European Parliament
2014-2019

TEXTS ADOPTED

P8_TA(2019)0174

Visa Information System ***I

European Parliament legislative resolution of 13 March 2019 on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA (COM(2018)0302 – C8-0185/2018 – 2018/0152(COD))

(Ordinary legislative procedure: first reading)

The European Parliament,

– having regard to the Commission proposal to Parliament and the Council (COM(2018)0302),

– having regard to Article 294(2) and Article 16(2), Article 77(2)(a), (b), (d) and (e), Article 78(2)(d), (e) and (g), Article 79(2)(c) and (d), Article 87(2)(a) and Article 88(2)(a) of the Treaty on the Functioning of the European Union, pursuant to which the Commission submitted the proposal to Parliament (C8-0185/2018),

– having regard to Article 294(3) of the Treaty on the Functioning of the European Union,

– having regard to Rule 59 of its Rules of Procedure,

– having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs and the opinion of the Committee on Budgets (A8-0078/2019),

1. Adopts its position at first reading hereinafter set out;

2. Calls on the Commission to refer the matter to Parliament again if it replaces, substantially amends or intends to substantially amend its proposal;

3. Instructs its President to forward its position to the Council, the Commission and the national parliaments.

P8_TC1-COD(2018)0152

Position of the European Parliament adopted at first reading on 13 March 2019 with a view to the adoption of Regulation (EU) …/… of the European Parliament and of the Council *reforming the Visa Information System by* amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and *repealing* Decision 2004/512/EC and ~~repealing~~ Council Decision 2008/633/JHA [Am. 1]

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty of the Functioning of the European Union, and in particular, Article 16(2), Article 77(2)(a) (b), (d) and (e), Article 78(2)(d),(e) and (g), Article 79(2)(c), and (d), Article 87(2)(a) and Article 88(2)(a),

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[1],

Having regard to the opinion of the Committee of the Regions[2],

Acting in accordance with the ordinary legislative procedure[3],

---

1 OJ C , , p. .

2 OJ C , , p. .

3 Position of the European Parliament of 13 March 2019.

Whereas:

(1) The Visa Information System (VIS) was established by Council Decision 2004/512/EC[4] to serve as the technology solution to exchange visa data between Member States. Regulation (EC) No 767/2008 of the European Parliament and of the Council[5] laid down the VIS purpose, functionalities and responsibilities, as well as the conditions and procedures for the exchange of short-stay visa data between Member States to facilitate the examination of short-stay visa applications and related decisions. Regulation (EC) No 810/2009 of the European Parliament and of the Council[6] set out the rules on the registration of biometric identifiers in the VIS. Council Decision 2008/633/JHA[7] laid down the conditions under which Member States' designated authorities and Europol may obtain access to consult the VIS for the purposes of preventing, detecting and investigating terrorist offences and other serious criminal offences. ***The VIS started operations on 11 October 2011[8] and was gradually rolled out in all Member States' consulates around the world between October 2011 and February 2016.*** **[Am. 2]**

---

4 Council Decision 2004/512/EC of 8 June 2004 establishing the Visa information System (VIS) (OJ L 213, 15.6.2004, p. 5).

5 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 ~~echange~~ ***exchange*** of data between Member States on short-stay visas (VIS Regulation) (OJ L 218, 13.8.2008, p. 60).

6 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) (OJ L 243, 15.9.2009, p. 1).

7 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).

8 ***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 (OJ L 249, 27.9.2011, p. 18).***

(2) The overall objectives of the VIS are to improve the implementation of the common visa policy, consular cooperation and consultation between central visa authorities by facilitating the exchange of data between Member States on applications and on the decisions relating thereto, in order to: facilitate the visa application procedure; prevent 'visa shopping'; facilitate the fight against identity fraud; facilitate checks at external border crossing points and within the Member States' territory; assist 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; facilitate the application of the Regulation (EU) No 604/2013 of the European Parliament and of the Council[9] and contribute to the prevention of threats to the internal security of any of the Member States.

---

[9] Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (OJ L 180, 29.6.2013, p. 31).

(3) The Communication of the Commission of 6 April 2016 entitled 'Stronger and Smarter Information Systems for Borders and Security'[10] outlined the need for the EU to strengthen and improve its IT systems, data architecture and information exchange in the area of border management, law enforcement and counter-terrorism and emphasised the need to improve the interoperability of IT systems. The Communication also identified a need to address information gaps, including on third country nationals holding a long-stay visa ***given that Article 21 of the Convention implementing the Schengen Agreement provides a right to free movement within the territory of the States parties to the Agreement for a period of not more than 90 days in any 180 days, by instituting the mutual recognition of the residence permits and long-stay visas issued by these States***. ***The Commission therefore conducted two studies: the first feasibility study[11] concluded that developing a repository would be technically feasible and that re-using the VIS structure would be the best technical option, whereas the second study[12] conducted an analysis of necessity and proportionality and concluded that it would be necessary and proportionate to extend the scope of VIS to include the documents mentioned above***. **[Am. 3]**

---

10 COM(2016)0205.

11 ***"Integrated Border Management (IBM) – Feasibility Study to include in a repository documents for Long-Stay visas, Residence and Local Border Traffic Permits" (2017).***

12 ***"Legal analysis on the necessity and proportionality of extending the scope of the Visa Information System (VIS) to include data on long stay visas and residence documents" (2018).***

~~(4) The Council endorsed a Roadmap to enhance information exchange and information management[13] on 10 June 2016. In order to address the existing information gap in the documents issued to third-country nationals, the Council invited the Commission to assess the establishment of a central repository of residence permits and long-stay visas issued by Member States, to store information on these documents, including on expiry dates and on their possible withdrawal. Article 21 of the Convention implementing the Schengen Agreement provides a right to free movement within the territory of the states party to the Agreement for a period of not more than 90 days in any 180 days, by instituting the mutual recognition of the residence permits and long stay visas issued by these States.~~ **[Am. 4]**

~~[13] Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area (9368/1/16 REV 1).~~

(5) In Council Conclusions of 9 June 2017 on the way forward to improve information exchange and ensure the interoperability of EU information systems[14], the Council acknowledged that new measures might be needed in order to fill the current information gaps for border management and law enforcement, in relation to border crossings by holders of long-stay visas and residence permits. The Council invited the Commission to undertake a feasibility study as a matter of priority for the establishment of a central EU repository containing information on long-stay visas and residence permits. On this basis, the Commission conducted two studies: the first feasibility study[15] concluded that developing a repository would be technically feasible and that re-using the VIS structure would be the best technical option, whereas the second study[16] conducted an analysis of necessity and proportionality and concluded that it would be necessary and proportionate to extend the score of VIS to include the documents mentioned above. **[Am. 5]**

[14] Council Conclusions on the way forward to improve information exchange and ensure the interoperability of EU information systems (10151/17).

[15] "Integrated Border Management (IBM) – Feasibility Study to include in a repository documents for Long-Stay visas, Residence and Local Border Traffic Permits" (2017).

[16] "Legal analysis on the necessity and proportionality of extending the scope of the Visa Information System (VIS) to include data on long stay visas and residence documents" (2018).

(6) The Communication of the Commission of 27 September 2017 on the 'Delivery of the European Agenda on Migration'[17] stated that the EU's common visa policy is not only an essential element to facilitate tourism and business, but also a key tool to prevent security risks and risks of irregular migration to the EU. The Communication acknowledged the need to further adapt the common visa policy to current challenges, taking into account new IT solutions and balancing the benefits of facilitated visa travel with improved migration, security and border management. The Communication stated that the VIS legal framework would be revised, with the aim of further improving the visa processing, including on data protection related aspects and access for law enforcement authorities, further expanding the use of the VIS for new categories and uses of data and to make full use of the interoperability instruments.

(7) The Communication of the Commission of 14 March 2018 on adapting the common visa policy to new challenges[18] reaffirmed that the VIS legal framework would be revised, as part of a broader process of reflection on the interoperability of information systems.

---

17 COM(2017)0558, p.15.

18 COM(2018)0251.

(8) When adopting Regulation (EC) No 810/2009, it was recognised that the issue of the sufficient reliability for identification and verification purposes of fingerprints of children under the age of 12 and, in particular, how fingerprints evolve with age, would have to be addressed at a later stage, on the basis of the results of a study carried out under the responsibility of the Commission. A study[19] carried out in 2013 by the Joint Research Centre concluded that fingerprint recognition of children aged between 6 and 12 years is achievable with a satisfactory level of accuracy under certain conditions. A second study[20] confirmed this finding in December 2017 and provided further insight into the effect of aging over fingerprint quality. On this basis, the Commission conducted in 2017 a further study looking into the necessity and proportionality of lowering the fingerprinting age for children in the visa procedure to 6 years. This study[21] found that lowering the fingerprinting age would contribute to better achieving the VIS objectives, in particular in relation to the facilitation of the fight against identity fraud, facilitation of checks at external border crossing points, and could bring additional benefits by strengthening the prevention and fight against children's rights abuses, in particular by enabling the identification/verification of identity of third-country national (TCN) children who are found in Schengen territory in a situation where their rights may be or have been violated (e.g. child victims of trafficking in human beings, missing children and unaccompanied minors applying for asylum). ***At the same time, children are a particularly vulnerable group and collecting special categories of data, such as fingerprints, from them should be subject to stricter safeguards and a limitation of the purposes for which these data may be used to situations where it is in the child's best interests, including by limiting the retention period for data storage. The second study also identified that fingerprints of persons above 70 years of age are of low quality and medium accuracy. The Commission and Member States should cooperate in exchanging best practices and address those shortcomings.*** **[Am. 6]**

---

19 Fingerprint Recognition for Children (2013 - EUR 26193).

20 "Automatic fingerprint recognition: from children to elderly" (2018 – JRC).

21 "Feasibility and implications of lowering the fingerprinting age for children and on storing a scanned copy of the visa applicant's travel document in the Visa Information System (VIS)" (2018).

(9) The best interests of the child shall be a primary consideration for Member States with respect to all procedures provided for in this Regulation. The child's well-being, safety and security and the views of the child shall be taken into consideration and given due weight in accordance with his or her age and maturity. The VIS is in particular relevant where there is a risk of a child being a victim of trafficking.

(10) The personal data provided by the applicant for a short-stay visa should be processed by the VIS to assess whether the entry of the applicant in the Union could pose a threat to the public security ~~or to public health~~ in the Union and also assess the risk of irregular migration of the applicant. As regards third country nationals who obtained a long stay visa or a residence permit, these checks should be limited to contributing to assess the identity of the document holder, the authenticity and the validity of the long-stay visa or residence permit as well as whether the entry of the third country national in the Union could pose a threat to public security ~~or to public health~~ in the Union. They should not interfere with any decision on long-stay visas or residence permits. **[Am. 7]**

(11) The ~~assessement~~ ***assessment*** of such risks cannot be carried out without processing the personal data related to the person's identity, travel document, and, as the case may be, sponsor or, if the applicant is minor, identity of the responsible person. Each item of personal data in the applications should be compared with the data present in a record, file or alert registered in an information system (the Schengen Information System (SIS), the Visa Information System (VIS), the Europol data, the Interpol Stolen and Lost Travel Document database (SLTD), the Entry/Exit System (EES), the Eurodac, ~~the ECRIS-TCN system as far as convictions related to terrorist offences or other forms of serious criminal offences are concerned and/or the Interpol Travel Documents Associated with Notices database (Interpol TDAWN))~~ or against the ~~watchlists~~ ***ETIAS watchlist***, or against specific risk indicators. The categories of personal data that should be used for comparison should be limited to the categories of data present in the queried information systems, the watchlist or the specific risk indicators. **[Am. 8]**

(12) Interoperability between EU information systems was established by [Regulation (EU) XX on interoperability ***(borders and visas)***] ~~so that these EU information systems and their data supplement each other~~ with a view to improving the management of the external borders, contributing to preventing and combating illegal migration and ensuring a high level of security within the area of freedom, security and justice of the Union, including the maintenance of public security and public policy and safeguarding the security in the territories of the Member States. **[Am. 9. This amendment applies throughout the text]**

(13) The interoperability between the EU information systems allows systems ~~to supplement each other~~ to facilitate the correct identification of persons, contribute to fighting identity fraud, improve and harmonise data quality requirements of the respective EU information systems, facilitate the technical and operational implementation by Member States of existing ~~and future~~ EU information systems, strengthen***, harmonise*** and simplify the data security and data protection safeguards that govern the respective EU information systems, streamline the ***controlled*** law enforcement access to the EES, the VIS, the ┤ETIAS├ and Eurodac, and support the purposes of the EES, the VIS, the ┤ETIAS├, Eurodac, the SIS and the ┤ECRIS-TCN system├. **[Am. 10]**

(14) The interoperability components cover the EES, the VIS, the ┤ETIAS├, Eurodac, the SIS, and the ┤ECRIS-TCN system├, and Europol data to enable it to be queried simultaneously with these EU information systems and therefore it is appropriate to use these components for the purpose of carrying out the automated checks and when accessing the VIS for law enforcement purposes. The European search portal (ESP) should be used for this purpose to enable a fast, seamless, efficient, systematic and controlled access to the EU information systems, the Europol data and the Interpol databases needed to perform their tasks, in accordance with their access rights, and to support the objectives of the VIS. **[Am. 11]**

(15) The comparison against other databases should be automated. Whenever such comparison reveals that a correspondence (a 'hit') exists with any of the personal data or combination thereof in the applications and a record, file or alert in the above information systems, or with personal data in the watchlist, the application should be***, where the hit cannot be automatically confirmed by VIS,*** processed manually by an operator in the responsible authority. ***Depending on the type of data triggering the hit, the hit should be assessed either by consulates or by a national single point of contact, with the latter being responsible for hits generated in particular by law enforcement databases or systems.*** The assessment performed by the responsible authority should lead to the decision to issue or not the short-stay visa. **[Am. 12]**

(16) Refusal of an application for a short-stay visa should not be based only on the automated processing of personal data in the applications.

(17) Applicants who have been refused a short-stay visa on the basis of an information resulted from VIS processing should have the right to appeal. Appeals should be conducted in the Member State that has taken the decision on the application and in accordance with the national law of that Member State. Existing safeguards and rules on appeal in Regulation (EC) No 767/2008 should apply.

(18) Specific risk indicators corresponding to previously identified security, irregular migration or ~~public health risk~~ ***high epidemic risks*** should be used to analyse the application file for a short stay visa. The criteria used for defining the specific risk indicators should in no circumstances be based solely on a person's sex or age. They shall in no circumstances be based on information revealing a person's race, colour, ethnic or social origin, genetic features, language, political or any other opinions, religion or ~~philosofical~~ ***philosophical*** belief, trade union membership, membership of a national minority, property, birth, disability or sexual orientation. **[Am. 13]**

(19) The continuous emergence of new forms of security ~~threats~~ ***risks***, new patterns of irregular migration and ~~public health threats~~ ***high epidemic risks*** requires effective responses and needs to be countered with modern means. Since these means entail the processing of important amounts of personal data, appropriate safeguards should be introduced to keep the interference with the rights to respect for private and family life and to the personal data limited to what is necessary ***and proportionate*** in a democratic society. **[Am. 14]**

(20) It should be ensured that at least a similar level of checks is applied to applicants for a short-stay visa, or third country nationals who obtained a long stay visa or a residence permit, as for visa free third country nationals. To this end a watchlist is also established with information related to persons who are suspected of having committed an act of serious crime or terrorism, or regarding whom there are factual indications or reasonable grounds to believe that they will commit an act of serious crime or terrorism should be used for verifications in respect of these categories of third country nationals as well.

(21) In order to fulfil their obligation under the Convention implementing the Schengen Agreement, international carriers should ~~be able to~~ verify whether or not third country nationals holding a short-stay visa, a long stay visa or a residence permit are in possession of the required valid travel documents ***by sending a query to VIS***. This verification should be made possible through the daily extraction of VIS data into a separate read-only database allowing the extraction of a minimum necessary subset of data to enable a query leading to an ok/not ok answer. ***The application file itself should not be accessible to carriers. The technical specifications for accessing VIS through the carrier gateway should limit the impact on passenger travel and carriers to the extent possible. For this purpose, integration with the EES and ETIAS should be considered.*** **[Am. 15]**

(21a) With a view to limiting the impact of the obligations set out in this Regulation on international carriers transporting groups overland by coach, user-friendly mobile solutions should be made available. **[Am. 16]**

(21b) Within two years following the start of application of this Regulation, the appropriateness, compatibility and coherence of provisions referred to in Article 26 of the Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders for the purposes of the VIS provisions for overland transport by coaches should be assessed by the Commission. The recent evolution of overland transport by coaches should be taken into account. The need for amending provisions concerning overland transport by coaches referred to in Article 26 of that Convention or this Regulation should be considered. **[Am. 17]**

(22) This Regulation should define the authorities of the Member States which may be authorised to have access to the VIS to enter, amend, delete or consult data on long stay visas and residence permits for the specific purposes set out in the VIS for this category of documents and their holders, and to the extent necessary for the performance of their tasks.

(23) Any processing of VIS data on long stay visas and residence permits should be proportionate to the objectives pursued and necessary for the performance of tasks of the competent authorities. When using the VIS, the competent authorities should ensure that the human dignity and integrity of the person, whose data are requested, are respected and should not discriminate against persons on grounds of sex, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

(23a) Biometric data, which in the context of this Regulation entails fingerprints and facial images are unique and therefore much more reliable than alphanumeric data for the purposes of identifying a person. However, biometric data constitute sensitive personal data. This Regulation thus lays down the basis and safeguards for processing such data for the purpose of uniquely identifying the persons concerned. **[Am. 18]**

(24) It is imperative that law enforcement authorities have the most up-to-date information if they are to perform their tasks in the fight against terrorist offences and other serious criminal offences. Access of law enforcement authorities of the Member States and of Europol to VIS has been established by Council Decision 2008/633/JHA. The content of this Decision should be integrated into the VIS Regulation, to bring it in line with the current treaty framework.

(25) Access to VIS data for law enforcement purpose has already proven its usefulness in identifying people who died violently or for helping investigators to make substantial progress in cases related to trafficking in human beings, terrorism or drug trafficking. Therefore, the data in the VIS related to long stays should also be available to the designated authorities of the Member States and the European Police Office ('Europol'), subject to the conditions set out in this Regulation.

(26) Given that Europol plays a key role with respect to cooperation between Member States' authorities in the field of cross-border crime investigation in supporting Union-wide crime prevention, analyses and investigation. Europol's current access to the VIS within the framework of its tasks should be codified and streamlined, taking also into account recent developments of the legal framework such as Regulation (EU) 2016/794 of the European Parliament and of the Council[22].

(27) Access to the VIS for the purpose of preventing, detecting or investigating terrorist offences or other serious criminal offences constitutes an interference with the fundamental rights to respect for private and family life and to the protection of personal data of persons whose personal data are processed in the VIS. Any such interference must be in accordance with the law, which must be formulated with sufficient precision to allow individuals to adjust their conduct and it must protect individuals against arbitrariness and indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise. Any interference must be necessary in a democratic society to protect a legitimate and proportionate interest and proportionate to the legitimate objective to achieve.

---

22 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

(28) [Regulation 2018/XX on interoperability ***(borders and visas)***] provides the possibility for a Member State police authority which has been so empowered by national legislative measures, to identify a person with the biometric data of that person taken during an identity check. However specific circumstances may exist where identification of a person is necessary in the interest of that person. Such cases include situations where the person was found after having gone missing, been abducted or having been identified as victim of trafficking. In such cases ***alone***, quick access for law enforcement authorities to VIS data to enable a fast and reliable identification of the person, without the need to fulfill all the preconditions and additional safeguards for law enforcement access, should be provided. **[Am. 19]**

(29) Comparisons of data on the basis of a latent fingerprint, which is the dactyloscopic trace which may be found at a crime scene, is fundamental in the field of police cooperation. The possibility to compare a latent fingerprint with the fingerprint data which is stored in the VIS in cases where there are reasonable grounds for believing that the perpetrator or victim may be registered in the VIS ***and after prior search under Council Decision 2008/615/JHA***[23] should provide the law enforcement authorities of the Member States with a very valuable tool in preventing, detecting or investigating terrorist offences or other serious criminal offences, when for example the only evidence at a crime scene are latent fingerprints. **[Am. 20]**

---

[23] ***Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 1).***

(30) It is necessary to designate the competent authorities of the Member States as well as the central access point through which the requests for access to VIS data are made and to keep a list of the operating units within the designated authorities that are authorised to request such access for the specific purposes for the prevention, detection or investigation of terrorist offences or of other serious criminal offences.

(31) Requests for access to data stored in the Central System should be made by the operating units within the designated authorities to the central access point and should be justified. The operating units within the designated authorities that are authorised to request access to VIS data should not act as a verifying authority. The central access points should act independently of the designated authorities and should be responsible for ensuring, in an independent manner, strict compliance with the conditions for access as established in this Regulation. In exceptional cases of urgency, where early access is necessary to respond to a specific and actual threat related to terrorist offences or other serious criminal offences, the central access point should be able to process the request immediately and only carry out the verification afterwards.

(32) To protect personal data and to exclude systematic searches by law enforcement, the processing of VIS data should only take place in specific cases and when it is necessary for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences. The designated authorities and Europol should only request access to the VIS when they have reasonable grounds to believe that such access will provide information that will substantially assist them in preventing, detecting or investigating a terrorist offence or other serious criminal offence ***and after prior search under Decision 2008/615/JHA***. **[Am. 21]**

(32a) As a general practice, Member States' end-users carry out searches in relevant national data bases prior or in parallel to querying European databases. **[Am. 22]**

(33) The personal data of holders of long stay ~~documents~~ ***visas*** stored in the VIS should be kept for no longer than is necessary for the purposes of the VIS. It is appropriate to keep the data related to third country nationals for a period of five years in order to enable data to be taken into account for the assessment of short-stay visa applications, to enable detection of overstay after the end of the validity period and in order to conduct security assessments of third country nationals who obtained them. The data on previous uses of a document could facilitate the issuance of future short stay visas. A shorter storage period would not be sufficient for ensuring the stated purposes. The data should be erased after a period of five years, unless there are grounds to erase them earlier. **[Am. 23]**

(34) Regulation (EU) 2016/679 of the European Parliament and of the Council[24] applies to the processing of personal data by the Member States in application of this Regulation. Processing of personal data by law enforcement authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties is governed by Directive (EU) 2016/680 of the European Parliament and of the Council[25].

---

24 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

25 Directive (EU) 2016/680 of the European parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

(35) Members of the European Border and Coast Guard (EBCG) teams~~, as well as teams of staff involved in return-related tasks~~ are entitled by Regulation (EU) 2016/1624 of the European Parliament and the Council to consult European databases where necessary for fulfilling operational tasks specified in the operational plan on border checks, border surveillance and return, under the authority of the host Member State. ~~For the purpose of facilitating that consultation and enabling the teams an effective access to the data entered in VIS, the ECBGA should be given access to VIS.~~ Such access should follow the conditions and limitations of access applicable to the Member States' authorities competent under each specific purpose for which VIS data can be consulted. **[Am. 24]**

(36) The return of third-country nationals who do not fulfil or no longer fulfil the conditions for entry, stay or residence in the Member States, in accordance with Directive 2008/115/EC of the European Parliament and of the Council[26], is an essential component of the comprehensive efforts to tackle irregular migration and represents an important reason of substantial public interest.

---

26 Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals (OJ L 348, 24.12.2008, p. 98).

(37) ~~The third countries of return are often not subject to adequacy decisions adopted by the Commission under Article 45 of~~ ***Personal data obtained by a Member State pursuant to this*** Regulation ~~(EU) 2016/679 or under national provisions adopted to transpose Article 36 of Directive (EU) 2016/680. Furthermore, the extensive efforts of the Union in cooperating with the main countries of origin of illegally staying third-country nationals subject to an obligation to return has not been able to ensure the systematic fulfilment by such~~ ***should not be transferred or made available to any*** third ***country, international organisation or private entity*** ~~countries of the obligation~~ established ~~by~~ ***in or outside the Union. As an exception to that rule, however, it should be possible to transfer such personal data to a third country or to an*** international ~~law to readmit their own nationals. Readmission agreements, concluded or being negotiated by the Union or the Member States and providing for appropriate safeguards for the~~ ***organisation where such a*** transfer ~~of data to third countries~~ ***is subject to strict conditions and necessary in individual cases in order to assist with the identification of a third-country national in relation to his or her return. In the absence of an adequacy decision by means of implementing act*** pursuant to ~~Article 46 of~~ Regulation (EU) 2016/679 or ~~to the national provisions adopted to transpose Article 37 of Directive (EU) 2016/680, cover a limited number of such third countries and conclusion of any new agreement remains uncertain. In such situations, personal data could be processed~~ ***of appropriate safeguards to which transfers are subject*** pursuant to ~~this~~ ***that*** Regulation ~~with third-country authorities~~***, it should be possible to exceptionally transfer,*** for the purposes of ~~implementing the~~ return ~~policy of the Union provided that the conditions laid down in Article 49(1)(d) of~~***, VIS data to a third country or to an international organisation, only where it is necessary for important reasons of public interest as referred to in that*** Regulation ~~(EU) 2016/679 or in the national provisions transposing Article 38 or 39 of Directive (EU) 2016/680 are met.~~ **[Am. 25]**

~~(38) Member States should make available relevant personal data processed in the VIS, in accordance with the applicable data protection rules and where required in individual cases for carrying out tasks under Regulation (EU) …/… of the European Parliament and the Council[27],Union Resettlement Framework Regulation], to the [European Union Asylum Agency] and relevant international bodies such as the United Nations High Commissioner for Refugees, the International Organisation on Migration and to the International Committee of the Red Cross refugee and resettlement operations, in relation to third-country nationals or stateless persons referred by them to Member States in the implementation of Regulation (EU) …/… [*the Union Resettlement Framework Regulation*].~~ **[Am. 26]**

(39) Regulation ~~(EC) No 45/2001~~ (***EU***) ***2018/1725*** of the European Parliament and the Council[28] applies to the activities of the Union institutions or bodies when carrying out their tasks as responsible for the operational management of VIS. **[Am. 27]**

(40) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on ~~…~~ ***12 December 2018.*** **[Am. 28]**

~~[27] Regulation (EU) …/… of the European Parliament and the Council [full title] (OJ L …, …, p. …).~~

[28] Regulation ~~(EC) No 45/2001~~ (***EU***) ***2018/1725*** of the European Parliament and ***of*** the Council of ~~18 December 2000~~ ***23 October 2018*** on the protection of ~~individuals~~ ***natural persons*** with regard to the processing of personal data by the ~~Community~~ ***Union*** institutions***,*** ~~and~~ bodies***, offices and agencies*** and on the free movement of such data ~~(OJ L 8, 12.1.2001, p. 1).~~***, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).***

(41) In order to enhance third countries' cooperation on readmission of irregular migrants and to facilitate the return of illegally staying third country nationals whose data might be stored in the VIS, the copies of the travel document of applicants for a short stay visa should be stored in the VIS. Contrary to information extracted from the VIS, copies of travel documents are a proof of nationality more widely recognised by third countries.

(42) Consultation of the list of travel documents which entitle the holder to cross the external borders and which may be endorsed with a visa, as established by Decision No 1105/2011/EU of the European Parliament and of the Council[29], is a compulsory element of the visa examination procedure. Visa authorities should systematically implement this obligation and therefore this list should be incorporated in the VIS to enable automatic verification of the recognition of the applicant's travel document.

(43) Without prejudice to Member States' responsibility for the accuracy of data entered into VIS, eu-LISA should be responsible for reinforcing data quality by introducing**,** ***maintaining and continuously upgrading*** a central data quality monitoring tool, and for providing reports at regular intervals to the Member States. **[Am. 29]**

---

29 Decision No 1105/2011/EU of the European Parliament and of the Council of 25 October 2011 on the list of travel documents which entitle the holder to cross the external borders and which may be endorsed with a visa and on setting up a mechanism for establishing this list (OJ L 287, 4.11.2011, p. 9).

(44) In order to allow better monitoring of the use of VIS to analyse trends concerning migratory pressure and border management, eu-LISA should be able to develop a capability for statistical reporting to the Member States, the Commission, and the European Border and ~~Cost~~ ***Coast*** Guard Agency without jeopardising data integrity. Therefore, ~~a central~~ ***eu-LISA should store certain*** statistical ***data in the central*** repository ~~should be established~~ ***for the purposes of the reporting and providing statistics in accordance with [Regulation 2018/XX on interoperability (borders and visa)]***. None of the produced statistics should contain personal data. **[Am. 30]**

(45) This Regulation is without prejudice to the application of Directive 2004/38/EC of the European Parliament and of the Council.[30]

(46) Since the objectives of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of the need to ensure the implementation of a common policy on visas, a high level of security within the area without controls at the internal borders and the gradual establishment of an integrated management system for the external borders, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

---

30 Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ L 158, 30.4.2004, p. 77).

(47) This Regulation establishes strict access rules to the VIS and the necessary safeguards. It also foresees individuals' rights of access, rectification, erasure and remedies in particular the right to a judicial remedy and the supervision of processing operations by public independent authorities. Additional safeguards are introduced by this Regulation to cover for the specific needs of the new categories of data that will be processed by the VIS. This Regulation therefore respects the fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union, in particular the right to human dignity , the right to liberty and security, the respect for private and family life, the protection of personal data, the right to asylum and protection of the principle of non-refoulement and protection in the event of removal, expulsion or extradition, the right to non-discrimination, the rights of the child and the right to an effective remedy.

(47a) This Regulation is without prejudice to the obligations deriving from the Geneva Convention Relating to the Status of Refugees of 28 July 1951, as supplemented by the New York Protocol of 31 January 1967, and to all the international commitments entered into by the Union and its Member States. **[Am. 31]**

(48) Specific provisions should apply to third country nationals who are subject to a visa requirement, who are family members of a Union citizen to whom Directive 2004/38/EC applies or of a national of a third country enjoying the right of free movement under Union law and who do not hold a residence card referred to under Directive 2004/38/EC. Article 21(1) of the Treaty on the Functioning of the European Union stipulates that every citizen of the Union shall have the right to move and reside freely within the territory of the Member States, subject to the limitations and conditions laid down in the Treaties and by the measures adopted to give them effect. The respective limitations and conditions are to be found in Directive 2004/38/EC.

(49) As confirmed by the Court of Justice of the European Union, such family members have not only the right to enter the territory of the Member State but also to obtain an entry visa for that purpose. Member States must grant such persons every facility to obtain the necessary visas which must be issued free of charge as soon as possible and on the basis of an accelerated procedure.

(50) The right to obtain a visa is not unconditional as it can be denied to those family members who represent a risk to public policy, public security or public health pursuant to Directive 2004/38/EC. Against this background, the personal data of family members can only be verified where the data relate to their identification and their status only insofar these are relevant for assessment of the security threat they could represent. Indeed, the examination of their visa applications should be made exclusively against the security concerns, and not those related to migration risks.

(51) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law.

(52) This Regulation constitutes a development of the provisions of the Schengen acquis in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC[31]; the United Kingdom is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(53) This Regulation constitutes a development of the provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC[32]; Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(54) As regards Iceland and Norway, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latters' association with the implementation, application and development of the Schengen acquis[33] which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC[34].

---

31 Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis (OJ L 131, 1.6.2000, p. 43).

32 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 (OJ L 64, 7.3.2002, p. 20).

33 OJ L 176, 10.7.1999, p. 36.

34 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 association of those two States with the implementation, application and development of the Schengen acquis (OJ L 176, 10.7.1999, p. 31).

(55) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning 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*[35] which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC[36] and with Article 3 of Council Decision 2008/149/JHA[37].

---

35 OJ L 53, 27.2.2008, p. 52.

36 Council Decision 2008/146/EC of 28 January 2008 on the conclusion, on behalf of the European Community, 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.

37 Council Decision 2008/149/JHA 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. 50).

(56) As regards Liechtenstein, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning 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*[38] which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU[39] and with Article 3 of Council Decision 2011/349/EU.[40]

---

38 OJ L 160, 18.6.2011, p. 21.

39 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).

40 Council Decision 2011/349/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 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 in particular to judicial cooperation in criminal matters and police cooperation (OJ L 160, 18.6.2011, p. 1).

(57) This Regulation, with the exception of Article 22r, constitutes an act building upon, or otherwise relating to, the Schengen *acquis* within, respectively, the meaning of Article 3(2) of the 2003 Act of Accession, Article 4(2) of the 2005 Act of Accession and Article 4(2) of the 2011 Act of Accession, with the exception of provisions rendered applicable to Bulgaria and Romania by Council Decision (EU) 2017/1908[41],

HAVE ADOPTED THIS REGULATION:

[41] Council Decision (EU) 2017/1908 of 12 October 2017 on the putting into effect of certain provision of the Schengen acquis relating to the Visa Information System in the Republic of Bulgaria and Romania (OJ L 269, 19.10.2017, p. 39).

Article 1

Regulation (EC) No 767/2008 is amended as follows:

(-1) The title is replaced by the following:

"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 information between Member States on short-stay visas, long-stay visas, and residence permits (VIS Regulation)"; **[Am. 32]**

(1) In Article 1 the following paragraphs are added:

"This Regulation also lays down procedures for the exchange of information between Member States on long-stay visas and residence permits, including on certain decisions on long-stay visas and residence permits.

By storing identity, travel document and biometric data in the common identity repository (CIR) established by Article 17 of Regulation 2018/XX of the European Parliament and of the Council* [Regulation 2018/XX on interoperability ***(borders and visas)***], the VIS contributes to facilitating and assisting in the correct identification of persons registered in the VIS."

_____

* Regulation 2018/XX of the European Parliament and of the Council* [Regulation 2018/XX on interoperability ***(borders and visas)***] (OJ L).";

(2) Article 2 is replaced by the following:

"Article 2

Purpose of VIS

1. The VIS shall have the purpose of improving the implementation of the common visa policy ***on short-stay visas***, consular cooperation and consultation between central visa authorities by facilitating the exchange of data between Member States on applications and on the decisions relating thereto, in order: **[Am. 33]**

   (a) to facilitate ***and expedite*** the visa application procedure; **[Am. 34]**

   (b) to prevent the bypassing of the criteria for the determination of the Member State responsible for examining the application;

   (c) to facilitate the fight against fraud;

   (d) to facilitate checks at external border crossing points and within the territory of the Member States;

(e) to assist in the identification and return 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;

(f) to assist in the identification of persons ***referred to in Article 22o*** who have gone missing; **[Am. 35]**

(g) to facilitate the application of Regulation (EU) No 604/2013 of the European Parliament and of the Council* and of Directive 2013/32/EU of the European Parliament and of the Council**;

(h) to contribute to ***the prevention of threats to the internal security of any of the Member States, namely through*** the prevention, detection and investigation of terrorist offences or of other serious criminal offences ***in appropriate and strictly defined circumstances***; **[Am. 36]**

~~(i) to contribute to the prevention of threats to the internal security of any of the Member States;~~ **[Am. 37]**

(j) to ensure the correct identification of persons;

(k) support the objectives of the Schengen Information System (SIS) related to the alerts in respect of third country nationals subject to a refusal of entry, persons wanted for arrest or for surrender or extradition purposes, on missing persons, on persons sought to assist with a judicial procedure and on persons for discreet checks or specific checks."

2. As regards long stay visas and residence permits, the VIS shall have the purpose of facilitating the exchange of data between Member States on the decisions related thereto, in order to:

(a) support a high level of security ***in all Member States*** by contributing to the assessment of whether the applicant ***or holder of a document*** is considered to pose a threat to public policy, internal security ~~or public health prior to their arrival at the external borders crossing points~~; **[Am. 38]**

(b) ***facilitate checks at external border crossing points and*** enhance the effectiveness ~~of border checks and~~ of checks within the territory ***of the Member States***; **[Am. 39]**

(c) contribute to ***the prevention of threats to the internal security of any of the Member States, namely through*** the prevention, detection and investigation of terrorist offences or of other serious criminal offences ***in appropriate and strictly defined circumstances***; **[Am. 40]**

(d) ensure the correct identification of persons;

(da) assist in the identification of persons referred to in Article 22o who have gone missing; **[Am. 41]**

(e) facilitate the application of Regulation (EU) No 604/2013 and of Directive 2013/32/EU;

(f) support the objectives of the Schengen Information System (SIS) related to the alerts in respect of third country nationals subject to a refusal of entry, persons wanted for arrest or for surrender or extradition purposes, on missing persons, on persons sought to assist with a judicial procedure and on persons for discreet checks or specific checks."

* Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (OJ L 180, 29.6.2013, p. 31).

** Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (OJ L 180, 29.6.2013, p. 60).";

(2a) the following Article is inserted:

"Article 2a

Architecture

1. VIS shall be based on a centralised architecture and shall consist of:

(a) the common identity repository established by [Article 17(2)(a) of Regulation 2018/XX on interoperability (borders and visa)];

(b) a central information system (the 'VIS Central System');

(c) an interface in each Member State (the 'national interface' or 'NI-VIS') which shall provide the connection to the relevant central national authority of the respective Member State, or a national uniform interface (NUI) in each Member State based on common technical specifications and identical for all Member States enabling the VIS Central System to connect to the national infrastructures in Member States;

(d) a communication infrastructure between the VIS Central System and the national interfaces;

(e) a secure communication channel between the VIS Central System and the EES Central System;

(f) a secure communication infrastructure between the VIS Central System and the central infrastructures of the European search portal established by [Article 6 of Regulation 2018/XX on interoperability (borders and visa)], shared biometric matching service established by [Article 12 of Regulation 2018/XX on interoperability (borders and visa)], the common identity repository established by [Article 17 of Regulation 2018/XX on interoperability (borders and visa)] and the multiple-identity detector established by [Article 25 of Regulation 2018/XX on interoperability (borders and visa)];

(g) a mechanism of consultation on applications and exchange of information between central visa authorities ('VISMail');

(h) a carrier gateway;

(i) a secure web service enabling communication between the VIS Central System on the one hand and the carrier gateway and international systems on the other hand;

(j) a repository of data for the purposes of reporting and statistics;

(k) a tool enabling applicants to give or withdraw their consent for an additional retention period of their application file.

The VIS Central System, the national uniform interfaces, the web service, the carrier gateway and the VIS communication infrastructure shall share and re-use as much as technically possible the hardware and software components of respectively the EES Central System, the EES national uniform interfaces, the ETIAS carrier gateway, the EES web service and the EES communication infrastructure.

2. The NI-VIS shall consist of:

(a) one local national interface (LNI) for each Member State which is the interface that physically connects the Member State to the secure communication network and contains the encryption devices dedicated to VIS. The LNI shall be located at the Member State premises;

(b) one backup LNI (BLNI) which shall have the same content and function as the LNI.

3. The LNI and BLNI are to be used exclusively for purposes defined by the Union legislation applicable to VIS.

4. Centralised services shall be duplicated to two different locations namely Strasbourg, France, hosting the principal VIS Central System, central unit (CU) and St Johann im Pongau, Austria, hosting the backup VIS Central System, backup central unit (BCU). The connection between the principal VIS Central System and the backup VIS Central System shall allow for the continuous synchronisation between the CU and BCU. The communication infrastructure shall support and contribute to ensuring the uninterrupted availability of VIS. It shall include redundant and separated paths for the connections between VIS Central System and the backup VIS Central System and shall also include redundant and separated paths for the connections between each national interface and VIS Central System and backup VIS Central System. The communication infrastructure shall provide an encrypted, virtual, private network dedicated to VIS data and to communication between Member States and between Member States and the authority responsible for the operational management for the VIS Central System."; **[Am. 42]**

(3) Article 3 is deleted;

(4) ~~in~~ Article 4~~,~~ ***is amended as follows:***

(a) the following point is inserted:

(3a) 'central authority' means the authority established by a Member State for the purposes of Regulation (EC) No 810/2009; **[Am. 43]**

(b) the following points are added:

(12) 'VIS data' means all data stored in the VIS Central System and in the CIR in accordance with Articles 9 to14, 22c, to 22f;

(13) 'identity data' means the data referred to in Article 9(4)(a) and (aa);

(14) 'fingerprint data' means the data relating fingerprints that is stored in a VIS file;

(15) 'facial image' means digital image of the face ***with sufficient image resolution and quality to be used in automated biometric matching***; **[Am. 44]**

(16) 'Europol data' means personal data processed by Europol for the purpose referred to in Article 18(2)(a) of Regulation (EU) 2016/794 of the European Parliament and of the Council*;

(17) 'residence permit' means all residence permits issued by the Member States in accordance with the uniform format laid down by Council Regulation (EC) No 1030/2002** and all other documents referred to in Article 2(16)(b) of Regulation (EU) 2016/399;

(18) 'long-stay visa' means an authorisation issued by a Member State as provided for in Article 18 of the Schengen Convention;

(19) ’~~national~~ supervisory ~~authority~~ ***authorities***’ ~~as regards law enforcement purposes~~ means the supervisory authorities ~~established in accordance with~~ ***referred to in Article 51(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council*** and the supervisory authorities referred to in*** Article 41 of Directive (EU) 2016/680 of the European Parliament and of the Council****; **[Am. 45]**

(19a) 'hit' means the existence of a correspondence established by comparing the relevant data recorded in an application file of VIS with the relevant data present in a record, file or alert registered in VIS, Schengen Information System, the EES, ETIAS, Eurodac, Europol data or in Interpol’s SLTD database; **[Am. 46]**

(20) 'law enforcement' means the prevention, detection or investigation of terrorist offences or other serious criminal offences ***within a strictly defined framework***; **[Am. 47]**

(21) 'terrorist offences' mean the offences under national law ~~which correspond or are equivalent to those~~ referred to in ***Articles 3 to 14 of*** Directive (EU) 2017/541 of the European Parliament and of the Council***** ***or equivalent to one of those offences for the Member States which are not bound by that Directive***; **[Am. 48]**

(22) 'serious criminal offences' means the offences which correspond or are equivalent to those referred to in Article 2(2) of Council Framework Decision 2002/584/JHA******, if they are punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years.

---

* Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

** Council Regulation (EC) No 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals (OJ L 157, 15.6.2002, p. 1)

*** ***Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).*** **[Am. 49]**

**** Directive (EU) 2016/680 of the European parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

***** Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).

****** Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1)";

(5) Article 5 is replaced by the following:

"Article 5
Categories of data

1. Only the following categories of data shall be recorded in the VIS:

(a) alphanumeric data on the short stay visa applicant and on visas requested, issued, refused, annulled, revoked or extended referred to in Article 9(1) to (4) and Articles 10 to 14, alphanumeric data on long stay visa and residence permits issued, withdrawn, refused, annulled, revoked or extended referred to in Articles 22c, 22d, 22e and 22f, as well as information regarding the hits referred to in Articles 9a and 22b, and the results of verifications referred to in Article 9c(6);

(b) facial images referred to in Article 9(5) and Article 22c(2)(f);

(c) fingerprint data referred to in Article 9(6) ~~and~~**,** Article 22c(2)(g) ***and Article 22d(g)***; **[Am. 50]**

(ca) scans of the biographic data page of the travel document referred to in Article 9(7); **[Am. 51]**

(d) links to other applications referred to in Article 8(3) and (4) and Article 22a(3)."

2. The messages transmitted by the VIS, referred to in Article 16, Article 24(2) and Article 25(2), shall not be recorded in the VIS, without prejudice to the recording of data processing operations pursuant to Article 34.

3. The CIR shall contain the data referred to in Article 9(4)(a) to (cc), Article 9(5) and 9(6), Article 22c(2)(a), to (cc), (f) and (g), and Article 22d(a) to ~~(cc)~~***(c)***, (f) and (g). The remaining VIS data shall be stored in the VIS Central System." **[Am. 52]**

(6) the following Article 5a is inserted:

"Article 5a

List of recognised travel documents

~~(~~1~~)~~**.** The list of travel documents which entitle the holder to cross the external borders and which may be endorsed with a visa, as established by Decision No 1105/2011/EU of the European Parliament and of the Council*, shall be integrated in the VIS. **[Am. 53]**

~~(~~2~~)~~**.** The VIS shall provide the functionality for the centralised management of the list of recognised travel documents and of the no²tification of the recognition or non-recognition of the listed travel documents pursuant to Article 4 of Decision No 1105/2011/EU. **[Am. 54]**

~~(~~3~~)~~**.** The detailed rules on managing the functionality referred to in paragraph 2 shall be laid down in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 49(2). **[Am. 55]**

---

* Decision No 1105/2011/EU of the European Parliament and of the Council of 25 October 2011 on the list of travel documents which entitle the holder to cross the external borders and which may be endorsed with a visa and on setting up a mechanism for establishing this list (OJ L 287, 4.11.2011, p. 9).";

(7) Article 6 is amended as follows:

(-a) paragraph 1 is replaced by the following:

"1. Without prejudice to Article 22a, access to the VIS for entering, amending or deleting the data referred to in Article 5(1) in accordance with this Regulation shall be reserved exclusively to the duly authorised staff of the visa authorities. The number of duly authorised members of staff shall be strictly limited by the actual needs of their service."
[Am. 56]

(a) paragraph 2 is replaced by the following:

"2. Access to the VIS for consulting the data shall be reserved exclusively for the duly authorised staff of the national authorities of each Member State and of the EU bodies which are competent for the purposes laid down in Articles 15 to 22~~, Articles 22c to 22f~~, ***and*** Articles 22g to ~~22j~~ ***22l***, as well as for the purposes laid down in Articles 20 and 21 of [Regulation 2018/XX on interoperability ***(borders and visa)***].

The authorities entitled to consult or access VIS in order to prevent, detect and investigate terrorist offences or other serious criminal offences shall be designated in accordance with Chapter IIIb.

That access shall be limited to the extent that the data are required for the performance of their tasks in accordance with those purposes, and proportionate to the objectives pursued."; **[Am. 57]**

(aa) paragraph 3 is replaced by the following:

"3. Each Member State shall designate the competent authorities, the duly authorised staff of which shall have access to enter, amend, delete or consult data in the VIS. Each Member State shall without delay communicate to eu-LISA a list of these authorities, including those referred to in Article 29(3a), and any amendments thereto. That list shall specify for each authority, which data it may search and for what purposes.

eu-LISA shall ensure annual publication of the list and of lists of designated authorities referred to in Article 22k(2) and the central access points referred to in Article 22k(4) in the Official Journal of the European Union. eu-LISA shall maintain a continuously updated list on its website containing changes sent by Member States between the annual publications."; **[Am. 58]**

(b) the following paragraph 4 is added:

"4. The VIS shall provide the functionality for the centralised management of this list."

(c) the following paragraph 5 is added:

"5. ***The Commission shall adopt delegated acts in accordance with Article 48a concerning*** the detailed rules on managing the functionality for the centralised management of the list in paragraph 3 ~~shall be laid down in implementing acts~~. ~~Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 49(2).~~" **[Am. 59]**

(7a) In Article 7, paragraph 2 is replaced by the following:

"2. Processing of personal data within the VIS by each competent authority shall not result in discrimination against applicants, visa holders or applicants and holders of long-stay visas, and residence permits on the grounds of sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation. It shall fully respect human dignity and integrity and fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union, including the right to respect for one's private life and to the protection of personal data. Particular attention shall be paid to children, the elderly and persons with a disability and persons in need of international protection. The best interests of the child shall be a primary consideration."; **[Am. 60]**

(8) In Article 7 ~~a new paragraph 3 is inserted~~ ***the following paragraphs are added***:

"3. The best interests of the child shall ~~be a primary~~ ***take precedence over any other*** consideration for Member States with respect to all procedures provided for in this Regulation***, in full compliance with the International Convention on the Rights of the Child***. The child's well-being, safety and security, in particular where there is a risk of the child being a victim of human trafficking in human beings, and the views of the child shall be taken into consideration and given due weight in accordance with his or her age ~~and maturity~~."

[Am. 61]

3a. Member States shall apply this Regulation in full conformity with the Charter of Fundamental Rights of the European Union, in particular the right to human dignity, the right to liberty and security, the respect for private and family life, the protection of personal data, the right to asylum and protection of the principle of non-refoulement and protection in the event of removal, expulsion or extradition, the right to non-discrimination, the rights of the child and the right to an effective remedy."; **[Am. 62]**

(8a) The following Article is inserted:

"Article 7a

Fingerprint data of children

1. By way of derogation to Article 22c(2)(g) no fingerprints of children under the age of 6 shall be entered into VIS.

2. The biometric data of minors from the age of six shall be taken by officials trained specifically to take a minor's biometric data in a child-friendly and child-sensitive manner and in full respect of the best interests of the child and the safeguards laid down in the United Nations Convention on the Rights of the Child.

The minor shall be accompanied by, where present, an adult family member while his or her biometric data are taken. An unaccompanied minor shall be accompanied by a guardian, representative or, where a representative has not been designated, a person trained to safeguard the best interests of the minor and his or her general wellbeing, while his or her biometric data are taken. Such a trained person shall not be the official responsible for taking the biometric data, shall act independently and shall not receive orders either from the official or the service responsible for taking the biometric data. No form of force shall not be used against minors to ensure their compliance with the obligation to provide biometric data.

3. By way of derogation from Article 13(2) of Regulation (EC) No 810/2009 consulates shall not request that children between the age of 6 and 12 appear in person at the consulate for the collection of biometric identifiers where this would constitute an excessive burden and costs for families. In such cases, biometric identifiers shall be taken at the external borders where particular attention shall be paid to avoid child trafficking.

4. By way of derogation from the provisions on the use of data provided for in Chapters II, III, IIIa and IIIb fingerprint data of children may only be accessed for the following purposes:

(a) to verify the child's identity in the visa application procedure in accordance with Article 15 and at the external borders in accordance with Articles 18 and 22g and

(b) under Chapter IIIb to contribute to the prevention of and fight against abuses of children's right's, subject to all of the following conditions being satisfied:

(i) such access must be necessary for the purpose of the prevention, detection or investigation of child trafficking;

(ii) access is necessary in a specific case;

(iii) the identification is in the best interest of the child."; **[Am. 63]**

(9) The title of Chapter II is replaced by the following:

"ENTRY AND USE OF DATA ON ~~SHORY STAY~~ ***SHORT-STAY*** VISA BY VISA AUTHORITIES" **[Am. 64]**

(10) Article 8 is amended as follows:

(a) paragraph 1 is replaced by the following:

"1. When the application is admissible pursuant to Article 19 of Regulation (EC) No 810/2009, the visa authority shall create the application file within 2 working days, by entering the data referred to in Article 9 in the VIS, as far as those data are required to be provided by the applicant.";

(b) the following paragraph 1a is inserted:

"1a. Upon creation of the application file, the VIS shall automatically launch the query pursuant to Article 9a and return results.

(c) paragraph 5 is replaced by the following:

5. Where particular data are not required to be provided for legal reasons or factually cannot be provided, the specific data field(s) shall be marked as 'not applicable'. The absence of fingerprints should be indicated by "VIS0"; furthermore, the system shall permit a distinction to be made between the cases pursuant to Article 13(7)(a) to (d) of Regulation (EC) No 810/2009."

(11) Article 9 is amended as follows:

(a) in point 4, points (a), (b) and (c) are replaced by the following:

"(a) surname (family name); first name or names (given names); date of birth; nationality or nationalities; sex;

(aa) surname at birth (former surname(s)); place and country of birth; nationality at birth;

(b) the type and number of the travel document or documents and the three-letter code of the issuing country of the travel document or documents;

(c) the date of expiry of the validity of the travel document or documents;

(cc) the authority which issued the travel document and its date of issue;";

(b) point 5 is replaced by the following:

"5. the facial image of the applicant, in accordance with Article ~~13(1)~~ ***13*** of Regulation (EC) No 810/2009."; **[Am. 65]**

(ba) point 6 is replaced by the following:

"6. fingerprints of the applicant, in accordance with Article 13 of Regulation (EC) No 810/2009."; **[Am. 66]**

(c) the following point 7 is added:

"7. a scan of the biographic data page.";

(d) the following two paragraphs are added:

"~~8.~~ The facial image of third country nationals referred to in point 5 of the first paragraph shall have sufficient image resolution and quality to be used in automated biometric matching. ***If it lacks sufficient quality, the facial image shall not be used for automated matching.*** **[Am. 67]**

By way of derogation from the ~~second~~ ***first*** paragraph, in exceptional cases where the quality and resolution specifications set for the enrolment of the live facial image in the VIS cannot be met, the facial image may be extracted electronically from the chip of the electronic Machine Readable Travel Document (eMRTD). In such cases, the facial image shall only be inserted into the individual file after electronic verification that the facial image recorded in the chip of the eMRTD corresponds to the live facial image of the third-country national concerned."; **[Am. 68]**

(12) the following new Articles 9a to 9d are inserted:

"Article 9a

Queries to other systems

1. The application files shall be automatically processed by the VIS to identify hits. The VIS shall examine each application file individually.

2. When an application is created ~~or a visa is issued~~, the VIS shall check whether the travel document related to that application is recognised in accordance to Decision No 1105/2011/EU, by performing an automatic search against the list of recognised travel documents referred to in Article 5a, and shall return a result. **[Am. 69]**

3. For the purpose of the verifications provided for in Article 21(1) and Article 21(3)(a)~~, (c) and (d)~~ ***and (c)*** of Regulation (EC) No 810/2009, the VIS shall launch a query by using the European Search Portal defined in Article 6(1) [of the Interoperability Regulation ***(borders and visas)***] to compare the relevant data referred to in ~~point (4)~~ ***points (4), (5) and (6)*** of Article 9 of this Regulation ~~to the data present in a record, file or alert registered in the VIS, the Schengen Information System (SIS), the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS), including the watchlist referred to in Article 29 of Regulation (EU) 2018/XX for the purposes of establishing a European Travel Information and Authorisation System], the Eurodac, [the ECRIS-TCN system as far as convictions related to terrorist offences and other forms of serious criminal offences are concerned], the Europol data, the Interpol Stolen and Lost Travel Document database (SLTD) and the Interpol Travel Documents Associated with Notices database (Interpol TDAWN)~~***. VIS shall verify:***

(a) whether the travel document used for the application corresponds to a travel document reported lost, stolen, misappropriated or invalidated in SIS;

(b) whether the travel document used for the application corresponds to a travel document reported lost, stolen or invalidated in the SLTD database;

(c) whether the applicant is subject to a refusal of entry and stay alert in SIS;

(d) whether the applicant is subject to an alert in respect of persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes in SIS;

(e) whether the applicant and the travel document correspond to a refused, revoked or annulled travel authorisation in the ETIAS Central System and its holder;

(f) whether the applicant and the travel document are in the watch list referred to in Article 34 of Regulation (EU) 2018/1240 of the European Parliament and of the Council*;

(g) whether data on the applicant is already recorded in VIS;

(h) whether the data provided in the application concerning the travel document correspond to another application for a visa associated with different identity data;

(i) whether the applicant is currently reported as an overstayer or whether he or she has been reported as an overstayer in the past in the EES;

(j) whether the applicant is recorded as having been refused entry in the EES;

(k) whether the applicant has been subject to a decision to refuse, annul or revoke a short-stay visa recorded in VIS;

(l) whether the applicant has been subject to a decision to refuse, annul or revoke a long-stay visa, or residence permit recorded in VIS;

(m) whether data specific to the identity of the applicant are recorded in Europol data;

(n) whether the applicant for a short-stay visa is registered in Eurodac;

(o) in cases where the applicant is a minor, whether the applicant's holder of parental authority or legal guardian:

(i) is subject to an alert in respect of persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes in SIS;

(ii) is subject to a refusal of entry and stay alert entered in SIS;

(iii) holds a travel document contained in the watch list referred to in Article 34 of Regulation (EU) 2018/1240. **[Am. 70]**

3a. When querying SLTD, the data used by the user of the ESP to launch a query shall not be shared with the owners of Interpol data. **[Am. 71]**

4. The VIS shall add a reference to any hit obtained pursuant to paragraph 3 to the application file. Additionally, the VIS shall identify, where relevant, the Member State(s) that entered or supplied the data having triggered the hit(s) or Europol, and shall record this in the application file. ***No information other than the reference to any hit and the originator of the data shall be recorded.*** **[Am. 72]**

5. For the purposes of Article 2(1)(k), the queries carried out under paragraph 3 of this Article shall compare the relevant data referred to in Article 15(2) to the data present in the SIS in order to determine whether the applicant is subject to one of the following alerts:

(a) an alert in respect of persons wanted for arrest for surrender purposes or extradition purposes;

(b) an alert in respect of missing persons;

(c) an alert in respect of persons sought to assist with a judicial procedure;

(d) an alert on persons and objects for discreet checks***,*** ~~or~~ specific checks ***or inquiry checks***. **[Am. 73]**

5a. Any hit resulting from the queries pursuant to Article 9a(3)(a), (b), (c), (e), (g), (h), (i), (j), (k), (l) and (n) shall be assessed, where necessary following verification by the central authority in accordance with Article 9c, by the consulate where the visa application was lodged. **[Am. 74]**

5b. Any hit resulting from the queries pursuant to Article 9a(3)(d), (f),(m), and (o) shall be verified, where necessary, and assessed by the single point of contact of the Member States that entered or supplied the data having triggered the hits, in accordance with Article 9ca. **[Am. 75]**

5c. Any hit against SIS shall also be automatically notified to the SIRENE Bureau of the Member State that created the alert having triggered the hit.
[Am. 76]

5d. The notification provided to the SIRENE Bureau of the Member State or the single point of contact that entered the alert shall contain the following data:

(a) surname(s), first name(s) and, if any, alias(es);

(b) place and date of birth;

(c) sex;

(d) nationality and, if any, other nationalities;

(e) Member State of first intended stay, and if available, the address of first intended stay;

(f) the applicant's home address or, if not available, his or her city and country of residence;

(g) a reference to any hits obtained, including the date and time of the hit.
[Am. 77]

5e. ***This Article shall not impede the submission of an application for asylum on any grounds. If a visa application is submitted by a victim of violent crime such as domestic violence or trafficking in human beings committed by their sponsor, the file submitted to VIS shall be separated from that of the sponsor in order to protect the victims from further danger.*** **[Am. 78]**

---

* ***Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).***

Article 9b

Specific provisions applicable to the queries to other systems for family members of EU citizens or of other third country nationals enjoying the right of free movement under Union law

1. As regards third country nationals who are members of the family of a Union citizen to whom Directive 2004/38/EC applies or of a national of a third country enjoying the right of free movement equivalent to that of Union citizens under an agreement between the Union and its Member States, on the one hand, and a third country, on the other, the automated checks in Article 9a(3) shall be carried ~~our~~ ***out*** solely for the purpose of checking that there are no factual indications or reasonable grounds based on factual indications to conclude that the presence of the person on the territory of the Member States poses a risk to security ~~or high epidemic risk~~ in accordance with Directive 2004/38/EC. **[Am. 79]**

2. The VIS shall not verify whether:

   a) the applicant is currently reported as overstayer or whether he or she has been reported as overstayer in the past through consultation of the EES;

   b) the applicant corresponds to a person whose data is recorded in the Eurodac.

3. Where the automated processing of the application as referred to in Article 9a(3) has reported a hit corresponding to a refusal of entry and stay alert as referred to in Article 24 of Regulation ~~(EC) No 1987/2006~~ ***(EU) 2018/1861***, the visa authority shall verify the ground for the decision following which this alert was entered in the SIS. If this ground is related to an illegal immigration risk, the alert shall not be taken into consideration for the assessment of the application. The visa authority shall proceed according to Article ~~25(2) of the SIS II~~ ***26(2) of*** Regulation ***(EU) 2018/1861***. **[Am. 80]**

Article 9c

Verification by the central authorities ***and the national single point of contact***

[Am. 81]

1. Any hit ***as referred to in Article 9a(5b)*** resulting from the queries pursuant to Article 9a(3) ***which cannot automatically be confirmed by VIS*** shall be manually verified by ***the national single point of contact in accordance with Article 9ca.*** The central authority of the Member State processing the application ***shall be notified***. **[Am. 82]**

2. ~~Where~~ ***Any hit as referred to in Article 9a(5a) resulting from the queries pursuant to Article 9a(3) which cannot automatically be confirmed by VIS shall be manually verified by the central authority. When*** manually verifying the hits, the central authority shall have access to the application file and any linked application files, as well as to all the hits triggered during the automated processing pursuant to Article 9a~~(3)~~***(5a)***. **[Am. 83]**

3. The central authority shall verify whether the identity of the applicant recorded in the application file corresponds to the data present in the VIS, or one of the consulted databases.

4. Where the personal data do not correspond, and no other hit has been reported during the automated processing pursuant to Article 9a(3), the central authority shall erase the false hit from the application file.

5. Where the data correspond to or where doubts remain concerning the identity of the applicant, ***in justified cases*** the central visa authority processing the application shall inform the central authority of the other Member State(s), which were identified as having entered or supplied the data that triggered the hit pursuant to Article 9a(3). Where one or more Member States were identified as having entered or supplied the data that triggered such hit, the central authority shall consult the central authorities of the other Member State(s) using the procedure set out in Article 16(2). ***The applicant shall have the benefit of any doubt.*** **[Am. 84]**

6. The result of the verifications carried out by the central authorities of the other Member States shall be added to the application file.

~~7. By derogation from paragraph 1, where the comparison referred to in Article 9a(5) reports one or more hits, the VIS shall send an automated notification to the central authority of the Member State that launched the query to take any appropriate follow-up action.~~ **[Am. 85]**

~~8. Where Europol is identified as having supplied the data having triggered a hit in accordance with Article 9a(3), the central authority of the responsible Member State shall consult the Europol national unit for follow-up in accordance with Regulation (EU) 2016/794 and in particular its Chapter IV.~~

[Am. 86]

Article 9ca

Verification and assessment by the national single point of contact

1. Each Member State shall designate a national authority, operational 24 hours a day, 7 days a week, which shall ensure the relevant manual verifications and assessment of hits for the purposes of this Regulation ("the single point of contact"). The single point of contact shall be composed of liaison officers of SIRENE Bureau, Interpol National Central Bureaux, Europol national central point, ETIAS National Unit and all relevant national law enforcement authorities. Member States shall ensure sufficient staffing enabling the single point of contact to verify hits notified to it pursuant to this Regulation and taking into account the deadlines provided for in Article 23 of Regulation (EC) No 810/2009.

2. The single point of contact shall manually verify the hits referred to it. The procedures set out in Article 9c(2) to (6) shall apply.

3. Where following the verification referred to in paragraph 2 of this Article the data correspond and a hit is confirmed, the single point of contact shall contact, where necessary, the responsible authorities, including Europol, that provided the data having triggered the hit. It shall then assess the hit. The single point of contact shall provide a reasoned opinion in view of the decision on the application to be taken under Article 23 of Regulation (EC) No 810/2009. This reasoned opinion shall be included in the application file. **[Am. 87]**

Article 9cb

Manual

The Commission shall adopt a delegated act in accordance with Article 48a to lay down in a manual the relevant data to be compared in the queries of the other systems in accordance with Article 9a(3), and the procedures and rules necessary for these queries, verifications and assessments provided for in Articles 9a to 9ca. This delegated act shall include the combination of data categories for querying each system in accordance with Article 9a. **[Am. 88]**

Article 9d

Responsibilities of Europol

Europol shall adapt its information system to ensure that automatic processing of the queries referred to in Article 9a(3) and Article 22b(2) is possible."

(13) In Article 13, the following paragraph 4 is added:

"4. When the application file is updated pursuant to paragraphs 1 and 2, the VIS shall send a notification to the Member State that issued the visa, informing of the ***reasoned*** decision to annul or revoke that visa. Such notification shall be generated automatically by the central system and transmitted via the mechanism provided in Article 16."; **[Am. 89]**

(14) Article 15 is amended as follows:

(a) in paragraph 2, the following point (ea) is inserted:

"ea) facial image;";

(b) the following paragraph 2a is inserted:

“2a. The facial image referred to in point (ea) of paragraph 2 shall not be the only search criterion.”;

(15) In Article 16, paragraphs 2 and 3 are replaced by the following:

"2. When an application file is created in the VIS regarding a national of a specific third country or belonging to a specific category of such nationals for which prior consultation is requested pursuant to Article 22 of Regulation (EC) No 810/2009, the VIS shall automatically transmit the request for consultation to the Member State or the Member States indicated.

The Member State or the Member States consulted shall transmit their response to the VIS, which shall transmit that response to the Member State which created the application.

Solely for the purpose of carrying out the consultation procedure, the list of Member States requiring that their central authorities be consulted by other Member States' central authorities during the examination of visa applications for uniform visas lodged by nationals of specific third countries or specific categories of such nationals, according to Article 22 of Regulation (EC) No 810/2009, ~~and of the third country nationals concerned,~~ shall be integrated into the VIS." **[Am. 90]**

3. The procedure set out in paragraph 2 shall also apply to:

(a) the transmission of information pursuant to Article 25(4) on the issuing of visas with limited territorial validity, Article 24(2) on data amendments ***of this Regulation*** and Article 31 of Regulation (EC) No 810/2009 on ex post notifications; **[Am. 91]**

(b) all other messages related to consular cooperation that entail transmission of personal data recorded in the VIS or related to it, to the transmission of requests to the competent visa authority to forward copies of ~~travel documents pursuant to point 7 of Article 9 and other~~ documents supporting the application and to the transmission of electronic copies of those documents, as well as to requests pursuant to Article 9c and Article 38(3). The competent visa authorities shall respond to any such request within two working days."; **[Am. 92]**

(16) Article 17 is deleted;

(17) the title of Chapter III is replaced by the following:

"ACCESS TO SHORT STAY VISA DATA BY OTHER AUTHORITIES"

(18) In Article 18(6) the second subparagraph is replaced by the following:

"The competent authorities for carrying out checks at borders at which the EES is operated shall verify the fingerprints of the visa holder against the fingerprints recorded in the VIS. For visa holders whose fingerprints cannot be used, the search mentioned under paragraph 1 shall be carried out with the alphanumeric data foreseen under paragraph 1 in combination with the facial image.";

(18a) Article 18a is replaced by the following:

"Article 18a
Retrieval of VIS data for creating or updating an entry/exit record or a refusal of entry record of a visa holder in the EES

Solely for the purpose of creating or updating an entry/exit record or a refusal of entry record of a visa holder in the EES in accordance with Article14(2) and Articles 16 and 18 of Regulation (EU) 2017/2226, the competent authority for carrying out checks at borders at which the EES is operated shall be given access to retrieve from the VIS and import into the EES the data stored in the VIS and listed in point (d) of Article 16(1) and points (c) to (f) of Article 16(2) of that Regulation." **[Am. 93]**

(19) the following Article 20a is inserted:

″Article 20a

Use of VIS data for the purpose of entering SIS alerts on missing persons ***or vulnerable persons who need to be prevented from travelling*** and the subsequent access to those data **[Am. 94]**

1. Fingerprint data ***and facial images*** stored in the VIS may be used for the purpose of entering an alert on missing persons***, children at risk of abduction or vulnerable persons who need to be prevented from travelling*** in accordance with Article 32~~(2)~~ of Regulation (EU) … of the European Parliament and of the Council* [Regulation (EU) on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters]. In those cases, the exchange of fingerprint data ***and facial images*** shall take place via secured means to the SIRENE bureau of the Member State owning the data. **[Am. 95]**

2. Where there is a hit against a SIS alert ***through the use of fingerprint data and facial images stored in VIS*** as referred to in paragraph 1, child protection authorities and national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charge and their coordinating authorities, as referred to *in Article ~~43~~ **44** of* Regulation (EU) … [COM(2016)0883 – SIS ~~LE~~ ***(police cooperation)***], may request ***from an authority with access to VIS***, in the performance of their tasks, access to the data entered in VIS. The conditions provided for in Union and national legislation shall apply. ***Member States shall ensure that the data are transmitted in a secure manner.*** **[Am. 96]**

---

* Regulation (EU) .. of the European Parliament and of the Council of … (OJ L .., p. …).";

(20) in Article 22, ~~paragraph~~ ***paragraphs 1 and*** 2 ~~is~~ ***are*** replaced by the following:

"***1. For the sole purpose of examining an application for asylum, the competent asylum authorities shall have access in accordance with Article 21 of Regulation (EC) No 343/2003 to search with the fingerprints of the asylum seeker. Where the fingerprints of the asylum seeker cannot be used or the search with the fingerprints fails, the search shall be carried out with the data referred to in Article 9(4)(a) and/or (b) to (cc); this search may be carried out in combination with the data referred to in Article 9(4)(aa).*** **[Am. 97]**

2. If the search with the data listed in paragraph 1 indicates that data on the applicant for international protection is recorded in the VIS, the competent asylum authority shall have access to consult the following data of the applicant and of any linked application files of the applicant pursuant to Article 8(3), for the sole purpose referred to in paragraph 1:

(a) the application number;

(b) the data taken from the application form(s), referred to in points (4), (5) and (7) of Article 9*;*

(c) ~~photographs~~ ***facial images***; **[Am. 98]**

(d) the data entered in respect of any visa issued, annulled, revoked, or whose validity is extended, referred to in Articles 10, 13 and 14;

(e) the data referred to in ~~points~~ ***point*** (4) ~~and (5)~~ of Article 9 of the linked application files pursuant to Article 8(4)."; **[Am. 99]**

(21) Article 23 is replaced by the following:

"Article 23

Retention period for data storage

1. Each ***application*** file shall be stored in the VIS for a maximum of five years, without prejudice to the deletion referred to in Articles 24 and 25 and to the keeping of records referred to in Article 34. **[Am. 100]**

That period shall start:

(a) on the expiry date of the visa, the long-stay visa or *the residence permit*, if a visa, a long-stay visa *or a residence permit* has been issued;

(b) on the new expiry date of the visa~~,~~ ***or*** the long-stay visa ~~or the residence permit~~, if a visa~~,~~ ***or*** a long-stay visa ~~or a residence permit~~ has been extended; **[Am. 101]**

(c) on the date of the creation of the application file in the VIS, if the application has been withdrawn, closed or discontinued;

(d) on the date of the decision of the responsible authority if a visa, a long-stay visa or a residence permit has been refused, annulled, shortened, withdrawn or revoked, as applicable.

2. Upon expiry of the period referred to in paragraph 1, the VIS shall automatically erase the file and the link(s) to this file as referred to in Article 8(3) and (4) and Article ~~22a~~ 22a(3) ~~and (5)~~."; **[Am. 102]**

2a. By way of derogation from paragraph 1:

(a) application files pertaining to a residence permit shall be deleted after a maximum period of 10 years;

(b) application files pertaining to children below the age of 12 shall be deleted upon the child exiting the Schengen area. **[Am. 103]**

2b. By way of derogation from paragraph 1, for the purpose of facilitating a new application the application file referred therein may be stored for an additional period of no more than three years from the end of the validity period of the long-stay visa or residence permit and only where, following a request for consent, the applicant freely and explicitly consents by means of a signed declaration. Requests for consent shall be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form and using clear and plain language, in accordance with Article 7 of Regulation (EU) 2016/679. The applicant may withdraw his or her consent at any time, in accordance with Article 7(3) of Regulation (EU) 2016/679. If the applicant withdraws consent, the application file shall automatically be erased from VIS.

eu-LISA shall develop a tool to enable applicants to give and withdraw their consent.

The Commission shall adopt delegated acts in accordance with Article 48a to further define the tool to be used by the applicants to give and withdraw their consent."; **[Am. 104]**

(22) in Article 24, ~~paragraph~~ ***paragraphs*** 2 ***and 3*** ~~is~~ ***are*** replaced by the following:

"2. If a Member State has evidence to suggest that data processed in the VIS are inaccurate or that data were processed in the VIS contrary to this Regulation, it shall inform the Member State responsible immediately. Such message shall be transmitted in accordance with the procedure in Article 16(3).

Where the inaccurate data refers to links created pursuant to Article 8(3) or (4), and Article 22a(3), the responsible Member State shall make the necessary verifications and provide an answer within 48 hours, and, as the case may be, rectify the link. If no answer is provided within the set timeframe, the requesting Member State shall rectify the link and notify the responsible Member State of the rectification made via VISMail.

3. The Member State responsible shall, as soon as possible, check the data concerned and, if necessary, correct or delete them immediately."; **[Am. 105]**

(23) Article 25 is amended as follows:

(a) paragraph 1 is replaced by the following:

"1. Where, before expiry of the period referred to in Article 23(1), an applicant has acquired the nationality of a Member State, the application files, the files and the links referred to in Article 8(3) and (4)~~,~~ ***and in*** Article 22a(3) relating to him or her shall be erased without delay from the VIS by the Member State which created the respective application file(s) and links."; **[Am. 106]**

(b) in paragraph 2, the words "infrastructure of the VIS" are replaced by "the VISMail".

(23a) Article 26 is amended as follows:

(a) paragraphs 1 and 2 are replaced by the following:

"1. eu-LISA shall be responsible for the operational management of VIS and its components as set out in Article 2a. It shall ensure, in cooperation with the Member States, that at all times the best available technology, subject to a cost-benefit analysis, is used for those components. **[Am. 107]**

2. Operational management of VIS shall consist of all the tasks necessary to keep VIS functioning 24 hours a day, 7 days a week in accordance with this Regulation, in particular the maintenance work and technical developments necessary to ensure that VIS functions at a satisfactory level of operational quality, in particular as regards the response time for queries of the VIS Central System by consular posts and border authorities. Such response times shall be as short as possible.";
[Am. 108]

(b) paragraphs 3 to 8 are deleted; **[Am. 109]**

~~(24) in Article 26, the following paragraph 8a is inserted:~~

~~"8a. Eu-LISA shall be permitted to use anonymised real personal data of the VIS production system for testing purposes in the following circumstances:~~

~~(a) for diagnostics and repair when faults are discovered with the Central System;~~

~~(b) for testing new technologies and techniques relevant to enhance the performance of the Central System or transmission of data to it.~~

~~In such cases, the security measures, access control and logging activities at the testing environment shall be equal to the ones for the VIS production system. Real personal data adopted for testing shall be rendered anonymous in such a way that the data-subject is no longer identifiable.";~~ **[Am. 110]**

(c) the following paragraphs are added:

"9a. Where eu-LISA cooperates with external contractors in any VIS-related tasks, it shall closely monitor the activities of the contractor to ensure compliance with this Regulation, in particular on security, confidentiality and data protection.

9b. The operational management of the VIS Central System shall not been trusted to private companies or private organisations.";

[Am. 111]

(25) Article 27 is replaced by the following:

"Article 27

Location of the central Visa Information System

The principal central VIS, which performs technical supervision and administration functions, shall be located in Strasbourg (France) and a back-up central VIS, capable of ensuring all functionalities of the principal central VIS, shall be located in Sankt Johann im Pongau (Austria).

~~Both sites may be used simultaneously for active~~ ***eu-LISA shall implement technical solutions to ensure the uninterrupted availability of VIS either through the simultaneous*** operation of ~~the~~ VIS ***Central System and the backup VIS Central System,*** provided that the ~~second site~~ ***backup VIS Central System*** remains capable of ensuring ~~its~~ ***the*** operation ~~in case~~ of ***VIS in the event of a*** failure ***of VIS Central System, or through duplication*** of the system ***or its components***."; **[Am. 112]**

(26) Article 29 is amended as follows:

(a) the title is replaced by the following:

"Responsibility for the use and quality of data";

(b) ~~in~~ paragraph 1~~,~~ ***is amended as follows:***

(i) point (c) is replaced by the following:

"(c) the data are accurate, up-to-date and of an adequate level of quality and completeness when they are transmitted to the VIS.";

(ii) the following subparagraph is added:

"For this purpose, Member States shall ensure that consular staff and the staff of any external service provider with which they are cooperating as referred to in Article 43 of Regulation (EC) No 810/2009 receive regular training on data quality."; **[Am. 113]**

(c) in point (a) of paragraph 2, the word "VIS" is replaced by the words "VIS or the CIR" in both instances where it appears;

(d) the following ~~paragraph 2a is~~ ***paragraphs are*** inserted:

"2a. ~~The management authority~~ ***eu-LISA*** together with the Commission shall develop***,*** ~~and~~ maintain ***and continuously upgrade*** automated data quality control mechanisms and procedures for carrying out quality checks on the data in VIS and shall provide regular reports to the Member States. ~~The management authority~~ ***eu-LISA shall ensure adequate levels of professionally trained staff to implement the technical innovations and upgrades required to operate the data quality control mechanisms. eu-LISA*** shall provide a regular report to the Member states and Commission on the data quality controls. ***The Commission shall provide the European Parliament and the Council with a regular report on data quality issues that are encountered and how they were addressed.***
[Am. 114]

This mechanism, procedures and the interpretation of data quality compliance shall be established by means of implementing measures in accordance with the procedure referred to in Article 49(2).

2b. The Commission shall present a report to the European Parliament and to the Council on the feasibility, availability, readiness and reliability of the required technology to use facial images to identify a person."; **[Am. 115]**

(da) the following paragraph is added:

"3a. In relation to the processing of personal data in VIS, each Member State shall designate the authority which is to be considered as controller in accordance with point (7) of Article 4 of Regulation (EU) 2016/679 and which shall have central responsibility for the processing of data by that Member State. Each Member State shall notify the Commission of the designation."; **[Am. 116]**

(27) the following Article 29a is inserted:

"Article 29a

Specific rules for entering data

1. Entering data referred to in Articles 9, 22c and 22d into the VIS shall be subject to the following preliminary conditions:

   (a) data pursuant to Articles 9, 22c and 22d and Article 6(4) may only be ~~sent~~ ***entered*** to the VIS following a quality check performed by the responsible national authorities; **[Am. 117]**

   (b) data pursuant to Articles 9, 22c and 22d and Article 6(4) will be processed by the VIS, following a quality check performed by the VIS pursuant to paragraph 2.

2. Quality checks shall be performed by VIS, as follows:

   (a) when creating application files or files of third country nationals in VIS, quality checks shall be performed on the data referred to in Articles 9, 22c and 22d ; should these checks fail to meet the established quality criteria, the responsible authority(ies) shall be automatically notified by the VIS;

(b) the automated procedures pursuant to Article ~~9(a)(3)~~ ***9a(3)*** and 22b(2) may be triggered by the VIS only following a quality check performed by the VIS pursuant to this Article; should these checks fail to meet the established quality criteria, the responsible authority(ies) shall be automatically notified by the VIS; **[Am. 118]**

(c) quality checks on facial images and dactylographic data shall be performed when creating application files of third country nationals in VIS, to ascertain the fulfilment of minimum data quality standards allowing ***for*** biometric matching; **[Am. 119]**

(d) quality checks on the data pursuant to Article 6(4) shall be performed when storing information on the national designated authorities in the VIS.

3. Quality standards shall be established for the storage of the data referred to in paragraph 1 and 2 of this Article. The specification of these standards shall be laid down in implementing acts. Those implementing acts shall be adopted ~~.~~ in accordance with the examination procedure referred to in Article 49(2).”; **[Am. 120]**

~~(28) in Article 31, paragraphs 1 and 2 are replaced by the following:~~

~~"1. Without prejudice to Regulation (EU) 2016/679, the data referred to in Article 9(4)(a), (b), (c), (k) and (m); 9(6) and 9(7) may be transferred or made available to a third country or to an international organisation listed in the Annex, only if necessary in individual cases for the purpose of proving the identity of third-country nationals, and only for the purpose of return in accordance with Directive 2008/115/EC or of resettlement in accordance with the Regulation …[Resettlement Framework Regulation], and provided that the Member State which entered the data in the VIS has given its approval.";~~

[Am. 121]

(28a) Article 31 is amended as follows:

(a) paragraphs 2 and 3 are replaced by the following:

"2. By way of derogation from paragraph 1 of this Article, the data referred to in Article 9(4)(a), (aa), (b), (c), (cc), (k) and (m), (6) and (7) may be transferred by border authorities or immigration authorities to a third country or to an international organisation listed in the Annex to this Regulation in individual cases, if necessary in order to prove the identity of third-country nationals for the sole purpose of return, only where one of the following conditions is satisfied:

(a) the Commission has adopted a decision on the adequate protection of personal data in that third country in accordance with Article 45(3) of Regulation (EU) 2016/679;

(b) appropriate safeguards as referred to in Article 46 of Regulation (EU) 2016/679 have been provided, such as through a readmission agreement which is in force between the Union or a Member State and the third country in question; or

(c) point (d) of Article 49(1) of Regulation (EU) 2016/679, applies.

[Am. 122]

3. The data referred to in Article 9(4)(a), (b), (c), (k) and (m), (6) and (7) may be transferred in accordance with paragraph 2 of this Article only where all of the following conditions are satisfied:

(a) the transfer of the data is carried out in accordance with the relevant provisions of Union law, in particular provisions on data protection, including Chapter V of Regulation (EU) 2016/679, and readmission agreements, and the national law of the Member State transferring the data;

(b) the Member State which entered the data in the VIS has given its approval;

(c) the third country or international organisation has agreed to process the data only for the purposes for which they were provided; and

(d) a return decision adopted pursuant to Directive 2008/115/EC has been issued in relation to the third-country national concerned, provided that the enforcement of such a return decision is not suspended and provided that no appeal has been lodged which may lead to the suspension of its enforcement."; **[Am. 123]**

(b) the following paragraphs are added:

"3a. Transfers of personal data to third countries or to international organisations pursuant to paragraph 2 shall not prejudice the rights of applicants for and beneficiaries of international protection, in particular as regards non-refoulement.

3b. Personal data obtained from the VIS by a Member State or by Europol for law enforcement purposes shall not be transferred or made available to any third country, international organisation or private entity established in or outside the Union. The prohibition shall also apply where those data are further processed at national level or between Member States pursuant to Directive (EU) 2016/680."; **[Am. 124]**

(28b) in Article 32, paragraph 2 is amended as follows:

(a) the following point is inserted:

"(ea) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment;"; **[Am. 125]**

(b) the following points are inserted:

"(ja) ensure that, in the event of an interruption, installed systems can be restored to normal operation;

(jb) ensure reliability by making sure that any faults in the functioning of VIS are properly reported and that the necessary technical measures are put in place to ensure that personal data can be restored in the event of corruption due to a malfunctioning of VIS;"; **[Am. 126]**

(28c) the following Article is inserted:

"Article 32a

Security incidents

1. *Any event that has or may have an impact on the security of VIS or may cause damage or loss to VIS data shall be considered to be a security incident, especially where unlawful access to data may have occurred or where the availability, integrity and confidentiality of data has or may have been compromised.*

2. *Security incidents shall be managed in a way as to ensure a quick, effective and proper response.*

3. *Without prejudice to the notification and communication of a personal data breach pursuant to Article 33 of Regulation (EU) 2016/679 or to Article 30 of Directive (EU) 2016/680, Member States, Europol and the European Border and Coast Guard Agency shall notify the Commission, eu-LISA, the competent supervisory authority and the European Data Protection Supervisor without delay of security incidents. eu-LISA shall notify the Commission and the European Data Protection Supervisor without delay of any security incident concerning the VIS Central System.*

4. ***Information regarding a security incident that has or may have an impact on the operation of VIS in a Member State or, within eu-LISA, on the availability, integrity and confidentiality of the data entered or sent by other Member States, shall be provided to all Member States without delay and reported in compliance with the incident management plan provided by eu-LISA.***

5. ***The Member States and eu-LISA shall collaborate in the event of a security incident.***

6. ***The Commission shall report serious incidents to the European Parliament and to the Council immediately. These reports shall be classified as EU RESTRICTED/RESTREINT UE in accordance with applicable security rules.***

7. ***Where a security incident is caused by the misuse of data, Member States, Europol and the European Border and Coast Guard Agency shall ensure that penalties are imposed in accordance with Article 36.";*** **[Am. 127]**

(28d) Article 33 is replaced by the following:

"Article 33

Liability

1. Without prejudice to the right to compensation from, and liability of the controller or processor under Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EU) 2018/1726:

(a) any person or Member State that has suffered material damage as a result of an unlawful personal data processing operation or any other act incompatible with this Regulation by a Member State shall be entitled to receive compensation from that Member State;

(b) any person or Member State that has suffered material or non-material damage as a result of any act by Europol, the European Border and Coast Guard Agency or eu-LISA incompatible with this Regulation shall be entitled to receive compensation from the agency in question.

The Member State concerned, Europol, the European Border and Coast Guard Agency or eu-LISA shall be exempted from their liability under the first subparagraph, in whole or in part, if they prove that they are not responsible for the event which gave rise to the damage.

2. ***If any failure of a Member State to comply with its obligations under this Regulation causes damage to the VIS Central System, that Member State shall be held liable for such damage, unless and insofar as eu-LISA or another Member State participating in the VIS Central System failed to take reasonable measures to prevent the damage from occurring or to minimise its impact.***

3. ***Claims for compensation against a Member State for the damage referred to in paragraphs 1 and 2 shall be governed by the national law of that Member State. Claims for compensation against the controller, Europol, the European Border and Coast Guard Agency or eu-LISA for the damage referred to in paragraphs 1 and 2 shall be subject to the conditions provided for in the Treaties.";*** **[Am. 128]**

(29) Article 34 is replaced by the following:

"Article 34

Keeping of logs

1. Each Member State, the European Border and Coast Guard Agency and ~~the Management Authority~~ ***eu-LISA*** shall keep logs of all data processing operations within the VIS. These logs shall show the purpose of access referred to in Article 6(1), Article 20a(1), Article 22k(1) and Articles 15 to 22 and 22g to 22j, the date and time, the type of data transmitted as referred to in Articles 9 to 14 ***and 22c to 22f***, the type of data used for interrogation as referred to in Article 15(2), Article 18, Article 19(1), Article 20(1), Article 21(1), Article 22(1), Article 22g, Article 22h, Article 22i, Article 22j, Article 45a, and Article 45d and the name of the authority entering or retrieving the data. In addition, each Member State shall keep logs of the staff duly authorised to enter or retrieve the data. **[Am. 129]**

2. For the operations listed in Article 45b a log of each data processing operation carried out within the VIS and the EES shall be kept in accordance with ~~this~~ ***that*** Article and Article ~~41~~ ***46*** of the Regulation (EU) 2017/2226 establishing an Entry/Exit System (EES). ***For the operations listed in Article 17a, a record of each data processing operation carried out in VIS and the EES shall be kept in accordance with this Article and Article 46 of Regulation (EU) 2017/2226.*** **[Am. 130]**

3. Such logs may be used only for the data-protection monitoring of the admissibility of data processing as well as to ensure data security. The logs shall be protected by appropriate measures against unauthorised access and deleted after a period of one year after the retention period referred to in Article 23(1) has expired, if they are not required for monitoring procedures which have already begun.";

(29a) ***Article 35 is replaced by the following:***

"Article 35

Self-monitoring

Member States shall ensure that each authority entitled to access VIS data takes the measures necessary to comply with this Regulation and cooperates with the National Supervisory Authority."; **[Am. 131]**

(29b) ***Article 36 is replaced by the following:***

"Article 36

Penalties

Member States shall take the necessary measures to ensure that any misuse or processing of data entered in VIS contrary to this Regulation is punishable by penalties, including administrative and/or criminal penalties in accordance with national law, that are effective, proportionate and dissuasive."; **[Am. 132]**

(30) Article 37 is amended as follows:

(a) ~~in~~ paragraph 1~~,~~ ***is amended as follows:***

(i) the introductory sentence ~~1~~ is replaced by the following:

"***1. Without prejudice to the right to information referred to in Articles 15 and 16 of Regulation(EU) 2018/1725, Articles 13 and 14 of Regulation(EU) 2016/679, and Article 13 of Directive (EU) 2016/680,*** third country nationals and the persons referred to in Articles 9(4)(f), 22c(2)(e) or 22d(e) shall be informed of the following by the Member State responsible:"; **[Am. 133]**

(ii) point (f) is replaced by the following:

"(f) the existence of the right of access to data relating to them, and the right to request that inaccurate data relating to them be corrected or that unlawfully processed data relating to them be deleted, including the right to receive information on the procedures for exercising those rights and about the contact details of the European Data Protection Supervisor and of the national supervisory authority of the Member State responsible for the collection of the data referred to in Article 41(1), which shall hear claims concerning the protection of personal data;"; [Am. 134]

(iii) the following point is added:

"(fa) the fact that VIS may be accessed by the Member States and Europol for law enforcement purposes."; **[Am. 135]**

(b) paragraph 2 is replaced by the following:

"2. The information referred to in paragraph 1 shall be provided ***clearly, concisely and accurately*** in writing to the third country national when the data, the ~~photograph~~ ***facial image*** and the fingerprint data as referred to in points (4), (5) and (6) of Article 9, Article 22c(2) and Article 22d (a) to (g) are collected~~, and where necessary, orally, in a language and manner that the data subject understands or is reasonably presumed to understand~~. Children must be informed in an age-appropriate manner, using leaflets and/or infographics and/or demonstrations specifically designed to explain the fingerprinting procedure."; **[Am. 136]**

(c) in paragraph 3, the second subparagraph is replaced by the following:

"In the absence of such a form signed by those persons this information shall be provided in accordance with Article 14 of Regulation (EU) 2016/679.";

~~(31) in Article 38, paragraph 3 is replaced by the following:~~

~~"3. If the request as provided for in paragraph 2 is made to a Member State other than the Member State responsible, the authorities of the Member State with which the request was lodged shall contact the authorities of the Member State responsible within a period of seven days. The Member State responsible shall check the accuracy of the data and the lawfulness of their processing in the VIS within a period of one month.";~~ **[Am. 137]**

(31a) Article 38 is replaced by the following:

"Article 38

Right of access to, of rectification, of completion, of erasure of personal data and of restriction of processing

1. Without prejudice to the right to information under Articles 15 and 16 of Regulation (EU) 2018/1725, applicants or holders of long-stay visa or residence permits whose data are stored in VIS shall be informed, at the time their data are collected, of the procedures for exercising the rights under Articles 17 to 20 of Regulation (EU) 2018/1725 and Articles 15 to 18 of Regulation (EU) 2016/679. They shall be provided with the contact details of the European Data Protection Supervisor at the same time.

2. In order to exercise their rights under Articles 17 to 20 of Regulation (EU) 2018/1725 and Articles 15 to 18 of Regulation (EU) 2016/679, the persons referred to in paragraph 1 shall have the right to address themselves to the Member State which entered their data into VIS. The Member State that receives the request shall examine and reply to it as soon as possible, and at the latest within 30 days. Where in response to a request, it is found that the data stored in VIS are factually inaccurate or have been recorded unlawfully, the Member State responsible shall rectify or erase those data in VIS without delay and at the latest within 30 days of receipt of the request in line with Article 12(3) and (4) of Regulation (EU) 2016/679. If the request is made to a Member State other than the Member State responsible, the authorities of the Member State with which the request was lodged shall contact the authorities of the Member State responsible within a period of seven days. The Member State responsible shall check the accuracy of the data and the lawfulness of their processing in VIS within a period of one month. The persons concerned shall be informed by Member State which contacted the authority of the Member State responsible that his or her request was forwarded, to whom and about the further procedure.

3. ***Where the Member State responsible does not agree with the claim that data stored in VIS are factually inaccurate or have been recorded unlawfully, it shall adopt without delay an administrative decision explaining in writing to the person concerned why it is not prepared to rectify or erase data relating to him or her.***

4. ***That decision shall also provide the person concerned with information explaining the possibility to challenge the decision taken in respect of the request referred to in paragraph 2 and, where relevant, information on how to bring an action or a complaint before the competent authorities or courts and any assistance available to the person, including from the competent national supervisory authorities.***

5. ***Any request made pursuant to paragraph 2 shall contain the necessary information to identify the person concerned. That information shall be used exclusively to enable the exercise of the rights referred to in paragraph 2.***

6. The Member State responsible shall keep a record in the form of a written document that a request referred to in paragraph 2 was made and how it was addressed. It shall make that document available to the competent national data protection supervisory authorities without delay, and not later than seven days following the decision to rectify or erase data referred to in the second subparagraph of paragraph 2 or following the decision referred to in paragraph 3 respectively."; **[Am. 138]**

(31b) Article 39 is replaced by the following:

"Article 39

Cooperation to ensure the rights on data protection

1. The competent authorities of the Member States shall cooperate actively to enforce the rights laid down in Article 38.

2. In each Member State, the supervisory authority referred to in Article 51(1) of Regulation (EU) 2016/679 shall, upon request, assist and advise the data subject in exercising his or her right to rectify, complete or erase personal data relating to him or her or to restrict the processing of such data in accordance with Regulation (EU) 2016/679.

In order to achieve the aims referred to in the first subparagraph, the supervisory authority of the Member State responsible which transmitted the data and the supervisory authority of the Member State to which the request has been made shall cooperate with each other."; **[Am. 139]**

(31c) Article 40 is replaced by the following:

"Article 40
Remedies

1. Without prejudice to Articles 77 and 79 of Regulation (EU) 2016/679, in each Member State any person shall have the right to bring an action or a complaint before the competent authorities or courts of that Member State which refused the right of access to, or right of rectification, completion or erasure of data relating to him or her provided for in Article 38 of this Regulation. The right to bring such an action or complaint shall also apply in cases where requests for access, rectification, completion or erasure were not responded to within the deadlines provided for in Article 38 or were never dealt with by the data controller.

2. The assistance of the supervisory authority referred to in Article 51(1) of Regulation (EU) 2016/679 shall remain available throughout the proceedings."; **[Am. 140]**

(31d) Article 41 is replaced by the following:

"Article 41

Supervision by the National Supervisory Authority

1. *Each Member State shall ensure that the supervisory authority referred to in Article 51(1) of Regulation (EU) 2016/679 independently monitors the lawfulness of the processing of personal data pursuant to this Regulation by the Member State concerned.*

2. *The supervisory authority or authorities referred to in Article 51(1) of Regulation (EU) 2016/679 shall ensure that an audit of the data processing operations by the responsible national authorities is carried out in accordance with relevant international auditing standards at least every three years. The results of the audit may be taken into account in the evaluations conducted under the mechanism established by Council Regulation (EU) No 1053/2013. The supervisory authority referred to in Article 51(1) of Regulation (EU) 2016/679 shall publish annually the number of requests for rectification, completion or erasure, or restriction of processing of data, the action subsequently taken and the number of rectifications, completions, erasures and restrictions of processing made in response to requests by the persons concerned*.

3. Member States shall ensure that their supervisory authority has sufficient resources to fulfil the tasks entrusted to it under this Regulation and has access to advice from persons with sufficient knowledge of biometric data.

4. Member States shall supply any information requested by the supervisory authority referred to in Article 51(1) of Regulation (EU) 2016/679 and shall, in particular, provide it with information on the activities carried out in accordance with its responsibilities as laid down in this Regulation. Member States shall grant the supervisory authority referred to in Article 51(1) of Regulation (EU) 2016/679 access to their logs and allow it access at all times to all their interoperability related premises."; **[Am. 141]**

(31e) Article 42 is replaced by the following:

"Article 42

Supervision by the European Data Protection Supervisor

1. The European Data Protection Supervisor shall be responsible for monitoring the personal data processing activities of eu-LISA, Europol and the European Border and Coast Guard Agency under this Regulation and for ensuring that such activities are carried out in accordance with Regulation (EU) 2018/1725 and with this Regulation.

2. The European Data Protection Supervisor shall ensure that an audit of eu-LISA's personal data processing activities is carried out in accordance with relevant international auditing standards at least every three years. A report of that audit shall be sent to the European Parliament, the Council, eu-LISA, the Commission and the Member States. eu-LISA shall be given an opportunity to make comments before the reports are adopted.

3. eu-LISA shall supply information requested by the European Data Protection Supervisor, give the European Data Protection Supervisor access to all documents and to its logs referred to in Articles 22r, 34 and 45b and allow the European Data Protection Supervisor access to all its premises at any time."; **[Am. 142]**

~~(32) in Article 43, paragraphs 1 and 2 are replaced by the following:~~

~~"1. The European Data Protection Supervisor shall act in close cooperation with national supervisory authorities with respect to specific issues requiring national involvement, in particular if the European Data Protection Supervisor or a national supervisory authority finds major discrepancies between practices of Member States or finds potentially unlawful transfers using the communication channels of the interoperability components, or in the context of questions raised by one or more national supervisory authorities on the implementation and interpretation of this Regulation.~~

~~2. In the cases referred to in paragraph 1, coordinated supervision shall be ensured in accordance with Article 62 of Regulation (EU) XXXX/2018 [revised Regulation (EC) No 45/2001].";~~ **[Am. 143]**

(32a) Article 43 is replaced by the following:

"Article 43

Cooperation between National Supervisory Authorities and the European Data Protection Supervisor

1. *The supervisory authorities and the European Data Protection Supervisor shall, each acting within the scope of their respective competences, cooperate actively within the framework of their respective responsibilities to ensure coordinated supervision of the interoperability components and the other provisions of this Regulation.*

2. *The European Data Protection Supervisor and the supervisory authorities shall exchange relevant information, assist each other in carrying out audits and inspections, examine any difficulties concerning the interpretation or application of this Regulation, assess problems in the exercise of independent supervision or in the exercise of the rights of the data subject, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary.*

3. For the purpose of paragraph 2, the supervisory authorities and the European Data Protection Supervisor shall meet at least twice a year within the framework of the European Data Protection Board. The costs of those meetings shall be borne by and their organisation shall be undertaken by the European Data Protection Board. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary.

4. A joint report of activities shall be sent by the European Data Protection Board to the European Parliament, to the Council, to the Commission, to Europol, to the European Border and Coast Guard Agency and to eu-LISA every two years. That report shall include a chapter on each Member State prepared by the supervisory authority of that Member State."; **[Am. 144]**

(32b) Article 44 is deleted; **[Am. 145]**

(33) in Article 45**,** the following ~~paragraph 3 is~~ ***paragraphs are*** added:

"2a. The measures necessary for the development of the VIS Central System, the national interface in each Member State, and the communication infrastructure between the VIS Central System and the national interfaces concerning the following matters shall be adopted in accordance with the procedure referred to in Article 49(2):

(a) the design of the physical architecture of the system including its communication network;

(b) technical aspects which have a bearing on the protection of personal data;

(c) technical aspects which have serious financial implications for the budgets of the Member States or which have serious technical implications for the national systems of the Member States;

(d) the development of security requirements, including biometric aspects. **[Am. 146]**

~~"~~3. The technical specifications for the quality, resolution and use of fingerprints and of the facial image for biometric verification and identification in the VIS shall be laid down in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 49(2).";

(34) the following Article 45a is inserted:

"Article 45a

Use of data for reporting and statistics

1. The duly authorised staff of the competent authorities of Member States, the Commission, eu-LISA and the European Border and Coast Guard Agency established by Regulation (EU) 2016/1624 shall have access to consult the following data, solely for the purposes of reporting and statistics without allowing for individual identification ***as a result of the data being completely anonymous***: **[Am. 147]**

(a) status information;

(b) the competent authority, including its location;

(c) sex, ~~date~~ ***year*** of birth and current nationality of the applicant; **[Am. 148]**

(d) Member State of first entry, only as regards short stay visas;

(e) date and place of the application and the decision concerning the application (issued or refused);

(f) the type of document issued, i.e. whether ATV, uniform or LTV, long stay visa or residence permit;

(g) the type of the travel document and the three letter code of the issuing country, only as regards short stay visas;

(h) the grounds indicated for any decision ~~concerning the document or the application, only as regards~~ ***to refuse a*** short stay ~~visas; as regards long stay visas and residence permits, the decision concerning the application (whether to issue or to refuse the application and on which ground)~~ ***visa, including the reference to any hits against Union information systems that are consulted, against Europol or Interpol data, against the watchlist referred to in Article 29 of Regulation (EU) 2018/1240 or against the specific risk indicators***; **[Am. 149]**

(ha) the grounds indicated for any decision to refuse a document, including the reference to any hits against Union information systems that are consulted, against Europol or Interpol data, against the watchlist referred to in Article 34 of Regulation (EU) 2018/1240 or against the specific risk indicators; **[Am. 150]**

(i) the competent authority, including its location, which refused the application and the date of the refusal, only as regards short stay visas;

(j) the cases in which the same applicant applied for a short stay visa from more than one visa authority, indicating these visa authorities, their location and the dates of refusals, only as regards short stay visas;

(k) As regards short stay visa, main purpose(s) of the journey; ~~as regards long stay visas and residence permit, the purpose of the application;~~ **[Am. 151]**

(l) the data entered in respect of any ***visa*** document withdrawn, annulled, revoked or whose validity is extended, as applicable; **[Am. 152]**

(m) where applicable, the expiry date of the long stay visa or residence permit;

(n) the number of persons exempt from the requirement to give fingerprints pursuant to Article 13(7) of Regulation (EC) No 810/2009.

(o) the cases in which the data referred to in point (6) of Article 9 could factually not be provided, in accordance with the second sentence of Article 8(5);

(p) the cases in which the data referred to in point (6) of Article 9 was not required to be provided for legal reasons, in accordance with the second sentence of Article 8(5);

(q) the cases in which a person who could factually not provide the data referred to in point (6) of Article 9 was refused a visa, in accordance with the second sentence of Article 8(5).

The duly authorised staff of the European Border and Coast Guard Agency shall have access to consult the data referred to in the first subparagraph for the purpose of carrying out risk analyses and vulnerability assessments as referred to in Articles 11 and 13 of Regulation (EU) 2016/1624.

2. For the purpose of paragraph 1 of this Article, eu-LISA shall store the data referred to in that paragraph in the central repository for reporting and statistics referred to in [Article 39 of the Regulation 2018/XX [on interoperability ***(borders and visas)***]

3. The procedures put in place by eu-LISA to monitor the functioning of the VIS referred to in Article 50(1) shall include the possibility to produce regular statistics for ensuring that monitoring.

4. Every quarter, eu-LISA shall compile statistics based on the VIS data on short stay visas showing, for each location where a visa was lodged, in particular:

   (a) total of airport transit visas applied for, including for multiple airport transit visas;

   (b) total of visas issued, including multiple A visas;

   (c) total of multiple visas issued;

   (d) total of visas not issued, including multiple A visas;

   (e) total of uniform visas applied for, including multiple-entry uniform visas;

(f) total of visas issued, including multiple-entry visas;

(g) total of multiple-entry visas issued, devided by length of validity (below 6 months, 1 year, 2 years, 3 years, 4 years, 5 years),

(h) total of uniform visas not issued, including multiple-entry visas;

(i) total of visas with limited territorial validity issued.

The daily statistics shall be stored in the central repository for reporting and statistics.

5. Every quarter, eu-LISA shall compile statistics based on the VIS data on long-stay visas and residence permits showing, for each location, in particular:

(a) total of long-stay visas applied for, issued, refused, extended and withdrawn;

(b) total of residence permits applied for, issued, refused, extended and withdrawn.

6. At the end of each year, statistical data shall be compiled in ~~the form of quarterly statistics~~ ***an annual report*** for that year. The statistics shall contain a breakdown of data for each Member State. ***The report shall be published and transmitted to the European Parliament, to the Council, to the Commission, to the European Border and Coast Guard Agency, to the European Data Protection Supervisor and to the national supervisory authorities.*** **[Am. 153]**

7. At the request of the Commission, eu-LISA shall provide it with statistics on specific aspects related to the implementation of the common visa policy or of the migration policy, including on aspects pursuant to the application of Regulation (EU) No 1053/2013.";

(35) the following Articles 45b, 45c, 45d and 45e are inserted:

"Article 45b

Access to data for verification by carriers

1. In order to fulfil their obligation under point (b) of Article 26(1) of the Convention implementing the Schengen Agreement, air carriers, sea carriers and international carriers transporting groups overland by coach shall send a query to the VIS in order to verify whether or not third country nationals holding a short-stay visa, a long stay visa or a residence permit are in possession of a valid short stay visa, long stay visa or residence permit, as applicable. ~~For this purpose, as regards short stay visas~~ ***In cases where passengers are not allowed to board due to a query in VIS***, carriers shall provide ~~the data listed under points (a), (b) and (c) of Article 9(4) of this Regulation or under points (a), (b) and (c) of Article 22c, as applicable~~ ***passengers with that information and the means to exercise their rights to access, rectification and erasure of personal data stored in VIS***. **[Am. 154]**

2. For the purpose of implementing paragraph 1 or for the purpose of resolving any potential dispute arising from its application, eu-LISA shall keep logs of all data processing operations carried out within the carrier gateway by carriers. Those logs shall show the date and time of each operation, the data used for interrogation, the data transmitted by the carrier gateway and the name of the carrier in question.

   Logs shall be stored for a period of two years. Logs shall be protected by appropriate measures against unauthorised access.

3. Secure access to the carrier gateway referred to in Article ~~1(2) (h) of Decision 2004/512/EC as amended by this Regulation~~ ***2a(h), including the possibility to use mobile technical solutions,*** shall allow carriers to proceed with the query consultation referred to in paragraph 1 prior to the boarding of a passenger. ~~For this purpose,~~ The carrier shall ~~send the query to be permitted to consult the VIS using~~ ***provide*** the data contained in the ~~machine readable~~ ***machine-readable*** zone of the travel document ***and indicate the Member State of entry***. ***By way of derogation, in the case of airport transit, the carrier shall not be obliged to verify whether the third-country national is in possession of a valid short-stay visa, long-stay visa or residence permit, as applicable***. **[Am. 155]**

4. The VIS shall respond by indicating whether or not the person has a valid ~~visa~~ ***short-stay visa, long-stay visa or residence permit, as applicable***, providing the carriers with an OK/NOT OK answer. ***If a short-stay visa has been issued with limited territorial validity in accordance with Article 25 of Regulation (EC) No 810/2009, the response provided by VIS shall take into account the Member State(s) for which the visa is valid as well as the Member State of entry indicated by the carrier. Carriers may store the information sent and the answer received in accordance with the applicable law. The OK/NOT OK answer shall not be regarded as a decision to authorise or refuse entry in accordance with Regulation (EU) 2016/399. The Commission shall, by means of implementing acts, adopt detailed rules concerning the conditions for the operation of the carrier gateway and the data protection and security rules applicable. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 49(2).*** **[Am. 156]**

5. An authentication scheme, reserved exclusively for carriers, shall be set up in order to allow access to the carrier gateway for the purposes of paragraph 2 to the duly authorised members of the carriers' staff. ***When setting up the authentication scheme, information security risk management and the principles of data protection by design and by default shall be taken into account.*** The authentication scheme shall be adopted by the Commission by means of implementing acts in accordance with the examination procedure referred to in Article 49(2). **[Am. 157]**

5a. The carrier gateway shall make use of a separate read-only database updated on a daily basis via a one-way extraction of the minimum necessary subset of data stored in VIS. eu-LISA shall be responsible for the security of the carrier gateway, for the security of the personal data it contains and for the process of extracting the personal data into the separate read-only database. **[Am. 158]**

5b. The carriers referred to in paragraph 1 of this Article shall be subject to the penalties provided for in accordance with Article 26(2) of the Convention Implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders ('the Convention implementing the Schengen Agreement') and Article 4 of Council Directive 2001/51/EC when they transport third-country nationals who, although subject to the visa requirement, are not in possession of a valid visa. **[Am. 159]**

5c. If third-country nationals are refused entry, any carrier which brought them to the external borders by air, sea and land shall be obliged to immediately assume responsibility for them again. At the request of the border authorities, the carriers shall be obliged to return the third-country nationals to one of either the third country from which they were transported, the third country which issued the travel document on which they travelled, or any other third country to which they are certain to be admitted. **[Am. 160]**

5d. By way of derogation from paragraph 1, for carriers transporting groups overland by coach, for the first three years following the start of application of this Regulation, the verification referred to in paragraph 1 shall be optional and the provisions referred to in paragraph 5b shall not apply to them. **[Am. 161]**

Article 45c

Fall-back procedures in case of technical impossibility to access data by carriers

1. Where it is technically impossible to proceed with the consultation query referred to in Article 45b(1), because of a failure of any part of the VIS ~~or for other reasons beyond the carriers' control~~, the carriers shall be exempted of the obligation to verify the possession of a valid visa or travel document by using the carrier gateway. Where such failure is detected by ~~the Management Authority~~ ***eu-LISA***, it shall notify the carriers. It shall also notify the carriers when the failure is remedied. Where such failure is detected by the carriers, they may notify ~~the Management Authority~~ ***eu-LISA***. **[Am. 162]**

1a. The penalties referred to in Article 45b(5b) shall not be imposed on carriers in the cases referred to in paragraph 1 of this Article. **[Am. 163]**

1b. Where for other reasons than a failure of any part of VIS it is technically impossible for a carrier to proceed with the consultation query referred to in Article 45b(1) for a prolonged period of time, that carrier shall inform eu-LISA. **[Am. 164]**

2. The details of the fall-back procedures shall be laid down in an implementing act adopted in accordance with the examination procedure referred to in Article 49(2).

Article 45d

Access to VIS data by European Border and Coast Guard teams

1. To exercise the tasks and powers pursuant to Article 40(1) of Regulation (EU) 2016/1624 of the European Parliament and of the Council* ~~and in addition to the access provided for in Article 40(8) of that Regulation,~~ the members of the European Border and Coast Guard teams~~, as well as teams of staff involved in return-related operations,~~ shall, within their mandate, have the right to access and search data entered in VIS. **[Am. 165]**

2. To ensure the access referred to in paragraph 1, the European Border and Coast Guard Agency shall designate a specialised unit with duly empowered European Border and Coast Guard officials as the central access point. The central access point shall verify that the conditions to request access to the VIS laid down in Article 45e are fulfilled.

---

* Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC (OJ L 251, 16.9.2016, p. 1).

Article 45e

Conditions and procedure for access to VIS data by European Border and Coast Guard teams

1. In view of the access referred to in paragraph 1 of Article 45d, a European Border and Coast Guard team may submit a request for the consultation of all data or a specific set of data stored in the VIS to the European Border and Coast Guard central access point referred to in Article 45d(2). The request shall refer to the operational plan on border checks~~,~~ ***and*** border surveillance ~~and/or return~~ of that Member State on which the request is based. Upon receipt of a request for access, the European Border and Coast Guard central access point shall verify whether the conditions for access referred to in paragraph 2 are fulfilled. If all conditions for access are fulfilled, the duly authorised staff of the central access point shall process the requests. The VIS data accessed shall be transmitted to the team in such a way as not to compromise the security of the data. **[Am. 166]**

2. For the access to be granted, the following conditions shall apply:

   a) the host Member State authorises the members of the team to consult VIS in order to fulfil the operational aims specified in the operational plan on border checks~~,~~ ***and*** border surveillance ~~and return~~, and **[Am. 167]**

   b) the consultation of VIS is required for performing the specific tasks entrusted to the team by the host Member State.

3. In accordance with Article 40(3) of Regulation (EU) 2016/1624, members of the teams~~, as well as teams of staff involved in return-related tasks~~ may only act in response to information obtained from the VIS under instructions from and, as a general rule, in the presence of border guards ~~or staff involved in return-related tasks~~ of the host Member State in which they are operating. The host Member State may authorise members of the teams to act on its behalf. **[Am. 168]**

4. In case of doubt or if the verification of the identity of the visa holder, long stay visa holder or residence permit holder fails, the member of the European Border and Coast Guard team shall refer the person to a border guard of the host Member State.

5. Consultation of the VIS data by members of the teams shall take place as follows:

   a) When exercising tasks related to border checks pursuant to Regulation (EU) 2016/399, the members of the teams shall have access to VIS data for verification at external border crossing points in accordance with Articles 18 or 22g of this Regulation respectively;

   b) When verifying whether the conditions for entry to, stay or residence on the territory of the Member States are fulfilled, the members of the teams shall have access to the VIS data for verification within the territory of third country nationals in acordance with Articles 19 or 22h of this Regulation respectively;

   c) When identifying any person that may not or may no longer fulfil the conditions for the entry to, stay or residence on the territory of the Member States, the members of the teams shall have access to VIS data for identification in accordance with Article 20 of this Regulation.

6. Where such access and search reveal the existence of a hit in VIS, the host Member State shall be informed thereof.

7. Every log of data processing operations within the VIS by a member of the European Border and Coast Guard teams ~~or teams of staff involved in return-related tasks~~ shall be kept by the Management Authority in accordance with the provisions of Article 34. **[Am. 169]**

8. Every instance of access and every search made by the European Border and Coast Guard Agency shall be logged in accordance with the provisions of Article 34 and every use made of data accessed by the European Border and Coast Guard Agency ***teams*** shall be registered. **[Am. 170]**

9. ~~Except where necessary to perform the tasks for the purposes of the Regulation establishing a European Travel Information and Authorisation System (ETIAS),~~ No parts of VIS shall be connected to any computer system for data collection and processing operated by or at the European Border and Coast Guard Agency nor shall the data contained in VIS to which the European Border and Coast Guard Agency has access be transferred to such a system. No part of VIS shall be downloaded. The logging of access and searches shall not be construed as constituting to be the downloading or copying of VIS data. **[Am. 171]**

10. Measures to ensure security of data as provided for in Articles 32 shall be adopted and applied by the European Border and Coast Guard Agency."

(35a) Articles 46, 47 and 48 are deleted; **[Ams. 172, 173 and 174]**

(35b) the following Article is inserted:

"Article 48a
Exercise of delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 9cb and Article 23 shall be conferred on the Commission for a period of five years from … [date of entry into force of this Regulation]. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. ***The delegation of power referred to in Article 9cb and Article 23 may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.***

4. ***Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making.***

5. ***As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.***

6. ***A delegated act adopted pursuant to Article 9cb and Article 23 shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.";*** **[Am. 175]**

(36) Article 49 is replaced by the following:

"Article 49

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council*.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

---

* Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).";

(37) the following Article 49a is inserted:

"Article 49a

Advisory group

An Advisory Group shall be established by eu-LISA and provide it with the expertise related to the VIS in particular in the context of the preparation of its annual work programme and its annual activity report." ;

(38) Article 50 is replaced by the following:

"Article 50

Monitoring and evaluation ***of impact on fundamental rights*** **[Am. 176]**

1. ~~The Management Authority~~ ***eu-LISA*** shall ensure that procedures are in place to monitor the functioning of the VIS against objectives relating to output, cost-effectiveness, security and quality of service***, and to monitor the compliance with fundamental rights including the right of protection of personal data, the right to non-discrimination, the rights of the child and the right to an effective remedy***. **[Am. 177]**

2. For the purposes of technical maintenance, ~~the Management Authority~~ ***eu-LISA*** shall have access to the necessary information relating to the processing operations performed in the VIS. **[Am. 178]**

3. Every two years eu-LISA shall submit to the European Parliament, the Council and the Commission a report on the technical functioning of VIS, including ~~the~~ ***its*** security ~~thereof~~ ***and costs***. ***That report shall include an overview of the current progress of the development of the project and the associated costs, a financial impact assessment, and information on any technical issues and risks that may affect the overall cost of the system.*** **[Am. 179]**

3a. In the event of delays in the development process, eu-LISA shall inform the European Parliament and the Council as soon as possible about the reasons for the delays and their impact in terms of time and finances. **[Am. 180]**

4. While respecting the provisions of national law on the publication of sensitive information, each Member State and Europol shall prepare annual reports on the effectiveness of access to VIS data for law enforcement purposes containing information and statistics on:

(a) the exact purpose of the consultation including the type of terrorist or serious criminal offence ***and accesses to data on children below 12 years of age***; **[Am. 181]**

(b) reasonable grounds given for the substantiated suspicion that the suspect, perpetrator or victim is covered by this Regulation;

(c) the number of requests for access to the VIS for law enforcement purposes;

(ca) the number and type of cases in which the urgency procedures referred to in Article 22m(2) were used, including those cases where the urgency was not accepted by the ex post verification carried out by the central access point; **[Am. 182]**

(d) the number and type of cases which have ended in successful identifications.

(da) statistics on child trafficking, including cases of successful identifications. **[Am. 183]**

Member States' and Europol's annual reports shall be transmitted to the Commission by 30 June of the subsequent year. ***The Commission shall compile the annual reports into a comprehensive report to be published by 30 December of the same year.*** **[Am. 184]**

5. Every ~~four~~ ***two*** years ,the Commission shall produce an overall evaluation of the VIS. This overall evaluation shall include an examination of results achieved against objectives ***and costs sustained*** and an assessment of the continuing validity of the underlying rationale, ***and its impact on fundamental rights,*** the application of this Regulation in respect of the VIS, the security of the VIS, the use made of the provisions referred to in Article 31 and any implications for future operations. The Commission shall transmit the evaluation to the European Parliament and the Council. **[Am. 185]**

6. Member States shall provide the Management Authority and the Commission with the information necessary to draft the reports referred to in paragraph 3, 4 and 5.

7. The Management Authority shall provide the Commission with the information necessary to produce the overall evaluations referred to in paragraph 5.";

~~(39) The title of annex 1 is replaced by the following:~~

~~"List of international organisations referred to in Article 31(1)“.~~ **[Am. 186]**

(40) After Article 22, the following chapters IIIa and IIIb are inserted:

CHAPTER IIIa

ENTRY AND USE OF DATA ON LONG STAY VISAS AND RESIDENCE PERMITS

Article 22a

Procedures for entering data upon decision on an application for a long stay visa or residence permit

1. Upon decision on an application for a long stay visa or residence permit, the authority that issued that decision shall create without delay the individual file, by entering the data referred to in Article 22c or Article 22d in the VIS.

1a. The authority competent to issue a decision shall create an individual file before issuing it. **[Am. 187]**

2. Upon creation of the individual file, the VIS shall automatically launch the query pursuant to Article 22b.

3. If the holder has applied as part of a group or with a family member, the authority shall create an individual file for each person in the group and link the files of the persons having applied together and who were issued a long stay visa or residence permit. ***Applications from parents or legal guardians shall not be separated from those of their children.*** **[Am. 188]**

4. Where particular data are not required to be provided in accordance with Union or national legislation or factually cannot be provided, the specific data field(s) shall be marked as 'not applicable'. In the case of fingerprints, the system shall permit a distinction to be made between the cases where fingerprints are not required to be provided in accordance with Union or national legislation and the cases where they cannot be provided factually.

Article 22b

Queries to other systems

1. Solely for the purpose of assessing whether the person could pose a threat to the public policy~~,~~ or internal security ~~or public health~~ of the Member States, pursuant to Article 6(1)(e) of Regulation (EU) 2016/399, the files shall be automatically processed by the VIS to identify hit(s). The VIS shall examine each file individually. **[Am. 189]**

2. Every time an individual file is created ~~upon issuance or refusal~~ pursuant to Article ~~22d of~~ ***22c in connection with*** a long-stay visa or residence permit~~,~~ the VIS ~~shall~~ shall launch a query by using the European Search Portal defined in Article 6(1) of [the Interoperability Regulation ***(borders and visas)***] to compare the ~~relevant~~ data referred to in Article 22c(2)(a), (b), (c), (f) and (g) of this Regulation***.*** ~~with the relevant data, in~~ The VIS~~, the Schengen Information System (SIS), the Entry/Exit System (EES), the~~ ***shall verify:***

(a) whether the travel document used for the application corresponds to a travel document reported as lost, stolen, misappropriated or invalidated in SIS;

(b) whether the travel document used for the application corresponds to a travel document reported as lost, stolen or invalidated in the SLTD database;

(c) whether the applicant is subject to a refusal of entry and stay alert entered in SIS;

(d) whether the applicant is subject to an alert in respect of persons wanted for arrest for surrender purposes on the basis of a European ***Arrest Warrant or wanted for arrest for extradition purposes in SIS;***

(e) ***whether the applicant and the*** travel ~~Information and~~ ***document correspond to a refused, revoked or annulled travel*** authorisation ***in the ETIAS Central*** System ~~(ETIAS) including the watchlist~~ ***;***

(f) ***whether the applicant and the travel document are in the watch list*** referred to in Article ~~29~~ ***34*** of Regulation (EU) ~~2018/XX for the purposes of establishing a European Travel Information and Authorisation System, [the ECRIS-TCN system as far as convictions related to terrorist offences and other forms of serious criminal offences are concerned], the Europol data, the Interpol Stolen and Lost~~ ***2018/1240;***

(g) ***whether data on the applicant is already recorded in VIS on the same person;***

(h) ***whether the data provided in the application concerning the*** travel document ~~database (SLTD), and the Interpol Travel Documents~~ ***correspond to another application for a long-stay visa or residence permit*** associated with ~~Notices database (Interpol TDAWN)~~ ***different identity data;***

(i) whether the applicant is currently reported as an overstayer or whether he or she has been reported as an overstayer in the past in the EES;

(j) whether the applicant is recorded as having been refused entry in the EES;

(k) whether the applicant has been subject to a decision to refuse, annul or revoke a short-stay visa recorded in VIS;

(l) whether the applicant has been subject to a decision to refuse, annul or revoke a long-stay visa or residence permit recorded in VIS;

(m) whether data specific to the identity of the applicant are recorded in Europol data;

(n) in cases where the applicant is a minor, whether the applicant's parental authority or legal guardian:

(i) is subject to an alert in respect of persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes in SIS;

(ii) is subject to a refusal of entry and stay alert in SIS;

(iii) holds a travel document in the watch list referred to in Article 34 of Regulation (EU) 2018/1240.

This paragraph must not impede the submission of an application for asylum on any grounds. If a visa application is submitted by a victim of violent crime such as domestic violence or trafficking in human beings committed by their sponsor, the file submitted to VIS shall be separated from that of the sponsor in order to protect the victim from further danger.

To avoid the risk of false hits, any query concerning children under the age of 14 or people older than 75 years carried out with biometric identifiers taken more than five years before the match and which that does not confirm the identity the third-country national, shall be subject to a compulsory manual check by experts on biometric data. **[Am. 190]**

3. The VIS shall add a reference to any hit obtained pursuant to paragraphs (2) and (5) to the individual file. Additionally, the VIS shall identify, where relevant, the Member State(s) that entered or supplied the data having triggered the hit(s) or Europol, and shall record this in the individual file. ***No information other than the reference to any hit and the originator of the data shall be recorded.*** **[Am. 191]**

3a. When querying SLTD, the data used by the user of the ESP to launch a query shall not be shared with the owners of Interpol data. **[Am. 192]**

4. For the purposes of Article 2(2)(f) in respect of an issued or extended long stay ~~visathe~~ ***visa the*** queries carried out under ~~22bparagraph~~ ***paragraph*** 2 of this Article shall compare the relevant data referred to in Article 22c(2), to the data present in the SIS in order to determine whether the holder is subject to one of the following alerts: **[Am. 193]**

   (a) an alert in respect of persons wanted for arrest for surrender purposes or extradition purposes;

   (b) an alert in respect of missing persons;

   (c) an alert in respect of persons sought to assist with a judicial procedure;

   (d) an alert on persons and objects for discreet checks ~~or~~**,** specific checks ***or inquiry checks***. **[Am. 194]**

   ~~Where the comparison referred to in this paragraph reports one or several hit(s), the VIS shall send an automated notification to the central authority of the Member State that launched the request and shall take any appropriate follow-up action.~~ ***Article 9a(5a), (5b), (5c), (5d), and Articles 9c, 9ca, 9cb shall apply mutatis mutandis subject to the following specific provisions.*** **[Am. 195]**

5. As regards the consultation of EES, ETIAS and VIS data pursuant to paragraph 2, the hits shall be limited to indicating refusals of a travel authorisation, of entry or of a visa which are based on security grounds.

~~6. Where the long stay visa or residence permit is issued or extended by a consular authority of a Member State, Article 9a shall apply.~~ **[Am. 196]**

~~7. Where the residence permit is issued or extended or where a long stay visa is extended by an authority in the territory of a Member State, the following apply:~~

~~(a) that authority shall verify whether the data recorded in the individual file corresponds to the data present in the VIS, or one of the consulted EU information systems/databases, the Europol data, or the Interpol databases pursuant to paragraph 2;~~

~~(b) where the hit pursuant to paragraph 2 is related to Europol data, the Europol national unit shall be informed for follow up;~~

~~(c) where the data do not correspond, and no other hit has been reported during the automated processing pursuant to paragraphs 2 and 3, the authority shall delete the false hit from the application file;~~

~~(d) where the data correspond to or where doubts remain concerning the identity of the applicant, the authority shall take action on the data that triggered the hit pursuant to paragraph 4 according to the procedures, conditions and criteria provided by EU and national legislation.~~

[Am. 197]

Article 22c

Individual file to be created for a long stay visa or residence permit issued

An individual file created pursuant to Article 22a(1) shall contain the following data:

(1) the authority which issued the document, including its location;

(2) the following data of the holder:

(a) surname (family name); first name(s); ~~date~~ ***year*** of birth; current nationality or nationalities; sex; ~~date,~~ place and country of birth;

[Am. 198]

(b) type and number of the travel document and the three letter code of the issuing country of the travel document;

(c) the date of expiry of the validity of the travel document;

(cc) authority which issued the travel document;

(d) in the case of minors, surname and first name(s) of the holder's parental authority or legal guardian;

(e) the surname, first name and address of the natural person or the name and address of the employer or any other organisation on which the application was based;

(f) a facial image of the holder~~, where possible~~ taken live; **[Am. 199]**

(g) two fingerprints of the holder, in accordance with the relevant Union and national legislation;

(3) the following data concerning the long stay visa or residence permit issued:

(a) status information indicating that a long-stay visa or residence permit has been issued;

(b) place and date of the decision to issue the long-stay visa or residence permit;

(c) the type of document issued (long-stay visa or residence permit);

(d) the number of the issued long-stay visa or residence permit;

(e) the expiry date of the long-stay visa or residence permit.

Article 22d

Individual file to be created in certain cases of refusal of a long stay visa or residence permit

Where a decision has been taken to refuse a long stay visa or a residence permit because the applicant is considered to pose a threat to public policy~~,~~ ***or*** internal security ~~or to public health~~ or the applicant has presented documents which were fraudulently acquired, or falsified, or tampered with, the authority which refused it shall create without delay an individual file with the following data: **[Am. 200]**

a) surname, surname at birth (former surname(s)); first name(s); sex; date, place and country of birth;

b) current nationality and nationality at birth;

c) type and number of the travel document, the authority which issued it and the date of issue and of expiry;

d) in the case of minors, surname and first name(s) of the applicant's parental authority or legal guardian;

e) the surname, first name and address of the natural ~~personon~~ ***person on*** whom the application is based; **[Am. 201]**

f) a facial image of the applicant~~, where possible~~ taken live; **[Am. 202]**

g) two fingerprints of the applicant, in accordance with the relevant Union and national legislation;

h) information indicating that the long-stay visa or residence permit has been refused because the applicant is considered to pose a threat to public policy~~,~~ ***or*** public security ~~or to public health~~, or because the applicant presented documents which were fraudulently acquired, or falsified, or tampered with; **[Am. 203]**

i) the authority that refused the long-stay visa or residence permit, including its location;

j) place and date of the decision to refuse the long stay-visa or residence permit.

Article 22e

Data to be added for a long stay visa or residence permit withdrawn

1. here a decision has been taken to withdraw a residence permit or long-stay visa or to shorten the validity period of a long stay visa, the authority that has taken the decision shall add the following data to the individual file:

   (a) status information indicating that the long-stay visa or residence permit has been withdrawn or, in the case of a long stay visa, that the validity period has been shortened;

   (b) authority that withdrew the long-stay visa or residence permit or shortened the validity period of the long stay visa, including its location;

   (c) place and date of the decision;

   (d) the new expiry date of the validity of the long stay visa, where appropriate;

   (e) the number of the visa sticker, if the reduced period takes the form of a new visa sticker.

2. The individual file shall also indicate the ground(s) for withdrawal of the long-stay visa or residence permit or shortening of the validity period of the long stay visa, in accordance with point (h) of Article 22d.

Article 22f

Data to be added for a long stay visa or residence permit extended

Where a decision has been taken to extend a residence permit or a long-stay visa, the authority which extended it shall add the following data to the individual file:

(a) status information indicating that the long-stay visa or residence permit has been extended;

(b) the authority that extended the long-stay visa or residence permit, including its location;

(c) place and date of the decision;

(d) in the case of a long stay visa, the number of the visa sticker, if the extension of the long-stay visa takes the form of a new visa sticker;

(e) the expiry date of the extended period.

Article 22g

Access to data for verification of long stay visas and residence permits at external border crossing points

1. For the sole purpose of verifying the identity of the document holder and/or the authenticity and the validity of the long-stay visa or residence permit and whether the person is not considered to be a threat to public policy~~,~~ ***or*** internal security ~~or public health~~ of any of the Member States in accordance with Article 6(1)(e) of Regulation (EU) 2016/399, the competent authorities for carrying out checks at external border crossing points in accordance with that Regulation shall have access to search using the number of the document in combination with one or several of the data in Article 22c(2)(a), (b) and (c) of this Regulation. **[Am. 204]**

2. If the search with the data listed in paragraph 1 indicates that data on the document holder are recorded in the VIS, the competent border control authority shall be given access to consult the following data of the individual file, solely for the purposes referred to in paragraph 1:

(a) the status information of the long-stay visa or residence permit indicating if it has been issued, withdrawn or extended;

(b) data referred to in Article 22c(3)(c), (d), and (e);

(c) where applicable, data referred to in Article 22e(1)(d) and (e);

(d) where applicable, data referred to in Article 22f(d) and (e);

(e) ~~photographs~~ ***facial images*** as referred to in Article 22c(2)(f). **[Am. 205]**

Article 22h

Access to data for verification within the territory of the Member States

1. For the sole purpose of verifying the identity of the holder and the authenticity and the validity of the long-stay visa or residence permit ~~or whether the person is not a threat to public policy, internal security or public health of any of the Member States ,~~the authorities competent for carrying out checks within the territory of the Member States as to whether the conditions for entry to, stay or residence on the territory of the Member States are fulfilled and~~, as applicable, police authorities,~~ shall have access to search using the number of the long-stay visa or residence permit in combination with one or several of the data in Article 22c(2)(a), (b) and (c). **[Am. 206]**

2. If the search with the data listed in paragraph 1 indicates that data on the holder are recorded in the VIS, the competent authority shall be given access to consult the following data of the individual file as well as, if applicable, of linked file(s) pursuant to Article 22a(4), solely for the purposes referred to in paragraph 1:

(a) the status information of the long-stay visa or residence permit indicating if it has been issued, withdrawn or extended;

(b) data referred to in Article 22c(3)(c), (d), and (e);

(c) where applicable, data referred to in Article 22e(1)(d) and (e);

(d) where applicable, data referred to in Article 22f(d) and (e);

(e) ~~photographs~~ ***facial images*** as referred to in Article 22c(2)(f). **[Am. 207]**

Article 22i

Access to data for determining the responsibility for applications for international protection

1. For the sole purpose of determining the Member State responsible for examining an application for international protection in accordance with Article 12 of Regulation (EU) No 604/2013, the competent asylum authorities shall have access to search with the fingerprints of the applicant for international protection.

   Where the fingerprints of the applicant for international protection cannot be used or the search with the fingerprints fails, the search shall be carried out using the number of the long stay visa or residence permit in combination with the data in Article 22c(2)(a), (b) and (c).

2. If the search with the data listed in paragraph 1 indicates that a long-stay visa or residence permit is recorded in the VIS, the competent asylum authority shall be given access to consult the following data of the application file, and as regards the data listed in point (g) of linked application file(s) of the spouse and children, pursuant to Article 22a(4), for the sole purpose referred to in paragraph 1:

(a) the authority that issued or extended the long-stay visa or residence permit;

(b) the data referred to in Article 22c(2)(a) and (b);

(c) the type of document;

(d) the period of validity of the long-stay visa or residence permit;

(f) photographs as referred to in Article 22c(2)(f);

(g) the data referred to in Article 22c(2)(a) and (b) of the linked application file(s) on the spouse and children.

3. The consultation of the VIS pursuant to paragraphs 1 and 2 of this Article shall be carried out only by the designated national authorities referred to in Article 27 of Regulation (EU) No 603/2013 of the European Parliament and of the Council*.

Article 22j

Access to data for examining the application for international protection

1. For the sole purpose of examining an application for international protection, the competent asylum authorities shall have access in accordance with Article 27 of Regulation (EU) No 603/2013 to search with the fingerprints of the applicant for international protection.

   Where the fingerprints of the applicant for international protection cannot be used or the search with the fingerprints fails, the search shall be carried out using the number of the long stay visa or residence document in combination with the data in Article 22c(2)(a), (b) and (c), or a combination of data in Article 22d(a), (b), (c) and (f).

2. If the search with the data listed in paragraph 1 indicates that data on the applicant for international protection is recorded in the VIS, the competent asylum authority shall have access to consult, for the sole purpose referred to in paragraph 1, the data entered in respect of any long-stay visa or residence permit issued, refused, withdrawn or whose validity is extended, referred to in Articles 22c, 22d, 22e and 22f of the applicant and of the linked application file(s) of the applicant pursuant to Article 22a(3).

3. The consultation of the VIS pursuant to paragraphs 1 and 2 of this Article shall be carried out only by the designated national authorities referred to in Article 27 of Regulation (EU) No 603/2013.

CHAPTER IIIb

Procedure and conditions for access to the VIS for law enforcement purposes

Article 22k

Member States' designated authorities

1. Member States shall designate the authorities which are entitled to consult the data stored in the VIS in order to prevent, detect and investigate terrorist offences or other serious criminal offences ***in appropriate and strictly defined circumstances as referred to in Article 22n***. ***Those authorities shall only be allowed to consult data of children below 12 years of age to protect missing children and children who are victims of serious crimes.*** **[Am. 208]**

2. Each Member State shall keep a ***strictly limited*** list of the designated authorities. Each Member State shall notify eu-LISA and the Commission of its designated authorities and may at any time amend or replace its notification. **[Am. 209]**

3. Each Member State shall designate a central access point which shall have access to the VIS. The central access point shall verify that the conditions to request access to the VIS laid down in Article 22n are fulfilled.

   The designated authority and the central access point may be part of the same organisation if permitted under national law, but the central access point shall act fully independently of the designated authorities when performing its tasks under this Regulation. The central access point shall be separate from the designated authorities and shall not receive instructions from them as regards the outcome of the verification which it shall perform independently.

   Member States may designate more than one central access point to reflect their organisational and administrative structure in the fulfilment of their constitutional or legal requirements.

4. Each Member State shall notify eu-LISA and the Commission of its central access point and may at any time amend or replace its notification.

5. At national level, each Member State shall keep a list of the operating units within the designated authorities that are authorised to request access to data stored in the VIS through the central access point(s).

6. Only duly empowered staff of the central access point(s) shall be authorised to access the VIS in accordance with Articles 22m and 22n.

Article 22l

Europol

1. Europol shall designate one of its operating units as 'Europol designated authority' and shall authorise it to request access to the VIS through the VIS designated central access point referred to in paragraph 2 in order to support and strengthen action by Member States in preventing, detecting and investigating terrorist offences or other serious criminal offences.

2. Europol shall designate a specialised unit with duly empowered Europol officials as the central access point. The central access point shall verify that the conditions to request access to the VIS laid down in Article 22p are fulfilled.

The central access point shall act ***fully*** independently when performing its tasks under this Regulation and shall not receive instructions from the Europol designated authority referred to in paragraph 1 as regards the outcome of the verification. **[Am. 210]**

Article 22m

Procedure for access to the VIS for law enforcement purposes

1. The operating units referred to in Article 22k(5) shall submit a reasoned electronic or written request to the central access points referred to in Article 22k(3) for access to data stored in the VIS. Upon receipt of a request for access, the central access point(s) shall verify whether the conditions for access referred to in Article 22n are fulfilled. If the conditions for access are fulfilled, the central access point(s) shall process the requests. The VIS data accessed shall be transmitted to the operating units referred to in Article 22k(5) in such a way as to not compromise the security of the data.

2. In a case of exceptional urgency, where there is a need to prevent an imminent danger to the life of a person associated with a terrorist offence or another serious criminal offence, the central access point(s) shall process the request immediately and shall only verify ex post whether all the conditions of Article 22n are fulfilled, including whether a case of urgency actually existed. The ex post verification shall take place without undue delay and in any event no later than 7 working days after the processing of the request

3. Where an ex post verification determines that the access to VIS data was not justified, all the authorities that accessed such data shall ***immediately*** erase the information accessed from the VIS and shall inform the central access points of the erasure. **[Am. 211]**

Article 22n

Conditions for access to VIS data by designated authorities of Member States

1. ***Without prejudice to Article 22 of Regulation 2018/XX [on interoperability (borders and visas)]*** designated authorities may access the VIS for consultation if all of the following conditions are met: **[Am. 212]**

   (a) access for consultation is necessary and proportionate for the purpose of the prevention, detection or investigation of a terrorist offences or another serious criminal offence;

   (b) access for consultation is necessary and proportionate in a specific case;

   (c) reasonable grounds exist to consider that the consultation of the VIS data will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation;

(ca) in case of searches with fingerprints, a prior search has been launched in the automated fingerprint identification system of the other Member States under Decision 2008/615/JHA where comparisons of fingerprints are technically available, and either that search has been fully carried out, or that search has not been fully carried out within 24 hours of being launched. **[Am. 213]**

(d) where a query to the CIR was launched in accordance with Article 22 of Regulation 2018/XX [on interoperability ***(borders and visas)***], the reply received as referred to in paragraph 5 of [Article 22 of Regulation ***2018/XX [on interoperability (borders and visas)]]*** reveals that data is stored in the VIS." **[Am. 214]**

2. The condition provided in point (d) of paragraph 1 does not need to be fulfilled for situations where the access to the VIS is needed as a tool to consult the visa history or the periods of authorised stay on the territory of the Member States of a known suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence.

3. Consultation of the VIS shall be limited to searching with any of the following data in the ***application file or*** individual file: **[Am. 215]**

(a) surname(s) (family name), first name(s) (given names), ~~date~~ ***year*** of birth, nationality or nationalities and/or sex; **[Am. 216]**

(b) type and number of travel document or documents, three letter code of the issuing country and date of expiry of the validity of the travel document;

(c) visa sticker number or number of the long-stay visa or residence document and the date of expiry of the validity of the visa, long-stay visa or residence document, as applicable;

(d) fingerprints, including latent fingerprints;

(e) facial image.

3a. The Commission shall present a report to the European Parliament and to the Council on the feasibility, availability, readiness and reliability of the required technology to use facial images to identify a person. **[Am. 217]**

3b. The facial image referred to in point (e) of paragraph 3 shall not be the only search criterion. **[Am. 218]**

4. Consultation of the VIS shall, in the event of a hit, give access to the data listed in ~~this~~ paragraph ***3 of this Article*** as well as to any other data taken from the ***application file or*** individual file, including data entered in respect of any document issued, refused, annulled, revoked or extended. Access to the data referred to in point (4)(l) of Article ~~9as~~ ***9 as*** recorded in the application file shall only be given if consultation of that data was ~~explicitely~~ ***explicitly*** requested in a reasoned request and approved by independent verification. **[Am. 219]**

Article 22o

Access to VIS for identification of persons in specific circumstances

By derogation from Article 22n(1), designated authorities shall not be obliged to fulfil the conditions laid down in that paragraph to access the VIS for the purpose of identification of persons***, particularly children,*** who had gone missing, abducted or identified as victims of trafficking in human beings and in respect of whom there are ~~reasonable~~ ***serious*** grounds to consider that consultation of VIS data will support their identification~~, and/or~~ ***and*** contribute in investigating specific cases of human trafficking. In such circumstances, the designated authorities may search in the VIS with the fingerprints of those persons. **[Am. 220]**

Where the fingerprints of those persons cannot be used or the search with the fingerprints fails, the search shall be carried out with the data referred to in points (a) and (b) of Article 9***(4) or points (a) and (b) of Article 22c(2)***. **[Am. 221]**

Consultation of the VIS shall, in the event of a hit, give access to any of the data in Article 9, ***Article 22c or Article 22d,*** as well as to the data in Article 8(3) and (4) ***or Article 22a(3)***. **[Am. 222]**

Article 22p

Procedure and conditions for access to VIS data by Europol

1. Europol shall have access to consult the VIS where all the following conditions are met:

   (a) the consultation is necessary and proportionate to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling under Europol's mandate;

   (b) the consultation is necessary and proportionate in a specific case;

   (c) reasonable grounds exist to consider that the consultation of the VIS data will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation;

(d) where a query to the CIR was launched in accordance with Article 22 of Regulation 2018/XX [on interoperability ***(borders and visas)***], the reply received as referred to in Article 22(3) of that Regulation reveals that data is stored in the VIS.

2. The conditions laid down in Article 22n(2), (3) and (4) shall apply accordingly.

3. Europol's designated authority may submit a reasoned electronic request for the consultation of all data or a specific set of data stored in the VIS to the Europol central access point referred to in Article ~~22k(3)~~ ***22l(2)***. Upon receipt of a request for access the Europol central access point shall verify whether the conditions for access referred to in paragraphs 1 and 2 are fulfilled. If all conditions for access are fulfilled, the duly authorised staff of the central access point(s) shall process the requests. The VIS data accessed shall be transmitted to the operating units referred to in Article 22l(1) in such a way as not to compromise the security of the data. **[Am. 223]**

4. The processing of information obtained by Europol from consultation with VIS data shall be subject to the authorisation of the Member State of origin. That authorisation shall be obtained via the Europol national unit of that Member State.

Article 22q

Logging and documentation

1. Each Member State and Europol shall ensure that all data processing operations resulting from requests to access to VIS data in accordance with Chapter ~~IIIc are logged~~ ***IIIb are recorded*** or documented for the purposes of ~~checking~~ ***monitoring*** the admissibility of the request, monitoring the lawfulness of the data processing and data integrity and security, and ***possible impact on fundamental rights, and*** self-monitoring.

   The records or documents shall be protected by appropriate measures against unauthorised access and erased two years after their creation, unless they are required for monitoring procedures that have already begun. **[Am. 224]**

2. The log or documentation shall show, in all cases:

   (a) the exact purpose of the request for access to VIS data, including the terrorist offence or other serious criminal offence concerned and, for Europol, the exact purpose of the request for access;

   (b) the national file reference;

(c) the date and exact time of the request for access by the central access point to the VIS Central System;

(d) the name of the authority which requested access for consultation;

(e) where applicable, the decision taken with regard to the ex-post verification;

(f) the data used for consultation;

(g) in accordance with national rules or with Regulation (EU) 2016/794 ***or, where applicable, Regulation (EU) 2018/1725***, the unique user identity of the official who carried out the search and of the official who ordered the search. **[Am. 225]**

3. Logs and documentation shall be used only for monitoring the lawfulness of data processing***, for monitoring the impact on fundamental rights,*** and for ensuring data integrity and security. Only logs which do not contain personal data may be used for the monitoring and evaluation referred to in Article 50 of this Regulation. The supervisory authority established in accordance with Article 41(1) of Directive (EU) 2016/680, which is responsible for ~~checking the admissibility of the request and~~ monitoring the lawfulness of the data processing and data integrity and security, shall have access to these logs at its request for the purpose of fulfilling its duties. **[Am. 226]**

Article 22r

Conditions for access to VIS data by designated authorities of a Member State in respect of which this Regulation has not yet been put into effect

1. Access to the VIS for consultation by designated authorities of a Member State in respect of which this Regulation has not yet been put into effect shall take place where the following conditions are met:

   (a) the acces is within the scope of their powers;

   (b) the acces is subject to the same conditions as referred to in Article 22n(1);

   (c) the acces is preceded by a duly reasoned written or electronic request to a designated authority of a Member State to which this Regulation applies; that authority shall then request the national central access point(s) to consult the VIS.

2. A Member State in respect of which this Regulation has not yet been put into effect shall make its visa information available to Member States to which this Regulation applies, on the basis of a duly reasoned written or electronic request, subject to compliance with the conditions laid down in Article 22n(1).

---

* Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 180, 29.6.2013, p. 1).”.

Article 22ra

Protection of personal data accessed in accordance with Chapter IIIb

1. ***Each Member State shall ensure that the national laws, regulations and administrative provisions adopted pursuant to Directive (EU) 2016/680 are also applicable to the access to VIS by its national authorities under this chapter, including in relation to the rights of the persons whose data are so accessed.***

2. ***The supervisory authority referred to in Article 41(1) of Directive (EU) 2016/680 shall monitor the lawfulness of the access to personal data by the Member States in accordance with this Chapter, including their transmission to and from VIS. Article 41(3) and (4) of this Regulation shall apply accordingly.***

3. ***The processing of personal data by Europol pursuant to this Regulation shall be carried out in accordance with Regulation (EU) 2016/794 and shall be supervised by the European Data Protection Supervisor.***

4. Personal data accessed in VIS in accordance with this Chapter shall only be processed for the purposes of the prevention, detection or investigation of the specific case for which the data have been requested by a Member State or by Europol.

5. eu-LISA, the designated authorities, the central access points and Europol shall keep logs as referred to in Article 22q of the searches for the purpose of enabling the supervisory authority referred to in Article 41(1) of Directive (EU) 2016/680 and the European Data Protection Supervisor to monitor the compliance of data processing with Union and national data protection rules. With the exception of data held for that purpose, personal data and the records of searches shall be erased from all national and Europol files after 30 days, unless those data and records are required for the purposes of the specific ongoing criminal investigation for which they were requested by a Member State or by Europol. **[Am. 227]**

Article 2

~~Amendments to~~ ***Repeal of*** Decision 2004/512/EC **[Am. 228]**

~~Article 1(2) of~~ Decision 2004/512/EC is ~~replaced by the following:~~ ***repealed. References to that Decision shall be construed as references to Regulation (EC) No 767/2008 and shall be read in accordance with the correlation table in Annex 2.***

~~"2. The Visa Information System shall be based on a centralised architecture and consist of:~~

~~(a) the common identity repository as referred to in [Article 17(2)(a) of Regulation 2018/XX on interoperability],~~

~~(b) a central information system, hereinafter referred to as 'the Central Visa Information System' (VIS),~~

~~(c) an interface in each Member State, hereinafter referred to as 'the National Interface' (NI-VIS) which shall provide the connection to the relevant central national authority of the respective Member State, or a National Uniform Interface (NUI) in each Member State based on common technical specifications and identical for all Member States enabling the Central System to connect to the national infrastructures in Member States,~~

~~(d) a communication infrastructure between the VIS and the National Interfaces;~~

~~(e) a Secure Communication Channel between the VIS and the EES Central System;~~

~~(f) a secure communication infrastructure between the VIS Central System and the central infrastructures of the European search portal established by [Article 6 of Regulation 2017/XX on interoperability], shared biometric matching service established by [Article 12 of Regulation 2017/XX on interoperability], the common identity repository established by [Article 17 of Regulation 2017/XX on interoperability] and the multiple-identity detector (MID) established by [Article 25 of Regulation 2017/XX on interoperability];~~

~~(g) a mechanism of consultation on applications and exchange of information between central visa authorities ('VISMail');~~

~~(h) a carrier gateway;~~

~~(i) a secure web service enabling communication between the VIS, on the one hand and the the carrier gateway, and the international systems (Interpol systems/databases), on the other hand;~~

~~(j) a repository of data for the purposes of reporting and statistics.~~

~~The Central System, the National Uniform Interfaces, the web service, the carrier gateway and the Communication Infrastructure of the VIS shall share and re-use as much as technically possible the hardware and software components of respectively the EES Central System, the EES National Uniform Interfaces, the ETIAS carrier gateway, the EES web service and the EES Communication Infrastructure).".~~ **[Am. 229]**

Article 3

Amendments to Regulation (EC) No 810/2009

Regulation (EC) No 810/2009 is amended as follows:

(1) in Article 10(3), point (c) is replaced by the following:

"(c) ~~present a photograph in accordance with the standards set out in Regulation (EC) No 1683/95 or,~~ ***allow the live-taking of a facial image*** upon a first application and subsequently at least every 59 months following that, in accordance with the standards set out in Article 13 of this Regulation.";
[Am. 230]

(2) Article 13 is amended as follows:

(a) in paragraph 2, the first indent is replaced by the following:

"- a ~~photograph~~ ***facial image*** taken live ~~and collected digitally~~ at the time of the application;"; **[Am. 231]**

(b) in paragraph 3, the first subparagraph is replaced by the following:

"Where fingerprints and a live photograph of sufficient quality were collected from the applicant and entered in the VIS as part of an application lodged less than 59 months before the date of the new application, these ~~[data] may~~ ***shall*** be copied to the subsequent application."; **[Am. 232]**

(c) in paragraph 7, point (a) is replaced by the following:

"(a) children under the age of *6* ***and persons over the age of 70***;"; **[Am. 253]**

(d) paragraph 8 is deleted;

(3) Article 21 is amended as follows:

(a) paragraph 2 is replaced by the following:

"2. In respect of each application the VIS shall be consulted in accordance with Articles 8(2), 15 and 9a of the Regulation (EC) No 767/2008. Member States shall ensure that full use is made of all search criteria pursuant to these articles, in order to avoid false rejections and identifications.

(b) the following paragraphs 3a and 3b are inserted:

"3a. For the purpose of assessing the entry conditions provided for in paragraph 3, the consulate shall take into account the result of the verifications pursuant to Article 9c of the Regulation (EC) No 767/2008 of the following databases:

(a) SIS and the SLTD to check whether the travel document used for the application corresponds to a travel document reported lost, stolen or invalidated ~~in the and whether the travel document used for the application corresponds to a travel document recorded in a file in the Interpol TDAWN~~; **[Am. 233]**

(b) the ETIAS Central System to check whether the applicant correspond to a refused, revoked or annulled application for travel authorisation;

(c) the VIS to check whether the data provided in the application concerning the travel document correspond to another application for a visa associated with different identity data, as well as whether the applicant has been subject to a decision to refuse, revoke or annul a short stay visa;

(d) the EES to check whether the applicant is currently reported as overstayer, whether he has been reported as overstayer in the past or whether the applicant was refused entry in the past;

(e) the Eurodac to check whether the applicant was subject to a withdrawal or rejection of the application for international protection;

(f) the Europol data to check whether the data provided in the application corresponds to data recorded in this database;

~~(g) the ECRIS-TCN system to check whether the applicant corresponds to a person whose data is recorded in this database for terrorist offences or other serious criminal offences;~~ **[Am. 234]**

(h) the SIS to check whether the applicant is subject to an alert in respect of persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes.

The consulate shall have access to the application file and the linked application file(s), if any, as well as to all the results of the verifications pursuant to Article 9c of Regulation (EC) No 767/2008.

3b. The visa authority shall consult the multiple-identity detector together with the common identity repository referred to in Article 4(37) of Regulation 2018/XX [on interoperability ***(borders and visas)***] or the SIS or both to assess the differences in the linked identities and shall carry out any additional verification necessary to take a decision on the status and colour of the link as well as to take a decision on the issuance or refusal of the visa of the person concerned.

In accordance with Article 59(1) of Regulation 2018/XX [on interoperability ***(borders and visas)***], this paragraph shall apply only as from the start of operations of the multiple-identity detector.";

(c) paragraph 4 is replaced by the following:

"4. The consulate shall verify, using the information obtained from the EES, whether the applicant will not exceed with the intended stay the maximum duration of authorised stay in the territory of the Member States, irrespective of possible stays authorised under a national long-stay visa or a residence permit issued by another Member State.";

(4) the following Article 21a is inserted:

"Article 21a

Specific risk indicators

-1. The specific risk indicators shall be an algorithm enabling profiling as defined in point (4) of Article 4 of Regulation (EU) 2016/679 through the comparison of the data recorded in an application file with specific risk indicators pointing to security, illegal immigration or high epidemic risks. The specific risk indicators shall be registered in VIS. **[Am. 235]**

1. ~~Assessment of~~ ***The Commission shall adopt a delegated act in accordance with Article 51a to further define the risks related to*** security or illegal immigration or ~~a~~ high epidemic risks ~~shall be based~~ on ***the basis of***: **[Am. 236]**

   (a) statistics generated by the EES indicating abnormal rates of overstayers and refusals of entry for a specific group of travellers holding a visa;

   (b) statistics generated by the VIS in accordance with Article 45a indicating abnormal rates of refusals of visa applications due to an irregular migration~~,~~ ***or*** security ~~or public health~~ risk associated with ~~a specific group of travellers~~ ***an applicant***; **[Am. 237]**

(c) statistics generated by the VIS in accordance with Article 45a and the EES indicating correlations between information collected through the application form and overstay or refusals of entry;

(d) information substantiated by factual and evidence-based elements provided by Member States concerning specific security risk indicators or threats identified by that Member State;

(e) information substantiated by factual and evidence-based elements provided by Member States concerning abnormal rates of overstayers and refusals of entry for a specific group of travellers for that Member State;

(f) information concerning specific high epidemic risks provided by Member States as well as epidemiological surveillance information and risk assessments provided by the European Centre for Disease Prevention and Control (ECDC) and disease outbreaks reported by the World Health Organisation (WHO).

~~2. The Commission shall adopt an implementing act specifying the risks referred to in paragraph 1. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 52(2).~~ **[Am. 238]**

3. Based on the specific risks determined in accordance with ***this Regulation and the delegated act referred to in*** paragraph ~~2~~ ***1*** specific risk indicators shall be established, consisting of a combination of data including one or several of the following: **[Am. 239]**

(a) age range, sex, nationality;

(b) country and city of residence;

(c) Member State(s) of destination;

(d) Member State of first entry;

(e) purpose of travel;

(f) current occupation.

4. The specific risk indicators shall be targeted and proportionate. They shall in no circumstances be based solely on a person's sex or age. They shall in no circumstances be based on information revealing a person's race, colour, ethnic or social origin, genetic features, language, political or any other opinions, religion or philosofical belief, trade union membership, membership of a national minority, property, birth, disability or sexual orientation.

5. The specific risk indicators shall be adopted by the Commission by implementing act. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 52(2).

6. The specific risk indicators shall be used by the visa authorities when assessing whether the applicant presents a risk of illegal immigration~~,~~ ***or*** a risk to the security of the Member States, ~~or a high epidemic risk~~ in accordance to Article 21(1). **[Am. 240]**

7. The specific risks and the specific risk indicators shall be regularly reviewed by the Commission ***and the European Union Agency for Fundamental Rights***."; **[Am. 241]**

(4a) Article 39 is replaced by the following:

"Article 39

Conduct of staff and respect for fundamental rights

1. *Member States' consulates shall ensure that applicants are received courteously. Consular staff shall fully respect human dignity when carrying out their duties.*

2. *Consular staff shall fully respect fundamental rights and observe the principles recognised by the Charter of Fundamental Rights of the European Union when carrying out their duties. Any measures taken shall be proportionate to the objectives pursued by such measures.*

3. *While performing their tasks, consular staff shall not discriminate against persons on any grounds such as sex, racial or ethnic origin, colour, social origin, genetic features, language, political or any opinion, membership of a national minority, property, birth, religion or belief, disability, age or sexual orientation. The best interests of the child shall be a primary consideration.";*

[Am. 242]

(4b) the following Article is inserted:

"Article 39a

Fundamental Rights

When applying this Regulation, Member States shall act in full compliance with relevant Union law, including the Charter of Fundamental Rights of the European Union, relevant international law, including the Convention Relating to the Status of Refugees done at Geneva on 28 July 1951, obligations related to access to international protection, in particular the principle of non-refoulement, and fundamental rights. In accordance with the general principles of Union law, decisions under this Regulation shall be taken on an individual basis. The best interests of the child shall be a primary consideration."; **[Am. 243]**

(5) Article 46 is replaced by the following:

"Article 46

Compilation of statistics

The Commission shall, by 1 March each year, publish the compilation of the following annual statistics on visas per consulate and border crossing point where individual Member States process visa applications:

(a) number of airport transit visas applied for, issued and refused;

(b) number of uniform single entry, and multiple entry visa applied for, issued (disaggregated by length of validity: 1, 2, 3, 4 and 5 years) and refused;

(c) number of visas with limited territorial validity issued.

These statistics shall be compiled on the basis of the reports generated by the central repository of data of the VIS in accordance with Article 17 of Regulation (EC) No 767/2008.";

(5a) the following Article is inserted:

"Article 51a

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 21a shall be conferred on the Commission for a period of five years from … [date of entry into force of this Regulation]. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. The delegation of power referred to in Article 21a may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 21a shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.";
[Am. 244]

(6) In Article 57, paragraphs 3 and 4 are deleted.

Article 4

Amendments to Regulation (EU) 2017/2226

Regulation (EU) 2017/2226 is amended as follows:

(1) in Article 9(2), the following sub-paragraph is added:

"The EES shall provide the functionality for the centralised management of this list. The detailed rules on managing this functionality shall be laid down in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 68(2) of this Regulation.";

(2) in Article 13, paragraph 3 is replaced by the following:

"3. In order to fulfil their obligation under point (b) of Article 26(1) of the Convention implementing the Schengen Agreement, carriers shall use the web service to verify whether a short-stay visa is valid, including if the number of authorised entries have already been used or if the holder has reached the maximum duration of the authorised stay or, as the case may be, if the visa is valid for the territory of the port of destination of that travel. Carriers shall provide the data listed under points (a), (b) and (c) of Article 16(1) of this Regulation. On that basis, the web service shall provide carriers with an OK/NOT OK answer. Carriers may store the information sent and the answer received in accordance with the applicable law. Carriers shall establish an authentication scheme to ensure that only authorised staff may access the web service. It shall not be possible to regard the OK/NOT OK answer as a decision to authorise or refuse entry in accordance with Regulation (EU) 2016/399. ***In cases where passengers are not allowed to board due to a query in VIS, carriers shall provide passengers with that information and the means to exercise their rights to access, rectification and erasure of personal data stored in VIS.***"; **[Am. 245]**

(2a) In Article 14, paragraph 3 is replaced by the following:

"3. Where it is necessary to enter or update the entry/exit record data of a visa holder, the border authorities may retrieve from the VIS and import into the EES the data provided for in point (d) of Article 16(1) and points (c) to (f) of Article 16(2) of this Regulation in accordance with Article 8 of this Regulation and Article 18a of Regulation (EC) No 767/2008."; **[Am. 246]**

(2b) Article 15 is amended as follows:

(a) paragraph 1 is replaced by the following:

"1. Where it is necessary to create an individual file or to update the facial image referred to in point (b) of Article 17(1), the facial image shall be taken live."; **[Am. 247]**

(b) the following paragraph is inserted:

"1a. The facial image referred to in point (d) of Article 16(1) shall be retrieved from VIS and imported into the EES."; **[Am. 248]**

(c) paragraph 5 is deleted; **[Am. 249]**

(3) in Article 35(4), the expression "through the infrastructure of the VIS" is deleted.

Article 5

Amendments to Regulation (EU) 2016/399

Regulation (EU) 2016/399 is amended as follows:

(1) in Article 8(3), the following point (ba) is added:

"(ba) if the third-country national holds a long stay visa or a residence permit, the thorough checks on entry shall also comprise verification of the identity of the holder of the long-stay visa or residence permit and the authenticity of the long-stay visa or residence permit by consulting the Visa Information System (VIS) in accordance with Article 22g of Regulation (EC) No 767/2008;

in circumstances where verification of the document holder or of the document in accordance with Articles 22g of that Regulation, as applicable, fails or where there are doubts as to the identity of the holder, the authenticity of the document and/or the travel document, the duly authorised staff of those competent authorities shall proceed to a verification of the document chip.";

(2) in Article 8(3), points (c) to (f) are deleted.

Article 7

Amendments to Regulation (EU) XXX on establishing a framework for interoperability between EU information systems (borders and visa) [interoperability Regulation]

Regulation (EU) XXX on establishing a framework for interoperability between EU information systems (borders and visa) [interoperability Regulation] is amended as follows:

(1) in Article 13(1), point (b) is replaced by the following:

"(b) the data referred to in Article 9(6), Article 22c(2)(f) and (g) and Article 22d(f) and (g) of Regulation (EC) No 767/2008;"

(2) In Article 18(1), point (b) is replaced by the following:

"(b) the data referred to in Article 9(4)(a)~~, (b) and (c)~~ ***to (cc)***, Article 9 (5) and (6), Article 22c(2)(a) to (cc), (f) and (g), Article 22d(a), (b), (c), (f) and (g) of Regulation (EC) No 767/2008;" **[Am. 250]**

(3) in Article 26(1), point (b) is replaced by the following:

"(b) competent authorities referred to in Article 6(1) and (2) of Regulation (EC) No 767/2008 when creating or updating an application file or an individual file in the VIS in accordance with Article 8 or Article 22a of Regulation (EC) No 767/2008;";

(4) Article 27 is amended as follows:

(a) in paragraph 1, point (b) is replaced by the following:

"(b) an application file or an individual file is created or updated in the VIS in accordance with Article 8, or Article 22a of Regulation (EC) No 767/2008;";

(b) in paragraph 3, point (b) is replaced by the following:

"(b) surname (family name); first name(s) (given name(s)); date of birth, sex and nationality(ies) as referred to in Article 9(4)(a), in Article 22c(2)(a) and in Article 22d(a) of Regulation (EC) No 767/2008;";

(5) in Article 29(1), point (b) is replaced by the following:

"(b) the competent authorities referred to in Article 6(1) and (2) of Regulation (EC) No 767/2008 for hits that occurred when creating or updating an application file or an individual file in the VIS in accordance with Article 8 or Article 22a of Regulation (EC) No 767/2008;".

Article 8

Repeal of Decision 2008/633/JHA

Decision 2008/633/JHA is repealed. References to Decision 2008/633/JHA shall be construed as references to Regulation (EC) No 767/2008 and shall be read in accordance with the correlation table in Annex 2“.

Article 9

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from ... [two years after the date of entry into force] with the exception of the provisions on implementing and delegated acts provided for in points (6), (7), (26), (27), (33) and (35) of Article 1, point (4) of Article 3 and point (1) of Article 4, which shall apply from the date of entry into force of this Regulation.

By ... [one year after the entry into force of this Regulation] the Commission shall submit a report to the European Parliament and to the Council on the state of play of the preparation of the full implementation of this Regulation. That report shall also contain detailed information on the costs incurred and information as to any risks which may impact the overall costs. **[Am. 251]**

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

ANNEX 2

CORRELATION TABLE

Council Decision 2008/633/JHA	Regulation (EC) No 767/2008
Article 1 Subject matter and scope	Article 1 Subject matter and scope
Article 2 Definitions	Article 4 Definitions
Article 3 Designated authorities and central access points	Article 22k Member States' designated authorities Article 22l Europol
Article 4 Procedure for access to the VIS	Article 22m Procedure for access to the VIS for law enforcement purposes
Article 5 Conditions for access to VIS data by designated authorities of Member States	Article 22n Conditions for access to VIS data by designated authorities of Member States
Article 6 Conditions for access to VIS data by designated authorities of a Member State in respect of which Regulation (EC) No 767/2008 has not yet been put into effect	Article 22r Conditions for access to VIS data by designated authorities of a Member State in respect of which this Regulation has not yet been put into effect
Article 7 Conditions for access to VIS data by Europol	Article 22p Procedure and conditions for access to VIS data by Europol
Article 8 Protection of personal data	Chapter VI Rights and supervision on data protection
Article 9 Data security	Article 32 Data security
Article 10	Article 33

Liability	Liability
Article 11 Self-monitoring	Article 35 Self-monitoring
Article 12 Penalties	Article 36 Penalties
Article 13 Keeping of VIS data in national files	Article 30 Keeping of VIS data in national files
Article 14 Right of access, correction and deletion	Article 38 Right of access, correction and deletion
Article 15 Costs	N/A
Article 16 Keeping of records	Article 22q Logging and documentation
Article 17 Monitoring and evaluation	Article 50 Monitoring and evaluation