



CIS Supervision Coordination Group

ACTIVITY REPORT 2018-2019

Secretariat of the Supervision Coordination Group of the Customs Information System
European Data Protection Supervisor
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, 1000 Brussels
Email: EDPS-CIS@edps.europa.eu

Contents

1. Introduction	3
2. General Framework	3
2.1. Legal Framework	3
2.2. Relationship with Customs JSA	5
3. Organisation of coordinated supervision	5
3.1. Main principles	5
3.2. Overview of meetings in 2018-2019	6
4. Activities of the CIS SCG during the year 2018	7
5. Activities of the CIS SCG during the year 2019	7
6. What to expect in 2020-2021	7

1. Introduction

The aim of the Customs Information System (CIS) is to create an alert system within the fight against fraud framework so as to enable any Member State entering data in the system to request another Member State to carry out sighting and reporting, discreet surveillance, a specific check or operational and strategic analysis.

For these purposes, the CIS stores information on commodities, means of transport, persons and companies and on goods and cash detained, seized or confiscated in order to assist in preventing, investigating and prosecuting actions which are in breach of customs and agricultural legislation (the former EU 'first pillar') or serious contraventions of national laws (the former EU 'third pillar'). The former 'first pillar' part is supervised by the CIS Supervision Coordination Group (SCG), while the latter 'third pillar' part is supervised by a Joint Supervisory Authority (JSA) composed of representatives of the national data protection authorities (DPAs).

The CIS SCG is set up as a platform in which the DPAs responsible for the supervision of the CIS in accordance with Regulation (EC) No 766/2008 - i.e. the EDPS and national DPAs - cooperate in line with their responsibilities in order to ensure coordinated supervision of the CIS.

The Coordination Group shall:

- examine implementation problems in connection with the CIS operations;
- examine difficulties experienced during checks by the supervisory authorities;
- examine difficulties of interpretation or application of the CIS Regulation;
- draw up recommendations for common solutions to existing problems;
- endeavour to enhance cooperation between the supervisory authorities.

This document reports on the activities of the CIS SCG during the years 2018 and 2019.

2. General Framework

2.1. Legal Framework

The CIS¹ was created to store information on commodities, means of transport, persons and companies, and in addition on goods and cash detained, seized or confiscated in order to assist in preventing, investigating and prosecuting actions which are in breach of customs and agricultural legislation or serious contraventions of national laws. The Customs Files Identification Database (FIDE) is a related database storing information on legal and natural persons under investigation for breaches of customs legislation established under the same legal bases.

¹ The CIS is based on Regulation No 515/1997, OJ L 82, 22.3.1997, p. 1, as amended by Regulation No 766/2008, OJ L 218, 13.8.2008, p. 48 as well as on Council Decision No 2009/917/JHA, OJ L 323, 10.12.2009, p. 20.

One special characteristic of CIS and FIDE is that they are based on a double legal basis. In addition to Council Regulation (EC) No 515/1997 governing CIS as it relates to customs and agricultural legislation ("CIS former 1st pillar"), Council Decision No 2009/917/JHA ("CIS former 3rd pillar") provides a separate legal basis in the former third pillar for the use of CIS in relation to serious contraventions of national laws, replacing the CIS Convention.

The aim of the CIS is to create an alert system in the framework of the fight against customs fraud and breaches of certain other laws by enabling the Member State which enters data into the system to request another Member State to carry out one of the following actions:

- sighting and reporting,
- discreet surveillance,
- a specific check,
- operational and strategic analysis.

The CIS can contain a range of data on suspects, such as names, addresses, numbers of identity documents, description of physical characteristics, warnings (armed, violent, escaping) and the reasons for inclusion in the database.

Since 2008, Regulation 515/1997 also includes a legal framework for the FIDE, which enables the national authorities responsible for carrying out customs investigations on persons or businesses to identify competent authorities of other Member States which are investigating or have investigated the same persons or businesses in order to coordinate their investigations. This database stores only basic information on investigations (such as reference, start date and the status of the investigation), investigating authorities (names and contacts) and persons or companies under investigation.

The functionalities of CIS and FIDE under the two legal bases are identical; the difference is to which kind of (suspected) breaches entries relate: CIS former 1st pillar contains entries on (suspected) breaches of Union customs and agricultural legislation², while CIS former 3rd pillar contains entries on (suspected) certain other serious breaches of national laws.³

As regards supervision, Article 37 of Regulation 515/1997, as amended by Regulation 766/2008, sets out the legal framework for CIS former 1st pillar. National DPAs are responsible for supervising that the processing of personal data in CIS by national authorities does not violate data subjects' rights in accordance with the respective national legislation. The European Data Protection Supervisor (EDPS) in turn shall supervise compliance of the Commission's processing operations with Regulation (EU) 2018/1725. Article 37(4) establishes that the EDPS shall –at least once a year– convene a meeting with the national DPAs competent for the supervision of the CIS. This provision is the basis for the work of the CIS SCG.

² See Article 2 of Regulation No 515/1997.

³ See the list in Article 2(1) of Council Decision 2009/917/JHA. Examples include drug trafficking and arms sales.

As the provisions on FIDE do not contain specific rules on supervision and data protection, the general rules for CIS apply, in accordance with Article 41a (1).

The supervision regime for CIS former 3rd pillar is different. Under this legal basis, Article 26(1) of the Council Decision states that the EDPS shall supervise the activities of the Commission regarding the CIS. Article 25 sets up a Joint Supervisory Authority ("Customs JSA"), consisting of two representatives of each national DPA, with a secretariat provided by Council staff.

This means that there are two forums for the coordinated supervision of the CIS and FIDE, the CIS SCG and the Customs JSA. The relationship and working arrangements between the two will be described in the next section.

2.2. Relationship with Customs JSA

As outlined above, the CIS is based on a double legal basis. While the EDPS, national DPAs and the CIS SCG are competent for the system under Council Regulation (EC) 515/1997, under Council Decision 2009/917/JHA, the EDPS is competent for supervising the Commission's activities regarding CIS, but he is not a member of the Customs JSA, which supervises the system.

Article 26 (2) establishes that the JSA and the EDPS shall cooperate, each acting within their own competences. To this end, both groups shall meet at least once a year (Article 26(3)). Because the members of both groups are largely identical – with the exception of the EDPS and the respective secretariats–, the meetings of the CIS SCG – to which the secretariat of the Customs JSA is always invited – are at the same time considered to also be the meeting of the EDPS with the Customs JSA. The other way around, the EDPS is invited to parts of the Customs JSA meetings as observer.

Close cooperation between the Customs JSA and the CIS SCG is essential. While CIS former 1st pillar and CIS former 3rd pillar are legally and technically separated, their functionalities are identical, meaning that any issues needing supervisory attention are likely to occur in both databases. Additionally, from the users' perspective, there is no visible difference between CIS former 1st pillar and CIS former 3rd pillar.

3. Organisation of coordinated supervision

3.1. Main principles

According to the legal basis, meetings must take place at least once a year. It is standing practice to organise two meetings per year.

In the meetings, the DPAs of all EU Member States are represented, as well as the EDPS, who also provides the secretariat for the Group, and the Data Protection Secretariat of the Council, which provides the secretariat for the Customs JSA. As the members of the Group and the Customs JSA are largely identical, these meeting also serve as meetings between the EDPS and the Customs JSA, as foreseen in Article 26 (3) of Council Decision 2009/917/JHA.

Documents to be discussed are usually prepared by a rapporteur from the Group or the secretariat; where appropriate, the secretariat of the Customs JSA can also be involved. Setting priorities for the work of the Group is the prerogative of the Members.

Due to the changes in the working of the JSA Secretariat, the CIS SCG has not held any meeting with the JSA during the reporting period.

3.2. Overview of meetings in 2018-2019

This is the fifth activity report of the CIS SCG and covers its activities during the years 2018 and 2019.

In 2018, the CIS SCG held two meetings in Brussels, the first one in May (29.05.2018) and the second one in October (02.10.2018).

In the May meeting, following the entry into application of the General Data Protection Regulation (EU) 2016/679 and the expiry of the deadline to transpose the Data Protection Police Directive (EU) 2016/680, the Group identified the need to update the Guide of access adopted by the CIS SCG in December 2015. Persons, whose personal data are collected, held or otherwise processed in the CIS, are entitled to rights of access subject to strict limitations, correction of inaccurate data and deletion of unlawfully stored data. This Guide aims to help data subjects identify the competent authority and the modalities to exercise these rights in relation to the CIS. Furthermore, the Group adopted the Activity Report of the CIS SCG that covers the activities carried out by the group during the period from 2016 to 2017. The Group continued to work on the common format for national inspections, as developed in SCGs for other large-scale IT systems. The group also started to work on a common questionnaire for inspection in relation to the AFIS security policy. Finally, the Group re-elected the representative of the Polish DPA, Mr Piotr Drobek, as chair of the CIS SCG for a term of office of two years.

In the October meeting, the Group continued to work on the update of the CIS Guide of access following the entry into application of the General Data Protection Regulation (EU) 2016/679 and the expiry of the deadline to transpose the Data Protection Police Directive (EU) 2016/680. Persons, whose personal data are collected, held or otherwise processed in the CIS, are entitled to rights of access subject to strict limitations, correction of inaccurate data and deletion of unlawfully stored data. This Guide aims to help data subjects identify the competent authority and the modalities to exercise these rights in relation to the CIS. Furthermore, the Group continued its work and finalised the common format for national inspections and the common questionnaire for inspection in relation to the AFIS security policy. The Group also discussed the update of the CIS SCG webpage. Finally, the Group elected the representative of the EDPS, Mr Owe Langfeldt, as vice-chair of the CIS SCG for a term of office of two years.

In 2019, the CIS supervision coordination Group held one meeting in Brussels: in May (07.05.2019).

In the meeting, the Group started to discuss the content of the next work programme for the following years, and to identify activities and follow up activities to plan over that period. The Group also finalised the update of the CIS SCG webpage. Furthermore, the Group continued to work on the update of the CIS Guide of access following the entry into application of the General Data Protection Regulation (EU)

2016/679 and the expiry of the deadline to transpose the Data Protection Police Directive (EU) 2016/680. Persons whose personal data are collected, held or otherwise processed in the CIS are entitled to rights of access subject to strict limitations, correction of inaccurate data and deletion of unlawfully stored data. This Guide aims to help data subjects identify the competent authority and the modalities to exercise these rights in relation to the CIS.

4. Activities of the CIS SCG during the year 2018

The Group identified the need to update the Guide of access adopted by the CIS SCG in December 2015 and continued such work throughout the year. Furthermore, the Group adopted the Activity Report of the CIS SCG that covers the activities carried out by the group during the period from 2016 to 2017. The Group continued to work on the common format for national inspections, as developed in SCGs for other large-scale IT systems. The group also started to work on a common questionnaire for inspection in relation to the AFIS security policy and continue such work throughout the year.

5. Activities of the CIS SCG during the year 2019

In 2019, the Group started to discuss the content of the next work programme for the following years, and to identify activities and follow up activities to plan over that period. The Group also finalised the update of the CIS SCG webpage. Furthermore, the Group continued to work on the update of the CIS Guide of access following the entry into application of the General Data Protection Regulation (EU) 2016/679 and the expiry of the deadline to transpose the Data Protection Police Directive (EU) 2016/680.

6. What to expect in 2020-2021

In 2020-2021, the Group will:

- follow up and finalise the adopted Guide of Access to CIS;
- continue to develop working methods and will assess the supervision model appropriate to the Registered Exporters System (“REX”) database;
- start working on a questionnaire and report on the training on data protection for staff of authorities accessing the CIS;
- remain in touch with OLAF and DG TAXUD on relevant common points of interest;
- follow the developments of the review of the CIS Regulation 515/97.

In addition, a new election for the position of Chair and Vice-Chair will be held.