Customs Joint Supervisory Authority

Guide to your responsibilities under Article 13 of the CIS Council Decision 2009/917/JHA and Article 8(2) of the Data Protection Framework Decision 2008/977/JHA

What does the law say?

Article 13 of the CIS Council Decision 2009/917/JHA

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.

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 those referred to in Article 23(1), concerning rectification or erasure, the Member State which entered the data in question shall erase them from the System.

Article 8(2) of the Data Protection Framework Decision 2008/977/JHA

If it emerges that incorrect data have been transmitted or data have been unlawfully transmitted, the recipient must be notified without delay. The data must be rectified, erased, or blocked without delay in accordance with the national law implementing Article 4.

What does this mean?

Essentially, both articles say that CIS data controllers must amend, rectify, add to or delete any inaccurate or unlawfully processed information which are processed in the CIS and used at national level.

Example:

Member State A inputs data into the CIS: Mr X is suspected to be involved in unlawful activities. An essential element justifying that suspicion is that Mr. X was in Member State B at a specific moment and in a specific place.

Member State B, investigating Mr. X notices the data in CIS and uses them for their own investigation. Europol and Eurojust are involved in these investigations and the case against Mr X is brought before a court in Member State B.

Member State A then detects that Mr X has never been in Member State B, and that the suspicion against Mr. X was not justified and that the information inputted into the CIS was thus not correct.

What should I do if I become aware of inaccurate or unlawfully processed data?

1. If your authority transmitted the data

If you become aware that data transmitted by your authority are not correct then you should correct or delete those data.

If you are told by another authority that data you sent are incorrect you must check the data and correct or delete as appropriate.

You must then tell the other authorities who received those data about the inaccurate data and their correction or deletion.

2. If you receive data from another authority

If you discover that information you received might not be correct, you must inform the authority that provided the data.

As a recipient of data, you have a responsibility to correct, amend, block or delete data when you are informed about the correction or deletion of the data by the authority that provided the data.

Upon taking such action, you should also inform any other authorities to whom you provided those data that the information has been corrected or deleted.

What if there is a dispute over whether the data are correct or not?

If two or more authorities dispute the accuracy of data in the CIS you should try to resolve the issue. If you cannot agree, then the first report stands. You should still enter into the CIS any data within the report that is not in dispute. Then, when a national court has made its decision about any amendment, supplementation, rectification or erasure of the alleged inaccurate data in the CIS, both authorities should follow and enforce this decision.

If there are conflicting decisions made by courts in different Member States then the authority that originally entered the data should erase them from the system.

What happens if you used inaccurate data transmitted via the CIS?

If you use information obtained from the CIS for an investigation at national level and are subsequently informed by the authority that made the information available that the information is incorrect or unlawfully stored on CIS you should do one or more of the following:

- amend, correct, delete or block the data
- archive the data separately provided that it's within the law
- block the data only if you believe that by deleting the data it would prejudice the individual's rights
- if the data were used in criminal proceedings before a court, the data should be deleted, corrected, erased or blocked in accordance with your national law.

What safeguards could or should be in place to ensure that data sent but subsequently found to be inaccurate, unlawful or not in compliance with either of the Decisions has been sent either a receiving authority or onwardly transferred to another law enforcement agency on the receiving authority's jurisdiction?

Once personal data is noted as being unlawfully stored in the CIS or is inaccurate, or is not in compliance with the safeguards laid down by the sending customs authority, then the guiding principle should be to comply with that safeguard. For example if the sending authority states that the data can only be processed for 2 years, after which, it must be deleted, then the receiving authority should delete the data.

However problems do arise when an administrative procedure is being followed. There could be a conflict of law as administrative procedure itself or another law enforcement agency using the data in the administrative procedure are governed by national law. In these circumstances, the receiving authority must try as far as possible to comply with the above guiding principle – and comply with the safeguards of the sending authority. If it is unable to do that, because of national law, the receiving state must at least take the safeguards into account and assess the impact that the data it now has is unlawful under the Decisions or is inaccurate. Therefore, in these circumstances there needs to be careful consideration of the interaction between national law and the Decisions to ensure that the rights of the individual regarding their personal data are balanced with the requirement apprehend those breaking the law.