

Data Privacy statement for Import Control System 2 (ICS2) for the monitoring and evaluating of the implementation of ICS2 processes to ensure harmonised and uniform implementation of common risk criteria and standards, risk analysis and control measures and priority control areas

1. Introduction

The European Commission (hereafter ‘the Commission’) is committed to protect your personal data and to respect your privacy. The Commission collects and further processes personal data, pursuant to 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 (repealing Regulation (EC) No 45/2001), hereafter referred as EIDPR as well as Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) (hereafter “EU legislation”

This privacy statement explains the reason for the processing of your personal data, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer.

The processing of personal data in ICS2 for most processing operations occurs by the Customs Authorities of Member States, acting as controllers and the Commission acting as “processor”. Member States are the controllers in ICS2. These processing operations are covered by the separate privacy statement of the Member States acting as controllers.

However, the Commission is “joint controller” together with the Member States for specific personal data processing operations, which are in the scope of this privacy statement. This processing covers the monitoring and evaluation of how Member States implement the ICS2 processes in the context of the need for harmonised and uniform implementation of common risk criteria and standards, control measures and priority control areas. This monitoring and evaluation is based on using the data in the ICS2 central components – ICS2 shared trader interface and ICS2 common repository.

In the Commission, the ENS data is processed by Directorate General for Taxation and Customs, Directorate A – Customs, Unit A3: Risk Management and Security, which has determined the purpose(s) of processing on the basis of the legal basis and empowerments provided in the Union customs legislation.

We are required to notify you the data contained in this privacy statement. It is important that you read this privacy statement so that you are aware on how and why we are using your data.

This privacy statement:

- explains the reasons for processing your personal data,
- describes how we collect, use and protect your personal data in accordance with EU legislation, what data we process, how it is used; for how long it is maintained/stored, who has access to it,
- informs about your rights as the data owner; and how you can exercise these rights.

2. Why and how we process your personal data?

The Commission process the data in ICS2 in order to fulfil its legally assigned role and obligation of ensuring harmonised and uniform implementation of customs risk analysis and controls by customs authorities of the Member States, in accordance with the Union Customs Code (Council Regulation (EU) 952/2013, in particular Article 46 (3) and 50). The processing is lawful and necessary for compliance with a legal obligation to which the Commission is subject.

The Commission processes data in ICS2, in its role as a controller jointly with the Member States, through the ICS2 central component - common repository.

2.1. We process your personal data for the following purposes, pursuant to the obligations set by the Union customs legislation:

- Authentication and authorisation to access the ICS2, via UUM&DS Uniform User Management & Digital Signature (data of economic operators and natural persons logging into the ICS2. Data of authorised staff from the Commission - referred as authorised users hereafter);
- Authentication and authorisation to access the ICS2, via CCN2 (data on authorised staff from the Member States, Switzerland, Norway and the United Kingdom, referred as authorised users hereafter) (DPR-EC-01106.1);
- Processing of the entry summary declaration data (ENS) and related data collected and exchanged by the customs authorities of the Member States through the ICS2 common repository, for monitoring and evaluating of the implementation of ICS2 processes to ensure harmonised and uniform implementation of common risk criteria and standards, risk analysis and control measures and priority control areas.

2.2. How do we obtain your personal data?

We collect your personal data indirectly:

- from the customs authority of a Member State, Switzerland, Norway, and the United Kingdom (in the context of Northern Ireland), when you – as a declarant or its representative - submit and lodge your ENS declaration data (and other related data necessary for ICS2 processes) to those customs authorities (i.e. your EORI

number). Those authorities are making this data available to us through the ICS2 common repository;

- from the customs authority of a Member State, Switzerland, Norway, and the United Kingdom (in the context of Northern Ireland), when a declarant of ENS or its representative, submits the ENS or other related data necessary for ICS2 processes, and your personal data is contained in the ENS and related data. Those authorities are making this data available to us through the ICS2 common repository;
- from another IT customs system who have already your consent (e.g. in case of EORI).

3. On what legal ground(s) do we process your personal data?

The legal basis for processing your personal data in the ICS2 system is the following:

Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code (UCC) and its implementing acts, Articles 16(1), 46(3) and 50 of UCC. Article 182 of Implementing Regulation (EU) 2015/2447 as amended by the Regulation (EU) 2020/893, Articles 42, 43 (2), Articles 44 to 49, and Article 85(6) of the Commission Implementing Regulation (EU) 2021/414. Commission Implementing decision (EU) 2019/2151 and its relevant Annex.

4. Which personal data do we collect and further process?

Personal data in this context means any information relating to you, as an identified or identifiable natural person.

The Commission processes declared ENS declaration data and results of their processing (such as risk analysis and control results), insofar as they are related to the natural person.

This includes:

- First and last name
- Address
- Name of the trader, company or undertaking
- E-mail address
- Phone number
- Economic Operator's Registration and Identification number (EORI)
- Trader Identification Number (TIN).

5. How long do we keep your personal data?

We aim to retain your personal data for a maximum of seven (7) years and in line with Article 51 of the Union Customs Code which provides that the data shall be kept for, at least, three years for the purposes of customs controls. After the expiry of the data retention period, your data will be deleted.

6. How do we protect and safeguard your personal data?

We guarantee all the appropriate organisational and technical security measures are in place, aimed at protecting your personal data against accidental and unlawful destruction or loss, as well as against non-authorized access, alteration or transmission.

We implemented, amongst other, , the following security measures:

- Authentication and authorisation to access the ICS2 common repository is ensured, via CCN2 (DPR-EC-01106.1). This network is protected by firewalls and provides limited access to encrypted user data within the legally defined boundaries;
- Established Information Security Management System (ISMS);
- All data in electronic format (ENS declarations and related data exchanged in format of electronic messages, e-mails, documents, uploaded batches of data etc.), are stored on the servers of the European Commission and its contractors; the operations of which abide by the European Commission's security decision of 10 January 2017 (EU, Euratom) 2017/46 concerning the security of data systems in the European Commission.

The Commission's contractors are bound by a specific contractual clause for any processing operations of your data, on behalf of us or the Commission, and by the confidentiality obligations deriving from the transposition of 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.

7. Who has access to your personal data and to whom is it disclosed?

6.1. Internally

Access to your data is provided to authorised users - within the Commission - on a 'need to know principle', who are assigned to process the data covered in Section 2.1 of this privacy statement.

Such authorised users abide by statutory, and when required, additional confidentiality agreements.

The information is disclosed to the authorised National Administrations, while the security management is enforced by a TEMPO (TAXUD Electronic Management of Projects On-line) quality management system.

6.2. Externally

Externally refers to all other entities than the internal organisation.

The contractors have a nominated security officer whose role is to ensure adequate security implementation. Compliance with data protection regulation is required by its individual contract.

Authorised users from customs administrations of Switzerland, Norway and the United Kingdom have right to access to ICS2 in line with the bilateral agreements^{1 2 3}.

8. What are your rights and how can you exercise them?

You are at any given moment and under certain conditions in compliance with EU customs legislation, entitled to address to the customs authority of a Member State, Switzerland, Norway or the United Kingdom entitled to the access and rectification of your personal data in case the data is inaccurate or incomplete. You have the rights to request restriction of processing or erasure ('right to be forgotten'), to data portability, to object to the processing, to withdraw your consent, and not to be subject to automated individual decision-making, including profiling.

When a Member State is processing data related to Economic Operator and natural person:

This is not under the responsibility of the Commission. This will have to be covered by a Joint Controller Agreement.

The ICS2 system will not make automated decisions as such.

Automated processing of the ICS2 data for monitoring and evaluating of the implementation of ICS2 processes to ensure harmonised and uniform implementation of common risk criteria

¹ For Switzerland: Decision No 1/2021 of the EU-Switzerland Joint Committee, of 12 March 2021, amending Chapter III of, and Annexes I and II to, the Agreement between the European Community and the Swiss Confederation on the simplification of inspections and formalities in respect of the carriage of goods and on customs security measures .

² For Norway: Decision of the EEA Joint Committee No 130/2021 of 15. March 2021, amending Protocol 10 to the EEA Agreement, on simplification of inspections and formalities in respect of carriage of goods (amended parts – Chapter IIa of, and Annexes I and II to, the Agreement) .

³ For the United Kingdom: United Kingdom with respect to Northern Ireland and Protocol on Ireland and Northern Ireland and [Draft decision on the adequate protection of personal data by the United Kingdom - General Data Protection Regulation decision]

and standards, risk analysis and control measures and priority control areas may result in some data being identified for a human review.

The automated identification of the declaration for review by the authorised staff of the Commission has no legal effect on a person. The subsequent human review is done for the evaluation purposes only and does not involve any decision making by the Commission which affects natural persons.

If, at any time in the future, we want to use automated decision-making that has legal consequences for you or affects you to a significant degree, we will make this clear to you beforehand by updating this privacy statement. We will inform you of your rights, such as your right to be given an explanation of the decision reached by automated means, your right to express your point of view, your right to challenge the decision and your right to human intervention.

You also have the right to object to the processing of your personal data on legitimate compelling grounds, to the customs authority of a Member State, Switzerland, Norway or the United Kingdom, except when: it is collected in order to comply with a legal obligation or is necessary for the performance of a contract to which you are a party, or is to be used for a purpose for which you have given unambiguous consent.

9. Exercising your rights

You can verify the accuracy of the information pertaining to you and processed in the ICS2 system, by addressing your request to customs authority of a Member State, Switzerland, Norway or the United Kingdom.

10. What will be done in case of data breaches

In case of a data breach, we will fulfil our obligation in compliance with our duties stipulated in Regulation (EU) 2018/1725.

Where that personal data breach is likely to result in a high risk to your rights and freedoms we are committed to inform you immediately in order to allow for you to take the necessary precautions and measures.

Where personal data breach is likely to result in a high risk to your rights and freedoms we are responsible to inform the customs authority of a Member State, Switzerland, Norway or the United Kingdom immediately, in order to allow them to take the necessary precautions and measures.

11. Contact information

If you have comments or questions, any concerns regarding the collection and use of your personal data, please feel free to contact the Data Controllers using the following contact information:

The Data Controllers:

- Customs administration of the Member States, Switzerland, Norway and the United Kingdom for processing data related to Economic Operator and natural person:

Under the responsibility of your Member State, Switzerland, Norway and the United Kingdom.

- Commission for processing of ICS2 authorised user's data:

- DG TAXUD-A3 (for data concerning authorised users of ICS2)
- 0032 2 29 69751
- TAXUD-UNIT-A3@ec.europa.eu

You may contact the Data Protection Officer (DPO) of the customs administration of your Member State, Switzerland, Norway and the United Kingdom with regard to issues related to the processing of your personal data under Regulation (EU) 2016/679 (GDPR).

If you consider that your rights under Regulation (EU) 2016/679 (GDPR) have been infringed you can lodge a complaint to the competent national data protection supervisory authority of your Member State.

You may contact the Data Protection Officer (DPO) of the Commission (DATA-PROTECTION-OFFICER@ec.europa.eu) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725 for monitoring and evaluating of the implementation of ICS2 processes to ensure harmonised and uniform implementation of common risk criteria and standards, risk analysis and control measures and priority control areas.

If you consider that your rights under Regulation (EU) 2018/1725 (EUIDR) have been infringed (i.e. when processing your personal data for monitoring and evaluating of the implementation of ICS2 processes to ensure harmonised and uniform implementation of common risk criteria and standards, risk analysis and control measures and priority control areas) you can lodge a complaint to the European Data Protection Supervisor (edps@edps.europa.eu).