

Changes introduced by the Commission proposal to amend the Council Decision 2009/917/JHA are highlighted in grey and marked as underlined text for additions and ~~striketrough~~ for deletions. The markings are applied only to the text of Articles, and not Recitals that were copied from the Commission proposal.

Changes introduced by the Presidency in the first Presidency compromise texts (WK 10974/2023) which remain in this second Presidency compromise texts are highlighted in green and marked as **bold and underlined text for additions and ~~striketrough~~ for deletions.**

Changes introduced by the Presidency with regard to previous Presidency compromise texts (WK 10974/2023) are highlighted in yellow and marked as ***italic, bold and underlined text for additions*** and ~~*italic, striketrough for deletions.*~~

2023/0143 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Council Decision 2009/917/JHA, as regards its alignment with Union rules on the protection of personal data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) thereof,

Having regard to the proposal from the European Commission,

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

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Directive (EU) 2016/680 of the European Parliament and of the Council¹ provides for harmonised rules for the protection and the free movement of personal data processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, including the safeguarding against, and the prevention of threats to, public security. That Directive requires the Commission to review relevant other acts of Union law in order to assess the need to align them with that Directive and to make, where necessary, the proposals to amend those acts to ensure a consistent approach to the protection of personal data falling within the scope of that Directive.

(2) Council Decision 2009/917/JHA² on the use of information technology for customs purposes establishes the Customs Information System (CIS) to assist in preventing, investigating and prosecuting serious contraventions of national laws by making information available more rapidly and increase the effectiveness of the customs administrations. In order to ensure a consistent approach to the protection of personal data in the Union, that Decision should be amended to align it with Directive (EU) 2016/680. **In particular, the personal data protection rules should respect the principle of purpose specification, be limited to specified categories of data subjects and categories of personal data, respect data security requirements, include additional protection for special categories of personal data and respect the conditions for subsequent processing. Moreover, provision should be made for the coordinated supervision model as introduced by Article 62 of Regulation (EU) 2018/1725³:-** **The system consists of a central database facility which stores personal data such as names and forenames, addresses, number of identity papers related to commodities, means of transport, businesses, persons, detained, seized or confiscated items and cash. The centralised database is managed by the Commission, which does not have access to the personal data stored in it. The central database is, accessible by the designated authorities of the Member States, which may enter and consult the information stored in it. Europol and Eurojust have, within their mandate and for the fulfilment of their tasks, the right to access to the data entered in the central database by the competent authorities of the Member States and to search those data.**

¹ Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

² Council Decision 2009/917/JHA on the use of information technology for customs purposes (OJ L 323, 10.12.2009, p. 20).

³ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

(2a) In order to ensure a consistent approach to the protection of personal data in the Union, that Decision should be amended to align it with Directive (EU) 2016/680. In particular, the personal data protection rules should respect the principle of purpose specification, be limited to specified categories of data subjects and categories of personal data, respect data security requirements, include additional protection for special categories of personal data and respect the conditions for subsequent processing. Moreover, provision should be made for the coordinated supervision model as introduced by Article 62 of Regulation (EU) 2018/1725¹.

(3) In particular, in order to ensure a clear and consistent approach ensuring adequate protection of personal data, the term ‘serious contraventions’ should be replaced by ‘criminal offences’ **as referred to in Article 1(1) of the Directive EU 2016/680**, bearing in mind that the fact that a given conduct is prohibited under the criminal law of a Member State in itself implies a certain degree of seriousness of the contravention. Moreover, the **objective purpose** of the CIS should remain limited to assisting in connection to the prevention, investigation, detection or prosecution of the criminal offences under national laws as defined in Council Decision 2009/917/JHA, that is, national laws in respect of which national customs administrations are competent and that are therefore particularly relevant in the context of customs. Therefore, whereas qualification as a criminal offence is a necessary requirement, not all criminal offences should be considered to be covered. By way of example, the covered criminal offences include illicit drugs trafficking, illicit weapons trafficking and money laundering. Furthermore, other than the introduction of the term ‘criminal offences’, this amendment should not be understood as affecting the specific requirements set out in that Council Decision regarding the establishment and sending of a list of criminal offences under national laws that meet certain conditions, those requirements relating only to the particular purpose of the customs files identification database.

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

(4) *[It is necessary to clarify the respective roles of applicable legislation to the processing of personal data under the Council Decision 2009/917/JHA by the Commission, Europol, Eurojust and of the Member States by the national authorities designated by each Member State competent national authorities with regard to the personal data. The Commission is considered the processor acting on behalf of the national authorities designated by each Member State, which are considered the controllers of the personal data, and the supervisory authorities responsible for monitoring the processing of personal data by each of them.]*

When processing personal data under Council Decision 2009/917/JHA, without prejudice to specific rules contained in the Decision, Member States are subject to the national provisions adopted by them pursuant to Directive (EU) 2016/680; the European Commission is subject to the rules laid down in Regulation (EU) 2018/1725; Europol is subject to the rules laid down in Regulation (EU) 2016/794; Eurojust is subject to the rules laid down in Regulation (EU) 2016/1727. Those rules govern inter alia the obligations and responsibilities of controllers, joint controllers, processors and their relationship. National supervisory authorities responsible for monitoring and ensuring the application of Directive (EU) 2016/680 in each Member State shall be competent for monitoring and ensuring the application of the provisions of this regulations.. The European Data Protection Supervisor is responsible for monitoring and ensuring the application of the provisions of this Regulation relating to the protection of fundamental rights and freedoms of natural persons with regard to the processing of personal data by the European Commission, Europol, and Eurojust.

(5) To ensure the optimal preservation of the data while reducing the administrative burden for the competent authorities **and in line with Article 33 of Regulation (EU) 515/1997**, the procedure governing the retention of personal data in the CIS should be simplified by removing the obligation to review data annually and by setting a maximum retention period of five years which can be increased, subject to justification, by an additional period of two years. That retention period is necessary and proportionate in view of the typical length of criminal proceedings and the need for the data for the conduct of joint customs operations and of investigations.

(5a) The processing of personal data under Council Decision 2009/917/JHA involves the processing, exchange and subsequent use of relevant information for the purposes set out in Article 87 of the Treaty on the Functioning of the European Union (TFEU). In the interests of consistency and the effective protection of personal data, the processing of personal data under Council Decision 2009/917/JHA should comply with Union and Member States law on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. It should be possible for personal data contained in information lawfully entered in the Customs Information System to be processed for purposes other than those for which the System was set up, such as subsequent criminal or related administrative or civil procedures or parliamentary scrutiny, only in accordance with the conditions laid down in the applicable Union and Member States Law, including in particular that it be necessary and proportionate to its purpose.

(6) In accordance with Article 6a of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union (TEU) and to the TFEU, Ireland is bound by Council Decision 2009/917/JHA and is therefore taking part in the adoption of this Regulation.

(7) In accordance with Articles 1, 2 and 2a of Protocol No 22 on the Position of Denmark annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, Denmark is ~~not taking part in the adoption of this Regulation and is not bound by it or subject to its application~~ **bound by Council Decision 2009/917/JHA and is therefore taking part in the adoption of this Regulation.**

(8) The European Data Protection Supervisor was consulted in accordance with Article 42 of Regulation (EU) 2018/1725 and delivered an opinion on **04/07/2023**.

(9) Council Decision 2009/917/JHA should therefore be amended accordingly,

HAVE ADOPTED THIS REGULATION:

CHAPTER I

ESTABLISHMENT OF A CUSTOMS INFORMATION SYSTEM

Article 1

1. A joint automated information system for customs purposes (hereinafter referred to as the "Customs Information System" or the "System") is hereby established.

2. ~~The aim of the Customs Information System, in accordance with this Decision, shall be to assist in preventing, investigating and prosecuting serious contraventions of national laws by making information available more rapidly, thereby increasing the effectiveness of the cooperation and control procedures of the customs administrations of the Member States.~~

The **objective purpose** of the Customs Information System, **in accordance with this Decision**, is to assist the competent authorities in the Member States with the prevention, investigation, detection or prosecution of criminal offences under national laws, by making information available more rapidly, thereby increasing the effectiveness of the cooperation and control procedures of the customs administrations of the Member States.

CHAPTER II

DEFINITIONS

Article 2

For the purposes of this Decision:

1. "national laws" mean laws or regulations of a Member State, in the application of which the customs administration of that Member State has total or partial competence, concerning:

- (a) the movement of goods subject to measures of prohibition, restriction or control, in particular those measures covered by Articles 30 and 296 of the Treaty establishing the European

Community ("the EC Treaty");

(b) measures to control cash movements within the Community, where such measures are taken in accordance with Article 58 of the EC Treaty;

(c) the transfer, conversion, concealment, or disguise of property or proceeds acquired or obtained directly or indirectly through illicit international drug trafficking or by infringement of:

(i) the laws, regulations or administrative provisions of a Member State in the application of which the customs administration of that Member State has partial or total competence, concerning the cross-border movement of goods subject to measures of prohibition, restriction or control, in particular those measures referred to in Articles 30 and 296 of the EC Treaty, and non-harmonised excise duties;

(ii) the body of Community provisions and associated implementing provisions governing the import, export, transit and presence of goods traded between Member States and third countries, and between Member States in the case of goods that do not have Community status within the meaning of Article 23 of the EC Treaty or goods subject to additional controls or investigations for the purposes of establishing their Community status;

(iii) the body of provisions adopted at Community level under the common agricultural policy and the specific provisions adopted with regard to goods resulting from the processing of agricultural products; or

(iv) the body of provisions adopted at Community level for harmonised excise duties and for value-added tax on importation together with the national provisions implementing them, or those which have been used in that context;

~~2. "personal data" mean any information relating to an identified or identifiable natural person (data subject), whereby an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;~~

‘2. “personal data” means personal data as defined in point (1) of Article 3 of Directive (EU) 2016/680.’

3. "supplying Member State" means a Member State which enters an item of data into the Customs Information System;

4. "operational analysis" means analysis of operations which constitute, or appear to constitute, breaches of national laws, involving the following stages:

- (a) the collection of information, including personal data;
- (b) evaluation of the reliability of the information source and the information itself;
- (c) research, methodical presentation and interpretation of links between these items of information or between them and other significant data;
- (d) the formulation of observations, hypotheses or recommendations directly usable as risk information by the competent authorities to prevent and detect other operations in breach of national laws and/or to identify with precision the person or businesses-implicated in such operations;

5. "strategic analysis" means research and presentation of the general trends in breaches of national laws through an evaluation of the threat, scale and impact of certain types of operation in breach of national laws, with a view to setting priorities, gaining a better picture of the phenomenon or threat, reorienting action to prevent and detect fraud and reviewing departmental organisation. Only data from which identifying factors have been removed may be used for strategic analysis.

CHAPTER III

OPERATION AND USE OF THE CUSTOMS INFORMATION SYSTEM

Article 3

1. The Customs Information System shall consist of a central database facility, accessible through terminals in each Member State. It shall comprise exclusively data necessary to achieve its **purpose** as stated in Article 1(2), including personal data, in the following categories:

- (a) commodities;
- (b) means of transport;
- (c) businesses;
- (d) persons;
- (e) fraud trends;
- (f) availability of expertise;
- (g) items detained, seized or confiscated;
- (h) cash detained, seized or confiscated.

2. The Commission shall ensure the technical management of the infrastructure of the Customs Information System in accordance with the rules provided for by the implementing measures adopted by the Council. ~~In relation to the processing of personal data in the Customs Information System, the Commission shall be considered the processor, within the meaning of point (12) of Article 3 of Regulation (EU) 2018/1725, acting on behalf of the national authorities designated by each Member State, which shall be considered the controllers of the personal data.~~

The Commission shall report on management to the Committee referred to in Article 27

3. The Commission shall communicate to that Committee the practical arrangements adopted for technical management.

Article 4

1. Member States shall determine the items to be entered into the Customs Information System relating to each of the categories referred to in Article 3(1), to the extent that this is necessary to achieve the **aim purpose** of the System. No items of personal data shall be entered in any event within the category set out in point (e) of Article 3(1).

2. With regard to the categories set out in points (a) to (d) of Article 3(1), the items of information entered in respect of persons shall comprise no more than:

- (a) name, maiden name, forenames, former surnames and aliases;
- (b) date and place of birth;
- (c) nationality;
- (d) sex;
- (e) number and place and date of issue of the identity papers (passports, identity cards, driving licences);
- (f) address;
- (g) any particular objective and permanent physical characteristics;
- (h) reason for entering data;
- (i) suggested action;
- (j) a warning code indicating any history of being armed, violent or of escaping;
- (k) registration number of the means of transport.

3. With regard to the category set out in point (f) of Article 3(1), the items of information entered in respect of persons shall comprise no more than the experts' surnames and forenames.

4. With regard to the categories set out in points (g) and (h) of Article 3(1), the items of information entered in respect of persons shall comprise no more than:

- (a) name, maiden name, forenames, former surnames and aliases;
- (b) date and place of birth;
- (c) nationality;
- (d) sex;
- (e) address.

5. ~~In no case shall personal data listed in Article 6 of the Framework Decision 2008/977/JHA be entered into the Customs Information System.~~

In no case shall **the special categories of** personal data referred to in Article 10 of Directive (EU) 2016/680 be entered into the Customs Information System.

Article 5

1. Data in the categories referred to in points (a) to (g) of Article 3(1) shall be entered into the Customs Information System only for the purpose of sighting and reporting, discreet surveillance, specific checks and strategic or operational analysis.

Data in the category referred to in point (h) of Article 3(1) shall be entered into the Customs Information System only for the purpose of strategic or operational analysis.

2. ~~For the purpose of the actions referred to in paragraph 1, personal data in any of the categories referred to in Article 3(1) may be entered into the Customs Information System only if there are real indications, in particular on the basis of prior illegal activities, to suggest that the person concerned has committed, is in the act of committing or will commit serious contraventions of national laws.~~

For the purpose of the actions referred to in paragraph 1, personal data in any of the categories referred to in Article 3(1) may be entered into the Customs Information System only if there are reasonable grounds, in particular on the basis of prior illegal activities, to suggest that the person concerned has committed, is in the act of committing or will commit criminal offences under national laws.

Article 6

1. If the actions referred to in Article 5(1) are carried out, the following information may in whole or in part be collected and transferred to the supplying Member State:

- (i) the fact that the commodity, means of transport, business or person reported has been found;
- (ii) the place, time and reason for the check;
- (iii) the route and destination of the journey;
- (iv) persons accompanying the person concerned or occupants of the means of transport;
- (v) the means of transport used;
- (vi) objects carried;
- (vii) the circumstances under which the commodity, means of transport, business or person was found.

When such information is collected in the course of discreet surveillance, steps have to be taken to ensure that the discreet nature of the surveillance is not jeopardised.

2. In the context of a specific check referred to in Article 5(1), persons, means of transport and objects may be searched to the extent permissible and in accordance with the laws, regulations and procedures of the Member State in which the search takes place. If the specific check is not permitted by the law of a Member State, it shall automatically be converted by that Member State into sighting and reporting or discreet surveillance.

Article 7

1. Direct access to data entered into the Customs Information System shall be reserved to the national authorities designated by each Member State. Those national authorities shall be customs administrations, but may also include other authorities competent, according to the laws, regulations and procedures of the Member State in question, to act in order to achieve the **aim purpose** stated in Article 1(2).

2. Each Member State shall send the other Member States and the Committee referred to in Article 27 a list of its competent authorities which have been designated in accordance with paragraph 1 of this Article to have direct access to the Customs Information System stating, for each authority, to which data it may have access and for what purposes.

3. Notwithstanding paragraphs 1 and 2, the Council may, by a unanimous decision, permit access to the Customs Information System by international or regional organisations. In making this decision the Council shall take account of any reciprocal arrangements and any opinion on the adequacy of data protection measures by the Joint Supervisory Authority referred to in Article 25.

~~Notwithstanding paragraphs 1 and 2, the Council may exceptionally, by a unanimous decision and after consultation of the European Data Protection Board, permit access to the Customs Information System by international or regional organisations, provided that both of the following conditions are met:~~

~~(a) the access complies with the general principles for transfers of personal data set out in Article 35 or, where applicable, Article 39 of Directive (EU) 2016/680;~~

~~(b) the access is based either on an adequacy decision adopted under Article 36 of that Directive or is subject to appropriate safeguards under Article 37 thereof;~~

Article 8

1. Member States, Europol and Eurojust may use data obtained from the Customs Information System only in order to achieve the aim stated in Article 1(2). However, they may use it for administrative or other purposes with the prior authorisation of, and subject to any conditions imposed by, the Member State which entered the data in the System. Such other use shall be in accordance with the laws, regulations and procedures of the Member State which seeks to use it in accordance with Article 3(2) of Framework Decision 2008/977/JHA, and should take into account Principle 5.2.i of the Recommendation No R (87) 15.

The national authorities designated by each Member State in accordance with Article 7(1) Member States, Europol and Eurojust may process personal data obtained from the Customs Information System only in order to achieve the **aim** purpose stated in Article 1(2) **or for other purposes in accordance with Union or Member States law** *adopted pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council, in particular Article 4(2) and Article 9(1) and (3) thereof; or, where applicable, Regulation (EU) 2018/1725 of the European Parliament and of the Council, in particular Article 71(2) and Article 75 thereof; and with the prior authorisation of, and subject to in compliance with any conditions imposed by, the designated national authorities of* the Member State which entered the personal data in that system, **in accordance with the applicable rules of Union law on the processing of personal data.**

Member States, Europol and Eurojust may process non-personal data obtained from the Customs Information System in order to achieve the **aim** purpose stated in Article 1(2) or for other purposes, including administrative ones, in compliance with any conditions imposed by the **designated national authorities** **authorities of the** Member State which entered the non-personal data in that system.

2. Without prejudice to paragraphs 1 and 4 of this Article, Article 7(3) and Articles 11 and 12, data obtained from the Customs Information System shall only be used by national authorities in each Member State designated by the Member State in question, which are competent, in accordance with the laws, regulations and procedures of that Member State, to act in order to achieve the **aim** purpose stated in Article 1(2).

3. Each Member State shall send the other Member States and the Committee referred to in Article 27 a list of the competent authorities it has designated in accordance with paragraph 2 of this Article.

4. ~~Data obtained from the Customs Information System may, with the prior authorisation of, and subject to any conditions imposed by, the Member State which entered them into the System, be transferred for use by national authorities other than those designated under paragraph 2 of this Article, third countries, and international or regional organisations wishing to make use of them. Each Member State shall take special measures to ensure the security of such data when they are being transferred to services located outside its territory. Details of such measures have to be communicated to the Joint Supervisory Authority referred to in Article 25.~~

Personal data obtained from the Customs Information System may, with the prior authorisation of, and subject to compliance with any conditions imposed by, the **designated national authorities of the** Member State which entered that data into that system, be:

(a) transmitted to, and further processed by, national authorities other than those designated under paragraph 2, in accordance with **Union or Member States law on the processing of personal data** the applicable rules of Union law on the processing of personal data; or

(b) transferred to, and further processed by, the competent authorities of third countries and international or regional organisations, in accordance with **Union or Member States law on the processing of personal data, adopted pursuant to Chapter V of Directive (EU) 2016/680 and, where relevant, with Chapter V of Regulation (EU) 2018/1725.**

Non-personal data obtained from the Customs Information System may be transferred to, and further processed by national authorities other than those designated under paragraph 2, third countries, and international or regional organisations, in compliance with any conditions imposed by the Member State which entered the non-personal data in that system.

Article 9

1. The entry of data into the Customs Information System shall be governed by the laws, regulations and procedures of the supplying Member State unless this Decision lays down more stringent provisions.

2. The use of data obtained from the Customs Information System, including performance of any action under Article 5(1) suggested by the supplying Member State, shall be governed by the laws, regulations and procedures of the Member State using such data, unless this Decision lays down more stringent provisions.

Article 10

1. Each Member State shall designate a competent customs administration which shall have national responsibility for the Customs Information System.
2. The administration referred to in paragraph 1 shall be responsible for the correct operation of the Customs Information System within the Member State and shall take the measures necessary to ensure compliance with this Decision.
3. Member States shall inform one another of the administration referred to in paragraph 1.

Article 11

1. Europol shall, within its mandate and for the fulfilment of its tasks, have the right to have access to the data entered into the Customs Information System in accordance with Articles 1, 3 to 6 and 15 to 19 and to search those data.
2. Where a search by Europol reveals the existence of a match between information processed by Europol and an entry in the Customs Information System, Europol shall, through the channels defined in Council Decision 2009/371/JHA of 6 April 2009 establishing a European Police Office (Europol)¹, inform the Member State which made the entry.
3. Use of information obtained from a search in the Customs Information System is subject to the consent of the Member State which entered the data into the System. If that Member State allows the use of such information, the handling thereof shall be governed by the Decision 2009/371/JHA. Europol may transfer such information to third countries and third bodies only with the consent of the Member State which entered the data into the System.
4. Europol may request further information from the Member States concerned, in accordance with the Decision 2009/371/JHA.

¹ OJ L 121, 15.5.2009, p. 37.

5. Without prejudice to paragraphs 3 and 4, Europol shall not connect the parts of the Customs Information System to which it has access to any computer system for data collection and processing operated by or at Europol, nor transfer the data contained therein to any such system, nor download or otherwise copy any part of the Customs Information System.

Europol shall limit access to data entered into the Customs Information System to duly authorised staff of Europol.

Europol shall allow the Joint Supervisory Body, set up under Article 34 of the Decision 2009/371/JHA, to review the activities of Europol in the exercise of its right to accede to and to search data entered into the Customs Information System.

6. Nothing in this Article shall be interpreted as affecting the provisions of the Decision 2009/371/JHA concerning data protection and the liability for any unauthorised or incorrect processing of such data by Europol staff, or as affecting the powers of the Joint Supervisory Body set up pursuant to that Decision.

Article 12

1. The national members of Eurojust, their deputies, assistants and specifically authorised staff shall, within their mandate and for the fulfilment of Eurojust's tasks, have the right to have access to the data entered into the Customs Information System in accordance with Articles 1, 3 to 6 and 15 to 19 and to search those data.

2. Where a search by a national member of Eurojust, their deputies, assistants or specifically authorised staff reveals the existence of a match between information processed by Eurojust and an entry in the Customs Information System, he or she shall inform the Member State which made the entry. Any communication of information obtained from such a search may be communicated to third countries and third bodies only with the consent of the Member State which made the entry.

3. Nothing in this Article shall be interpreted as affecting the provisions of Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime¹ which concern data protection and the liability for any unauthorised or incorrect processing of such data by national members of Eurojust, their deputies, assistants and specifically authorised staff, or as affecting the powers of the Joint Supervisory Body set up pursuant to that Decision.

4. No parts of the Customs Information System to which the national members of Eurojust, their deputies, assistants and specifically authorised staff have access shall be connected to any computer system for data collection and processing in operation by or at Eurojust, nor shall any data contained in the former be transferred to the latter, nor shall any part of the Customs Information System be downloaded.

5. Access to data entered in the Customs Information System shall be limited to the national members of Eurojust, their deputies, assistants and specifically authorised staff and shall not be extended to other Eurojust staff.

CHAPTER IV

AMENDMENT OF DATA

Article 13

1. Only the supplying Member State shall have the right to amend, supplement, rectify or erase data which it has entered in the Customs Information System.

2. Should a supplying Member State note, or have drawn to its attention, that the data it entered are factually inaccurate or were entered, or are stored contrary to this Decision, it shall amend, supplement, rectify or erase the data, as appropriate, and shall inform the other Member States, Europol and Eurojust accordingly.

¹ OJ L 138, 4.6.2009, p. 14.

3. If a Member State, Europol or Eurojust has evidence to suggest that an item of data is factually inaccurate, or was entered or is stored in the Customs Information System, contrary to this Decision, it shall inform thereof the supplying Member State as soon as possible. The latter shall check the data concerned and, if necessary, rectify or erase the item without delay. The supplying Member State shall inform the other Member States, Europol and Eurojust of any rectification or erasure effected.

4. If, when entering data in the Customs Information System, a Member State notes that its report conflicts with a previous report as to content or suggested action, it shall immediately inform thereof the Member State which made the previous report. The two Member States shall then attempt to resolve the matter. In the event of disagreement, the first report shall stand, but those parts of the new report which do not conflict with the first report shall be entered in the System.

5. Subject to this Decision, where in any Member State a court, or other competent authority within that Member State, makes a final decision as to amendment, supplementation, rectification or erasure of data in the Customs Information System, the Member States undertake mutually to enforce such a decision. In the event of conflict between such decisions of courts or other competent authorities in different Member States, including the corresponding data processing supervisory authority those referred to in Article 23(1) Articles 26 and 26a, concerning rectification or erasure, the Member State which entered the data in question shall erase them from the System.

CHAPTER V

RETENTION OF DATA

Article 14

Personal data entered into the Customs Information System shall be kept only for the time necessary to achieve the **aim** purpose stated in Article 1(2) and may not be retained for more than five years. However, exceptionally, that data may be kept for an additional period of at most two years, where and insofar as a strict need to do so in order to achieve that **aim** purpose is established in an individual case.

~~1. — Data entered into the Customs Information System shall be kept only for the time necessary to achieve the purpose for which they were entered. The need for their retention shall be reviewed at least annually by the supplying Member State.~~

~~2. The supplying Member State may, within the review period, decide to retain data until the next review if their retention is necessary for the purposes for which they were entered. Without prejudice to Articles 22 and 23, if there is no decision to retain data, they shall automatically be transferred to that part of the Customs Information System to which access shall be limited in accordance with paragraph 4 of this Article.~~

~~3. The Customs Information System shall automatically inform the supplying Member State of a scheduled transfer of data from the Customs Information System under paragraph 2, giving one month's notice.~~

~~4. Data transferred under paragraph 2 of this Article shall continue to be retained for one year within the Customs Information System but, without prejudice to Articles 22 and 23, shall be accessible only to a representative of the Committee referred to in Article 27 or to the supervisory authorities referred to in Articles 24 and 25(1). During that period they may consult the data only for the purposes of checking their accuracy and lawfulness, after which the data have to be erased.~~

CHAPTER VI

CREATION OF A CUSTOMS FILES IDENTIFICATION DATABASE

Article 15

1. The Customs Information System shall contain data in accordance with this Chapter, in addition to data contained in accordance with Article 3, in a special database (hereinafter referred to as "the customs files identification database"). Without prejudice to the provisions of this Chapter and of Chapters VII and VIII, all the provisions of this Decision shall also apply to the customs files identification database. However, the exception in Article 21(2) shall not apply.

2. The ~~aim~~ **purpose** of the customs files identification database shall be to enable the national authorities responsible for carrying out customs investigations designated pursuant to Article 7, when opening a file on or investigating one or more persons or businesses, and for Europol and Eurojust, to identify competent authorities of other Member States which are investigating or have investigated those persons or businesses, in order, through information on the existence of investigation files, to achieve the ~~aim~~ **purpose** referred to in Article 1(2).

3. For the purposes of the customs files identification database, each Member State shall send the other Member States, Europol, Eurojust and the Committee referred to in Article 27 a list of criminal offences under its national laws.

This list shall comprise only criminal offences that are punishable:

(a) by deprivation of liberty or a detention order for a maximum period of not less than 12 months; or

(b) by a fine of at least EUR 15 000.

~~For the purposes of the customs files identification database, each Member State shall send the other Member States, Europol, Eurojust and the Committee referred to in Article 27 a list of serious contraventions of its national laws.~~

~~This list shall comprise only contraventions that are punishable:~~

~~(a) by deprivation of liberty or a detention order for a maximum period of not less than 12 months; or~~

~~(b) by a fine of at least EUR 15 000.~~

4. If the Member State retrieving data from the customs files identification database requires further information on the stored investigation file on a person or a business, it shall request the assistance of the supplying Member State on the basis of the instruments in force relating to mutual assistance.

CHAPTER VII

OPERATION AND USE OF THE CUSTOMS FILES IDENTIFICATION DATABASE

Article 16

1. Data from investigation files will be entered into the customs files identification database only for the purposes set out in Article 15(2). The data shall only cover the following categories:

- (a) a person or a business which is or has been the subject of an investigation file opened by a competent authority of a Member State, and which:
 - (i) in accordance with the national law of the Member State concerned, is suspected of committing or having committed, or participating or having participated in the commission of, a serious infringement of national laws;
 - (ii) has been the subject of a report establishing that such an infringement has taken place; or
 - (iii) has been the subject of an administrative or judicial sanction for such an infringement;
- (b) the field covered by the investigation file;
- (c) the name, nationality and contact information of the Member State's authority handling the case, together with the file number.

Data referred to in points (a) to (c) shall be entered in a data record separately for each person or business. Links between data records shall not be permitted.

2. The personal data referred to in point (a) of paragraph 1 shall consist of only the following:

- (a) for persons: name, maiden name, forenames, former surnames and aliases, date and place of birth, nationality and sex;
- (b) for businesses: business name, name under which trade is conducted, address, VAT identifier and excise duties identification number.

3. Data shall be entered for a limited period in accordance with Article 19.

Article 17

A Member State shall not be obliged to make entries pursuant to Article 16 in any particular case if, and for such time as, this would harm public policy or other essential interests, especially as this would present an immediate and serious threat to its public security or to the public security of another Member State or a third country; or where other essential interests of equal importance are at stake; or where such entries could pose serious harm to the rights of individuals or would prejudice an ongoing investigation.

Article 18

1. Entry of data in the customs files identification database and consultation thereof shall be reserved to the authorities referred to in Article 15(2).
2. Any consultation concerning the customs files identification database shall cover the following personal data:
 - (a) for persons: forename, and/or name, and/or maiden name, and/or former surnames, and/or aliases, and/or date of birth;
 - (b) for businesses: business name, and/or name under which trade is conducted, and/or address, and/or VAT identifier, and/or excise duties identification number.

CHAPTER VIII

PERIOD OF RETENTION OF DATA IN THE CUSTOMS FILES IDENTIFICATION DATABASE

Article 19

1. Storage periods shall be determined in accordance with the laws, regulations and procedures of the Member State entering the data. However, the following time-limits, starting on the date on which the data were entered in the file, shall not be exceeded:
 - (a) data relating to current investigation files shall not be retained beyond a period of three years if it has not been established that an infringement has taken place within that time period. The data shall be erased before the expiry of the three-year period if 12 months have passed since the last investigative act;
 - (b) data relating to investigation files which have established that an infringement has taken place but which have not yet led to a conviction or to imposition of a fine shall not be retained beyond a period of six years;
 - (c) data relating to investigation files which have led to a conviction or a fine shall not be retained beyond a period of 10 years.
2. At all stages of an investigation as referred to in points (a) to (c) of paragraph 1, as soon as a person or business within the scope of Article 16 is eliminated from an investigation pursuant to the laws and administrative regulations of the supplying Member State, all data relating to that person or business shall be erased immediately.
3. Data shall automatically be erased from the customs files identification database as from the date on which the data retention periods laid down in paragraph 1 are exceeded.

CHAPTER IX

PERSONAL DATA PROTECTION

Article 20

~~Directive (EU) 2016/680 shall apply to the processing of personal data under this Decision.~~

1. Without prejudice to this Decision, national provisions adopted pursuant Directive (EU) 2016/680 shall apply to the processing of personal data under this Decision by national authorities designated by each Member State in accordance to Article 7.

2. Without prejudice to this Decision, Regulation (EU) 2018/1725 shall apply to the processing of personal data under this Decision by the European Commission

3. Without prejudice to this Decision, Regulation (EU) 2016/794 shall apply to the processing of personal data under this Decision by Europol

4. Without prejudice to this Decision, Regulation (EU) 2018/1727 shall apply to the processing of personal data under this Decision by Eurojust.

~~Framework Decision 2008/977/JHA shall apply to the protection of the data exchange in accordance with this Decision unless otherwise provided in this Decision.~~

Article 21

1. Data may be duplicated only for technical purposes, provided that such duplication is necessary for direct searching by the authorities referred to in Article 7.

2. Subject to Article 8(1), personal data entered by other Member States may not be copied from the Customs Information System into other national data files, except those copies held in systems of risk management used to direct national customs controls or copies held in an operational analysis system used to coordinate actions. Such copies may be made to the extent necessary for specific cases or investigations.

3. In the two exceptional cases provided for in paragraph 2, only the analysts authorised by the national authorities of each Member State shall be empowered to process personal data obtained from the Customs Information System within the framework of a risk management system used to direct customs controls by national authorities or of an operational analysis system used to coordinate actions.

4. Each Member State shall send other Member States and the Committee referred to in Article 27 a list of the risk-management departments whose analysts are authorised to copy and process personal data entered in the Customs Information System.

5. Personal data copied from the Customs Information System shall be kept only for the time necessary to achieve the purpose for which they were copied. The need for their retention shall be reviewed at least annually by the Member State which carried out the copying. The storage period shall not exceed ten years. Personal data which are not necessary for the continuation of the operational analysis shall be erased immediately or have any identifying factors removed.

Article 22

~~The rights of persons with regard to personal data in the Customs Information System, in particular their right of access, to rectification, erasure or blocking shall be exercised in accordance with the laws, regulations and procedures of the Member State implementing Framework Decision 2008/977/JHA in which such rights are invoked. Access shall be refused to the extent that such refusal is necessary and proportionate in order not to jeopardise any ongoing national investigations, or during the period of discreet surveillance or sighting and reporting. When the applicability of such an exemption is assessed, the legitimate interests of the person concerned shall be taken into account.~~

Article 23

~~1. In the territory of each Member State, any person may, in accordance with the laws, regulations and procedures of the Member State in question, bring an action or, if appropriate, a complaint before the courts or the authority competent under the laws, regulations and procedures of that Member State concerning personal data relating to himself on the Customs Information System, in order to:~~

- ~~(a) rectify or erase factually inaccurate personal data;~~
- ~~(b) rectify or erase personal data entered or stored in the Customs Information System contrary to this Decision;~~
- ~~(c) obtain access to personal data;~~
- ~~(d) block personal data;~~
- ~~(e) obtain compensation pursuant to Article 30(2).~~

~~2. Without prejudice to the provisions of Article 31, the Member States concerned undertake mutually to enforce the final decisions taken by a court, or other competent authority, pursuant to points (a) to (e) of paragraph 1 of this Article.~~

Article 24

~~Each Member State shall designate a national supervisory authority or authorities responsible for personal data protection to carry out independent supervision of such data included in the Customs Information System in accordance with Framework Decision 2008/977/JHA.~~

Article 25

~~1. A Joint Supervisory Authority shall be set up, consisting of two representatives from each Member State's respective independent national supervisory authority or authorities.~~

2.—— The Joint Supervisory Authority shall monitor and ensure the application of the provisions of this Decision and Framework Decision 2008/977/JHA as concerns the protection of natural persons with respect to the processing of personal data through the Customs Information System.

3.—— To that end, the Joint Supervisory Authority shall be competent to supervise operation of the Customs Information System, to examine any difficulties of application or interpretation which may arise during its operation, to study problems which may arise with regard to the exercise of independent supervision by the national supervisory authorities of the Member States, or in the exercise of rights of access by individuals to the System, and to draw up proposals for the purpose of finding joint solutions to problems.

4.—— For the purpose of fulfilling its responsibilities, the Joint Supervisory Authority shall have access to the Customs Information System.

5.—— Reports drawn up by the Joint Supervisory Authority shall be forwarded to the authorities to which the national supervisory authorities submit their reports, to the European Parliament and the Council.

Article 26

~~Coordinated supervision among national supervisory authorities and the European Data Protection Supervisor shall be ensured in accordance with Article 62 of Regulation (EU) 2018/1725.~~

~~The independent supervisory authorities designated in each Member State and endowed with the powers referred to in Chapter VI of Directive (EU) 2016/680 shall monitor the lawfulness of the processing of personal data in CIS on their territory, its transmission from their territory and the exchange and further processing of supplementary information on their territory.~~

~~Coordinated supervision among national supervisory authorities and the European Data Protection Supervisor shall be ensured in accordance with Article 62 of Regulation (EU) 2018/1725.~~

1. — The European Data Protection Supervisor shall supervise the activities of the Commission regarding the Customs Information System. The duties and powers referred to in Articles 46 and 47 of Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data¹ shall apply accordingly.

2. — The Joint Supervisory Authority and the European Data Protection Supervisor, each acting within the scope of their respective competences, shall cooperate in the framework of their responsibilities and shall ensure coordinated supervision of the Customs Information System, including for issuing relevant recommendations.

3. — The Joint Supervisory Authority and the European Data Protection Supervisor shall meet for that purpose at least once a year. The costs and servicing of these meetings shall be for the account of the European Data Protection Supervisor.

Article 26 a

The European Data Protection Supervisor shall be responsible for monitoring the processing of personal data by the Commission, Europol and Eurojust and for ensuring that it is carried out in accordance with this Decision. The tasks and powers referred to in Articles 57 and 58 of Regulation (EU) 2018/1725 shall apply accordingly.

Article 26 b

Coordinated supervision among national supervisory authorities and the European Data Protection Supervisor shall be ensured in accordance with Article 62 of Regulation (EU) 2018/1725.

¹ OJ L 8, 12.1.2001, p. 1.

CHAPTER X

INSTITUTIONAL FRAMEWORK

Article 27

1. A Committee consisting of representatives from the customs administrations of the Member States shall be set up. The Committee shall take its decisions unanimously where the provisions of point (a) of paragraph 2 are concerned and by a two-thirds majority where the provisions of point (b) of paragraph 2 are concerned. It shall adopt its rules of procedure by unanimity.
 2. The Committee shall be responsible:
 - (a) for the implementation and correct application of the provisions of this Decision, without prejudice to the powers of the **competent data protection supervisory** authorities ~~referred to in Articles 24, 25(1) and 26(1)~~ **Articles 26 and 26a**;
 - (b) for the proper functioning of the Customs Information System with regard to technical and operational aspects. The Committee shall take all necessary steps to ensure that the measures set out in Articles 14 and 28 are properly implemented with regard to the Customs Information System.
- For the purpose of applying this paragraph, the Committee may have direct access to, and use of, data from the Customs Information System.
3. The Committee shall report annually to the Council, in accordance with Title VI of the Treaty on European Union, regarding the efficiency and effectiveness of the Customs Information System, making recommendations as necessary. That report shall be sent to the European Parliament for information.
 4. The Commission shall take part in the Committee's proceedings.

CHAPTER XI

SECURITY OF THE CUSTOMS INFORMATION SYSTEM

Article 28

1. All necessary administrative measures to maintain security shall be taken:
 - (a) by the competent authorities of the Member States in respect of the terminals of the Customs Information System in their respective Member States and by Europol and Eurojust;
 - (b) by the Committee referred to in Article 27 in respect of the Customs Information System and the terminals located on the same premises as the System and used for technical purposes and the checks required by paragraph 3 of this Article.

2. In particular the competent authorities, Europol, Eurojust and the Committee referred to in Article 27 shall take measures:

- (a) to prevent any unauthorised person from having access to installations used for the processing of data;
- (b) to prevent data and data media from being read, copied, modified or removed by unauthorised persons;
- (c) to prevent the unauthorised entry of data and any unauthorised consultation, modification or erasure of data;
- (d) to prevent data in the Customs Information System from being accessed by unauthorised persons by means of data transmission equipment;
- (e) to guarantee that, with respect to the use of the Customs Information System, authorised persons have right of access only to data for which they have competence;
- (f) to guarantee that it is possible to check and establish to which authorities data may be transmitted by data-transmission equipment;
- (g) to guarantee that it is possible to check and establish *a posteriori* what data have been entered in the Customs Information System, when and by whom, and to monitor searches;
- (h) to prevent the unauthorised reading, copying, modification or erasure of data during the transmission of data and the transport of data media.
- (i) to ensure that installed systems may, in the case of interruption, be restored;
- (j) to ensure that the functions of the system perform, that the appearance of faults in the functions is reported and that stored personal data cannot be corrupted by means of a malfunctioning of the system.

3. The Committee referred to in Article 27 shall monitor queries of the Customs Information System for the purpose of checking that searches made were admissible and were made by authorised users. At least 1 % of all searches made shall be checked. A record of such searches and checks shall be maintained in the System and shall be used only for the abovementioned purpose by that Committee and the **competent data protection** supervisory authorities ~~referred to in Articles 24 and 25~~**26 and 26a**. It shall be erased after six months.

Article 29

The competent customs administration referred to in Article 10(1) shall be responsible for the security measures set out in Article 28, in relation to the terminals located in the territory of the Member State concerned, the review functions set out in Article 14(1) and (2) and Article 19, and otherwise for the proper implementation of this Decision so far as is necessary under the laws, regulations and procedures of that Member State.

CHAPTER XII

RESPONSIBILITIES AND LIABILITIES

Article 30

- ~~1. Each Member State shall ensure that the data it has entered into the Customs Information System in accordance with Articles 3, 4(1) and 8 of Framework Decision 2008/977/JHA are accurate, up to date, complete, reliable and entered lawfully.~~
2. Each Member State shall be liable in accordance with its national law for any damage caused to a person through the use of the Customs Information System. This shall also apply to damage caused by a Member State entering inaccurate data or entering or storing data unlawfully.
3. If a recipient Member State pays compensation for damage caused by the use of inaccurate data entered into the Customs Information System by another Member State, the latter Member States shall refund to the recipient Member State the amount paid in damages, taking into account any fault that may lie with the recipient Member State.
4. Europol and Eurojust shall be liable in accordance with the acts which established them.

Article 31

1. Costs relating to the acquisition, study, development and maintenance of central computer infrastructure (hardware), software and dedicated network connections, and to related production, support and training services, which cannot be kept separate from the operation of the Customs Information System for the purpose of applying the customs and agricultural rules of the Community, and costs relating to the use of the Customs Information System by the Member States in their territories, including communication costs, shall be borne by the general budget of the European Communities.
2. Costs relating to the maintenance of the national work stations/terminals incurred in the implementation of this Decision shall be borne by the Member States.

CHAPTER XIII

IMPLEMENTATION AND FINAL PROVISIONS

Article 32

The information provided for under this Decision shall be exchanged directly between the authorities of the Member States.

Article 33

The Member States shall ensure that their national law conforms to this Decision by 27 May 2011.

Article 34

1. This Decision replaces the CIS Convention, as well as the Protocol of 12 March 1999 drawn up on the basis of Article K.3 of the Treaty on European Union, on the scope of the laundering of proceeds in the Convention on the use of information technology for customs purposes and the inclusion of the registration number of the means of transport in the Convention¹ and the Protocol of 8 May 2003 established in accordance with Article 34 of the Treaty on European Union, amending, as regards the creation of a customs files identification database, the Convention on the use of information technology for customs purposes² with effect from 27 May 2011.
2. Consequently, the CIS Convention and the Protocols referred to in paragraph 1 shall be repealed with effect from the date of application of this Decision.

Article 35

Unless otherwise provided in this Decision, measures implementing the CIS Convention and Protocols referred to in Article 34(1) shall be repealed with effect from 27 May 2011.

Article 36

1. This Decision shall enter into force on the twentieth day following its publication in the *Official Journal of the European Union*.
2. It shall apply from 27 May 2011.

Done at,

For the Council

The President

¹ OJ C 91, 31.3.1999, p. 2.

² OJ C 139, 13.6.2003, p. 2.



Council of the European Union
General Secretariat

**Interinstitutional files:
2023/0143 (COD)**

Brussels, 04 October 2023

WK 10974/2023 REV 1

LIMITE

ENFOCUSTOM

ENFOPOL

DATAPROTECT

JAI

CODEC

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	Presidency
To:	Delegations
N° Cion doc.:	ST 9375 2023 REV 1
Subject:	Proposal for a Regulation of the European Parliament and of the Council amending Council Decision 2009/917/JHA, as regards its alignment with Union rules on the protection of personal data

In the Annex, delegations will find a revised informal working document consolidating the proposed Regulation amending the Council Decision 2009/917/JHA as regards its alignment with Union rules on the protection of personal data with the text of the *Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes* as currently in force and including Presidency compromise text.