

Data Protection in the Schengen Agreement

The "Convention implementing the Schengen agreement" (SDÜ in German) (Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common Borders - BGBl. III Nr. 90/1997) contains the following regulations concerning data protection:

CHAPTER 3 - Protection of personal data and security of data in the Schengen Information System

Article 102

(1) The Contracting Parties may use the data provided for in Articles 95 to 100 only for the purposes laid down for each category of alert referred to in those Articles.

(2) Data may only be copied for technical purposes, provided that such copying is necessary in order for the authorities referred to in Article 101 to carry out a direct search. Alerts issued by other Contracting Parties may not be copied from the national section of the Schengen Information System into other national data files.

(3) With regard to the alerts laid down in Articles 95 to 100 of this Convention, any derogation from paragraph 1 in order to change from one category of alert to another must be justified by the need to prevent an imminent serious threat to public policy and public security, on serious grounds of national security or for the purposes of preventing a serious criminal offence. Prior authorisation from the Contracting Party issuing the alert must be obtained for this purpose.

(4) Data may not be used for administrative purposes. By way of derogation, data entered under to Article 96 may be used in accordance with the national law of each Contracting Party for the purposes of Article 101 (2) only.

(5) Any use of data which does not comply with paragraphs 1 to 4 shall be considered as misuse under the national law of each Contracting Party.

Article 103

Each Contracting Party shall ensure that, on average, every tenth transmission of personal data is recorded in the national section of the Schengen Information System by the data file management authority for the purposes of checking whether the search is admissible or not. The record may only be used for this purpose and shall be deleted after six months.

Information: Article 103 obtains at a point in time decided unanimously by the council as soon as the conditions are existent the following composure (see Council Decision 2005/211/JI of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, Official Journal of the European Union No. L 68/44 of 15 March 2005. The modification go back on a initiative of Spain. The Council Decision changes the Articles 92, 94, 99, 100, 101, 103 and 113 SD?, new inclusions are the Articles 101a, 101b, 112a and 113a SD?):

Each Member State shall ensure that every transmission of personal data is recorded in the national section of the Schengen Information System by the data file management authority for the purposes of checking whether the search is admissible or not. The record may only be used for this purpose and shall be deleted at the earliest after a period of one year and at the latest after a period of three years.

Article 104

(1) Alerts shall be governed by the national law of the Contracting Party issuing the alert unless more stringent conditions are laid down in this Convention.

(2) Insofar as this Convention does not lay down specific provisions, the law of each Contracting Party shall apply to data entered in its national section of the Schengen Information System.

(3) Insofar as this Convention does not lay down specific provisions concerning performance of the action requested in the alert, the national law of the requested Contracting Party performing the action shall apply. Insofar as this Convention lays down specific provisions concerning performance of the action requested in the alert, responsibility for that action shall be governed by the national law of the requested Contracting Party. If the requested action cannot be performed, the requested Contracting Party shall immediately inform the Contracting Party issuing the alert.

Article 105

The Contracting Party issuing the alert shall be responsible for ensuring that the data entered into the Schengen Information System is accurate, up-to-date and lawful.

Article 106

(1) Only the Contracting Party issuing the alert shall be authorised to modify, add to, correct or delete data which it has entered.

(2) If one of the Contracting Parties which has not issued the alert has evidence suggesting that an item of data is factually incorrect or has been unlawfully stored, it shall advise the Contracting Party issuing the alert thereof as soon as possible; the latter shall be obliged to check the communication and, if necessary, correct or delete the item in question immediately.

(3) If the Contracting Parties are unable to reach agreement, the Contracting Party which did not issue the alert shall submit the case to the joint supervisory authority referred to in Article 115 (1) for its opinion.

Article 107

Where a person is already the subject of an alert in the Schengen Information System, a Contracting Party which enters a further alert shall reach agreement on the entry of the alert with the Contracting Party which entered the first alert. The Contracting Parties may also lay down general provisions to this end.

Article 108

(1) Each Contracting Party shall designate an authority which shall have central responsibility for its national section of the Schengen Information System.

(2) Each Contracting Party shall issue its alerts via that authority.

(3) The said authority shall be responsible for the smooth operation of the national section of the Schengen Information System and shall take the necessary measures to ensure compliance with the provisions of this Convention.

(4) The Contracting Parties shall inform one another, via the depositary, of the authority referred to in paragraph 1.

Article 109

(1) The right of persons to have access to data entered in the Schengen Information System which relate to them shall be exercised in accordance with the law of the Contracting Party before which they invoke that right. If national law so provides, the national supervisory authority provided for in Article 114 (1) shall decide whether information shall be communicated and by what procedures. A Contracting Party which has not issued the alert may communicate information concerning such data only if it has previously given the Contracting Party issuing the alert an opportunity to state its position.

(2) Communication of information to the data subject shall be refused if this is indispensable for the performance of a lawful task in connection with the alert or for the protection of the rights and freedoms of third parties. In any event, it shall be refused throughout the period of validity of an alert for the purpose of discreet surveillance.

Article 110

Any person may have factually inaccurate data relating to them corrected or unlawfully stored data relating to them deleted.

Article 111

(1) Any person may, in the territory of each Contracting Party, bring before the courts or the authority competent under national law an action to correct, delete or obtain information or to obtain compensation in connection with an alert involving them.

(2) The Contracting Parties undertake mutually to enforce final decisions taken by the courts or authorities referred to in paragraph 1, without prejudice to the provisions of Article 116.

Article 112

(1) Personal data entered into the Schengen Information System for the purposes of tracing persons shall be kept only for the time required to meet the purposes for which they were supplied. The Contracting Party which issued the alert must review the need for continued storage of such data not later than three years after they were entered. The period shall be one year in the case of the alerts referred to in Article 99.

(2) Each Contracting Party shall, where appropriate, set shorter review periods in accordance with its national law.

(3) The technical support function of the Schengen Information System shall automatically inform the Contracting Parties of scheduled deletion of data from the system one month in advance.

(4) The Contracting Party issuing the alert may, within the review period, decide to keep the alert should this prove necessary for the purposes for which the alert was issued. Any extension of the alert must be communicated to the technical support function. The provisions of paragraph 1 shall apply to the extended alert.

Information: Article 112a SD? comes into force 180 days after the date of release of the Council Decision by 15 March 2005 (that is the 11 September 2005). For Iceland and Norway the Article comes into force 270 days after the date of release (that is the 10 December 2005). See the Council Decision .

Article 112A

(1) Personal data held in files by the authorities referred to in Article 92 (4) as a result of information exchange pursuant to that paragraph, shall be kept only for such time as may be required to achieve the

purposes for which they were supplied. They shall in any event be deleted at the latest one year after the alert or alerts concerning the person or object concerned have been deleted from the Schengen Information System.

(2) Paragraph 1 shall not prejudice the right of a Member State to keep in national files data relating to a particular alert which that Member State has issued or to an alert in connection with which action has been taken on its territory. The period of time for which such data may be held in such files shall be governed by national law.

Article 113

(1) Data other than that referred to in Article 112 shall be kept for a maximum of ten years, data on issued identity papers and suspect banknotes for a maximum of five years and data on motor vehicles, trailers and caravans for a maximum of three years.

Information: Article 113 (1) obtains at a point in time decided unanimously by the council as soon as the conditions are existent the following composition (see Council Decision):

(1) Data other than that referred to in Article 112 shall be kept for a maximum of 10 years and data on objects referred to in Article 99 (1) for a maximum of five years.

(2) Data which have been deleted shall be kept for one year in the technical support function. During that period they may only be consulted for subsequent checking as to their accuracy and as to whether the data were entered lawfully. Afterwards they must be destroyed.

Information: Article 113A SD? comes into force 180 days after the date of release of the Council Decision by 15 March 2005 (that is the 11 September 2005). For Iceland and Norway the Article comes into force 270 days after the date of release (that is the 10 December 2005). See the Council Decision Council Decision .

Article 113A

(1) Data other than personal data held in files by the authorities referred to in Article 92 (4) as a result of information exchange pursuant to that paragraph, shall be kept only for such time as may be required to achieve the purposes for which they were supplied. They shall in any event be deleted at the latest one year after the alert or alerts concerning the person or object concerned have been deleted from the Schengen Information System.

(2) Paragraph 1 shall not prejudice the right of a Member State to keep in national files data relating to a particular alert which that Member State has issued or to an alert in connection with which action has been taken on its territory. The period of time for which such data may be held in such files shall be governed by national law.

Article 114

(1) Each Contracting Party shall designate a supervisory authority responsible in accordance with national law for carrying out independent supervision of the data file of the national section of the Schengen Information System and for checking that the processing and use of data entered in the Schengen Information System does not violate the rights of the data subject. For this purpose, the supervisory authority shall have access to the data file of the national section of the Schengen Information System.

(2) Any person shall have the right to ask the supervisory authorities to check data entered in the Schengen Information System which concern them and the use made of such data. That right shall be governed by the national law of the Contracting Party to which the request is made. If the data have been entered by another Contracting Party, the check shall be carried out in close coordination with that

Contracting Party's supervisory authority.

Article 115

(1) A joint supervisory authority shall be set up and shall be responsible for supervising the technical support function of the Schengen Information System. This authority shall consist of two representatives from each national supervisory authority. Each Contracting Party shall have one vote. Supervision shall be carried out in accordance with the provisions of this Convention, the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data, taking into account Recommendation No R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe regulating the use of personal data in the police sector, and in accordance with the national law of the Contracting Party responsible for the technical support function.

(2) As regards the technical support function of the Schengen Information System, the joint supervisory authority shall have the task of checking that the provisions of this Convention are properly implemented. For that purpose, it shall have access to the technical support function.

(3) The joint supervisory authority shall also be responsible for examining any difficulties of application or interpretation that may arise during the operation of the Schengen Information System, for studying any problems that may occur with the exercise of independent supervision by the national supervisory authorities of the Contracting Parties or in the exercise of the right of access to the system, and for drawing up harmonised proposals for joint solutions to existing problems.

(4) Reports drawn up by the joint supervisory authority shall be submitted to the authorities to which the national supervisory authorities submit their reports.

Article 116

(1) Each Contracting Party shall be liable in accordance with its national law for any injury caused to a person through the use of the national data file of the Schengen Information System. This shall also apply to injury caused by the Contracting Party which issued the alert, where the latter entered factually inaccurate data or stored data unlawfully.

(2) If the Contracting Party against which an action is brought is not the Contracting Party issuing the alert, the latter shall be required to reimburse, on request, the sums paid out as compensation unless the data were used by the requested Contracting Party in breach of this Convention.

Article 117

(1) As regards the automatic processing of personal data communicated pursuant to this Title, each Contracting Party shall, no later than the date of entry into force of this Convention, adopt the necessary national provisions in order to achieve a level of protection of personal data at least equal to that resulting from the principles laid down in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 and in accordance with Recommendation No R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe regulating the use of personal data in the police sector.

(2) The communication of personal data provided for in this Title may not take place until the provisions for the protection of personal data as specified in paragraph 1 have entered into force in the territories of the Contracting Parties involved in such communication.

Article 118

(1) Each Contracting Party undertakes, in relation to its national section of the Schengen Information System, to adopt the necessary measures in order to:

deny unauthorised persons access to data processing equipment used for processing personal data (equipment access control);
prevent the unauthorised reading, copying, modification or removal of data media (data media control);
prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);
prevent the use of automated data processing systems by unauthorised persons using data communication equipment (user control);
ensure that persons authorised to use an automated data processing system only have access to the data covered by their access authorisation (data access control);
ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);
ensure that it is subsequently possible to verify and establish which personal data have been input into automated data processing systems and when and by whom the data were input (input control);
prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control).v

(2) Each Contracting Party must take special measures to ensure the security of data while they are being communicated to services located outside the territories of the Contracting Parties. Such measures must be notified to the joint supervisory authority.

(3) For the processing of data in its national section of the Schengen Information System each Contracting Party may appoint only specially qualified persons who have undergone security checks.

(4) The Contracting Party responsible for the technical support function of the Schengen Information System shall adopt the measures laid down in paragraphs 1 to 3 in respect of that function.

TITLE VI - Protection of personal data

Article 126

(1) As regards the automatic processing of personal data communicated pursuant to this Convention, each Contracting Party shall, no later than the date of entry into force of this Convention, adopt the necessary national provisions in order to achieve a level of protection of personal data at least equal to that resulting from the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981.

(2) The communication of personal data provided for in this Convention may not take place until the provisions for the protection of personal data as specified in paragraph 1 have entered into force in the territories of the Contracting Parties involved in such communication.

(3) In addition, the following provisions shall apply to the automatic processing of personal data communicated pursuant to this Convention:
such data may be used by the recipient Contracting Party solely for the purposes for which this Convention stipulates that they may be communicated; such data may be used for other purposes only with the prior authorisation of the Contracting Party communicating the data and in accordance with the law of the recipient Contracting Party; such authorisation may be granted insofar as the national law of the Contracting Party communicating the data so permits;
such data may be used only by the judicial authorities and the departments and authorities carrying out tasks or performing duties in connection with the purposes referred to in paragraph (a);
the Contracting Party communicating such data shall be obliged to ensure the accuracy thereof; should it establish, either on its own initiative or further to a request by the data subject, that data have been provided that are inaccurate or should not have been communicated, the recipient Contracting Party or Parties must be immediately informed thereof; the latter Party or Parties shall be obliged to correct or destroy the data, or to indicate that the data are inaccurate or were unlawfully communicated;

a Contracting Party may not plead that another Contracting Party communicated inaccurate data, in order to avoid its liability under its national law vis-?-vis an injured party; if damages are awarded against the recipient Contracting Party because of its use of inaccurate communicated data, the Contracting Party which communicated the data shall refund in full to the recipient Contracting Party the amount paid in damages;

the transmission and receipt of personal data must be recorded both in the source data file and in the data file in which they are entered;

the joint supervisory authority referred to in Article 115 may, at the request of one of the Contracting Parties, deliver an opinion on the difficulties of implementing and interpreting this Article.

(4) This Article shall not apply to the communication of data provided for under Chapter 7 of Title II and Title IV. Paragraph 3 shall not apply to the communication of data provided for under Chapters 2 to 5 of Title III.

Article 127

(1) Where personal data are communicated to another Contracting Party pursuant to the provisions of this Convention, Article 126 shall apply to the communication of the data from a non-automated data file and to their inclusion in another non-automated data file.

(2) Where, in cases other than those governed by Article 126 (1), or paragraph 1 of this Article, personal data are communicated to another Contracting Party pursuant to this Convention, Article 126 (3), with the exception of subparagraph (e), shall apply. The following provisions shall also apply:

a written record shall be kept of the transmission and receipt of personal data; this obligation shall not apply where such a record is not necessary given the use of the data, in particular if they are not used or are used only very briefly;

the recipient Contracting Party shall ensure, in the use of communicated data, a level of protection at least equal to that laid down in its national law for the use of similar data;

the decision concerning whether and under what conditions the data subject shall, at his request, be provided information concerning communicated data relating to him shall be governed by the national law of the Contracting Party to which the request was addressed.

(3) This Article shall not apply to the communication of data provided for under Chapter 7 of Title II, Chapters 2 to 5 of Title III, and Title IV.

Article 128

(1) The communication of personal data provided for by this Convention may not take place until the Contracting Parties involved in that communication have instructed a national supervisory authority to monitor independently that the processing of personal data in data files complies with Articles 126 and 127 and the provisions adopted for their implementation.

(2) Where the Contracting Party has, in accordance with its national law, instructed a supervisory authority to monitor independently, in one or more areas, compliance with the provisions on the protection of personal data not entered in a data file, that Contracting Party shall instruct the same authority to supervise compliance with the provisions of this Title in the areas concerned.

(3) This Article shall not apply to the communication of data provided for under Chapter 7 of Title II and Chapters 2 to 5 of Title III.

Article 129

As regards the communication of personal data pursuant to Chapter 1 of Title III, the Contracting Parties undertake, without prejudice to Articles 126 and 127, to achieve a level of protection of personal data which complies with the principles of Recommendation No R (87) 15 of 17 September 1987 of the

Committee of Ministers of the Council of Europe regulating the use of personal data in the police sector. In addition, as regards the communication of data pursuant to Article 46, the following provisions shall apply:

the data may be used by the recipient Contracting Party solely for the purposes indicated by the Contracting Party which provided the data and in compliance with the conditions laid down by that Contracting Party;

the data may be communicated to police forces and authorities only; data may not be communicated to other authorities without the prior authorisation of the Contracting Party which provided them;

the recipient Contracting Party shall, upon request, inform the Contracting Party which provided the data of the use made of the data and the results thus obtained.

Article 130

If personal data are communicated via a liaison officer as referred to in Article 47 or Article 125, the provisions of this Title shall not apply unless the liaison officer communicates such data to the Contracting Party which seconded the officer to the territory of the other Contracting Party.