of the ***Visa*** Code does not provide the necessary flexibility to set up co-locations and CACs on the spot.

To date, not one fully-fledged CAC has been created, though, as for co-location, funding had been made ***available*** to develop consular cooperation projects under the Community Actions of the External Borders Fund. Only two such projects have been funded: the 'Schengen House' in Kinshasa, Democratic Republic of Congo and the 'Centro Comum de Vistos' in Praia, Cape Verde. However, these operate based on classical representation arrangements:

applications are lodged and examined at the centre, and decisions are also taken there, by the Belgian and Portuguese consulates, respectively.

The Commission continues to abide by its opinion expressed in the 2015 Report on the ***Visa*** Code that, from a practical and technical point of view, setting up such cooperation is cumbersome and not worthwhile if the purpose is only to collect ***visa*** applications, when there are fully equipped and staffed consulates to examine the applications. The money potentially saved by sharing facilities to receive applicants and equipment to collect biometric data is likely to be spent on costs linked to transferring data, files and staff from the 'co-location' to the 'back office'.

118

This shortcoming led the Commission to propose a revision of the provisions of co-location and CACs in the 2014 proposal to recast the ***Visa*** Code, currently under examination by co-legislators, and to introduce instead:

• a general notion/concept of 'Schengen ***Visa*** Centre' which would provide a ***more*** realistic and flexible definition of certain forms of consular cooperation;

• the concept of 'mandatory representation' according to which, if the Member State responsible for processing the ***visa*** application is neither present nor represented (under such an arrangement) in a given third country, any other Member State present in that country is obliged to process ***visa*** applications on their behalf.

The use of honorary consuls to collect ***visa*** applications is extremely limited. By the end of 2015, only three Member States used this possibility — Italy (mainly for applications for national ***visas***), Malta and Poland.

The ***Visa*** Code provides that no form of organisation should lead to the applicant being required to appear in person in ***more*** than one location to lodge an application. The Commission has taken action against certain Member States who violated this principle. One case concerned a Member State present in Lagos/Nigeria which used a two-***step*** procedure to collect fingerprints in some locations, until the ESP was given the necessary equipment. The applicant had to first submit a paper file and later on had to come to the consulate to give fingerprints. The problem was eventually solved and this practice was eliminated.

Some Member States (e.g. Spain, Denmark) practice both representation and use of ESPs in some locations (e.g. Minsk). This is an example of good practice.

This issue is closely linked to the possibility of direct access provided in Article 17(5) of the ***Visa*** Code, according to which Member States using outsourcing must maintain the possibility for applicants to lodge their application directly at the consulate so that no one is forced to pay an extra service fee.

The Commission had in the past received numerous complaints about Member States' violation of this provision, and has therefore conducted an investigation on their practices. It turned out that, in some cases, there was no possibility to lodge applications directly at the Member State's consulate, the only option was to lodge them at the premises of the external service provider.

The 2014 evaluation of the implementation of the ***Visa*** Code already looked into this matter and found that the formulation in the legal text ('maintain the possibility …. to lodge their application directly') made it difficult for Member States to enforce this provision. Bearing in mind that the main reason for using outsourcing is a Member State's lack of resources and facilities to receive applicants in high numbers or for security reasons, the requirement on direct access to the consulate can be seen as an impossible to meet. To ensure that emergency cases are treated promptly, priority access to the external service provider should always be possible.

119

To address this issue, the 2014 proposal to recast the ***Visa*** Code provided that Member States are no longer obliged to maintain the possibility of 'direct access' for lodging applications at the consulate in places where an external service provider has been mandated to collect ***visa*** applications (Article 17(5) was deleted). However, Member States may always maintain this possibility.

2.2 Experience with external service providers (ESPs)

2.2. 1 Member States' use of ESPs

The 26 Member States have representations in 175 countries worldwide. Outsourcing is steadily growing and practically all Member States do it in several locations. The main reason for outsourcing the collection of applications is the volume of applications and large territories. This is true for most countries in which outsourcing is used: Russia, China, Ukraine, Belarus, Turkey, Algeria, India, Morocco and Saudi Arabia. ESPs generally have ***visa*** application centres (VACs) in the capital and bigger cities, and 'satellite VACs' ('dropboxes') in other locations.

2.2. 2 Legal instrument governing cooperation between a Member State and an ESP

Cooperation between a Member State and an ESP must be based on a legal instrument (a 'contract'), to be drawn up based on ***Visa*** Code Article 43 and Annex X which set out a list of minimum requirements to be covered.

Under Article 43(13), Member States are required to provide a copy of their contracts to the Commission. In principle, this should happen when cooperation with an ESP starts, is renewed, suspended or terminated. Member States have failed to share contracts systematically.

In 2015, the Commission carried out a study of the state of affairs regarding the existence and content of contracts concluded by Member States. By March 2016, eleven Member States sent the Commission all their contracts relating to cooperation with ESPs. Three Member States have still not sent in their contracts, and information from twelve Member States on contracts that were terminated or are being renewed is pending.

An analysis of the submitted contracts makes it possible to draw a set of conclusions, and these are discussed below.

Generally, Member States' monitoring of ESPs is sub-optimal; records of announced and unannounced visits and reactions to possible malpractices are not kept. This is why the Commission has proposed to strengthen the monitoring and reporting provisions in the 2004 proposal on the recast ***Visa*** Code, in Article 41(12).

120

The type and extent of the contracts to be used are left to Member States' discretion and internal organisation. Based on the Commission's analysis and Member States' responses to the present evaluation, 30 % of Member States use global framework contracts and 70 % use local contracts.

Most local contracts are for the outsourcing of services in a given jurisdiction or third country, but there are also several examples of contracts covering specific regions (e.g. South Caucasus, Central Asia) or several countries (e.g. India and Nepal, South Africa and Swaziland).

The contracts often include the possibility to sub-contract work to a local service provider. In most cases, this is subject to prior approval by the Member State's Contracting Authority.

As regards the scope of the contracts, Member States generally outsource the collection of both long-stay and short-stay ***visa*** applications.

Under Article 43(1) of the ***Visa*** Code, Member States must select the ESPs without prejudice to public procurement and competition rules. Responses to the evaluation showed that practically all Member States launch calls for tender to select ESPs.

However, based on an analysis of submitted contracts, it seems that the existence of a tender procedure cannot be ascertained in all cases. Only an average of 50 % of contracts include a reference to a call for tender.

According to the information provided by Member States (only 20 % of the responding ones), contracts are negotiated and concluded either by embassies/consulates directly with ESPs, under the supervision and control of the central administration, or by Member States' central authorities (the latter happens in particular for Member States with minor consular representation).

Some Member States reported that the ESP is selected based on the best offer of price and quality.

Member States have concluded contracts with a limited number of companies: 80 % with VF Worldwide Holdings Limited/VFS Global, 8 % with TLS Contact, 12 % with local companies.

Finally, as regards the tenure of the contract, the average duration is three years. In most cases, this can be renewed up to a limited number of times. In some cases, however, a limit is not set or renewal is automatic.

Most contracts with ESPs contain a 'sauvegarde' clause to ensure service continuity if the contract is terminated (Article 43(12)). This clause states that the contract remains in force for a certain period of time after its expiry date. This period should not be indefinite.

The list of minimum requirements set out by Article 43(2) and Annex X of the ***Visa*** Code can be divided into two main areas. It requires that contracts include provisions governing the performance of ESP activities, such as those related to the conduct of staff (qualifications, training, behaviour) and to data protection and transmission. It also requires

specific provisions for the verification and monitoring of ESPs' performance, notably by granting consular staff the right to access ESP premises and the possibility to monitor them and the ESP's software system remotely.

An analysis of contracts provided to the Commission so far has shown that Member States' contracts by-and-large include these elements. In some cases, Member States even transpose them exactly as written in Annex X.

In the few cases where this is not the case, in particular with regard to the second set of provisions (monitoring of performance), the Commission will address the issue directly with the Member States concerned within the applicable legal framework.

The implementation of contracts is checked in the context of the periodic evaluation of the implementation of the Schengen acquis. ***Following*** on-site visits to ESP premises and related consular posts, the evaluating group of experts checks the conformity of the ESPs' practices against the contractual provisions. In cases where a problem was found, a list of recommendations was sent to the Member State concerned.

2.2. 3 Organisation and implementation of services

Most Member States train ESP staff when a new ***visa*** application centre is set up. A two-way process is usually in place: embassy staff visit the ESP to train the staff there and ESP staff visit the Member State's embassy in the host country or in a neighbouring country; only rarely is ESP staff trained in the Member State concerned. After the inception phase, training is provided upon need, and especially when new legislation or technical procedures are implemented (e.g. introduction of biometric data capture when the VIS was rolled out). The 'train the trainer' method is often used, where supervisors are invited to take part in training sessions given by instructors from the Member State's representation and they will in turn train ESP staff. However, based on information collected in the framework of SCHEVAL evaluations, continuous training and awareness raising on new legislation and practices appears to be suboptimal (e.g. changes of practices at the ***visa*** section are not systematically communicated to the ESP).

All responding Member States declared having procedures for monitoring ESPs' activity. Ways to ensure that ESPs provide all information required by ***visa*** law and meet the data protection requirements related to collecting the ***visa*** application and biometric data include:

− Inclusion of these requirements in agreements concluded with the ESPs, including the obligation for the ESP to put in place the necessary framework and procedures for quality assurance/control. The agreements usually include a description of the complete process of handling the application, from receiving the documentation to returning the travel document to the applicant.

122

− Conclusion of data processing agreements with the ESP. ESPs often have their own data protection system in place, and are accredited on personal data protection requirements by the host country in accordance with national regulations.

− Permanent monitoring by the consulates.

− Regular checks of VACs by national ***visa*** authorities, according to a checklist based on the ***Visa*** Code.

All Member States declared having the relevant information on ***visa*** requirements published on the ESP's website and in the VACs. However, SCHEVAL field monitoring showed that this was not always the case (e.g. there was a lack of updated information on ***visa*** requirements on the ESP's premises and on the consulate's website).

All Member States declared having technical and organisational security measures in place to ensure that personal data are adequately protected against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access. These measures are usually also part of contracts concluded with ESPs. In addition, guidance on how the consulate should supervise the ESP's activities is ***available***.

According to the ***Visa*** Code, ESPs do not have access to the VIS for encoding data, nor can they store data on own devices. Each ESP collects and stores biometric data on a secure server, from which Member States import them into the VIS. If the ESP does not have a direct secure IT connection to the consulate, the data are registered on a data carrier, which is electronically signed and encrypted. The data carrier is transported with physical files in a locked and sealed courier bag/suitcase/box, by the ESP's own courier or an external courier company.

According to replies from Member States on monitoring methods, the favoured way of monitoring ESPs is through announced and unannounced audits carried out by consulates, although inspection teams from headquarters and the national data protection authority are also mentioned. About 20 % of responding Member States mentioned monthly audits, though most had no fixed frequency. Test applicants are rarely used to monitor ESPs (only one Member State mentioned this method).

However, SCHEVAL field missions uncovered shortcomings in this, in particular as regards visits of consular staff to VACs (non-existant in some cases) and the consular staff's supervision of the ESP's process of delivering applications and collecting passports (no electronic tracking of document exchange; lack of an internal monitoring report; lack of remote access to the ESP's appointment system software).

In order to address this issue, the 2014 proposal to recast the ***Visa*** Code envisaged an amendment to the rules on cooperation with ESPs. It requested that Member States provide to the Commission annual reports on their cooperation with and their monitoring of ESPs worldwide, in accordance with Annex VI (former Annex X) to the ***Visa*** Code.

Two of the responding Member States declared having experienced situations of insolvency, unreliability, conflicts of interest or other problems with an ESP. One Member State found that staff at a specific ***visa*** application centre received commissions based on how many

123

additional services they sold. As additional services are optional, this was not considered to be in line with the agreement and this form of compensation was stopped. Another Member State experienced some reliability- and efficiency- related problems, mostly in IT, which were solved through contacts between the consulate and the ESP.

All responding Member States assessed the overall satisfaction of ***visa*** applicants with the ESPs' services as very good and mentioned having received very few or no complaints. Reasons for complaints include misunderstanding the VAC's role, problems with appointments, inadequacy of the premises (limited space, few attending staff, waiting times), or not receiving a satisfactory explanation for a ***visa*** refusal (the latter is the Member State's responsibility).

Most Member States ensure that complaints are sent directly to their consulate. If the ESP receives a complaint, it can ***follow*** the procedure for receiving and responding to complaints included in the contract. Complaints should be forwarded to the consulate, which then further decides on the matter. If the ESP proposes an answer itself, it must submit it to the consulate for approval ***before*** it sends it to the applicant.

None of the responding Member States received complaints regarding data protection or uncovered any data protection irregularities in ESPs' activities. There has never been any action taken under the host country's national law on an ESP's alleged breach of data protection obligations.

However, 40 % of responding Member States have terminated or suspended cooperation with an ESP. The three main reasons for such termination are:

− the closure of the consulate;

− granting the contract for activities to another ESP ***following*** a public tender;

− non-respect of the contract concluded between the Member State and the ESP (this seems to have occurred in a single case, due to the ESP's delayed start of services caused by an inadequate IT solution).

2.2. 4 The service fee

An ESP charges a service fee to cover the service offered (Article 17). The fee must be set in the contract between the Member State and the ESP.

According to Member States' reporting, the service fees charged by ESPs comply with the limitations imposed by the law (i.e. they are proportionate to the costs incurred by the ESP and do not exceed half of the amount of the ***visa*** fee, i.e. 30 euros). The fees charged worldwide vary between approximately 10 euros and 30 euros. Some ESPs charged lower fees ***before*** the VIS was rolled out (i.e. ***before*** the collection of biometric identifiers) and adapted them to local price levels. A good practice was identified in some Member States who have set a maximum fee of 20 euros regardless of location.

124

However, there were some cases where the fee exceeded the 30 euro ceiling, sometimes due to the addition of a mandatory courier fee for sending the application to the competent Member State's consulate or because of exchange rate variations. The two responding Member States whose ESPs exceeded the limit are the same ones that stated during the consultation that the fee limitation under the ***Visa*** Code has given rise to problems in practice. The fee limitation was contested by one Member State in particular, who argued that the limit is a hindrance in cases where a state intends to introduce a 'hub and spoke organisation' (where the application is handed in to the service provider in one country and transported to a regional or central hub for handling and decision). This is the case for example in Palestine, where the ESP requires a 30 euro service fee (plus 12 euro courier fee).

Responding Member States pointed out that the objective of harmonising the service fee in certain locations cannot be reached, for reasons which can be summarised as ***follows***:

− Member States negotiate their contracts individually, which leads to differences in the prices ESPs propose to them.

For example, Member States bring different volumes of ***visa*** applications when negotiating a contract with a local service provider, so even if several Member States use the same ESP in a given location, the prices quoted by the ESP will vary.

− Member States work with different service providers in the same location (since the contract with an ESP is the result of public procurement, the same ESP does not always win all contracts in a location).

− Member States do not always outsource the same tasks.

− Member States may provide the hardware/software solution or not.

In reality, this situation prevents the implementation of Article 17(3), according to which Member States 'shall aim to harmonise the service fee applied'. Since the ***Visa*** Code does not lay down a clear obligation ('shall aim to'), local harmonisation of the service fee is de facto not attained.

2.2. 5 Quality of the collection of biometrics by ESPs

All responding Member States declared satisfaction with their cooperation with ESPs regarding the collection of biometric data. Minor difficulties in the beginning (such as problems with the transfer of the biometrics via the national system, or problems with the quality of the biometrics collected by the ESP) were quickly resolved.

Member States often mentioned training as the most efficient way to address problems.

2.3 Equipment for the collection of biometric identifiers

125

Only seven of the responding Member States provided information on the level of equipment possessed by consulates and authorities responsible for processing ***visa*** applications at borders, with the required material for collecting biometric identifiers.

All responding Member States declared having sufficient infrastructure in consulates and at border control posts to handle the VIS-related requirements and to have all ***visa*** issuing authorities properly equipped. One Member State highlighted the need to equip border guards with mobile equipment do deal with specific situations.

2.4 Encryption and secure transfer of data

For representation arrangements between Member States, Member States' cooperation agreements with ESPs, or in cases of recourse to honorary consuls, the Member State concerned must ensure that all data are fully encrypted, whether they are electronically or physically transferred.

In third countries where electronic data transfer of encrypted data is not possible or is not possible without specific measures (potentially) damaging the data's confidentiality, most responding Member States (11) declared having avoided working with an ESP and/or being represented by another Member State.

None of the responding Member States concluded any agreements with third countries with the aim of lifting the prohibition against encryption of data to be electronically transferred. One Member State reported that it asked the ESP to send the encrypted data to the consulate via 'crypto-hub'. The encrypted data was then sent to the Member State's capital and was protected under Articles 27 and 33 of the Vienna Convention on Consular Cooperation.

If it is necessary to transfer data from an ESP to the consulate physically, the timing depends on the distance between the ESP and the consulate. Five responding Member States stated that transfers are normally done during

the same working day. However, in some specific circumstances such as problematic or vast countries, the transfer can take between two and (maximum) five days.

III RELIABILITY OF FINGERPRINTS OF CHILDREN UNDER THE AGE OF 12 FOR THE PURPOSES OF IDENTIFICATION AND VERIFICATION

3.1 Evolution of fingerprints with age (based on a study carried out under the Commission's responsibility)

Article 57(3) of the ***Visa*** Code requires that the issue of the sufficient reliability for identification and verification purposes of fingerprints of children under the age of 12 and, in particular, the issue of how fingerprints evolve with age, be addressed based on the results of a study carried out under the Commission's responsibility. The study was carried out in 2013 by the Digital Citizen Security Unit of the Joint Research Centre of the Institute for the

126

Protection and Security of the Citizen (JRC-IPSC). Its results were published in the 'Fingerprint Recognition for Children' report (Report EUR 26193 EN).

The JRC study addressed the question of whether or not automated fingerprint recognition for children is feasible, that is, if the recognition rates obtained with this technology for children are similar to those reached for adults. The study faced two major challenges in order to draw meaningful conclusions about the changes in children's fingerprints over time:

− As the data processed belonged to children, the JRC was logically required to implement the most stringent safeguards in order to guarantee the highest level of care in preserving their rights.

− On the other hand, large amounts of data were required in order for the studies to result in statistically significant data. Any quantity in the range of hundreds or even thousands of properly selected test people could produce some initial findings, but tens of thousands of people were required for a real performance analysis of state-of-the-art fingerprint recognition systems.

A solution that respects these requirements was found with the support of the Portuguese government, which made ***available*** a large source of children's fingerprint data from their national repository of passport data.

The study's main conclusions showed that:

− Growth has limited influence on fingerprint recognition — Although the passage of time was expected to be the most important factor influencing children's fingerprint recognition, all tested algorithms showed the same recognition rate regardless of the time elapsed between fingerprint collections (of up to 4.5 years).

− Size (in terms of the dimensions of the relevant fingerprint characteristics) does not constitute any theoretical barrier to automated fingerprint recognition. Within the ***available*** investigation window of up to 4.5 years between fingerprint colelctions, there was no theoretical barrier observed for the correct automated recognition by current matching algorithms, provided the images were of sufficient quality.

− Image quality (in terms of low contrast and distortion effects) is the ultimate problem for children's fingerprints, and image quality is strongly influenced by size. Though the observed image issues are well-known also in adults, the issues get worse and the probability of problems increases with the smaller structure sizes of children's fingerprints. Therefore, the correct recording of fingerprints is a key factor in successful recognition.

− Relevant quality metrics for fingerprints need revision with regard to the case of children. Otherwise, the reported quality scores might be misleading. The data and the results processed for this study can contribute to the correct revision of quality metrics.

− An isotropic growth model may serve as a good approximation to cover changes over time. The data from Portugal, with only two fingerprints per child, do not allow for a clear distinction of distortion from other effects. However, an isotropic model (i.e. linear

127

growth of the fingerprint in all directions) seems to be sufficient to estimate the real level of impact that the growth effect has, if any.

− Alternative acquisition devices for fingerprints should be seriously considered in the future. Experiments with multi-spectral and touchless fingerprint capture devices, as well as with traditional devices with enhanced user guidance, gave promising indications on how the quality issues could be better managed — on top of already existing best practice guidelines for the improvement of quality in fingerprint acquisition.

These conclusions confirm that, under certain technical conditions, fingerprint recognition of children aged between 6 and 12 years is achievable with a satisfactory level of accuracy.

In order to achieve this objective, the study also makes a series of recommendations, as ***follows***:

− Image quality is key. A certain minimum level of training of operators and data subjects is necessary to acquire high-quality images. Training needs to be designed for the particular setting in which the fingerprint acquisition will be carried out. Analysis of the context should be a strong prerequisite and guidelines for this purpose can be further developed and promoted.

− Matching algorithms can be further improved. Experiments with various versions of matching algorithms suggest that there is still room for improvement, at least with regard to time lapses beyond five years, which could not be addressed by this study. An earlier study had already demonstrated the benefits of such measures. Improvements can be made with respect to adaptations that addresss child feature dimensions and/or by applying the isotropic growth model. These improvements will then need to be tested and evaluated in a rigorous and fully independent way.

− Availability of relevant test data. The significant insights gained from the Portuguese data on realistic automated recognition of children’s fingerprints clearly emphasise the need for long-term availability of such data for research and development. The key aspects of such a data repository would be its permanence (as a unique and EU-wide reference), full compliance with security and data protection requirements, and efficient usage (in combination with security measures) with quality metrics.

− Selection of acquisition devices. Experiments with multi-spectral, touchless and novel four-finger capture devices gave promising indications on how the quality issues could be better managed. These emerging technologies should be further explored.

The study’s limitations are discussed in a chapter underlining the remaining open questions:

− Calibration with adult data. The impact of the children-specific issues still needs to be ***more*** clearly distinguished from general quality-degrading issues. Therefore, performance in the recognition of adult fingerprints needs to be

compared to that of children's fingerprints where the adult data were acquired under similar conditions to children's data. This would make it possible to predict the performance loss for children's data, if there are no other reasons for the difference.

128

− Trials on recording children's data. In order to quantify a practical age limit, given the best ***available*** technology, larger field trials on recording children's data need to be conducted. These trials should further investigate and quantify the impact of certain devices and procedures.

− Refined growth model. The current results do not contradict the assumptions of an almost isotropic growth model as suggested by an earlier study. At least, it seems suitable as a first order approximation for improving algorithms in cases where the time lapsed between fingerprint collections is not greater than the one considered in the present study (i.e. 4.5 years). However, it is desirable to draw conclusions for longer time windows (beyond five years) in order to give clear instructions to developers of fingerprint recognition systems.

3.2 Impact of the evolution of fingerprints with age on the reliability of their use for the purposes of the person's identification and verification

The results of the study seem to indicate that, from a technical point of view, automated fingerprint recognition for children is feasible, provided some technical obstacles related to image quality and the revision of quality metrics are overcome, and alternative acquisition devices for the fingerprints of children are considered.

Apart from the technology upgrade that is needed in order to ensure the reliable use of children's fingerprints for the purposes of identification and verification, there are other considerations to keep in mind ***before*** deciding on the collection of children's fingerprints. As biometric identifiers are taken with the main purpose of facilitating the fight against ***visa*** fraud, it needs to be assessed whether this policy objective is to be pursued in the case of children under the age of 12 — have cases of fraud, attempts to bypass the criteria for determination of the Member State responsible for examining the ***visa*** application, or any other of the objectives set out in the VIS Regulation been identified in relation to children under the age of 12? If yes, is the scope of such phenomena significant enough to justify this measure? The pertinence of and need for identifying and verifying children under the age of 12 must be clear for further action to be taken in this area.

129

Annex 4: Technical progress made regarding the use of fingerprints at external borders on the basis of Article 50(5) of Regulation 767/2008 (the VIS Regulation)

Technical readiness of VIS use at the external border crossing points

Summary: The gradual worldwide rollout of the ***Visa*** Information System (VIS) that completed on 20 November 2015 contributed to a progressive introduction of fingerprint-based verifications at borders as from October 2014. The vast majority of Member States started gradually to use the fingerprints from the moment the biometric checks became mandatory, although some states started checking fingerprints as part of pilot projects. When considering the number of issued ***visas*** with fingerprints and the related checks at borders, the evaluation found that Member States have overall made progress on the use of the fingerprints at external borders. The evaluation also identified ways of increasing the proportion of ***visa*** holders whose fingerprints are actually checked at borders.

The Member States have established the appropriate capacities and organisational framework to cope with tasks related to the use of fingerprints both at first and second lines. Although some regions were issuing ***visas*** without fingerprints ahead of the coordinated rollout of ***visas*** with fingerprints, the proportion of ***visas*** checked with the ***visa*** sticker number together with fingerprints has not yet reached the optimal figure. The evaluation also identified areas where improvement was needed: among the most noteworthy was the proportion of ***visa*** holders checked (with or without the fingerprints), which remained below 50 %.

Given Member States' limited contributions to the survey, the evaluation found that it remains difficult to determine a realistic figure for the number of border crossing points equipped with fixed or mobile devices for the capture of fingerprints.

The evaluation found that outside the first months of running the new system, Member States have experienced very few hardware or software problems and infrequent administrative impediments to checking fingerprints at external borders. Cases where multiple scans were needed to collect fingerprints of sufficient quality and attempts at spoofing have been reported as sporadic.

The evaluation found that the process to check ***visas*** at borders is significantly influenced by the ***visa*** marking though a slight difference exists between the meaning of the marking and its actual use. The evaluation also found that situations where capturing devices and the VIS are unavailable are managed using appropriate alternative procedures.

Most Member States started performing systematic checks against the VIS at the external borders on the basis of fingerprints, at least as concerns ***visa*** holders' data present in the VIS,

130

in October 2014 i.e. three years after the start of operations as per Regulation 81/2009, which amended Regulation (EC) No 562/2006 as regards the use of the VIS at borders.117

Figure 1: Number of Member States per start date for fingerprint-based checks

Seven Member States declared not having encountered technical problems or administrative impediments in checking fingerprints at external borders. Nine Member States declared having experienced such problems. Two Member States did not respond.

The main reasons were:

- limited hardware performance;

- problems with ***visa*** sticker scanning due to its variable location on the passport page;

- software not sufficiently prepared for ***visa*** applications with no fingerprints;

- possible negative match of the traveller's fingerprints with those in the VIS;

- insufficient quality of fingerprints collected in consular posts or damage to the traveller's fingerprints;

- the absence of fingerprints in the VIS for a region already rolled out;118

- resistance to fingerprint-based checks at borders;

- long waiting times for fingerprint-based identifications performed for second line checks;

- national system unavailability due to maintenance;

- care required in the capturing process because of the devices (cleaning of the surface, maintenance).

117 REGULATION (EC) No 81/2009 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 January 2009 amending Regulation (EC) No 562/2006 as regards the use of the ***Visa*** Information System (VIS) under the Schengen Borders Code.

118 The VIS Regulation allows for not capturing the fingerprints when it is factually not possible or when not legally required — e.g. for heads of state, royal families.

131

Out of the 19 Member States that contributed to the survey, 16 provided figures on the number of border crossing points equipped with fingerprint fixed stations or capturing devices.

For air border crossing points, the number amounts to 269. This figure is to be considered together with the 677 airports and aerodromes declared by Member States and documented in Annex 4 to the Schengen Handbook.119

In reality, the number of possible non-equipped air border crossing points might be compensated by organisational measures implemented by Member States. These measures consist for example in having mobile capturing devices or in conveying the travellers to another border crossing point hosting fingerprint stations. This can be the case for some aerodromes where travellers subject to fingerprint checks have to be conveyed to the nearest equipped border crossing points by the competent authorities. Although not specified in the survey, this practice is often cited by practitioners in Member States with a high number of small airports or aerodromes.

Due to the absence of information about the flow of passengers processed at equipped borders, one can only assume that the border crossing points facing the most substantial flows have been equipped as a priority.

Most of the Member States who provided the date from which the equipment is in use mentioned October 2014 or the subsequent months. Two Member States indicated October 2011, probably because of the existence of national programmes such as an entry-exit system.

Overall, 192 maritime border crossing points are equipped with a fixed station, with 77 for Norway in particular. The number of sea border crossing points is 842. Here also, the difference might be compensated by organisational measures consisting, as previously, in using mobile stations or conveying the travellers to the nearest border crossing point hosting fingerprint stations. Although not specified in the survey, this practice is cited by practitioners of Member States with a high number of sea ports.

The Frontex report on the use of the VIS at borders (‘Implementation and Operation of ***Visa*** Information System at National Level as of 2015’, section 3.1.1, February/March 2016) found that a majority of pedestrians (81 %) and cars (64 %) on ferries are checked with fixed readers.

The top three Member States in terms of maritime border crossing points (i.e. Denmark, Germany and Italy), have either not participated or not provided figures.

119 ‘Practical Handbook for Border Guards (Schengen Handbook)’ containing common guidelines, best practice and recommendations on border controls.

132

Most of the Member States who provided the date from which the equipment is in use mentioned October 2014 or the subsequent couple of months. Member State contributions, however, remain limited.

74 land border crossing points are equipped with fixed stations, with 18 for Greece, 4 for Slovakia, 7 for Estonia, 1 for Norway and 35 for Lithuania. The Member States presenting the highest number of land border crossing points (including on railways) are: Hungary (47), Slovenia (35, excluding crossing points for local border traffic), Poland (32), Greece (19), Finland (16), Lithuania (12) and France (10). The overall number of land border crossing points is 344 (including 85 on railways).

74 points are equipped with fixed stations. This provides coverage of 22 %, a figure that can be explained by factors such as:

• the presence of mobile stations;

• the very limited number of answers in this survey: the top three Member States in terms of number of land border crossing points did not provide figures.

The Frontex report on the use of the VIS at borders found that a majority of cars and lorries are checked with fixed readers installed in the booth.120

The number of air border crossing points declared as having a fingerprint mobile station or capturing devices is 53, which represents a small proportion (8 %) of all air borders (53 out of 677). The Frontex report found that mobile devices are used for private airplanes or military airports.

The top three Member States in terms of the number of air border crossing points did not participate or did not provide any figures. As five Member States provided positive replies and eight Member States provided a zero figure, the precision of the findings is questionable.

Out of the 27 reported air border crossing points equipped with fingerprint mobile readers for which the number of fingers checked was indicated:

• 18 are equipped with a 1-finger mobile reader (67 % of reported cases); and

• 9 (33 %) are equipped with two-finger readers.

The vast majority of Member States replying to the survey indicated that mobile stations or capturing devices in airports were ***available*** for the official date of the start of fingerprint-based checks, i.e. October 2014. Two Member States indicated that mobile solutions had been ***available*** since 2011. However, the response rate remains low so no general trend can be derived from these findings.

120 Section 3.1.1.

133

The number of sea border crossing points declared as having a mobile station or capturing devices (irrespective of the number of fingers checked), is 19, which represents a very small proportion (2.3 %) of all sea borders (19 out of 842 when excluding rivers). Without entering into detailed considerations about the volume of the traffic at declared crossing points, the figures show that mobile stations are used in limited cases. 9 % (1 out of 11) of declared maritime border crossing points are equipped with a 1-finger mobile reader; for the other border crossing points, the number of fingerprints checked is not specified.

No reply was provided by the top three Member States. To date, 4 Member States out of 20 with a maritime border have replied to the question. Although the contributions are insufficient to represent the overall community of Member States with a maritime border, the conclusion coincides with the Frontex report findings, namely that a minority of pedestrians (19 %) and cars (36 %) on ferries are checked using mobile readers.

One Member State replying to the survey indicated having mobile stations or capturing devices ***available*** in sea ports in time for the official date of the start of fingerprint-based checks, i.e. October 2014. One Member State indicated that a mobile solution had been ***available*** since 2011, while another Member State reported a date of June 2015.

Four Member States reported that land border crossing points are equipped with a mobile reader (one of these Member States uses 1-finger readers). The number of land border crossing points declared as having a mobile device is 13, which represents 72 % of those Member States' land border crossing points. Considering the number of Member States that declared having no mobile equipment, mobile stations are limited to 4 % of all land borders (13 out of 344 when excluding crossing points for local border traffic). One of the top three Member States in terms of the number of border crossing points responded that it has no mobile devices.

One Member State mentioned having mobile stations or capturing devices ***available*** at land border crossing points in time for the official date of the start of fingerprint-based checks, i.e. October 2014. One Member State indicated that a mobile solution has been ***available*** since 2011. The contributions are, however, insufficient to be considered as reflecting the overall reality.

For all types of border crossing points, Member States were not in a position to indicate the average number of attempts to collect fingerprints of sufficient quality in first line checks.

On the basis of information collected from the Member States participating in the survey, the usual border check procedure at the first line can be summarised as ***follows*** (the split is for readability purposes only).

134

Part 1:

- for land border checks that involve a car, the vehicle's registration documents are verified;

- the travel document is verified in order to establish whether it is valid;

- it is established by visual check that the person being checked is the same one as in the document;

- the machine readable zone (MRZ) of the travel document is scanned; otherwise the information is entered manually;

- the relevant European (SIS II), international (Interpol) and national databases are consulted.

Part 2:

- the ***visa*** MRZ is scanned;

- if there is a record in the VIS, fingerprints are collected only if the ***visa*** marking indicates the ***visa*** was issued in a region for which fingerprint-based checks have been rolled out.

Part 3:

- thorough check in accordance with Article 7 of the Schengen Borders Code;

- if entry conditions are met, including the availability of remaining days in the maximum duration of stay, the entry stamp is affixed. If not, the traveller goes through a second line check, ***following*** which entry can be refused.

It is frequently reported that, as per the procedure in Part 2, fingerprints are collected once there is evidence that the ***visa*** exists in the VIS and that fingerprints are attached to the application. This process in two ***steps*** is not precisely the one set out in the VIS Regulation, which requires the VIS to be consulted on the basis of the ***visa*** application and the fingerprints together.

The time processing ranges from 7 to 10 seconds from the submission of the verification request to the result delivery at border crossing points.

One Member State reported that during the processing of the consultation by national and central systems, border guards ask questions such as the purpose and duration of the journey, check the financial means, etc. Some Member States reported that a document drafted in the national tongue exists so as to describe the different ***steps*** to ***follow***.

Overall, 12 Member States replied to the question asking them to provide a brief description of the different ***steps followed*** in the border checking process at the first line, including the collection of fingerprints.

The ***visa*** marking significantly influences the border checking. Generally, the ***following*** approach is adopted:

135

- 'VIS' or 'VIS 0': verification of the ***visa*** in the VIS, based on the ***visa*** sticker number;

- 'VIS': verification of the ***visa*** in the VIS, based on the ***visa*** sticker number and the fingerprints;

- No marking: verification without fingerprints.

Unexpectedly, some Member States report that the VIS is only consulted when the ***visa*** marking is 'VIS'.

A two-***step*** approach was applied by some Member States until October 2014, when mandatory collection of up to four fingerprints commenced. The two-***step*** practice consists in:

1. consulting the VIS on the basis of the ***visa*** sticker number only;

2. if there are fingerprints in the VIS, possibly collecting fingerprints and proceeding with an electronic authentication.

There is no evidence that this practice has completely disappeared immediately since October 2014. The latest figures on border checks show a gradual replacement of verification based on the ***visa*** sticker number by verification based on the ***visa*** sticker number together with the fingerprints.

One Member State reported ***more*** values for the marking than just 'VIS' and 'VIS 0'. 'VIS 0' remains the most reliable means to decide whether fingerprints have to be collected. However, the survey shows that the ***visa*** marking is not entirely used as per the original meaning: 'VIS' does not mean that no fingerprints exist for the traveller, but that the ***visa*** was issued in a country where the collection of fingerprints was required. Similarly 'VIS 0' does not mean that there are no fingerprints but that fingerprints were not required for the country when the ***visa*** was issued. In practice, fingerprints are affixed to ***visas*** with a 'VIS' marking and Member States rarely collect fingerprints ahead of the official rollout date in countries where 'VIS 0' applies. One Member State noted that the marking VIS should unambiguously mean 'presence of fingerprints'.

The root causes of problems met during the border checking are documented as ***follows***.

11 Member States reported no or sporadic technical errors involving the scanning devices at first and second line checks. Some Member States reported that the number of issues decreased over time as end-users gained experience of the devices.

The details provided by four Member States for first line checks are as ***follows***:

- malfunction of the document & fingerprint scanner;

- long response time (6 seconds);

- device unable to scan correctly or multiple fingerprint scan.

For second line checks, one Member State mentioned long response times (sometimes without any result received) as a problem.

136

Judging from three Member State contributions, cases where multiple scans are needed to obtain sufficient fingerprint quality tend to occur occasionally at first line and even ***more*** rarely at second line.

Member States did not report other issues relating to the scanning device: few replies mentioned occasional problems at first line and rare problems at second line.

One Member State reported that some ***visa*** holders may require assistance during enrolment for first line checks.

Member States reported no issue on response times.

Four Member States reported that the absence of a match between the traveller's fingerprints and those in the VIS occurs rarely both at first and second lines. One Member State reported no such cases, while other Member States either did not respond or reported not having statistics on this topic.

Two Member States indicated that spoofing attempts occur rarely, while one Member State reported no such cases.

Four Member States reported that software or hardware issues occurred rarely.

One Member State reported issues with workstations during the initial launching of the system. However, for first and second lines, all computer workstations were replaced and contributed to increasing the overall efficiency.

Alternative solutions are used in the absence of applicable normal conditions i.e. when the fingerprints cannot be collected with a scanning device or when access to the VIS is not possible. Alternative solutions are reported as ***follows***.

When the fingerprints cannot be collected with a scanning device, Member States compare the traveller's document alphanumeric data and live face with the alphanumeric data and the facial image stored in the VIS.

When access to the VIS is impossible, the border guard ***follows*** the approach applied ***before*** the introduction of the VIS. Both the ***visa*** sticker and the travel document are checked to ensure they have not been counterfeited or falsified. A check of national, SIS II and Interpol databases is also carried out to verify that the document is not stolen, what the purpose of the journey is and whether there are any other prior records. However, this check is not reported as being carried out widely and systematically. In the event of suspicion of a false travel document, a second line check is performed. The border guard proceeds with a risk analysis and may contact the consular post that issued the ***visa*** to request the alphanumeric data and photo.

137

With the exception of three Member States that did not provide information, all Member States reported that the collection of fingerprints has not been automated in a border crossing system such as an ABC- or e-Gate.

Implications of technical progress in the use of fingerprints at external borders on the duration of searches

Summary

The evaluation found that the overall impact on the time taken to collect and verify fingerprints at air borders is on average 26 seconds, while for sea borders the figure is 44 seconds. For vehicles at land borders, the information provided was sparse. One Member State reported an impact of 15 seconds. For trains, two Member States provided contributions, resulting in an average of 42 seconds. The limited information provided meant that the impact on the queue length could not be determined. The evaluation found that no Member States reported searches entailing excessive waiting times at border crossing points. The average time taken for fingerprint authentication between sending data from the border crossing point and getting the result from the VIS is approximately six seconds.

Based on the input from eight Member States, the average time for fingerprint collection (including possible retries and other issues) is 23 seconds for air border crossing points. This correlates with the result of the Entry/Exit System (EES) pilot:121 ‘The added duration of the border-control process is directly linked to the number of fingerprints enrolled and the desired quality: enrolling four FPs (fingerprints) had the least impact on time and is considered to have a relatively limited impact on the border-crossing process, with the vast majority of cases being performed in under 30 seconds on average. At air borders, average durations ranged from 17 seconds for 4 FPs to 60 seconds for 10 FPs. [… 122]’.

On the basis of contributions from three Member States, the estimated average time for fingerprint collection was 30 seconds for sea borders. Four Member States replies supported an average of 26 seconds for land border crossing points (excluding trains). Three replies helped to approximate the average in trains to 30 seconds.

All border crossing points considered, the estimated maximum time to swiftly collect 90 % of ***visa*** holders’ fingerprints is 12 seconds, as calculated based on seven replies. One Member State mentioned that results were improving over time, citing the ***following*** five quarterly figures: 45, 30, 20 and finally 10 seconds by the last two quarters of 2015.

The average time for fingerprint authentication between sending data from the border crossing point and getting the result from the VIS is approximately 6 seconds. This figure is based on the contribution of nine Member States for figures on air and three for sea and land border crossing points.

121 Smart Borders Pilot Project — Report on the technical conclusions of the Pilot — Volume 1, doi: 10.2857/08, page 8.

122 ‘At sea, durations ranged from an average of 20 (4 FPs) to 46 seconds (10 FPs), and at land borders from 21 (4 FPs) to 49 seconds (10 FPs)’.

138

Based on the input from nine Member States, the maximum time taken to most swiftly authenticate 90 % of ***visa*** holders is 27 seconds. This average figure includes an outlier reply of 180 seconds.

All things considered, the overall impact on the time taken to collect and verify fingerprints at air borders is on average 26 seconds. This figure is based on seven contributions. One Member State indicated that it is quite difficult to provide a precise time, as it depends on whether the person knows the process of fingerprint checking or not. If the person already knows how the process works, it usually takes about 15 seconds to collect fingerprints correctly and the whole process takes no ***more*** than 30 seconds, system response time included. Another Member State reported by three-month periods figures of 60, 45, 32, and 30 seconds for the two last quarters of 2015.

The overall impact on the time taken to collect and verify fingerprints at sea borders is on average 44 seconds. This figure is based on two to three contributions depending on the type of border crossing point, which detracts from the level of confidence we can have in the figures.

The overall impact of the collection and verification of fingerprints on queues at airports cannot be reliably assessed on the basis of a single contribution. One Member State remarked that queue length does not depend only on the use of fingerprints, as there are other factors to consider and therefore no precise number can be provided. Only one contribution reported increasing lines at border crossing points for travel groups from China and Russia since the implementation of the VIS. No data were made ***available*** for sea borders.

For vehicles at land borders, one Member State reported an impact of 15 seconds. For trains, two Member States made contributions, resulting in an average of 42 seconds.

The average waiting time for a traveller's border crossing check is:

• one minute for air (five contributions);

• 55 seconds for sea (one contribution);

• 70 seconds for cars and trucks (one contribution);

• 35 seconds for trains (two contributions).

No relevant data were collected for buses.

140

Annex 5 – VIS evaluation questionnaire

Questionnaire I – Evaluation on the basis of Article 50(4) of Regulation 767/2008 (the VIS Regulation)

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

I. Results achieved against objectives

Art 2(a)

Facilitation of the ***visa*** application procedure

MS/***visa*** authorities

Quantitative

Qualitative

Rate on a scale of 1 to 5 1 – strong negative impact/significantly hampered the procedure, 2 – slightly negative impact/somewhat slowed the procedure with no significant improvement in quality, 3 - no impact, 4 - slightly positive impact/somewhat slowed the procedure but improved its quality, 5 – strong positive impact/significantly improved the quality of the procedure,) your view on how the introduction of the VIS facilitated the ***visa*** application procedure.

Give your views on whether the application of the VIS achieved the objective of simplifying and facilitating the ***visa*** procedure; provide brief examples, both positive and negative.

Art 2(b)

Preventing the bypassing of the criteria for the determination of the Member State responsible for examining the application

MS/***visa*** authorities Quantitative

Rate from a scale of 1 to 5 (1 – strong negative impact/helped bypassing the determination criteria, 2 – slightly negative impact/somewhat helped bypassing the determination criteria, 3 - no impact, 4 - slightly positive impact/somewhat improved preventing the bypassing of the determination criteria, 5 – strong positive impact/significantly prevented the bypassing of the determination criteria) your views on how the introduction of the VIS prevented the bypassing of the criteria for the determination of the Member State responsible for examining the application.

141

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

Qualitative

Give a general view/ briefly qualify in your own words the performance of the VIS for preventing the bypassing of the criteria for the determination of the Member State responsible for examining the application.

Art 2(c)

Facilitating the fight against fraud

MS/***visa*** authorities

Quantitative

Qualitative

Rate from a scale of 1 to 5 (1 – strong negative impact/facilitated fraud, 2 – slightly negative impact/somewhat facilitated fraud, 3 - no impact, 4 - slightly positive impact/somewhat facilitated the fight against fraud, 5 – strong positive impact/significantly facilitated the fight against fraud) your views on how the introduction of the VIS facilitated the fight against ***visa*** fraud.

Give a general view/ briefly qualify in your own words the performance of the VIS for facilitating the fight against fraud.

Art 2(d)

Facilitating checks at external border crossing points and within the territory of the Member States

MS/Border authorities, authorities responsible for conducting checks within the territory

Quantitative

Qualitative-

On a scale from 1 to 5 (1 – strong negative impact/worsened the situation as regards checks at SBCPs and within the territory, 2 – slightly negative impact/somewhat worsened the situation as regards checks at SBCPs and within the territory, 3 - no impact, 4 - slightly positive impact/somewhat facilitated the situation as regards checks at SBCPs and within the territory, 5 – strong positive impact/significantly facilitated the situation as regards checks at SBCPs and within the territory), rate how the introduction of the VIS facilitated the checks at external border crossing points and within the territory of the Member States.

Give a general view/ briefly qualify in your own words whether the application of the VIS achieved the objective of facilitating checks at the external border crossing points and within the territory of the Member States.

142

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

Art 2(e)

Assisting in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States

MS/immigration authorities

Quantitative

Qualitative

Rate from a scale of 1 to 5 (1 – strong negative impact/worsened the situation as regards the identification of persons, 2 – slightly negative impact/somewhat worsened the situation as regards as regards the identification of persons, 3 - no impact, 4 - slightly positive impact/somewhat improved the identification of persons, 5 – strong positive impact/significantly improved the identification of persons) your views on how the introduction of the VIS helped with the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States.

Give a general view/ briefly qualify in a short phrase the general performance and impact of VIS for facilitating checks at external border crossing points and within the territory of the Member States

Art 2(f)

Facilitating the application of Regulation (EC) No 343/2003 (as replaced by Regulation 604/2013, the "Dublin III Regulation")

MS/asylum authorities

Quantitative

Qualitative

Rate from a scale of 1 to 5 (1 – strong negative impact/worsened the application of the Dublin Regulation, 2 – slightly negative impact/somewhat worsened the application of the Dublin Regulation, 3 - no impact, 4 - slightly positive impact/somewhat improved the application of the Dublin Regulation, 5 – strong positive impact/significantly improved the application of the Dublin Regulation) your view on how the introduction of the VIS supported the application of the Dublin III Regulation.

Give a general view/ briefly qualify in your own words the performance/utility of VIS for determining the Member State responsible for examining an application for international protection.

Art 2(g) Contributing to the MS/law Quantitative Rate from a scale of 1 to 5 (1 – no impact on the prevention of threats to the

143

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

prevention of threats to the internal security of any of the Member States (on the basis of Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the ***Visa*** Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences)

enforcement authorities & Europol

Qualitative

internal security of the Member States, 5 – strong positive impact/significantly improved the prevention of threats to the internal security of any of the Member States) your view on how the introduction of the VIS contributed to the prevention of threats to the internal security of the Member State(s).

Please provide your views on whether the Decision supports the prevention, detection or investigation of terrorist or other serious criminal offences.

II. Assessment of the continuing validity of the underlying rationale

-

Assessment of the continuing validity of the VIS as an instrument for supporting the implementation of the common EU ***visa*** policy

MS/***visa*** authorities

Qualitative

Give your assessment in general terms of the continuing validity of the VIS as an instrument for supporting the implementation of the common EU ***visa*** policy

144

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

-

Assessment of the continuing validity of the VIS for performing biometric matching, primarily of fingerprints, for identification and verification purposes

MS/competent authorities123, including enforcement authorities, & Europol

Qualitative

Give your assessment in general terms of the continuing validity of the VIS for performing biometric matching, primarily of fingerprints, for identification and verification purposes

III. The application of the VIS Regulation

Entry and use of data by ***visa*** authorities

MS/***visa*** authorities

Qualitative

Art 8

Use of the procedures for entering data upon application

MS/***visa*** authorities

Give your general view on whether the procedures for entering data upon application are sufficient and effective for the purpose of further processing of the application.

Have you experienced any problems with the procedures for entering data upon application?

Is the existence of previous applications systematically checked? Are applications systematically linked to earlier applications, where applicable?

Has an application file been created for each applicant travelling in a group? Are these applications systematically linked?

123 In the meaning of Article 6(3) of the VIS Regulation.

145

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

Art 9-14

Use of the data to be entered

MS/***visa*** authorities

Have you experienced any problems when entering the data on application/***visa*** issuance/ discontinuation of an application/ refusal/ revocation/ extension, with regard to any category of data?

Provide, if possible in percentage, information on the non-applicable ("N/A") data entered in the VIS and the fields in respect of which this most often occurs.

In case not all information set out in Art. 9 is collected and entered in the VIS on a systematic basis, please explain why this is not done/what are the difficulties encountered preventing entering such data.

Please provide percentages of number of cases where the indication that fingerprints were previously collected was erroneously filled-in by the ***visa*** applicant, out of the total number of ***visa*** applications, as ***follows***:

• Percentage of cases in which the application mentioned that fingerprints have previously been collected but fingerprints were not found in the VIS (and fingerprints were to be collected anew);

• Percentage of cases in which the application mentioned that fingerprints have previously not been taken (and were collected) but fingerprints were present in the VIS.

Art 15

Use of the VIS for examining applications

MS/***visa*** authorities

Does the competent ***visa*** authority in your country systematically consult the VIS for the purposes of the examination of applications? If not, explain in which cases this is not done.

Have you experienced any problems when consulting the VIS for the purpose

146

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

of examining applications? If yes, please provide details on the nature of the problem.

Art 17

Use of the data for reporting and statistics

MS/ national controller

Does the competent ***visa*** authority in your country have access to consult all the data foreseen in Article 17 of Regulation 767/2008 for the purpose of reporting and statistics?

Has any access been given for other purposes than reporting or statistics? If yes, please provide details.

Access to data by other authorities

Art 18

Use of the data for verification at external border crossing points

− Level of implementation at external borders;

− Scale of verification at external borders.

MS/Border authorities Qualitative/quantitative

Do your authorities make use of the VIS for the identification of persons who may not, or may no longer, fulfil the conditions for entry to the territory of the Member States?

Which authorities are involved and have access to the VIS for the purpose of verification at external border crossing points?

Have you conducted any pilot projects on the VIS at the borders? (if 'yes', please describe the pilot(s) and the results). Has the obligation to verify the identity of the ***visa*** holder and the authenticity of the ***visa*** sticker at the border by searching the number of the ***visa*** sticker in combination with the fingerprints been implemented in your country? If yes, please mention the date as of which this verification has been carried out and whether the verification was systematically done as of October 2014 in combination with the fingerprints for all third country nationals whose data are in the VIS. In case the verification with fingerprints was not done systematically, please

147

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

provide details on which criteria the verification was performed (e.g. ***visa*** sticker number only, nationality of the person, reason for the verification etc).

What is the monthly percentage of ***visa*** holders recorded in the VIS and crossing an external border, who are checked at the border crossing points against the VIS?

Please provide the percentage of checks based on fingerprints out of the total number of checks on ***visa*** holders against the VIS at external borders, on a monthly basis.

Please provide figures on the number of cases where this verification led to doubts as to the identity of the ***visa*** holder or of the authenticity of the ***visa*** or travel document of the ***visa*** holders (thus requiring second line checks), as well as the percentage from the total number of verifications that it represents.)

Please provide on a monthly basis the number of refusals of entry based on information provided by the VIS (since the introduction of the use of the VIS for verification purposes) for counterfeit ***visa***.

Have you experienced any difficulty in carrying out the obligation to verify the identity of the ***visa*** holders at external border crossing points?

What is the quarterly percentage of cases where the data stored could not be used for the verification at external border crossing points, because of insufficient quality of the data?

In case of unsatisfactory data quality, which procedure is ***followed*** by the border guards (for example contact with the issuing MS or the consular post of

148

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

the issuing MS)? How long such a procedure can take? Would you suggest for another option to resolve those cases of insufficient data quality at borders?

Please provide the overall percentage of cases, on a monthly basis, in which the competent authorities accessed the data in accordance with Article 20(1) and (2) i.e. through a second line check – this figure can be calculated by dividing the number of second line checks by the number of first line checks over a period of several months.

As per article 7 of Regulation (EC) 562/2006 (Schengen Borders Code), derogation from the obligation of verification of the identity of the holder of the ***visa*** and of the authenticity of the ***visa*** by consulting the VIS can occur. Please provide quarterly the number of such occurrences and their average duration, for each of the ***following*** areas:

o intense traffic inducing excessive waiting time

o all resources exhausted (staff, facilities and organisation)

Please also mention how the border checks were making use of the VIS in those circumstances.

Please provide the number (and the applicable period) of cases where the ***visa*** holder opposed to provide the fingerprints and the percentage of such cases out of the total number of checks

Please provide the number (and the applicable period) of cases where it was

149

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

physically impossible to collect the ***visa*** holder fingerprints and the percentage of such cases out of the total number of checks

As per your experience, to which extent does the absence of fingerprints in the VIS (for legal or factual reasons) constitute an issue or a risk for the border crossing for a given traveller?

Art 19

Use of the data for verification within the territory

MS/migration authorities

Qualitative/quantitative

Do your authorities make use of the VIS for the identification of persons who may not, or may no longer, fulfil the conditions for stay or residence on the territory of the Member States?

Which authorities are involved and have access to the VIS?

Please mention the date as of which this verification has been carried out and whether the verification was systematically done in combination with the fingerprints, or only in respect of certain third country nationals.

In how many cases the VIS was used for the purpose mentioned above?

In how many cases an irregular staying person could be identified?

Have your authorities competent for carrying out checks within the territory experienced any difficulty in carrying out the obligation to verify the identity of the ***visa*** holders?

Art 20

Use of the data for identification

MS/migration authorities Qualitative/quantitative

Please provide percentages of cases out of the total number of checks in which the VIS helped to ascertain that the person had a ***visa*** no longer valid.

Please provide the percentage of cases out of the total number of searches in which the search with fingerprints could not be done. In such circumstances,

150

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

provide information on what the categories of data used to identify the person were.

Have you experienced any difficulty in carrying out the obligation to verify the identity of the ***visa*** holders at external border crossing points?

Art 21

Use of the data for determining the responsibility for asylum applications

MS/asylum authorities

Qualitative/quantitative

• Have your competent asylum authorities had access, and as of when, to search the VIS with the fingerprints of an applicant for international protection in order to determine the Member State responsible for examining his or her application? Do you have one or ***more*** competent authorities designated for that purpose? Do all officials within

this(ese) authority(ies) have access to VIS or only certain categories (e.g. all case officers, only specialised case officers)?

• Could you provide us with statistical information on the number of cases and/or their percentage out of the total number of applications for international protection, on a quarterly basis, in respect of whom checks with the VIS in view of determining the Member State responsible have been performed? What is the percentage of cases in which fingerprints of applicants for international protection cannot be used and where the search with the fingerprints failed, out of the total number of attempted VIS searches in view of determining the Member State responsible?

• Please describe succinctly the action taken in cases in which the search with the fingerprints or other data referred to in Article 21(1) indicates the presence in the VIS of a ***visa*** issued or extended with an expiry of ***more*** than six months.

151

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

• What is the percentage of cases in which a Member State was designated as responsible based on a search in VIS out of the total number of applicants for international protection and out of the total number of VIS searches in view of determining the Member State responsible? What was the most frequent reason for refusal of such a request based on a VIS hit? (Please provide both examples of where your MS has refused requests and where it has been refused by other MS and the reason of refusal).

• Provide some examples of the most relevant situations where the use of the VIS significantly contributed to solving/clarifying cases of responsibility for the examination of applications for international protection.

Art 22

Use of the data for examining the application for asylum

MS/asylum authorities

Qualitative/quantitative reporting

• Have your competent asylum authorities had access, and as of when, to search the VIS with the fingerprints of an applicant for international protection in order to examine his or her application? Do you have one or ***more*** competent authorities designated for that purpose? Do all officials within this(ese) authority(ies) have access to VIS or only certain categories (e.g. all case officers, only specialised case officers)?

• Could you provide us with statistical information on the number of cases and their percentage out of the total number of applications for international protection, in respect of whom checks with the VIS in view of examining such applications have been performed? What is the percentage of cases where fingerprints of applicants for international protection cannot be used and where the search with the fingerprints failed out of the total number of attempted VIS searches in view of

152

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

examining applications for international protection?

• How would you assess the utility of the VIS data in examining an application for international protection? In what way are checks in the VIS data used by the competent asylum authorities in order to assess the substance of such application? For instance, are the results of a check in the VIS used in the framework of the credibility assessment? Please explain, if relevant with specific examples.

Retention and amendment of the data

Art 23-25

Retention period, amendment and deletion of data

MS/national authorities/controller

Qualitative/quantitative

Please provide information on the period of retention of the data and on the situations where the data was not automatically deleted at the end of the retention period (if any).

Please provide information on the situations where Member States carried out corrections or deletions of data (including the total number during the reporting period).

Please provide the total number during the reporting period of the situations where Member States proceeded to advance data deletion due to an applicant acquiring the nationality of a Member State.

Please provide the total number during the reporting period of the situations where Member States proceeded to advance data deletion due to a refusal decision being overturned by a court or appeal body

VIS operation and responsibilities

153

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

Art 48

State of play of the VIS roll-out

MS authorities

Qualitative/quantitative

Had you started using the VIS ahead of the general rollout in any region (including at Schengen Borders)?

If yes, please let us know in which regions you rolled out the VIS ahead of the general schedule, whether with or without fingerprints, and your experience with that, both at technical level and as concerns the practical/political implications, if any.

When did you start VIS ***visa*** issuance at the border (dd.mm.yyyy)?

Briefly describe, if/where appropriate, any practical problems you encountered with the VIS after its rollout in a given region, the specificities of that situation and the way it was solved and the lessons learnt at national level and in relation with the other Member States, eu-LISA and the Commission.

Art 28

Relation of the VIS with the national systems

MS/VIS national authority124

Qualitative/quantitative Please provide a brief description of the institutional organisation, management, operation and maintenance of your national VIS;

Please provide a brief description of the management and arrangements for access of the duly authorised staff of the competent national authorities to the VIS.

Have you experienced incidents resulting in too long response times or downtime (unavailability of the national copy or the system) for the end users? If so, provide figures on how many there were, their origin (central or

124 In the meaning of Article 28(2) of the VIS Regulation.

154

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

national system), how long did they last, and how did the end users cope until the issues were resolved.

How are these incidents handled by the N.VIS Office? Describe the set of procedures in place to inform end users and other stakeholders of the incident, as well as provide progress reporting until resolution (if needed).

Please provide a brief overview of the financial costs incurred by the set up and running of the national VIS to date, including the investment and operational costs of the communication infrastructure between the national interface and the national system.

Do you have an emergency plan in place relating to situations where it is impossible for users to search SIS II due to a problem with a national system or network inaccessibility? If so, provide briefly some details on its type.

Please provide a brief (quantitative) overview of the training activities for the staff authorised to process data stored in the VIS and of the staff of the authorities having a right to access the VIS. Emphasize in particular whether/how much of the training concerns security issues and data protection.

Art 29, 30

Responsibility for the use of data and keeping in national files

MS/VIS national authority/controller

Qualitative/quantitative

In which circumstances and how frequent data retrieved from the VIS have been kept in national files? How long in average is the data kept?

Please provide information on any incident related to the non-respect of the provisions related to keeping data in national files in Article 30(1) of the VIS Regulation.

155

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

Art 33(2)&(3)

MSs liability towards the VIS

MS/competent authorities

Qualitative/quantitative

What have been cases of failing to comply with your obligations and that caused damages to the VIS?

Have you claimed for compensation against another MS failure to comply with its obligations and that caused damages to the VIS?

Art 34

Keeping of records

MS/national authorities/controller

Qualitative/quantitative

Which information is recorded by MS when a data processing operation is carried out within the VIS (logging)?

For which purpose are these records used?

What are the mechanisms in place to delete these records and according to which rule?

Which reasons prevented the deletion of these records?

How frequent is the data processing in the absence of recording?

Please provide information on any incident of unauthorised access to data and how the situation was solved.

Art 35, 36

Self-monitoring and penalties

MS/competent authorities, National Supervisory Authorities

Please provide brief information on the main findings of the self-monitoring performed by your authorities since operating the VIS and of the penalties incurred (if any).

Data protection issues

Art 37

Right of information

MS/ National

Qualitative/Please provide a brief description of the form and way in which the obligation of informing the data subjects pursuant to Article 37(1) has been complied

156

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

controller

quantitative

with.

Art 38

Access, correction and deletion of data

MS/***visa*** authorities

National Supervisory Authorities

Qualitative/quantitative

Please provide the total number of requests to access VIS data by data subjects during the reporting period, as well as the number of times these requests were groundless.

Please provide total number of the correction requests made during the reporting period and data on the ***follow*** up given to them. Please mention the total number of cases during the reporting period when the request involved information for which another MS was responsible and whether the 1 month delay in processing the request was respected in all cases.

Please provide the total number of complaints related to the personal data recorded in the VIS received during the reporting period.

Please provide brief information (quantitative and qualitative) on the situations in which the refusal to correct or delete data led to actions or complaints ***before*** the national competent authorities or courts.

National Supervisory Authority: Please provide information on the total number of complaints related to the personal data recorded in the VIS received during the reporting period.

Art 39&40

MSs cooperation on data protection and Remedies on data protection

MS/National Supervisory Authorities

Qualitative/quantitative

Please provide a brief general description of the cooperation with other Member States on data protection.

To National Supervisory Authority: Please provide statistics, if ***available***, on the number of persons assisted in exercising their right to correct or delete data, and provide information on the type of assistance offered to persons in

157

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

exercising their right to correct or delete data.

Art 33(1)

Liability towards persons

MS/competent authorities

National Supervisory Authorities

Qualitative/quantitative

Please provide information on the number of cases where a person has suffered damage as a result of a processing operation incompatible with the VIS Regulation as well as a brief description of the ***follow*** up given to these cases.

To National Supervisory Authority: Please provide information on the total number of cases where a person has made a complaint claiming a damage suffered as a result of a processing operation incompatible with the VIS Regulation, as well as a brief description of the ***follow*** up given to these cases.

Art 41

Supervision by the National Supervisory Authority and EDPS

National Supervisory Authority

Qualitative/quantitative

Provide a brief general description of the findings of the supervision exercised by the NSA since the entry into operation of the VIS.

IV. The security of the VIS

Art 32

Data security taking into account Commission Decision 2010/260/EU of 4 May 2010 on the Security Plan for the operation of the ***Visa*** Information System

MS authorities

Qualitative/quantitative

What measures have been enforced to ensure the security of the data ***before*** and during the transmission to the national interface as well as when receiving data from the national interface?

How these measures are documented?

What are the controlling procedures and their frequency?

Explain in which extend a Security Plan exists and how it does ensure the coverage of the provisions set out in §2 of Art. 32 of the VIS Reg.

V. The use made of the provisions

158

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

referred to in Article 31 and implications for future operations

Art 31

Communication of data to third countries or international organisations

MS/competent authorities

Qualitative/quantitative

Do you communicate VIS data to third countries or international organisations for the purpose of return?

Which authorities are involved?

In how many cases did you communicate VIS data to third countries or international organisations for the purpose of return? Please provide information regarding the main purpose for which the data were provided and the country/organisation to which it was transferred or made ***available***.

In how many cases a person could be successfully returned or at least achieved a travel document by using these data?

159

Questionnaire II - Evaluation on the basis of Article 50(5) of Regulation 767/2008 (the VIS Regulation)

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

I. Technical progress made regarding the use of fingerprints at external borders

Art 18

Technical readiness of VIS use at the external border crossing points

MS/border authorities

Qualitative/quantitative

When did you start performing VIS checks at the borders on the basis of fingerprints and on a systematic basis at least for ***visa*** holders present in the VIS (dd.mm.yyyy)?

Have you experienced any technical problems or administrative impediment in checking fingerprints at external borders? If so, please provide briefly some details on the type and scope of the problems, solutions identified, and any suggestions to improve the situation in the future.

Number of border crossing points equipped with fingerprint fix-station/capturing device and the date (month of 2015) as of which the equipment is in use:

• Air

• Sea

• Land border

o cars

o trucks

o buses

160

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

o trains

Number of border crossing points equipped with fingerprint mobile-station/capturing device (please indicate for each of: 1-, 2-, 4-finger) and the date (month of 2015) as of which the equipment is in use:

• Air (indicate for each of: 1-, 2-, 4-finger)

• Sea

• Land border

o cars

o trucks

o buses

o trains

Use of fingerprints:

− Introduction to fingerprinting and fingerprint technology;

− Description of processing fingerprints in the VIS.

Please provide on a quarterly basis the average number of attempts to collect fingerprints of sufficient quality in first line. Distinction can be made depending on the type of border crossing point - air, sea, land border (vehicles excluding trains, trains).

Please provide a brief description of the different ***steps*** ***followed*** in the border checking process, at the first line including the collection of fingerprints.

Please describe to which extent the ***Visa*** marking ("VIS", "VIS 0", no marking) plays a role in the border checking process with fingerprints.

Please list the root causes of problems met and their frequency (rare, occasionally, frequent) on a quarterly basis during the border checking

161

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

process (please choose among technical errors with the scanning devices; multiple scans for a sufficient fingerprint quality; other issues relating to the scanning device [can be specified]; response times; no fingerprint match; spoofing attempts; other software/hardware issue [can be specified]; other issues [can be specified]):

• At first line control

• At second line control

Please describe any degraded solution in place and used in the absence of applicable normal conditions i.e. when the fingerprints cannot be collected with a scanning device, when the access to the VIS is not possible, etc.

Has the collection of fingerprints been automated in a border crossing system such as an ABC- or e-Gate? What has been the impact of this integration in the border crossing process?

II. The implications of the technical progress in the use of fingerprints at external borders for the duration of searches

Art 18 (1)&(2) Implications for the duration of searches

MS/border authorities

Qualitative

Questions to MS:

Please provide on a quarterly basis the average time in seconds for the fingerprint collection (including possible retries and other issues) per type of border crossing point – please mention for each 1-, 2-, 4-fingers):

• Air

162

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

• Sea

• Land border

o cars

o trucks

o buses

o trains

Please provide on a quarterly basis the maximum time (in seconds) to collect the most swiftly 90% of fingerprints of the ***visa*** holders? (For example, 90% of all ***visa*** holders are scanned within less than 10 seconds.)

What is the average time in seconds for the fingerprint authentication (time between sending data from the border crossing point and getting the result from the VIS) per type of border crossing point – please mention for each 1-, 2-, 4-fingers):

• Air

• Sea

• Land border

o cars

o trucks

o buses

o trains

What is the maximum time (in seconds) to retrieve the most swiftly 90% of ***visa*** holders? (For example, 90% of all ***visa*** holders are authenticated within less than 6 seconds.)

All parameters being considered, please provide on a quarterly basis the overall implication for the duration in seconds of the collection and

163

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

verification of fingerprints? (For example, from 11 October 2014, the use of fingerprints at borders induces an overhead of 20 sec.)

Please specify per type of border crossing point:

• Air

• Sea

• Land border

o cars

o trucks

o buses

o trains

All parameters being considered, please provide on a quarterly basis the overall impact of the collection and verification of fingerprints on the queues? (For example, from 11 October 2014, the use of fingerprints at borders induces an increase of 5% of the queue length.)

Please specify per type of border crossing point:

• Air

• Sea

• Land border (in the absence of separate lanes the first 3 bullet points can be merged):

o cars

o trucks

o buses

o trains

Please provide on a quarterly basis the average waiting time in seconds for a traveller's border crossing check? Please specify per type of border crossing point:

164

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

• Air

• Sea

• Land border

o cars

o trucks

o buses

o trains

165

Questionnaire III - Evaluation on the basis of Article 57(3) & (4) of Regulation 810/2009 (the ***Visa*** Code)

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

Implementation of VIS related provisions of the ***Visa*** Code

I. Implementation of the collection and use of biometric identifiers

Art 13 VC

Implementation of the obligation to collect biometric identifiers of the applicant

MS/***visa*** authorities

Qualitative

Have you experienced any difficulties, of technical or administrative nature, in implementing the obligation to collect biometric identifiers of the applicant?

Art 13(2), (4) VC

Implementation of the technical requirements regarding the collection of biometric identifiers, including on the use of appropriate standards

MS/***visa*** authorities

Qualitative and quantitative

Do you take the photograph through scanning or direct collection?

Have you experienced situations in which the collection of biometric identifiers could not be carried out according to ICAO technical requirements?

Have you encountered any problems (and which) in the implementation of the technical requirements regarding the collection of biometric identifiers?

Are the difficulties met when collecting electronically 10 flat fingerprints of good quality or during the entry of such data in the VIS by ***visa*** authorities?

What are the difficulties met when collecting electronically a photograph or during the entry of such data in the VIS by ***visa*** authorities?

166

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

Where appropriate, please suggest alternative standards in the collection or transmission of the facial image and/or the fingerprint set, to address these difficulties

II. Suitability of the ICAO standard chosen

Art 13(4), (5) VC

Suitability of the ICAO standard chosen

MS/***visa*** authorities

Qualitative

Are the current ICAO standards relating to the facial image the most suitable in the context of the ***visa*** related activities?

Are the current ICAO standards relating to the fingerprints the most suitable in the context of the ***visa*** related activities?

Have you experienced any difficulties in implementing the technical specifications on the standards of the biometric features as presented in the Commission Decision 648/2006?

III. Experience with external service providers with specific reference to the collection of biometric data

Art 40(3) VC

Information on the level of use of external service providers by the MSs and the reason for this use

MS/***visa*** authorities

Qualitative

Briefly explain your experience with external service providers in respect of the collection of biometric data. Highlight cases where specific problems were encountered, as well as the way they were dealt with.

167

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

IV. Implementation of the 59-month rule for the copying of fingerprints

Art 13(3) second paragraph

Information regarding cases where fingerprints were collected within the period of 59 months due to doubts regarding the identity of the applicant

MS/***visa*** authorities

Quantitative

Where possible, provide figures on the number of cases where fingerprints were collected for a second (or ***more***) time(s) within 59 months from the previous collection, as well as the reason why a new collection was needed.

V. Cases in which fingerprints could factually not be provided or were not required to be provided for legal reasons, compared with the number of cases in which fingerprints were taken

Art 13(7)(b) VC

Art 17(12) VIS

Information/statistical data on cases in which fingerprints could factually not be provided

MS/***visa*** authorities

Quantitative

Please provide statistics of the number of cases in which the applicants were exempted from fingerprinting due to fingerprinting being physically impossible ["N/A"], as well as the percentages this figure represents out of the total number of ***visa*** applications and of the total number of fingerprinting exemptions (on a quarterly basis throughout the reporting period).

Art 13(7)

Information/statistical data

MS/***visa***

Quantitative

Please provide the number of cases annually in which the applicant was

168

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

(a),(c),(d) VC,

Art 17(13) VIS

on cases in which fingerprints were not required for legal reasons

authorities

exempted from fingerprinting due to their age (<12 years), as well as the percentage this figure represents from the total of ***visa*** applications and of the total of fingerprinting exemptions, respectively (on a quarterly basis throughout the reporting period).

Please provide statistics on the number of cases in which the applicant was exempted from fingerprinting due to their status as heads of State or Government, members of a national government, accompanying spouses or members of official delegation, as well as the percentage that represents from the total of ***visa*** applications and of the total of fingerprinting exemptions, respectively (on a quarterly basis throughout the reporting period).

Please provide statistics on the number of cases in which the applicant was not exempted from fingerprinting despite their status as heads of State or Government, members of national governments, accompanying spouses or members of official delegation, as well as the reasons for the non-exemptions.

Please provide a quantitative comparison between the number of cases in which fingerprints could factually not be provided or were legally not required, and the number of cases in which fingerprints were taken.

Please provide per MS the number of cases in which fingerprints were not required to be provided for legal reasons ["N/R"] and the percentage they represent from the total number of applications introduced in the VIS, the proportion they represent from the number of cases in which fingerprints were taken, reported on a quarterly basis:

169

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

VI. Cases of ***visa*** refusal where a person who could factually not provide fingerprints

Art 17(14) VIS

Information/data on cases in which a person who could factually not provide fingerprints was refused a ***visa***

MS/***visa*** authorities

Quantitative

Qualitative

Please provide statistics on the number of cases in which a person who could factually not provide fingerprints was refused a ***visa***, as well as the main reasons for refusing the ***visa*** in such cases.

VII. Compliance with data protection rules

MS/all authorities involved in processing personal data for VIS related purposes

How is access to VIS data supervised in consulates, central ***visa*** authorities, external border crossing points?

Please describe the IT infrastructure (hardware) in place in consulates and data flows in the national ***VISA*** system.

What technical and organisational security measures are in place to protect personal data recorded in the VIS?

How do you ensure the right to obtain communication of personal data recorded in the VIS (Article 38(1) of the VIS Regulation (767/2008/EC)? How are data subjects informed about their rights concerning data protection (i.e. exclusively through the application form or through other supplementary means, e.g. flyer, internet, ESPs etc.)?

How do you process requests to correct inaccurate personal data or to delete unlawfully recorded personal data (Article 38(2)-(6) of the VIS Regulation)? How

170

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

many cases have you had?

What kind of remedies are ***available*** (Article 40 of the VIS Regulation)?

How do you cooperate with other Member States to ensure individuals' right of access, correction and deletion of VIS data (Article 39 of the VIS Regulation)? Is this specific international cooperation regulated in national law?

How does the national supervisory authority monitor the lawfulness of the processing of personal data stored in the VIS (Article 41(1) of the VIS Regulation)?

Has the audit of the VIS data processing operations (required every four years) been carried out (Article 41(2) of the VIS Regulation)? If yes, what were the results? If not, when will such an audit take place?

On average, how long does it take the national supervisory authority to handle a case (complaint) related to the processing of data in the national systems?

Please provide statistics on the number of complaints and the outcome of the proceedings.

What procedures are in place to ensure the implementation of the decision taken by the authorized body of another Schengen state taken in accordance with Article 111 of the CISA? Have court decisions of another state been executed and if not, why?

How do you ensure that only authorised users' access VIS and that such an

171

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

access complies with legally authorised purposes?

What technical and organisational security measures are in place to protect VIS data?

VIII. Organisation of the procedures relating to applications

Art 17 & 43 VC

The service fee levied by external service providers, including compliance with the proportionality principle

MS/***visa*** authorities

Quantitative

Provide information on whether cooperation with external service provider(s) is based on a general framework contract, or whether contracts for individual locations and/or third countries are concluded. In the former case, provide information on the procedures for the conclusion of 'local' contracts.

Provide information per location on the service fee(s) charged by the external service providers referred to in Article 43 of the ***Visa*** Code.

Provide information on the situations, if any, in which the service fee charged by the external service provider you are employing is not harmonized with that of the service providers used by other Member States in a given location, as well as on the reasons for the lack of harmonization.

Has the fee limitation provided by Art. 17(4) of the ***Visa*** Code given rise to any problems? If yes, please specify the location(s) and provide any relevant additional information (relevant statistics, failure of contracting, agreement as part of a global package, etc.).

Provide information on the training your provided to the external service providers you have been employing.

172

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

Provide information concerning the monitoring of the external service providers in respect of the implementation of the ***following*** aspects:

a) the general information on ***visa*** requirements and application forms provided by the external service provider to applicants;

b) all the technical and organisational security measures required to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the cooperation involves the transmission of files and data to the consulate of the Member State(s) concerned, and all other unlawful forms of processing personal data;

c) the collection and transmission of biometric identifiers;

d) the measures taken to ensure compliance with data protection provisions.

e) the methods used to monitor the external service provider (test applicants, spot checks, unannounced visits, etc.) and the frequency of monitoring.

Have you experienced situations of solvency, reliability, conflicts of interests etc. with the external service providers, after entrusting them with a contract? If so, please provide a brief summary of the measures taken to correct the situation.

How do you assess the overall satisfaction of ***visa*** applicants with your ESPs? Is it ensured that complaints received by the ESPs reach the consulate/MFA? How often do your consulates receive complaints and what are the frequent concerns of the applicants?

173

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

In particular, have you received any complaint regarding data protection or uncovered any data protection irregularity in the activity of an external service provider? Has any action been taken under the national law of the host state in respect of an alleged breach of data protection obligations by an external service provider? In any of these cases, please provide details of the situation occurring as well as the measures undertaken to deal with the situation.

Have you ever terminated or suspended cooperation with an ESP? If yes, provide a brief description of the situation in particular whether you have been able to ensure the continuity of the service in accordance with Art. 43(12) of the ***Visa*** Code.

Art 40, 41, 42, VC

Cooperation on procedures related to applications

MS/***visa*** authorities

Qualitative/quantitative

Provide a brief summary of your experience as regards cooperation with other Member States on procedures related to applications and underline the lessons learnt as well as any suggestions to improve these forms of cooperation, if any.

Art 40(2)(a)

Information by MSs on the level of equipment in the consulates, offices of honorary consuls, and authorities responsible for issuing ***visas*** at the borders with the required material for the collection of biometric identifiers

MS/***visa*** authorities

Quantitative

If applicable, provide information on the consulates and authorities responsible for issuing ***visas*** at the borders which have not yet/not properly been equipped with the required material for the collection of biometric identifiers,

or where the equipment needs to be replaced, the reasons for this (whether financial or of other nature) as well as information on the timeframe for addressing any shortcomings.

174

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

Art 44 VC

Encryption and secure transfer of data

MS/***visa*** authorities

Qualitative/quantitative

Do you cooperate with ESPs/other MSs in third countries where electronic data transfer of encrypted data is not possible or is not possible without specific measures (potentially) damaging the transfer confidentiality?

Where required to transfer data from the ESP to the consulate physically, how long does that take on average?

Have you encountered situations which required the conclusion of agreements with the third countries with the aim of lifting the prohibition against encryption of data to be electronically transferred from authorities of the representing MS to the authorities of the represented MS(s) or from the external service provider of from the honorary consul to the authorities of the MS concerned?

175

Questionnaire IV - Evaluation on the basis of Article 17(4) of Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the ***Visa*** Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences).

Relevant law provision

Topics to be covered

Authority in charge with providing the data

Type of information requested

Specific questions

I. Results achieved against objectives

Capacity to support prevention, detection or investigation of terrorist or other serious criminal offences

MS/law enforcement authorities

Qualitative assessment

Please provide your view on whether the Decision supports the prevention, detection or investigation of terrorist or other serious criminal offences.

II. Assessment of the continuing validity of the underlying rationale

-

Assessment of the continuing validity of the VIS as an instrument for supporting the prevention, detection and investigation of terrorist offences and of other serious criminal

HOME/D3

Qualitative assessment

Please provide your view to what extent the Decision is – and remains - an effective and useful instrument for supporting the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

176

offences

III. The application of the VIS Decision

Access to data by designated authorities

Art 3, 4

Procedures for access to the VIS by designated authorities

MS/law enforcement authorities/designated authorities125

Quantitative/ qualitative

Qualitative:

Has your country designated authorities to access VIS data? If not, why not? If so, has your country established a list of such authorities? Has this list been notified to the Commission and the General Secretariat of the Council? If not, why not? In case this list has been amended or replaced, has this been notified? If not, why not?

Has your country designated central access points? If so, has your country notified these access points to the Commission and the General Secretariat of the Council? If not, why not?

Is the Decision clear as regards the authorities and central access points that may be designated to access VIS data?

Are the designated central access points easily accessible for law enforcement authorities?

Are law enforcement authorities fully aware of the possibility of getting access to the VIS and the possible effects that this may have on supporting the prevention, detection or investigation of terrorist offences and of other serious criminal

125 'designated authorities' as per Art 2(1)(e) of Decision 633/2008 (authorities responsible for the prevention, detection, investigation of terrorist offences or of other serious criminal offences.

177

offences?

To what extent does the procedure for access to the VIS corresponds with the needs of the designated authority/authorities?

Please give an example of a reasoned written or electronic request to access the VIS as referred to in Article 4 (1).

If applicable, please give an example of an 'exceptional case of urgency' as mentioned in Article 4 (2. Please describe the handling of the 'fast track procedure' as mentioned in Article 4 (2), including the ex-post verification.

Quantitative:

Please provide statistics on requests to access to the VIS. Please provide such statistics on a quarterly basis. How many written requests to access the VIS have been submitted? How many electronic requests to access the VIS have been submitted? How many oral requests have been handled under the urgency procedure?

How many requests have been submitted that were 'exceptional and urgent' as referred to in Article 4 (2)?

How many requests handled by the fast track procedure as referred to in Article 4 (2) appeared not to be 'exceptional and urgent' after verification? Please give an example, if any..

Art 5

Conditions for access by designated authorities

MS/law enforcement authorities

Quantitative/ qualitative

Please elaborate on how the specific conditions as mentioned in Article 5 (a)(b)(c) are applied. Please give an example.

What methods are in place to ensure the correct application of the conditions as referred to in Article 5?

Have there been requests to access to the VIS that did not meet the conditions

178

for access as referred to in Article 5? If so, how many?

Art 6

Conditions for access by designated authorities of MSs not participating in the VIS

MS/law enforcement authorities

Quantitative/ qualitative

Have any requests (accepted or declined) been made for access to the VIS for consultation by designated authorities in respect of which Regulation (EC) No 767/2008 was not yet put into effect?

Art 7

Access to the VIS by Europol

MS/VIS access points

Quantitative/ qualitative

Please provide statistics on all accepted and declined requests for access to the VIS by Europol. Please provide such statistics on a quarterly basis.

Has Europol designated a specialised unit for the purpose of the Decision to act as the central access point to access the VIS for consultation?

IV. Data protection

Art 8

Protection of personal data in the process of access by the designated authorities under the VIS Decision

MS/national data protection authorities/Europol Joint Supervisory Body

Quantitative/ qualitative

Has personal data been transferred or made ***available*** to a third country or an international organisation? If so, to which countries and to which international organisations?

What type of information was transferred or exchanged? What type of information was most often transferred of exchanged?

Please give an example of an 'exceptional case of urgency' as referred to in Article 8 (4), if any.

Please describe the training curriculum on data security and data protection for the staff of the authorities that have a right to access the VIS. Please indicate how much staff has been trained.

Has the national data protection authority undertaken any audits to verify the data processing under Article 8?

If so, can the authority provide information about possible findings, statistics and recommendations ***following*** such audits?

179

Can the authority also provide information about complaints lodged against the processing of personal data and provide any statistics in this respect?

Has the Joint Supervisory Body (JSB), overseeing data processing by Europol, undertaken any audits to verify the data processing under Article 8(2)?

If so, can the JSB provide information about possible findings, statistics and recommendations ***following*** such audits?

Can the JSB also provide information about complaints lodged against the processing of personal data by Europol and provide any statistics in this respect?

Art 13

Keeping of VIS data in national files

MS/designated authorities

Quantitative/ qualitative

Have there been cases in which data retrieved from the VIS was kept in national files? If so, please give an example of a case and provide information on how long the data was kept. How long, on average, was data kept in national files?

What security measures are in place with regard to the retrieved data? What methods are used for data storage?

Art 14

Access, correction and deletion of data related to them by persons

MS/designated authorities

Quantitative/ qualitative

Please provide statistics on complaints or appeals lodged against decisions to refuse the right of access. Please provide such statistics on a quarterly basis. Please give an example, if any.

Please describe how individuals requesting access to data relating to them are being informed as referred to in Article 14 (6).

What are the main reasons for not communicating data to the data subject? Please give an example of a case in which data was not communicated to the data subject.

Please describe the procedure / decision which is applied in case of a refusal of access.

Art 16

Keeping of records on

MS/designated

Quantitative

Please provide statistics on data processing operations resulting from access to

180

the processing operations resulting from accessing VIS data

authorities

/ qualitative

the VIS. Please provide such statistics on a quarterly basis.

Please describe how data processing operations resulting from access to the VIS are recorded.

Please describe what security measures are in place with regard to the records.

Art 10(1)

MSs' liability in case of damage to persons

MS/designated authorities

Quantitative/ qualitative

If applicable, please provide statistics on unlawful processing operations or any other acts of incompatibility with the Decision. Please provide such statistics on a quarterly basis.

If applicable, please give an example of an unlawful processing operation or any other act incompatible with the Decision.

If applicable, please describe how individuals or MS are compensated in case of unlawfulness or incompatibility.

V. The security of the VIS

Art 10(2)

MSs' liability in in case of damage towards the VIS

MS/designated authorities

Quantitative/ qualitative

If applicable, please provide information, including statistics, on failures of your country to comply with its obligations under the Decision that caused damage to the VIS.

If applicable, please provide information, including statistics, on your country's liability in case of damage towards the VIS. Please give an example, if any.

181

Annex 6 – VIS adopted legislation

• 10/08/2015 – Commission Implementing Decision C(2015) 5561 final of 10 August 2015 on the technical specifications for the VIS Mail Communication Mechanism for the purposes of Regulation (EC) No 767/2008 of the European Parliament and of the Council and repealing Commission Decision 2009/377/EC and Commission Implementing Decision C(2012) 1301

• 04/05/2010 - Commission Decision 2010/260/EU of 4 May 2010 on the Security Plan for the operation of the ***Visa*** Information System

• 30/11/2009 - Commission Decision 2009/876/EC of 30 November 2009 adopting technical implementing measures for entering the data and linking applications, for accessing the data, for amending, deleting and advance deleting of data and for keeping and accessing the records of data processing operations in the ***Visa*** Information System

• 09/10/2009 - Commission Decision 2009/756/EC of 9 October 2009 laying down specifications for the resolution and use of fingerprints for biometric identification and verification in the ***Visa*** Information System

• 13/09/2009 - 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) (consolidated version of February 2012)

• 14/01/2009 - Regulation (EC) no. 81/2009 of the European Parliament and of the Council of 14 January 2009 amending Regulation (EC) No 562/2006 as regards the use of the ***Visa*** Information System (VIS) under the Schengen Borders Code

• 09/07/2008 - Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the ***Visa*** Information System (VIS) and the exchange of data between Member States on short-stay ***visas*** (VIS Regulation) (consolidated version of April 2010)

• 23/06/2008 - Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the ***Visa*** Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences

• 17/06/2008 - Commission Decision 2008/602/EC of 17 June 2008 laying down the physical architecture and requirements of the national interfaces and of the communication infrastructure between the central VIS and the national interfaces for the development phase

• 22/09/2006 - Commission Decision 2006/648/EC of 22 September 2006 laying down the technical specifications on the standards for biometric features related to the development of the ***Visa*** Information System

• 08/06/2004 - Council Decision 2004/512/EC of 8 June 2004 establishing the ***Visa*** Information System (VIS) (corrigendum)

182

Adopted legislation - VIS roll out schedule

• 26/02/2016 - Commission Implementing Decision (EU) 2015/281 of 26 February 2016 determining the date from which the ***Visa*** Information System (VIS) is to start operations at external border crossing points

• 12/06/2015 - Commission Implementing Decision (EU) 2015/913 of 12 June 2015 determining the date from which the ***Visa*** Information System (VIS) is to start operations in the 20th region

• 12/06/2015 - Commission Implementing Decision (EU) 2015/912 of 12 June 2015 determining the date from which the ***Visa*** Information System (VIS) is to start operations in the 21st, 22nd and 23rd regions

• 01/06/2015 - Commission Implementing Decision (EU) 2015/854 of 1 June 2015 determining the date from which the ***Visa*** Information System (VIS) is to start operations in the 19th region

• 06/05/2015 - Commission Implementing Decision (EU) 2015/731 of 6 May 2015 determining the date from which the ***Visa*** Information System (VIS) is to start operations in the 17th and 18th regions

• 29/08/2014 - Commission Implementing Decision 2014/540/EU of 29 August 2014 determining the date from which the ***Visa*** Information System (VIS) is to start operations in a sixteenth region

• 07/05/2014 - Commission Implementing Decision 2014/262/EU of 7 May 2014 determining the date from which the ***Visa*** Information System (VIS) is to start operations in a twelfth, a thirteenth, a fourteenth and a fifteenth region

• 08/11/2013 - Commission implementing Decision 2013/642/EU of 8 November 2013 determining the date from which the ***Visa*** Information System (VIS) is to start operations in a ninth, a tenth and in an eleventh region

• 30/09/2013 - 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)

• 20/08/2013 - Commission implementing Decision 2013/441/EU of 20 August 2013 determining the date from which the ***Visa*** Information System (VIS) is to start operations in an eighth region

• 05/06/2013 - Commission implementing Decision 2013/266/EU of 5 June 2013 determining the date from which the ***Visa*** Information System (VIS) is to start operations in a sixth and a seventh region

• 07/03/2013 - Commission implementing Decision n° 2013/122/EU of 7 March 2013 determining the date from which the VIS is to start operations in a fourth and a fifth region

183

• 21/09/2012 - Commission implementing Decision 2012/512/EU of 21 September 2012 determining the date from which the VIS is to start operations in a third region

• 27/04/2012 - Commission implementing Decision 2012/233/EU of 27 April 2012 determining the date from which the VIS is to start operations in a second region

• 24/04/2012 - 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)

• 21/09/2011 - Commission Implementing Decision 2011/636/EU of 21 September 2011 determining the date from which the ***Visa*** Information System (VIS) is to start operations in a first region

• 30/11/2009 - Commission Decision 2010/49/EC of 30 November 2009 determining the first regions for the start of operations of the ***Visa*** Information System (VIS)

Classification

Language: ENGLISH

Publication-Type: Newswire

Subject: EUROPEAN UNION (95%); EUROPEAN UNION INSTITUTIONS (94%); PASSPORTS & ***VISAS*** (90%); EUROPEAN UNION REGULATION & POLICY (90%); LEGISLATIVE BODIES (90%); DATA PROTECTION LAWS (89%); INTERNATIONAL ECONOMIC ORGANIZATIONS (89%); BIOMETRICS (88%); TERRITORIAL & NATIONAL BORDERS (88%); BORDER CONTROL (78%); AGREEMENTS (78%); STATISTICS (78%); LITIGATION (76%); EMBASSIES & CONSULATES (72%); LAW COURTS & TRIBUNALS (71%); DECISIONS & RULINGS (71%)

Industry: DATA PROTECTION LAWS (89%); INFORMATION SECURITY & PRIVACY (89%); DATA SECURITY (89%)

Geographic: BRUSSELS, BELGIUM (93%); EUROPE (97%); EUROPEAN UNION MEMBER STATES (97%)

Load-Date: November 29, 2016