



Doc. 15600

06 September 2022

Misuse of the Schengen Information system by Council of Europe member States as a politically-motivated sanction

Report¹

Committee on Legal Affairs and Human Rights

Rapporteur: Mr Ziya ALTUNYALDIZ, Türkiye, Members not belonging to a Political Group

Summary

The Committee on Legal Affairs and Human Rights is concerned about new cases of unjustified alerts into the European Union's Schengen Information System (SIS), allegedly based on politically motivated grounds. The European Union legislation, by referring to the notion of a "threat to public policy or public security or to national security", gives a large amount of discretion to the Schengen Area member States in deciding whether and in which circumstances they can place alerts in SIS.

Although States have a sovereign right to decide on who shall be allowed to enter their territories, member States of the Schengen Area are bound not only by the European Union legal order, but also by the European Convention on Human Rights. Thus, the use of alerts should not lead to any misuse of the system and should not infringe the human rights of third country nationals trying to enter the Schengen Area, in particular the right to respect for private and family life, the right to freedom of expression and prohibition of discrimination.

The committee proposes that the European Union and its member States take additional measures such as introducing effective remedies, ensuring transparency and establishing mediation bodies and adequate monitoring mechanisms of large-scale information systems.

1. Reference to committee: [Doc. 14652](#), Reference 4417 of 21 January 2019.



Contents	Page
A. Draft resolution	3
B. Explanatory memorandum by Mr Ziya Altunyaldiz, rapporteur	5
1. Introduction	5
1.1. Procedure	5
1.2. The motion for a resolution	5
2. Issues at stake	6
3. Freedom of movement in the legal framework of the Council of Europe	7
4. The functioning of the Schengen Information System	8
4.1. The Schengen area	8
4.2. The Schengen Information System	9
5. Conclusion	16
Appendix – Summary of member States' responses to a questionnaire on the legislation and practice of member States concerning the Schengen Information System	20

A. Draft resolution²

1. The Parliamentary Assembly recalls its [Resolution 1894 \(2012\)](#) “The inadmissibility of restrictions on freedom of movement as punishment for political positions” and stresses that since its adoption, many changes to the functioning of the Schengen Information System (SIS), including its reshaping into a more advanced version – SIS II – have been put in place.
2. The Assembly recalls that, in principle, States have a sovereign right under international law to decide on who shall be allowed to enter their territories. The European Convention on Human Rights (ETS No. 5) does not guarantee a right to entry to a specific State, as the European Court of Human Rights has repeatedly stressed.
3. New cases of allegedly unjustified alerts, including ones on politically motivated grounds, have been reported. The Assembly condemns such practices and recalls that member States of the Schengen Area are bound not only by the European Union legal order, but also by the European Convention on Human Rights, which shall “secure” the rights and freedoms guaranteed therein to “everyone within their jurisdiction”, notably the right to respect for private and family life and the protection against discrimination. This includes foreigners applying for a visa or seeking entry at the external border of the Schengen Area, all of whose member States are States Parties to the Convention.
4. The free movement of persons is one of the four basic freedoms of the European Union. The existence of the Schengen Area, based on the 1985 Schengen Agreement and the 1990 Schengen Convention, has strengthened this right by abolishing checks at internal borders, whilst subjecting the crossing of the European Union’s external border to more stringent controls and various preventive measures. In this respect, the SIS, whose purpose is to maintain a high level of security within the Schengen Area, is a key tool. Its good functioning depends on mutual trust between national authorities.
5. The Assembly notes that the current European Union legal framework on SIS II, by referring to the notion of a “threat to public policy or public security or to national security”, gives a large amount of discretion to the Schengen Area member States in deciding whether and in which circumstances they can place alerts in SIS II. It stresses that the use of alerts should not lead to any misuse of the system and should not infringe the human rights of third country nationals trying to enter the Schengen Area, in particular the right to respect for private and family life, the right to freedom of expression, the right to freedom of movement and the right to an effective remedy. If need be, additional measures should be taken to prevent misuse of the SIS and improve the protection of human rights of third-country nationals subject to alerts in the SIS.
6. Therefore, the Assembly calls on member States of the Schengen Area to:
 - 6.1. enter only accurate and lawful data in SIS II;
 - 6.2. make sure that the data in SIS are not entered for political reasons against a third country;
 - 6.3. respect the principles of proportionality and individual assessment of each case, when issuing alerts in SIS II;
 - 6.4. introduce transparency and adequate monitoring and verification mechanisms concerning the interoperability of large-scale information systems so that the data registered in one system are not unduly used by the other systems;
 - 6.5. provide for persons subject to a SIS II alert effective remedies against national administrative or judicial authorities’ decisions which have been at the origin of the alert;
 - 6.6. observe the right of third-country nationals to be informed about the inclusion of an alert in SIS II;
 - 6.7. stop practices that prevent citizens of States not belonging to the Schengen Area from participating in the cultural, social and scientific activities in the Schengen Area and hamper free trade;
 - 6.8. avoid any misuse of SIS II that could prevent the establishment of commercial activities and a more effective investment co-operation;
 - 6.9. adjust their national legislations to ensure that administrative decisions on refusal to issue a Schengen visa due to political or other reasons are subject to judicial review in the relevant member State;

2. Draft resolution unanimously adopted by the committee on 23 June 2022.

- 6.10. take all measures to ensure that the use of SIS and related systems should not set an obstacle to the achievement of a greater unity between Council of Europe member States, as enshrined in the Council of Europe Statute (ETS No. 1);
 - 6.11. provide for persons subject to a SIS II alert the right to access data relating to them and to request the correction of inaccurate data or the deletion of data which have been unlawfully stored in SIS II;
 - 6.12. provide for such persons the possibility to bring effective legal action before the courts or other competent bodies in order to access, correct, delete or retrieve data, or to obtain, where relevant, compensation in connection with an alert relating to them;
 - 6.13. make use of the Supplementary Information Request at the National Entries network (SIRENE) to verify relevant information before denying admission or a short-term visa to a third-country national;
 - 6.14. enhance co-operation between the competent national authorities examining individual cases of alerts (courts, data protection controllers and other relevant bodies);
 - 6.15. establish a mediation (ombudsperson-type) body, whose main task would be to examine whether human rights standards have been observed by national authorities when entering an alert in SIS II or denying entry to third country nationals on the basis of such an alert.
7. The Assembly also invites the European Union and calls on its member States to conclude as soon as possible the revision of the Schengen Evaluation Mechanism and to examine ways in which current and possible future deficiencies in the functioning of SIS II could be avoided. It invites the European Union to involve the European Parliament in these processes.
8. It also invites the European Union and calls on its member States to:
- 8.1. adopt guidelines on minimum common standards governing the SIS II alert procedure that would be applicable to third-country nationals as well as substantive criteria for issuing SIS II alerts;
 - 8.2. consider establishing a mediation (ombudsperson-type) body, whose main task would be to examine whether human rights standards have been observed by national authorities when entering an alert in SIS II or denying entry to third country nationals, or granting this competence to the European Ombudsman, the Fundamental Rights Agency of the European Union, the European Data Protection Supervisor or another European Union body.
9. The Assembly also calls on member States of the Schengen Area to collect and exchange data about current national practices concerning the use of SIS II alerts and their impact on human rights, and to co-operate in this respect also with Council of Europe member States which are not members of the European Union.

B. Explanatory memorandum by Mr Ziya Altunyaldiz, rapporteur

1. Introduction

1.1. Procedure

1. Following the reference of a motion for a resolution entitled “Misuse of the Schengen system by Council of Europe member States as a politically-motivated sanction”,³ to the Committee on Legal Affairs and Human Rights, the committee appointed Ms Olena Sotnyk (Ukraine, ALDE) as rapporteur on this subject, at its meeting in Paris on 4 March 2019. After Ms Sotnyk’s departure from the Parliamentary Assembly, the committee appointed Ms Irina V. Rukavishnikova (Russian Federation, NR) as her successor. Following the exclusion of the Russian Federation from the Council of Europe, the committee appointed me as rapporteur, on 4 April 2022.

2. Ms Rukavishnikova’s prepared a revised introductory memorandum, which was considered by the committee at the meeting of 5 June 2020 (by videoconference). The committee then approved a revised draft questionnaire to be sent to national delegations through the European Centre for Parliamentary Research and Documentation (ECPRD) and noted that the rapporteur’s request for the authorisation of a hearing with three experts and of a fact-finding visit to Brussels had been approved in the written consultation procedure, both subject to the availability of funds. On 14 September 2021, during a meeting held in a hybrid manner, the committee considered Ms Rukavishnikova’s revised introductory memorandum and held a hearing with the participation of:

- Ms Evelien Brouwer, Senior Researcher, Amsterdam Centre for Migration and Refugee Law, Vrije Universiteit Amsterdam, the Netherlands;
- Ms Nuala Mole, Founder and Senior Lawyer of the Advice on Individual Rights in Europe Centre, London, United Kingdom;
- Mr Vyacheslav A. Postavnin, Expert on Migration, Head of the Center for Analytical and Practical Research on Migration (the Scientific Center for Eurasian Integration), Russian Federation.

3. As regards the fact-finding activities, on 17 November 2021, Ms Rukavishnikova had an exchange by videoconference with officials from the European Commission, Directorate General for Migration and Home Affairs (DG HOME), Unit B3-Schengen Information System, and Mr Jan-Christoph Oetjen, a member of the European Parliament (Germany, Renew Europe Group) and its working Group on Schengen Scrutiny (within the Committee on Civil Liberties, Justice and Home Affairs – LIBE). On 7-8 February 2022, she paid a fact-finding visit to Brussels (Belgium), where she met Mr Matthias Oel, European Commission, DG HOME, Director Schengen, Borders and Innovation, and Mr Jure Tanko, advisor to Ms Tanja Fajon, member of the European Parliament (Slovenia, Group of Progressive Alliance of Socialist and Democrats). The meetings with MEP Fabienne Keller (France, Renew Europe Group), Ms Clara Guerra, Vice-Chair and Acting Chair of the SIS II Schengen Coordination Group, and other officials of the European Commission, Directorate General for Justice and Consumers (DG JUST), Unit B2 – Procedural criminal law, took place by videoconference.

1.2. The motion for a resolution

4. The signatories of the motion for a resolution refer to the previous work of the Assembly on this subject, namely its [Recommendation 1648 \(2004\)](#) “Consequences of European Union enlargement for freedom of movement between Council of Europe member States” and [Resolution 1894 \(2012\)](#) “The inadmissibility of restrictions on freedom of movement as punishment for political positions”. They stress that since then, new cases of allegedly politically motivated misuse of the Schengen system have occurred in several Council of Europe member States, “which made use of their legal right to control access to their respective territories in order to deny entry to certain persons”. Moreover, “this would have had the result of unjustifiably denying those persons access to the entire Schengen territory”. According to the movers of the motion, “the Assembly cannot accept that there are still cases of misuse of the Schengen System” and therefore should prepare a new report on this issue

3. [Doc.14652](#).

2. Issues at stake

5. In its [Recommendation 1648 \(2004\)](#) “Consequences of European Union enlargement for freedom of movement between Council of Europe member States” adopted on 30 January 2004,⁴ the Assembly recalled that “the Schengen system is intended to establish free movement of persons within a multinational territory (the Schengen area) without internal borders” and that the Council of Europe, “since the early years of its existence” had also been “active in pursuing the same aims”, bearing in mind, in particular all the conventions concerning freedom of movement of persons adopted under its auspices.⁵ The Assembly was firmly opposed to “(...) any measures which might act to divide the peoples and States of a continent which has only recently achieved a historic level of political, social, economic and cultural unity and harmony”. The Committee of Ministers replied to this recommendation in June 2004 and April 2006.⁶ A few years later, in its [Resolution 1894 \(2012\)](#) “The inadmissibility of restrictions on freedom of movement as punishment for political positions” (adopted on 29 June 2012),⁷ it focused on the link between freedom of movement of persons and freedom of expression and stressed that “(...) freedom of movement should not be restricted as a sanction for the expression of peacefully held political opinions” and that entries into the Schengen Information System must not be misused in order to deny persons, who are not nationals of a European Union member State, access to the Schengen area as a punishment for expressing such views. It also recalled that the Schengen States had a duty “to provide for swift judicial or administrative review of any entry into the Schengen Information System”. Moreover, the issue of targeted sanctions adopted by the European Union Council or European Union member States was to a certain extent examined in Assembly [Resolution 1597 \(2008\)](#) and [Recommendation 1824 \(2008\)](#)⁸ “United Nations Security Council and European Union blacklists” and in the report by our former colleague Mr Dick Marty (Switzerland, ALDE).⁹ The Assembly also examined the issue of the misuse of Interpol’s red notices in its two Resolutions: 2315 (2019) on “Interpol reform and extradition proceedings: building trust by fighting abuse” and [2161 \(2017\)](#) on “Abusive use of the Interpol system: the need for more stringent legal safeguards”.

6. Since the adoption of the Assembly’s [Resolution 1894 \(2012\)](#) “The inadmissibility of restrictions on freedom of movement as punishment for political positions”, many changes to the functioning of the Schengen Information System (SIS) have been put in place. New cases of allegedly unjustified alerts have also been reported. For example, in August 2018, the head of the NGO Open Dialog Foundation, Lyudmyla Kozlovskaya, a Ukrainian national, residing in Poland and married to a Polish citizen, Bartosz Kramek, a civic activist, was denied entry to Belgium following an alert introduced to the Schengen Information System (now SIS II) by the Polish authorities. The alert was based on grounds of national security. Ms Kozlovskaya, who has since been granted a five-year residence permit in Belgium and whose name has been removed from SIS II, claims that the introduction of an alert in the SIS II was a form of political persecution because of her and her husband’s civic activities and their criticising the Polish Government.¹⁰ Following her appeal, on 16 April 2019, the regional administrative court in Warsaw delivered its judgment in her case. It considered that the alert was not sufficiently evidence-based and repealed the decisions of the Head of the Foreigners’ Office.

7. Other cases of allegedly unjustified alerts have also been reported. In November 2017, a Ukrainian political scientist and civil servant working on historical memory issues, Mr Svyatoslav Sheremeta, accused of being “anti-Polish”, was placed on the SIS list by the Polish authorities and refused entry to Poland, although he had a German Schengen visa. Despite the Polish authorities’ alert, he was allowed to enter Germany a few weeks later.¹¹ Moreover, in April 2019, Estonia issued five-year Schengen entry bans against two journalists of the Russia-1 TV channel after they used hidden cameras to videotape members of the Jehovah’s Witnesses community in Tallinn. The authorities believe “that the journalists’ actions were aimed at mocking this religious group and amounted to religious discrimination which may develop into incitement of hatred”.¹² Finally, an American pastor known for “his anti-LGBTI sermons and for questioning evidence of the Holocaust”, Steven Anderson, has been banned from entering the Schengen zone by the Netherlands (and also from entering the UK and Ireland).¹³

4. See report by the Committee on Legal Affairs and Human Rights, rapporteur: Mr Vitaliy Shybko (Ukraine, Socialist Group), [Doc. 9979](#) rev. of 15 October 2003.

5. Paragraph 6 of the recommendation.

6. [Doc. 10219](#) of 21 June 2004 and [Doc. 10873](#) of 7 April 2006. In the latter document, the Committee of Ministers referred extensively to the work of the European Committee on Legal Co-operation (CDCJ).

7. On the basis of a report of this committee, rapporteur: Mr Haluk Koç (Türkiye, SOC), [Doc. 12943](#).

8. See also the Committee of Ministers’ reply to this recommendation, [Doc. 11690](#) of 21 July 2008.

9. [Doc. 11454](#) of 16 November 2007.

10. <https://en.odfoundation.eu/t/bringherback-to-the-eu/>.

11. <https://wiadomosci.dziennik.pl/swiat/artykuly/563946,swiatoslaw-szeremeta-twierdzi-ze-ominal-zakaz-wjazdu-do-strefy-schengen.html>.

12. <https://news.err.ee/929589/iss-ministry-issued-schengen-entry-ban-against-russia-1-employees>.

8. There are also widespread allegations that certain Schengen Area member States use alerts as a political leverage against third-countries' nationals in such a way that the actual purpose of issuing alerts against individuals is in fact unrelated to the stated reasons. In such cases, issuing an alert against a third-country national on the basis of "national security" bears no relationship with that individual's personal situation or status, but appears to be a hidden sanction directly targeting the third country of which the person concerned is a national. Such abusive practices do not only entail a risk of violating several Council of Europe conventions but are also prone to undermining the whole SIS system by forcing the executing member State to unintentionally participate in the issuing State's hidden political agenda.

9. In addition to the misuse of the Schengen System for political reasons, it is observed that the System is used in a way that harms commercial relations and activities, although some countries have bilateral or multilateral co-operation on provisions based on and facilitated by certain agreements with the European Union.

10. Trade fairs and other commercial events are representative of the business world. However, applications for Schengen visas made for such purposes might not be found convincing and might be rejected as ungrounded, although trade fair invitations have been received, the rents for trade fair venues have been paid, procedures for booking transportation and accommodation have been completed and so on. Other problems have been reported as regards getting an appointment date in relation with a visa application, the excessive number of documents requested in the application procedure and the high level of visa application fees.

11. Moreover, in some areas that are not a priori subject to abuses, like commercial co-operation, some steps taken on the basis of international agreements might limit a systematic refusal to grant visas, unless political concerns have been raised.

12. Although States, in principle, have the sole competence in determining the conditions of entry of other countries' citizens into their territory, they are at the same time subject to obligations stemming from international treaties on human rights protection and the rule of law, when they take decisions on such matters. Excessively long bureaucratic procedures, complicated application forms, long queues at diplomatic representations, exaggerated conditionality on the applicants' financial situation, interrogative questioning and unexplained visa denials curtail the cross-border movement of persons.

13. These practices erect a barrier to those who would like to participate in cultural, social and scientific activities in Schengen Area member States, prevent them from visiting their relatives residing there and hamper free trade. In addition, they constitute an obstacle to the achievement of a greater unity between Council of Europe member States and prevent them from safeguarding and realising its ideals and principles.

14. Moreover, in accordance with international conventions which enshrine the right to freedom of movement and especially the European Convention on Human Rights (ETS No. 5), it is necessary to prevent the abuse of the principle of State sovereignty as regards regulating entry into its territory on the basis of political motives. In this context, it would be beneficial to include special provisions in legislation of States that refuse to grant visas for inappropriate reasons, including political ones. Since national legal remedies must be first exhausted, it is considered that the lack of such regulations in the legal systems of the Schengen Area member States hampers the effectiveness of the judicial proceedings.

15. In my report, I will therefore examine the current functioning of the SIS, with a special focus on alerts introduced to it in order to prevent the entry of third-country nationals, as well as on European Union member States' leeway in this respect and the implications of the arbitrary use of SIS alerts on human rights protection. Furthermore, I will also focus on inefficient and inappropriate usage of SIS alerts that could disrupt the enjoyment of freedom of movement and cause severe obstacles in particular to businesses and the commercial activities of some stakeholders. On the basis of this analysis, I will also elaborate further recommendations on how to prevent the misuse of alerts, especially if that leads to human rights violations.

3. Freedom of movement in the legal framework of the Council of Europe

16. Under public international law, notwithstanding norms on asylum, States can determine the terms and conditions under which non-nationals ("aliens") are admitted to their territory. Therefore, there is no right to enter and to remain in a State of which the individual is not a national, which the European Court of Human Rights has emphasised in its case law on very many occasions.¹⁴

13. <https://nltimes.nl/2019/05/01/american-hate-preacher-denied-access-netherlands> and <https://www.bbc.com/news/world-europe-48252527>.

17. The Council of Europe has, since the early years of its existence, been active in the domain of free movement of persons. A few conventions in this field have been adopted: the 1955 European Convention on Establishment (ETS No. 19); the 1957 European Agreement on Regulations Governing the Movement of Persons between Member States of the Council of Europe (ETS No. 25); the European Convention on the Legal Status of Migrant Workers (ETS No. 93); and the European Outline Convention on Transfrontier Co-operation between Territorial Communities or Authorities (ETS No. 106). However, with the exception of the last convention, these treaties have been ratified by a small number of member States. In particular, the European Agreement on Regulations governing the Movement of Persons between Member States of the Council of Europe, which is intended to facilitate personal travel, has been ratified by only seventeen member States¹⁵ and the monitoring of its implementation was abandoned in 1991 before many current member States joined the Council of Europe.¹⁶

18. The European Convention on Human Rights requires its States Parties to “secure” the rights and freedoms guaranteed therein to “everyone within their jurisdiction”, including foreigners applying for a visa or seeking entry at a border (Article 1). However, it does not provide for a right to entry to a specific State (including a specific member State of the Council of Europe). Article 2 of Protocol No. 4 (ETS No. 46) to the Convention enshrines the right to freely move *within* a country once lawfully there and the right to leave any country. It does not, however, deal with the right of entry *into* a country. Besides, not all member States of our Organisation have acceded to this Protocol.¹⁷ Moreover, the European Court of Human Rights has held that decisions regarding the entry, residence and expulsion of aliens do not fall within the scope of the “fair trial” guarantee of Article 6 (1) of the Convention, as they do not concern civil rights or obligations or a criminal charge.¹⁸

19. Member States’ right to determine aliens’ entry into their territory can be limited in certain circumstances for family reasons. The Court has held that, in specific situations, persons could rely on Article 8 of the Convention, enshrining the right to respect for private and family life, in order to enter and reside in a member State for the purposes of joining their family.¹⁹

20. The Court has not had many occasions to examine cases concerning Schengen blacklisting of third-country nationals wishing to enter the territory of European Union member States. In the case of *S.N. and T.D. v. Latvia*, which concerned the blacklisting and expulsion from Latvia of two Russian nationals considered to be a threat to national security and public order and safety, the former issue was not examined on the merits because of non-exhaustion of domestic remedies.²⁰ In the case of *Dalea v. France*²¹ a Romanian national who had business connections in France and Germany complained of a violation of Article 8 (under the right to respect for a private life) following his listing in the SIS by France. The complaint was found to be inadmissible as being manifestly ill-founded due to France’s wide margin of appreciation in relation to controlling the entry of non-nationals into its territory.

4. The functioning of the Schengen Information System

4.1. The Schengen area

21. The free movement of persons is one of the four freedoms of the European Union.²² It is a right guaranteed by the European Union treaties to all its citizens entitling them to travel, work or live in any European Union member State. Moreover, Article 45 of the [Charter of Fundamental Rights of the European Union](#) provides for freedom of movement within the territory of the member States for European Union citizens

14. [Handbook on European law relating to asylum, borders and immigration](#), 2015, p. 26. See, for example, *Vilvarajah and Others v. UK*, application No. 13163/87, judgment of 30 October 1991, para. 102.

15. As of 17 June 2022:

www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatyenum=025.

16. For more information, see Mr Koç’s report, [Doc. 12943](#) op. cit., para. 14.

17. 42 of the 46 have ratified the Protocol, see: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=046&CM=8&DF=09/01/2012&CL=ENG>.

18. See, for example, *Maaouia v. France*, application No. 39652/98, judgment of 5 October 2000 (Grand Chamber), para. 40.

19. See, for example, *Sen v. Netherlands*, application No. 31465/96, judgment of 21 December 2001.

20. See, for example, *S.N. and T.D. v. Latvia*, application No. 5794/13, decision of 6 December 2016, para. 85.

21. *Dalea v. France*, application No. 964/07, decision of 2 February 2010, para. 2.

22. Article 3(2) Treaty of the European Union (TEU) and provisions of Title IV of the Treaty on the Functioning of the European Union (TFEU).

and legally resident third country nationals. This freedom was further developed by enabling European Union citizens to cross internal borders without being subjected to border checks following European Union member States' co-operation in relation with the "Schengen area".

22. The establishment of the Schengen area dates back to the Schengen Agreement adopted on 14 June 1985 by France, Germany and the Benelux countries with the aim of gradually abolishing controls at the common borders and strengthening control of the external borders. On 19 June 1990, the same States also adopted the Convention implementing the Schengen Agreement ("the Schengen Convention"). In view of the possible security deficit resulting from the abolition of border controls, this convention, which came into force on 26 March 1995 for the original signatory countries, plus Spain and Portugal, introduced compensatory measures with regard to asylum and co-operation between police, judicial and customs authorities. It also provided for the creation of the Schengen Information System, which allowed the competent national authorities to access data on individuals who were not entitled to enter the free movement area, commonly referred to as the "Schengen Area". Today, the Schengen Area encompasses most European Union member States. All European Union member States, except for Bulgaria, Croatia, Cyprus, Ireland and Romania are part of the Schengen Area.²³ Non European Union members, Iceland, Norway, Switzerland and Liechtenstein, are also part of the Schengen Area and are connected to the SIS. This border-free area guarantees free movement to many third-country nationals (including tourists, businessmen and other persons legally residing in European Union member States) without requiring multiple visas to travel within the Schengen zone, in addition to more than 400 million European Union citizens.

23. Initially, States' co-operation in relation with the Schengen Area developed in a purely intergovernmental form, outside the framework of the founding treaties of the European Union, up until the time the Schengen Agreement and the Schengen Convention were written into a Protocol to the Treaty of Amsterdam, which entered into force on 1 May 1999 and created an "area of freedom, security and justice".²⁴ Until the Treaty of Lisbon entered into force on 1 December 2009, certain Schengen co-operation related policies such as police and judicial co-operation and security measures remained under intergovernmental governance. Since then all aspects of Schengen co-operation have fallen under the European Union regime (former "first pillar") and the measures taken in this context are now subject to the scrutiny of the Court of Justice of the European Union.²⁵ Moreover, several articles of the Schengen Convention have been replaced by European Community or European Union legal acts that participating non-European Union members (such as Iceland, Norway, Switzerland and Liechtenstein) have had to accept.²⁶ European Union candidate countries are required to adopt the *Schengen acquis*.²⁷

4.2. The Schengen Information System

4.2.1. General functioning

24. The lack of controls on internal borders between Schengen Area States is compensated for by stricter controls on the external borders and by the imposition of various preventative measures. The key principle of the Schengen Area is that while border controls are largely abolished within it, the external border of the area is carefully policed. The Schengen Information System is a key tool in this respect. It is a database that allows relevant officials (such as the police and border guards) across the Schengen area to access and consult alerts about wanted or missing persons and objects, as well as persons who are subject to entry bans.²⁸

25. The SIS II, a more advanced version of the SIS, became operational on 9 April 2013. SIS II has enhanced functionalities, such as the possibility to use biometrics, new types of alerts and the possibility to link different alerts and a facility for direct queries. Its legal basis is currently defined by Regulation (EC) No 1987/2006 called "SIS II Regulation",²⁹ Regulation (EC) No 1986/2006 concerning alerts on vehicles³⁰ and

23. However, Bulgaria, Croatia and Romania are now in the process of joining it.

24. See also Council Decision 1999/435/EC of 20 May 1999 concerning the definition of the Schengen acquis for the purpose of determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the acquis.

25. See, in particular, Article 77 of the TFEU.

26. E. de Capitani, *The Schengen system after Lisbon: from cooperation to integration*, ERA Forum (2014), published online on 21 May 2014, p. 108.

27. Which was defined in Council Decisions 1999/435/EC and 1999/436/EC of 20 May 1999 and includes mainly the Schengen Agreement, the Schengen Convention and agreements accession to the Schengen Convention by Italy, Spain, Portugal, Greece, Austria, Denmark, Finland and Sweden.

28. For more information: [European Parliament briefing, Use of the Schengen Information System for the return of illegally staying third-country nationals](#), 18 October 2018.

Council Decision 2007/533/JHA ("SIS II Decision").³¹ On 28 December 2018, three new regulations were added to the legal framework governing the SIS II.³² Their aim is to strengthen the current system by including new alerts on return decisions, requiring compulsory inclusion of entry bans in the system and introducing stronger data protection rules.

26. On May 2019, the EU adopted Regulation 2019/817,³³ which applies to information systems in the field of borders and visa, and Regulation 2019/818 on systems in the field of police and judicial co-operation, asylum and migration.³⁴ Both regulations aim at providing for easier information sharing and improving security in the European Union by establishing interoperability and multipurpose use of European Union large-scale databases so as to create a European-wide search portal, allowing competent authorities to search multiple information systems simultaneously, using both biographical and biometric data. Such interoperability structure is thus based on a network or a mechanism through which different authorities can check whether information on a particular individual is available in one of the European Union databases. The databases that can be connected via interoperability include systems such as SIS II, Eurodac, and Visa Information System as well as the European Police Office (Europol) databases.

27. The SIS II consists of three components: 1) a central system; 2) national systems in each member State that communicate with the central system,³⁵ and 3) a communication infrastructure. Member States can enter, update, delete and search data via their national systems and exchange information via the supplementary information request at the national entry bureaux (SIRENE). Member States are responsible for setting up, operating and maintaining their national systems and national SIRENE bureaux.

4.2.2. Alerts in the SIS II

28. One of the ways in which the external borders of the Schengen area can be controlled is through the issuing of alerts in the SIS II against individuals and objects.³⁶ As regards alerts against individuals, according to Article 3 a) of the SIS II Regulation, an "alert" is "a set of data entered in SIS II allowing the competent authorities to identify a person with a view to taking specific action".³⁷ Before issuing an alert, member States shall determine whether the case is adequate, relevant and important enough to warrant entry of the alert in the SIS II (Article 21 of the SIS II Regulation). An alert may not be entered without the following information concerning the given person: his/her surname(s) and forename(s), name(s) at birth and previously used names and any aliases, sex, a reference to the decision giving rise to the alert and action to be taken (Articles 23(1) and 20(2) of the SIS II Regulation).

29. SIS alerts cover the following categories of persons:

- third-country nationals to be refused entry into or stay within the Schengen Area (Article 24 of the SIS II Regulation);

29. Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II). To be soon replaced by Regulation (EU) 2018/1861 on the establishment, operation and use of the SIS in the field of border checks and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006.

30. Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates.

31. Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II).

32. Regulation (EU) 2018/1860 on the use of the Schengen Information System for the return of illegally staying third-country nationals; Regulation (EU) 2018/1861 on the establishment, operation and use of the SIS in the field of border checks and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006; Regulation (EU) 2018/1862 on the establishment, operation and use of the SIS in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU.

33. Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA.

34. Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816.

35. Here is the [list of such authorities](#).

36. See Article 96 of the Schengen Convention (concerning alerts on persons).

37. The definition of "alert" included in Article 3(1)(a) of the SIS II Decision also refers to an object.

- persons for whom a European Arrest Warrant was issued or who are wanted for arrest for extradition purposes, entered at the request of the judicial authority of the issuing member State (Article 26 of the SIS II Decision);³⁸
- missing persons (adults and minors) (Article 32 of the SIS II Decision);
- persons sought, summoned or witnesses in connection with criminal judicial proceedings (Article 34 of the SIS II Decision);
- persons for discreet or specific checks, including for the purposes of prosecuting criminal offences and preventing threats to public or national security (Article 36 of the SIS II Decision).³⁹

4.2.3. Alerts based on Article 24(1) of the SIS Regulation

30. For the purposes of my report, I plan to cover primarily the first category of persons. Article 24(1) of the SIS II Regulation stipulates that the data concerning such persons “shall be entered on the basis of a national alert resulting from a decision taken by the competent administrative authorities or courts in accordance with the rules of procedure laid down by national law taken on the basis of an individual assessment”⁴⁰ and that “appeals against these decisions shall lie in accordance with national legislation.”⁴¹ An alert shall be entered where the national body’s decision is based on a threat to public policy or public security or to national security which the presence of the third-country national in question in the territory of a member State may pose. This might be, in particular, the case of a third-country national who has been convicted in a member State of an offence carrying a penalty involving deprivation of liberty of at least one year or in respect of whom there are serious grounds for believing that he/she has committed a serious criminal offence⁴² or in respect of whom there are clear indications of an intention to commit such an offence in the territory of a member State (Article 24(2) of the SIS II Regulation). An alert may also be entered if the third-country national has been subject to a measure involving expulsion, refusal of entry or removal which has not been rescinded or suspended, that includes or is accompanied by a prohibition on entry or, where applicable, a prohibition on residence, based on a failure to comply with national regulations on the entry or residence of third-country nationals (Article 24(3) of the SIS II Regulation).⁴³

31. Article 25 (1) of the SIS II Regulation refers to alerts concerning third-country nationals who benefit from the right of free movement within the European Union, within the meaning of [Directive 2004/38/EC](#) on the right of citizens of the Union and their family members to move and reside freely within the territory of the member States and stipulates that such alerts shall be in conformity with the rules adopted in the implementation of that directive. If there is a hit on an alert concerning such a third-country national, the member State executing the alert shall consult immediately the issuing member State in order to decide without delay on the action to be taken (Article 25 (2) of the SIS II Regulation). Alerts issued in relation with entry bans based on legal acts adopted by the Council of the European Union, including measures implementing travel bans issued by the United Nations Security Council, fall within the scope of Article 26 of the SIS II Regulation. The member State responsible for entering, updating and deleting these alerts on behalf of all member States shall be designated at the moment of the adoption of the relevant measure (Article 26 (3) of the SIS II Regulation).

32. Article 6 (1) (d) of the [Schengen Borders Code](#)⁴⁴ stipulates explicitly that third-country nationals for whom an alert has been issued in the SIS for the purpose of refusing entry do not fulfil the conditions for entering the territory of the European Union member States. However, a derogation has been foreseen from this rule: a third-country national may be authorised by a member State to enter its territory on humanitarian grounds, on grounds of national interest or because of international obligations. If he/she is subject of an alert in the SIS, the member State authorising him/her to enter its territory shall inform the other member State accordingly (Article 6(5)(c)).

38. In practice, such alerts are inserted in the SIS II if the person subject to an European Arrest Warrant cannot be located.

39. In addition, Article 40 of Regulation (EU) 2018/1862 introduces a new category of alerts “on unknown wanted persons for the purposes of identification under national law”.

40. Article 24.1 a) of Regulation (EU) 2018/1862 stipulates that the individual assessment includes “an assessment of the personal circumstances of the third-country national concerned and the consequences of refusing him or her entry and stay”.

41. According to Article 24.4, second sentence, of Regulation (EU) 2018/1862, the appeal shall be conducted “in accordance with Union and national law, which shall provide for an effective remedy to be requested before a court”.

42. Article 24.1 b) of Regulation (EU) 2018/1862 specifies that this may be in particular a “terrorist offence”.

43. See the Return Directive 2008/115/EC.

44. Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code). It is now under revision.

33. Access to data entered in SIS II is given to national authorities responsible for border control, police, customs, visa and vehicle registration and, by extension, to national judicial authorities when this is necessary for the performance of their tasks.⁴⁵ A list of competent authorities which have access to the SIS II is published annually in the Official Journal of the European Union.⁴⁶ Europol and the European Union's Judicial Cooperation Unit (Eurojust) have limited access rights for performing certain types of queries. SIS checks are mandatory for the processing of short-stay visas, for border checks for third-country nationals and, on a non-systematic basis, for European Union citizens and other persons enjoying the right of free movement. Every police check on the territory of a Schengen State should include a check in SIS II.⁴⁷

34. According to Article 29(1) of the SIS II Regulation, alerts shall be kept "only for the time required to achieve the purposes for which they were entered". A member State issuing an alert shall, within three years of its entry, review the need to keep it (Article 29 (2)), but it may also do so earlier or, in some circumstances, keep the alert longer (Article 29 (3) and (4)). If no extension has been communicated to the central system, alerts are automatically erased after the three-year period (Article 29 (5)). Only the issuing member State is authorised to modify or delete the alert. It is also responsible for ensuring that the data are accurate, up-to-date and entered into SIS II lawfully (Article 34 of the SIS II Regulation). If another member State has evidence suggesting that an item of data is factually incorrect or has been unlawfully stored, it shall inform the issuing member State according to the procedure foreseen in Article 34 (3) and (4) of the SIS II Regulation.

35. In accordance with data protection principles,⁴⁸ all individuals whose data are processed in SIS II enjoy the following rights: the right of access to data relating to them stored in SIS II; the right to correction of inaccurate data or deletion when data have been unlawfully stored and the right to bring proceedings before the courts or competent authorities to obtain correction or deletion of data or to obtain compensation.⁴⁹ As regards the first right, any person wishing to find out about information relating to him or her stored in SIS II has the right to make a request in this respect, as provided for by the national law of the member State before which they invoke that right. Access may only be refused when "this is indispensable for the performance of a lawful task related to an alert and for protecting the rights and freedoms of other people" (Article 41 (1) and (4) of the SIS II Regulation). This right of access is direct in some member States (namely the request has to be made directly to the authorities processing the data) or indirect in others (namely the person has to apply to the national data protection authority of the State where the request is submitted).⁵⁰ Besides that, any person has the right to have factually inaccurate data relating to them corrected or unlawfully stored data deleted (Article 41 (5)). If individuals exercise one or both of these two rights, they shall be provided the information as soon as possible and in any event not later than 60 days from the date of request for access (Article 41 (6)). They shall also be informed about the follow-up given to the exercise of their rights of correction or deletion as soon as possible and in any event not later than three months from the date of their application (Article 41 (7)). Third-country nationals who are subject to an alert shall be informed in accordance with the European Union legislation on data protection; this shall be done in writing and a copy of or a reference to the national decision giving rise to the alert shall be provided. However, if the national law allows for the restriction of the right to information, in particular in order to safeguard national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences the information shall not be provided (Article 42). Moreover, individuals may bring actions before the courts or other authorities competent under the national law to access, correct, delete or retrieve information, or to obtain compensation in connection with an alert relating to them (Article 43 (1) of the SIS II Regulation) and member States "undertake mutually to enforce final decisions" handed down by the said courts or authorities (Article 43 (2)).

45. See, in particular, Article 27 of the SIS II Regulation.

46. [C-287/1](#) of 16 July 2021.

47. European Parliament briefing, *supra* note 28.

48. Unlike the Convention, the European Union Charter of Fundamental Rights explicitly guarantees data protection rights: "Article 8: Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law." See also the [European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data](#).

49. See Articles 41 and 43 of the SIS II Regulation. For more information see SIS II Supervision Coordination Group, [The Schengen Information System. A Guide for Exercising the Right of Access](#), which describes the procedures before national data protection authorities.

50. [The Schengen Information System. A Guide for Exercising the Right of Access](#), *op. cit.*, p. 8.

4.2.4. European Union bodies responsible for the management and oversight of SIS II

36. The European Union Agency for large-scale IT systems in the area of freedom, security and justice ([eu-LISA](#)), which was established in 2011 and became operational on 1 January 2012, is responsible for the operational management of the central system and the communication infrastructure. It ensures the continuous, uninterrupted exchange of data between national authorities 24 hours a day, 7 days a week, and is responsible for monitoring the performance of the system as well as providing training on SIS II to national operators, SIRENE staff and Schengen evaluators. It also ensures the operational management of other large-scale European Union information systems: the Visa Information System and Eurodac (dealing with the management of European asylum applications), as well as of the ones foreseen to enter into operation in the near future (the Entry/Exit System – EES, the European Travel Information and Authorisation System – ETIAS and the European Criminal Records Information System – Third Country Nationals – ECRIS-TCN). The headquarters of eu-LISA are in Tallinn (Estonia), whilst its operational centre is in Strasbourg.

37. The European Commission is responsible for the general oversight and evaluation of the system (the Schengen Evaluation Mechanism – SEM)⁵¹ and for the adoption of implementing measures.⁵² The European Data Protection Supervisor (EDPS) monitors the application of the data protection rules for the central system, while the national data protection authorities supervise the application of the data protection rules in their respective countries (see, in particular Articles 44 and 45 of the SIS II Regulation). The Schengen Information System II Supervision Coordination Group (“[SIS II SCG](#)”), a body composed of representatives of the national data protection authorities of the member States and the EDPS, ensures co-ordinated supervision in the area of personal data protection of SIS II. It meets at least twice a year to: share experience, discuss problems regarding the interpretation or the application of the SIS II legal framework, analyse difficulties regarding the supervision or the exercise of the rights of data subjects, assist each other when carrying out audits and inspections and draw up harmonised proposals for joint solutions and promote awareness of data protection rights.⁵³ As regards the European Parliament, although it has no specific role under the SIS II legal framework, it plays an active role in monitoring the application of the Schengen acquis. Its Working Group on Schengen Scrutiny (established within the LIBE Committee) liaises with the European Commission and the Council at the relevant stages of the evaluation and monitoring process.

38. According to eu-LISA, in 2020, member States performed on average more than 10 million searches per day in SIS II, compared with 18 million per day in 2019.⁵⁴ The decrease may well be due to reduced cross-border traffic during the Covid-19 pandemic. In the whole of 2020, SIS II was accessed over 3.7 billion times by all member States (a 44% decrease from 2019).⁵⁵ On 31 December 2020, there were a total of 93.4 million alerts stored in SIS II, out of which alerts on persons represented 1% (964 720). Italy, France, Germany and Spain issued the highest number of all SIS II alerts. Out of 964 720 alerts on persons, 519 530 concerned third country nationals to be refused entry into or stay within the Schengen area (Article 24 of the SIS II Regulation).⁵⁶ Such alerts generated 47 583 hits.⁵⁷

4.2.5. Practice of the Schengen area member States as regards the use of alerts based on Article 24(1) of the SIS II Regulation

39. In order to collect information on the practice of the Schengen area member States as regards their use of alerts based on Article 24(1) of the SIS II Regulation, I had sent, through the ECPRD, a questionnaire to national delegations. The 19 replies received in response to it are summarised in more detail in the Appendix

51. Put in place by the Council of the European Union and the European Parliament Regulation 1053/2013/EU establishing the Schengen evaluation and monitoring mechanism. It is shared between the European Commission and member States' experts and assesses the implementation measures in a number of areas, including the SIS. The SEM is now under revision. In November 2020, the European Commission adopted its latest report on the functioning of the SEM (for 2015-2019), [COM\(2020\) 779 final](#). See European Parliamentary Research Service's briefings: Revision of the Schengen Evaluation and Monitoring Mechanism. Regulation (EU) No 1053/2013, PE 662.633, May 2021, and Improving the Schengen evaluation and monitoring mechanism, PE 964.228, October 2021, and European Parliament, Committee on Civil Liberties, Justice and Home Affairs (rapporteur: Tanja Fajon), Annual Report on the Functioning of the Schengen Area, 2019/2196(INI), 1 June 2021.

52. Since 2014, the European Commission (DG HOME B3) received a total of 18 “information requests” concerning the functioning of the SIS II in general (including six in 2021).

53. [Schengen Information System](#), [European Data Protection Supervisor \(europa.eu\)](#). The SIS II Supervision Coordination Group was set up under Article 46 of the SIS II Regulation and Article 62 of the SIS II Decision.

54. [Eu-LISA, SIS II – Annual Statistics, Factsheet. March 2021](#).

55. *Ibidem*.

56. [Eu-LISA, SIS II – 2020 Statistics](#), March 2021, pp. 10, 12-13.

57. *Ibidem*, p. 14.

to this report. It results therefrom that the decisions on entering an alert in the SIS II because of an alleged threat to public policy, public security, or national security are usually taken by the police, border control authorities or administrative bodies. A person subject to an alert usually has access to a remedy before the authority that has issued the alert and/or to a court. Some delegations also provided information about the possibility of requesting access to data relating to the alert and the correction of stored data before the data protection body.

4.2.6. Areas of possible misuse of the SIS II

40. As indicated by Ms Evelien R. Brouwer at the hearing of 14 September 2021, the possible misuse of the Schengen Information System in relation to alerts might be related to five issues: 1) the respect of obligations of the issuing State when reporting a third country national as inadmissible in the SIS, 2) ensuring transparency and effective monitoring system as regards the interoperability of large-scale information systems, including SIS II; 3) guaranteeing that the SIS is not used by any member State as a hidden political sanction against any third country on issues unrelated to the security of the Schengen Area; 4) the respect of obligations of the executing State when deciding on a SIS alert and 5) the existence of the right to an effective remedy.

41. Concerning the obligations of the issuing State, the main problem might be related to the possibility to issue an alert on grounds of a threat to public policy or public security or to national security, including a situation where there are “serious grounds for believing that the third country national has committed a serious criminal offence” or if “there are clear indications of an intention to commit such an offence in the territory of a member State” (Article 24(2) of the SIS II Regulation). This gives national authorities much leeway. However, the national authorities’ discretionary power is subject to two important conditions: firstly, before issuing a SIS alert, a member State must determine whether the case is “adequate, relevant, and important enough” (the principle of proportionality) and, secondly, the alert must follow an individual assessment (Articles 21 and 24(1) of the SIS II Regulation).⁵⁸ Furthermore, the issuing State must inform third-country nationals about the fact they are reported into SIS and although this right to information can be restricted under some conditions (see above-mentioned Article 42 of SIS II Regulation), both the European Court of Human Rights⁵⁹ and the Court of Justice of the European Union⁶⁰ have found that such restrictions must be interpreted in a very restrictive way.

42. As regards the interoperability capacity of large scale information systems, the concern is that despite the legal and administrative guarantees provided in the relevant European Union legislation ensuring restricted access to and limited use of those systems, the information entered by an authority in one of the systems for a specific purpose may be used by another authority in another system for different purposes which are not explicitly provided by the European Union regulations in force. The typical example is that of the misuse of an alert entered in SIS II to deny a residence permit when such an alert is accessible through the ECRIS-TCN.

43. The misuse of alerts as a political leverage against third countries poses another challenge. Although under international law States have the right to determine the terms and conditions under which non-nationals are admitted to their territories, restrictions designed and placed for the sole purpose of inflicting harm to a third country disguised as a national security threat coming from an individual who is a national of that third country should not be permissible. If it is not scrutinised by the European Union bodies, this alleged practice may substantially undermine the legitimacy of SIS II and other large-scale information systems.

44. As regards the obligations of the State enforcing a SIS alert, its immigration and border authorities deciding upon a SIS alert must ensure that a person will not be refused entry, a short-term visa, and in the future, a travel authorisation, on unlawful grounds, in accordance with the respective provisions of the

58. The Court of Justice of the European Union, when dealing with a restriction measure taken in respect of illegally staying third-country nationals on the basis of a “risk to public policy” in the context of the Return Directive, stressed that States are obliged to fulfill these two requirements and respect fundamental freedoms; see *Z. Zh. v. Staatssecretaris voor Veiligheid en Justitie* and *Staatssecretaris voor Veiligheid en Justitie v. I. O.*, case C-554/13, judgment of 11 June 2015, para. 50.

59. See, for example, *Al-Nashif v. Bulgaria*, application No. 50963/99, judgment of 20 June 2002, para. 123 (as regards the use of and access to secret information in migration cases) or *Klass and others v. Germany*, application No. 5029/71, judgment of 6 September 1978 (as regards surveillance and the use of personal data), para. 42.

60. See, for example, *ZZ v. Secretary of State for the Home Department*, case C-300/11, judgment (Grand Chamber) of 4 June 2013, para. 51 (as regards the use of and access to secret information in migration cases) and *Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources etc.*, cases C-293/12 (joined with C-594/12), judgment (Grand Chamber) of 8 April 2014 (as regards the use of personal data), para. 52.

Schengen Borders Code, the Visa Code⁶¹ and the Regulation 2018/1240 establishing a European Travel Information and Authorisation System (ETIAS).⁶² This includes the obligation to respect the fundamental rights of the concerned person (in particular the freedom of movement of European Union citizens' family members, the right to respect for family life, freedom of expression and freedom of religion, conscience or belief and the principle of non-refoulement), before turning him/her back at the border. Another responsibility is related to the use of the SIRENE network, which should be used more actively to exchange necessary information before denying admission or a short-term visa to a third-country citizen. The Court of Justice of the European Union has pointed out this obligation in its Grand Chamber judgment in the case of *Commission v. Spain* of 2006.⁶³ The case concerned Spain's refusal of a visa and entry to third-country nationals who were spouses of European Union member State nationals, on the sole basis of a SIS alert issued by Germany. The Court of Justice stressed that the Spanish authorities should have checked whether the concerned persons presented "a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society" and therefore had failed to fulfil their obligations under Council Directive 64/221/EEC of 25 February 1964 on the co-ordination of special measures concerning the movement and residence of foreign nationals which are justified on grounds of public policy, public security or public health.⁶⁴

45. As regards access to an effective remedy, enshrined in Article 47 the European Union Charter of Fundamental Rights and Article 13 of the European Convention on Human Rights, this issue is crucial for ensuring respect of fundamental rights in the context of the use of SIS alerts.⁶⁵ Such a remedy should be available not only against the State executing a SIS alert but also against the State which has inserted the alert in the SIS. The above-mentioned provision of Article 43(1) of the SIS II, allowing third country nationals to bring an action before the courts or national authorities in "any member State" in relation to the use of SIS alerts, provides for an important protection against abuses. However, in practice, the effective implementation of the right to an effective remedy seems to be hampered in two ways. Firstly, third-country nationals often lack information about the fact that they are subject to a SIS alert and they only find out when arriving at the external border of the European Union or applying for a visa. Even if they have found out about the existence of a SIS alert, the exercise of their right to an effective remedy often depends on the good will of the border or immigration authorities, who do not always inform them correctly about their rights. Secondly, national courts may be reluctant to order other member States' authorities to delete or correct the information included in the SIS II, and even if they do so, they may lack the power to ensure the follow-up of such orders. In such a case, the inability to address effectively unlawful or inaccurate information included in the SIS II, can turn into a bureaucratic nightmare, especially for those who are repeatedly confronted with entry bans.⁶⁶

46. It should be stressed that the good functioning of the SIS, whose goal is to maintain a high level of security within the Schengen area (in particular to ensure protection from terrorist threats and threats to national security), is dependent on the mutual trust between national authorities of the Schengen area member States. National authorities must be able to trust that the data provided to the SIS are accurate and recorded according to national laws, including those on the protection of fundamental rights and freedoms.

4.2.7. Human rights implications of the misuse of alerts based on Article 24(1) of the SIS II Regulation

47. As stressed by Ms Nuala Mole at the hearing of 14 September 2021, certain provisions of the European Convention on Human Rights might be applicable in cases of ill-founded alerts entered into the SIS. Although the European Court of Human Rights has not yet found any violation of the Convention in such a case, it has

61. Regulation 810/2009/EC of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code).

62. 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.

63. *Commission v. Spain*, case C-503/03, judgment of 31 January 2006, paras 55-59.

64. *Ibid*, paras 55 and 59. The CJEU also stressed that the State issuing the alert (Germany) should have made supplementary information available to the consulting State "to enable it to gauge (...) the gravity of the threat that the person for whom an alert has been issued is likely to represent"; para. 56.

65. More specifically, with regard to data protection, see Article 79 of 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): "(...) each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation."

66. As illustrated in a 2010 report of the Dutch *Nationale Ombudsman*: www.nationaleombudsman.nl/uploads/rapport2010-115_1.pdf.

already examined a case of blacklisting on the basis of UN Security Council anti-terrorism sanctions: in the *Nada v. Switzerland*⁶⁷ judgment, concerning the applicant's inability to have his name removed from such a blacklist and a subsequent restriction on movement, it found violations of Articles 8 and 13 of the Convention.

48. Article 8 of the Convention is also applicable to the collection and retention of data⁶⁸ and the inclusion of a person's data in the SIS II could, in theory, violate this provision, if it is not in "accordance with the law" (including European Union law where applicable),⁶⁹ does not serve a "legitimate aim" and/or is not proportionate to that aim. The same reasoning would apply if a person considers that his/her blacklisting constitutes an interference with his/her reputation.⁷⁰

49. Moreover, the right to freedom of expression (Article 10 of the Convention) could potentially be invoked in such cases. The Court has already examined cases concerning violations of Article 10 of the Convention in cases of foreigners who have been prevented from entering the territory of a State Party to the Convention, although these cases did not concern hits on alerts in the SIS. In *Piermont v. France*, concerning the expulsion and exclusion order in French Polynesia and New Caledonia issued against a German member of the European Parliament who had made critical statements on French policies, it found that the impugned measures were not proportionate to the aims of "the prevention of disorder" and "the upholding of territorial integrity" (violation of Article 10 of the Convention).⁷¹ Similarly, in *Cox v. Turkey*, the Court considered that a permanent ban on the applicant's re-entry on grounds of her previously expressed opinions on Kurdish and Armenian issues, was not sufficiently and relevantly justified by national security and other grounds and therefore was not "necessary in a democratic society".⁷²

5. Conclusion

50. As explained above, the relevant authorities of Council of Europe members States which belong to the Schengen area have much leeway in deciding whether and in which circumstances they want to introduce alerts into SIS II. Without questioning the fact that national security may be at stake, it should be stressed that individual member States or a group of States belonging to the Schengen area may in fact decide to deny access to their territories to third-country nationals and that the SIS does not foresee common standards for inserting alerts or for interpreting and reporting information. Therefore, information of a similar nature may undergo different assessment depending on the security policy of the given State.

51. In light of the foregoing, it is even more important that States participating in SIS II observe human rights, as enshrined in the European Convention on Human Rights. The possible use of the Schengen system, including SIS II, as an instrument of politically motivated sanctions may raise concerns with regard to a range of rights guaranteed by the Convention, including the right to freedom of expression (Article 10), the right to respect for private and family life (Article 8), the right to freedom of movement (Article 2 of Protocol No. 4) and the right to an effective remedy (Article 13), including unhindered access to fair justice (Article 6). The SIS should under no circumstances be misused in order to deny citizens of Council of Europe member States not belonging to the European Union and other third-country nationals' access to the Schengen Area on grounds that are in violation with the requirements stemming from the Convention. Since all these rights are

67. Application No. 10593/08, judgment of 12 September 2012 (Grand Chamber). The applicant, an Italian-Egyptian citizen living in Switzerland, was placed on the "Federal Taliban Ordinance" by the Swiss authorities and was prevented from leaving his area. Although the Swiss authorities enjoyed a certain degree of discretion in the application of the UN sanctions, by failing to inform the Italian authorities and the UN Sanctions Committee and to adapt the effect of the sanction to his individual situation that there was no reasonable suspicion against the applicant, they violated Article 8 of the Convention. The applicant did not have any remedy to contest the measure (violation of Article 13).

68. See, in particular, *S. and Marper v. the United Kingdom*, application Nos. 30562/04 and 30566/04, judgment of 4 December 2008 (Grand Chamber), *Khellil v. Switzerland*, application No. 16188/07, judgment of 18 October 2011, and *Aycaguer v. France*, application No. 8806/12, judgment of 22 June 2017.

69. See, for instance, *Big Brother Watch and Others v. the United Kingdom*, applications Nos. 58170/13 62322/14 and 24960/15, judgment of 25 May 2021 (Grand Chamber), paras 518-519.

70. See, for instance, *Delfi A.S. v. Estonia*, application No. 64569/09, judgment of 16 June 2015 (Grand Chamber), para. 137.

71. Applications Nos. 15773/89 and 15774/89, judgment of 27 April 1995, paragraphs 77 and 85. Interestingly, in this case the Court found that Article 16 of the Convention, which allowed State Parties to the Convention to impose restrictions on political activity of aliens, did not authorise France to restrict the applicant's exercise of the right to freedom of expression because of Ms Piermont's possession of the nationality of a member State of the European Union and her status as a member of the European Parliament; *ibid*, para. 64.

72. Application No. 2933/03, judgment of 20 August 2010, paras. 43 and 44. The applicant was a national of the United States of America.

guaranteed by international conventions, it is unacceptable to prevent or attempt to prevent their exercise due to the misuse of the system for political reasons. Member States of the Schengen Area should pay attention to those risks as required by the agreements to which they are parties.

52. In this context, the issue of the relationship between the legal frameworks of the Council of Europe and the European Union deserves careful consideration. SIS II is an integral element of the European Union legal framework and the European Union is yet to become a party to the European Convention on Human Rights. Furthermore, there are a number of obstacles both within the practice of the European Court of Human Rights (the «Bosphorus criteria»)⁷³ as well as the European Union *acquis* (namely the so-called Plaumann criteria)⁷⁴ for taking action against decisions carried out under the European Union legal framework. All this leads to legitimate concerns regarding the possibility of challenging possible cases of misuse of the Schengen system, especially through the European Court of Human Rights by non-European Union citizens. In such cases, the European Court of Human Rights could question the grounds on which a SIS alert is based and check whether the alert was not arbitrary and whether it was proportionate to a legitimate aim. While being deferential to the authorities invoking national security, the Court should be vigilant to ensure that the invoked reasons were genuinely related to national security.

53. Against this background, several concrete recommendations can be made in order to prevent misuse of the SIS and improve the protection of fundamental rights of third-country nationals subject to alerts entered into the SIS. As regards member States issuing alerts, they should follow the principles of proportionality and individual assessment, despite the wide leeway granted to them on the basis of Article 24(2) of the SIS II Regulation. They should not restrict the right to be informed about the inclusion of an alert and should observe their data protection rights.

54. As regards the obligations of member States enforcing alerts, they should take into account other relevant provisions of European Union law concerning the freedom of movement of persons within the European Union. They should also actively use the SIRENE network, in order to verify the necessary information before denying admission or a short-term visa to a third-country national. They should also refrain from misusing SIS II against a third country as part of advancing their political agenda by entering unjustified alerts concerning nationals of that third country. Adequate monitoring and verification systems as well as reporting mechanisms should be put in place to prevent Schengen Area member States from taking such measures for political purposes.

55. European Union regulations on interoperability add enormous complexity to the practices and laws relating to the existing data systems and thus render the provisions of the General Data Protection Regulation and the Data Protection Directive insufficient in setting adequately transparent legal framework. In particular, the use of large-scale databases and the effects of interoperability, primarily as regards third-country citizens, make it extremely difficult for the data subject to understand not only which particular law applies but also which member State or institution should be addressed with regard to exercising their rights to access, correction or deletion of data and their right to effective judicial protection. The use for a specific purpose of one set of data duly registered in one of the information systems by another information system is of particular concern. In order to address these challenges, the interoperability of information systems must be rendered more transparent and clear rules and restrictions must be introduced concerning the controlling authority and the purpose of using and processing the registered data.

73. European Court of Human Rights, *Bosphorus Hava Yollari Turizm Ve Ticaret Anonim Şirketi v. Ireland*, application No. 45036/98, judgment of 30 June 2005 (Grand Chamber). In this case, the Court has stated that State action taken in compliance with legal obligations stemming from an international treaty is justified as long as the relevant organisation to which the State has transferred part of its sovereignty is considered to protect fundamental rights "(...) in a manner which can be considered at least equivalent to that for which the Convention provides (...) "(paragraph 155). If such "equivalent protection" is considered to be provided by the organisation, one can presume that a State "(...) has not departed from the requirements of the Convention when it does no more than implement legal obligations flowing from its membership of the organisation"; however, this presumption can be rebutted if in the circumstances of a particular case the protection of the Convention rights is "manifestly deficient" (paragraph 166). The concept of "equivalent protection" by EU law seems to be scarcely used by the Court now, as illustrated by the recent judgment in the case of *Bivolaru and Moldovan v. France*, application Nos 40324/16 and 12623/17, judgment of 25 March 2021, concerning the European Arrest Warrant.

74. CJEU, *Plaumann & Co. v Commission of the European Economic Community*, case 25-62, judgment of 15 July 1963. In this case, the CJEU held that the applicant company had no standing for judicial review of the Commission decision as it was not "individually concerned". The CJEU further specified the conditions in which natural and legal persons could bring actions for annulment against European institutions: "persons other than those to whom a decision is addressed may only claim to be individually concerned if that decision affects them by reason of certain attributes which are peculiar to them or by reason of circumstances in which they are differentiated from all other persons and by virtue of these factors distinguishes them individually just as in the case of the person addressed."

56. It goes without saying that member States of the Schengen area should do their utmost to ensure respect of human rights of the third country nationals subject to alerts, and in particular their right to an effective remedy. In order to make this right fully operational, decisions refusing entry, a visa or travel authorisation based on a SIS alert should indicate the member State issuing the SIS alert, the specific grounds for the refusal of admission and, to the extent possible, the essence of the reasons for the SIS alert.⁷⁵ Furthermore, the applicants should be informed about the available remedies against SIS alerts, including those relating to the protection of their data. Their rights to defence and effective judicial protection should be guaranteed. Moreover, co-operation should be improved between the competent national authorities examining individual cases of alerts (courts, data protection controllers and other relevant bodies).

57. The European Union and member States of the Schengen area should also collect more knowledge about current national practices concerning the use of SIS II and its impact on human rights. In particular, the European Union could carry out further inquiries amongst European Union member States and other stakeholders, including the European Ombudsman, the Fundamental Rights Agency (FRA), eu-LISA and the European Data Protection Supervisor. Such inquiries could be used to identify specific grounds for SIS alerts aimed at third-country nationals, the data retention periods for alerts (including the possibility of extending such periods), the annual number of hits based on SIS alerts and the number of actual entry or visa refusals based on alerts. They could also refer to the use of the SIRENE network and examine how often and in which circumstances national authorities make use of it.

58. The replies received in response to the questionnaire I had sent through the ECPRD show that there is a need for further inquiries of that type in order to obtain more information on the issues raised therein. Several other questions could be addressed in the framework of further research: is it possible to take action against an European Union member State which has not inserted the alert in the SIS (including the member State executing the alert)? How often have national courts and data protection authorities used the possibility to order another member State to correct or delete data in the SIS? Has the issuing State followed such orders? This additional information could then be used to develop further guidelines for national authorities on how to use the SIS in accordance with its rules and purposes, while preventing its misuse and respecting the fundamental rights of the individuals concerned. Taking this into account, the European Union could adopt guidelines on a minimum common standard for alert procedures applicable to third-country nationals. They could include the criteria for issuing SIS II alerts (for example, by drafting a specific list of serious crimes or offences, including a clear threshold of “severity” of the offence for which persons may be subjected to an alert, or a more precise definition of “public order and security risk”).⁷⁶

59. Another proposal is to introduce some sort of mediation/intervention organ (namely an ombudsperson), whose main task would be to examine the issue of whether human rights standards have been applied and respected by national authorities when entering an alert in the system or denying entrance to third country nationals. Such a mediator or ombudsperson need not be empowered to issue legally binding rulings but could exert a moderating influence on the competent authorities to discourage misuse of the system. Alternatively, competences in this field could be attributed to the European Ombudsman, FRA or the EDPS, provided that they are given sufficient resources. The Frontex (European Board and Coast Guard Agency) Fundamental Rights Officer, an independent expert who monitors and promotes fundamental rights within Frontex and handles complaints, could be a source of inspiration in this context.⁷⁷ Similarly, this type of body could be established also at the national level. During my fact-finding visit to Brussels, I have learned that the European Commission, DG JUST, is now preparing guidelines on politically motivated requests for extradition and it will propose the establishment of national focal points to examine such cases. I think that similar focal points could also be established to examine cases of misuse of SIS II alerts.

60. Moreover, the Schengen Evaluation Mechanism could be better used to examine the possible deficiencies in the functioning of SIS II and make appropriate recommendations for improvement. It would also be good to involve the European Parliament in this process.

75. In this regard, lessons could be learned from a recent judgment of the CJEU in two cases in which the Dutch visa authorities had refused short-term visas to third-country nationals following objections from other member States; CJEU, *R.N.N.S. and K.A. v. Minister van Buitenlandse Zaken*, cases C-225/19 and C-226/19, judgment (Grand Chamber) of 20 November 2020, paras 43-56.

76. For more information on these proposals, see P. Boels, E. Brouwer e.a., *Public Policy Restriction in EU Free Movement and Migration Law, General Principles and Guidelines*, publication by the Meijers Committee, Amsterdam 2021.

77. Established by [Regulation 1624/2016](#) on the European Border and Coast Guard.

61. As regards the Council of Europe's role in this context, the Commissioner for Human Rights and the Secretary General Special Representative on Migration and Refugees could follow the implications of the misuse of SIS II alerts on human rights and make the necessary recommendations to Council of Europe member States, including those belonging to the Schengen Area. Much will also depend on the case law of the European Court of Human Rights, which so far has not decided on the merits in cases of individuals who have been denied entry into the Schengen area following SIS alerts but may receive such applications in the future.

62. To conclude, preventing misuse of the Schengen Information System is not only essential to protect fundamental rights and free movement of individuals, but also to safeguard trust amongst national authorities and to allow them to rely on the accuracy and lawfulness of the information contained in the SIS. This is even more urgent in light of the recent developments related to the extensive use within the European Union of border technologies, such as biometrics and algorithms, and the scheme of interoperability which connects SIS with other large-scale databases. Innocent persons should not be victims of incorrect use or misuse of European Union databases or any automated decision made on this basis.

Appendix – Summary of member States’ responses to a questionnaire on the legislation and practice of member States concerning the Schengen Information System

1. Introduction

1. In response to the questionnaire sent through the European Centre for Parliamentary Research and Documentation (ECPRD), 19 national delegations from Council of Europe member States have answered, providing details about national legal provisions and practice. The following countries have responded to the questionnaire: Austria, Belgium, Bulgaria, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Latvia, Lithuania, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain and Switzerland. Two States – Croatia and Norway – indicated that they have decided not to reply to the questionnaire.⁷⁸ Ireland, which does not belong to the Schengen area, indicated that its Department of Justice and Equality and the *An Garda Síochána* (the national police force) were working towards joining the Schengen Information System (SIS II). The United Kingdom, which is also not a member of the Schengen area, indicated that it only participated in the police and judicial co-operation aspects of the SIS II.

2. How many persons (and from which Council of Europe member States) were prevented by your State authorities from entering your State because of an alert into the SIS II based on alleged “threat to public policy or public security or to national security”?

2. Most member States provided no statistics in reply to this question, some of them explicitly indicating that they were not in a position to do so. **Austria** indicated that its authorities had a different approach to data collection and that some of these data were publicly available. **Bulgaria and Greece** referred to the eu-LISA website. However, the following States provided statistics: the **Czech Republic, Estonia, Latvia, Lithuania, Poland, Portugal and the Slovak Republic**.⁷⁹

3. In the **Czech Republic**, in 2019, approximately 500 interventions were carried out on alerts in the SIS in accordance with Article 24 of the SIS II Regulation (when it was decided to refuse entry of a third-country national to the Czech Republic or to expel him/her from the Czech Republic after apprehension on Czech territory). These statistics do not distinguish between the nationalities of the third-country nationals concerned. In **Estonia**, in 2020 (as of 5 August 2020), eight decisions were taken to prevent a person to enter its territory on the basis of an alert into the SIS II based on an alleged “threat to public policy or public security or to national security”.

4. In **Latvia**, between 1 January 2018 and 30 June 2020, one person (in 2018) was refused entry at the border “as a threat to the public policy, internal security, public health or international relations of one or more member States of the European Union”. In **Lithuania**, nearly 950 people (the majority of whom came from Belarus, Ukraine and the Russian Federation), were refused entry because they were considered to be a threat to public policy by a European Union member State or internal security and were concerned by an SIS II alert (in total, as no timeframe has been indicated). In **Poland**, in 2019 and in the first half of 2020 respectively 2 109 and 684 decisions to refuse entry on its territory were taken because of SIS II alerts (the overwhelming majority of them concerned Ukrainian citizens and to a lesser extent – Georgians and Moldovans). In 2019, 116 people were prevented from entering **Portugal** because of a SIS II alert (of whom 23 from Council of Europe member States – the Republic of Moldova, Türkiye, Albania, Georgia, Ukraine and Romania); nevertheless, it is not possible to determine whether that happened on the basis of threats to public policy or public security or national security. In **Slovak Republic**, the number of persons who were refused entry because of a SIS alert was 957 in 2018, 799 – in 2019 and 201 in the first half of 2020 (mainly concerning Ukrainian citizens).

3. On the basis of decisions of what national bodies?

5. In some member States, such decisions are taken by police authorities (the Czech Republic, France, Greece, Slovak Republic and Slovenia) or border control authorities (Latvia, Lithuania and Poland). In some countries, both types of authorities are involved in such decision-making process (Estonia, Finland and Germany). Other countries have indicated that the decisions are taken by an administrative body, such as the ministry responsible for home affairs (in Romania – the Ministry of Internal and Administrative Reform), a specialised structure within such a ministry (in Bulgaria – the Migration Directorate and in Spain – the Sub-

78. Bulgaria, Croatia and Romania are soon to be part of the Schengen area.

79. France has provided statistics concerning visa requests and granting.

directorates General of Information and Communication Systems) or the Immigration Office (in Austria – the Federal Office for Immigration and Asylum, in Belgium – Office des Étrangers and in Portugal – the Immigration and Borders Service, SEF).

6. In certain countries, several bodies are involved in the decision making (in Finland – police, border control authorities and the Immigration Service; in Latvia – the State border guard, the Ministry of Interior and the Office of Citizenship and Migration Affairs, and in Switzerland – the Federal Police and the State Secretariat for Migration – SEM). In Slovenia, a SIS II alert is introduced on the basis of a decision of an administrative body, the police or a competent court.

4. Are there any criteria (recommendations) for classifying actions, wrongdoings and available information in relation to a person as a threat to State policy, public order or national security?

7. Most of the Member States who responded indicated that such criteria are included in their internal legislation (Austria, Bulgaria, the Czech Republic, Denmark, Greece, Latvia, Lithuania, Poland, Romania, Slovak Republic and Switzerland), internal instructions (Slovenia) or court decisions (Portugal). Some member States (Estonia, Finland, Germany and Latvia) referred to Article 24 of the SIS II Regulation, which is directly applicable.

8. In **Belgium**, an entry ban based on public or national security is issued only in exceptional cases, such as in case of the most severe crimes like espionage or terrorism related activities and only for persons who have previously stayed in that country. It may also be issued for “migration reasons” in case a return decision has been issued.

9. In **Denmark**, according to the Aliens Act, alerts in SIS II may be issued for acts that pose a serious threat to public order, but this has not happened in recent times. As regards the risk to the national security, it must be a serious one.

10. According to the **Finnish** Aliens Act (Section 146), when considering an entry ban, “account shall be taken of the facts on which the decision is based and the facts and circumstances otherwise affecting the matter as a whole”. If such an entry ban is based on the criminal activity of an alien, “account shall be taken of the seriousness of the act and the detriment, damage or danger caused to public or private security”.

11. In **Germany**, according to the case law of the Federal Constitutional Court, an alert on refusal of entry for reasons of threats to public security and public order or national security shall only be entered in case the threat associated with the presence of the foreigner has a **certain degree of seriousness**. The objectives pursued by an alert in the SIS must be balanced against the fundamental rights of the concerned person.⁸⁰

12. According to the **Latvian** Immigration Act (Section 61), a foreigner may be forbidden entry on the State territory, if the competent State institutions have a reason to believe that he/she participates in the activities of anti-State or criminal organisations or is a member thereof; he/she causes threats to national security or public order and safety or, by entering Latvia, may hinder pre-trial investigations or the work of law enforcement institutions in discovering a criminal offence; or if he/she has committed or is planning to commit a serious or extremely serious crime. Moreover, he/she may be forbidden entry if the competent foreign authorities have provided information which prohibits the foreigner from entering and residing in Latvia or his/her entry and stay in the country is not desirable for other reasons on the basis of an opinion delivered by competent State institutions. An entry ban is also issued if the foreigner has committed a crime against humanity, an international or war crime or has participated in mass repression if the latter has been determined by a court judgment, or if he/she has been convicted of a criminal offence committed in Latvia, involving deprivation of liberty for at least one year.

13. In **Poland**, according to the Act of 12 December 2013 on Foreigners, a foreigner may be refused entry if his/her stay would be “undesirable” and would then be included in a special register on the basis of a decision of the Head of the Office for Foreigners. This might be “due to the threat to State defence or security, protection of public safety and order or the possibility of violating the interests of Poland”, in case of conviction of certain offences, in case a return decision and/or a ban on entry on the territory of Poland has been issued or in relation to obligations stemming from international agreements. According to the Polish Border Guard, there is no enumerative list of conditions for obliging a foreigner to return on grounds of “State defence or security, protection of public safety and order or the possibility of violating the interests of Poland” and each case is assessed individually by a border guard officer or other national bodies (such as the Internal Security

80. Decision of 24 October 2006 – 2 BvR 1908/03.

Agency or the Intelligence Agency) performing tasks related to identifying, preventing and combating threats to the internal security of the State (which may request the Border Guard to issue an appropriate decision in respect to the foreigner).

14. In **Romania**, foreign citizens are denied entry into the territory of the Romanian State in particular if there are "solid indications" that they constitute "a real and present threat to public order, national security or public health". They are refused to enter the State territory, *inter alia*, if they are part of transnational organised criminal groups or support in any way the activity of these groups, or if there are serious reasons to consider that they have committed or participated in crimes against peace and humanity or of war crimes.

15. According to the **Slovakian** Act No. 404/2011 Coll. on Residence of Aliens and Amendment and Supplementation of Certain Acts, a "**threat to State safety**" shall be understood as an action of a person who threatens the democratic order, sovereignty, territorial cohesion or inviolability of the State borders; or an action of a person who violates the fundamental rights and freedoms, which protect the lives and health of persons, property and the environment. A "**threat to public order**" shall be understood as a violation or threat to the interests protected by law regarding fundamental human rights and freedoms or protection of minors.

5. What is the level of the officials/national authorities authorised to make such decisions?

16. Most member States responded that alerts are based on decisions of police authorities (Bulgaria, the Czech Republic, Finland, France, Germany, Greece, Lithuania, Slovak Republic, Slovenia and Switzerland), of border control authorities (Austria, Bulgaria, Finland, France and Lithuania), of administrative bodies (in Austria – of the Federal Office for Immigration and Asylum; in Belgium – of the Minister of Asylum; in Bulgaria – of the Ministry of Interior and the Director of Directorate "Migration"; in Denmark – of the Ministry of Immigration and Integration; in Estonia – of the Ministry of Interior; in Finland – of the Immigration Service; in Poland – of the Head of the Office for Foreigners; in Portugal – of the National Director of the SEP, in Romania – of the Minister of Interior, in Slovenia – of a competent administrative unit; and in Switzerland – of the SEM) and/or of national courts (Denmark, Slovak Republic and Slovenia).

17. In **Bulgaria**, the authorities habilitated to make these decisions include the Chair of the State National Security Agency, the director of the General Directorate for "Fight against Organized Crime", and the directors of the Sofia and Regional Directorates. In **Lithuania**, the assessment of the threat to State security is made by the Department of State Security.

6. Which legislation in your country regulates the issuing of SIS II alerts on the above-mentioned grounds?

18. Most member States provided information on pieces of legislation regulating the issue at stake. There is no national legislation regulating the issuing of SIS II alerts in **Spain** (the European Union norms applying directly).

19. The issuing of SIS II alerts is regulated by the following legislation in the countries which have replied to the questionnaire:

- **Austria**: paragraph 53 of the Aliens' Police Act;
- **Belgium**: Article 39/2, paragraph 2 of the Act of 15 December 1980 on access to the territory, stay, establishment and expulsion of foreigners (*Loi sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers*) and the Protocol between the Immigration Office and the Federal Police on operational and technical aspects;
- **Bulgaria**: the Law on Foreigners and Ordinance 8121h-465/2b 08 2014 on the organisation and functioning of the national Schengen Information System of the Republic of Bulgaria;
- **Czech Republic**: Section 9 paragraphs f) and h) and Section 154 of the Act 326/1999 Coll., on the Residence of Foreign Nationals in the Czech Republic;
- **Denmark**: Section 58g of the Aliens Act;
- **Estonia**: the Act on Obligation to Leave and Prohibition on Entry;
- **Finland**: Section 146 of the Aliens Act;
- **France**: The Code on Foreigners' Entry and Stay and the Right to Asylum (*Code de l'entrée et du séjour des étrangers et du droit d'asile – CESEDA*);
- **Germany**: paragraph 30 (5) of the Federal Police Act;

- **Greece:** Common Ministerial Decision 4000/4/32-λα/2012;
- **Latvia:** the Law on Operation of the Schengen Information System, the relevant decrees of the Cabinet of Ministers and the Immigration Law;
- **Lithuania:** paragraphs 7 and 8 of Article 133 of the Law on the Legal Status of Aliens and paragraph 15 of the Rules for Compiling and Maintaining the National List of Aliens Prohibited from Entering the Republic of Lithuania, approved by resolution No. 436 of 20 April 2005 by the Government of the Republic of Lithuania;
- **Poland:** the Law of 24 August 2007 on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System, the Law of 12 December 2013 on foreigners and the Code of Administrative Procedure (Act of 14 June 1960 as amended subsequently);
- **Portugal:** Law No. 23/2007 of 4 July 2007 on the legal framework of entry, permanence, exit and removal of foreigners, into and out of national territory;
- **Romania:** Law No. 141/2010 on the establishment, organisation and operation of the National Information System for Alerts and Romania's participation in the Schengen Information System, Emergency Ordinance (GEO) No. 128/2005 regarding the establishment, organisation and functioning of the National Signalling Information System (approved and modified by Law No. 345/2005), Government Decision No. 1411/2006 regarding the approval of the norms for the application of GEO No. 128/2005 and Government Emergency Ordinance No. 194/2002 regarding the regime of foreigners in Romania;
- **Slovak Republic:** Act No. 404/2011 Coll. on Residence of Aliens and Amendment and Supplementation of Certain Acts;
- **Slovenia:** Articles 55, 56, 62, 66 of the Aliens Act, Article 24 of the Minor Offences Act and Article 43 of the Criminal Code;
- **Switzerland:** Articles 67 and 68 of the Federal Law on Foreigners and Integration and Articles 77a and 77b of the Decree on Admission, Residence and Employment.

7. Do persons subject to an alert have an “effective remedy”? If so, to which authority (a court or an administrative body)?

20. Almost all member States which have responded to this question (with the exception of France and Spain) indicated that persons subject to an alert have access to a remedy. In some member States, the appeal must be filed directly with the authority that has issued the alert (Bulgaria, Denmark, Greece, Poland and Slovenia). In others, such appeals must be brought before the (usually administrative) courts (Austria, Belgium, Estonia, Finland, Germany, Latvia, Lithuania and Romania). In the Czech Republic, Portugal, Slovak Republic, Slovenia and Switzerland, it is possible to appeal directly to one or the other body.

21. **France, Germany, Latvia, Poland and Spain** have also indicated that a person concerned by an alert in the SIS II can request access to data relating to him/her and the correction or deletion of factually inaccurate or unlawfully stored data before the data controller body.

8. What are the national statistics for taking positive and negative decisions on these issues?

22. Most member States did not provide data in response to this question, as they lacked statistics in this respect. **Belgium** indicated that there had been no appeals against such decisions. In **Lithuania**, in 2019, following appeals, courts upheld four decisions on alerts and revoked one such decision.

9. What is the percentage of decisions taken by State authorities to pay compensation (including moral damages) to persons who have filed a claim in case an alert was not justified?

23. No data was provided in response to this question either. However, the **Czech Republic, Denmark and Lithuania** answered that such claims were not known to them.