

CENTRAL ELECTRONIC SYSTEM OF PAYMENT INFORMATION (CESOP)

- PRIVACY STATEMENT -

The processing of personal data occurs by the competent authorities of Member States referred to in Article 3 of Council Regulation (EU) No 904/2010 on administrative cooperation and combating fraud in the field of value added tax. They are listed in the Official Journal of the European Union ([2017/C 155/03](#)) and are jointly acting as controllers. Hereafter, the competent authorities of Member States are referred to as "we" or "us" or "ours". The Commission acts on behalf of the competent authorities of Member States as processor.

Where we refer throughout the document to "you" or "yours" as the data subject, this reference also includes data subjects who are taxable persons.

1. Introduction

We, the competent authorities of Member States, are committed to protecting and respecting your privacy.

As CESOP processes personal data, 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 (General Data Protection Regulation – GDPR) is applicable.

This privacy statement explains the reasons for processing your personal data, the way they are collected and handled, and how the protection of your personal data is ensured. In addition, this privacy statement covers:

- which of your personal data are processed;
- how your personal data are used;
- for how long your personal data are retained/stored;
- who has access to your personal data;
- what are your rights as the data subject, and
- how you can exercise these rights.

We, the competent authorities of Member States, act as joint controllers, the European Commission as a data processor only.

2. Why do we process your personal data?

Payment service providers (PSPs) offering payment services in the EU have to monitor the beneficiaries (payees) of cross-border payments. From 1 January 2024, they must transmit information on those who receive more than 25 cross-border payments per quarter to the administrations of EU Member States.

This information is stored in the Central Electronic System of Payment information (CESOP) database, where it will be aggregated and cross-checked with other European databases. All information in CESOP is made available to Member States' anti-fraud experts via [Eurofisc](#), the EU's network of anti-fraud experts from the 27 Member States and Norway.

These new measures give Member States' tax authorities the right instruments to detect possible VAT risks and VAT fraud carried out by sellers established in another Member State or non-EU country.

We are permitted to process your personal data based on:

- Council Directive 2006/112/EC
- Council Regulation (EU) 904/2010
- Commission Implementing Regulation (EU) 2022/1504
- Commission Implementing Regulation (EU) No 79/2012
- Council Regulation (EU) 2020/283
- National VAT legislation

The legal basis for information to be provided by the PSPs is laid down in Council Directive 2006/112/EC.

The legal basis for the exchange of data and VAT information is Council Regulation (EU) 904/2010 on administrative cooperation and combating fraud in the field of value added tax of 7 October 2010 and Commission Implementing Regulation (EU) No 79/2012 of 31 January 2012.

As part of the range of data to be submitted to CESOP, we process your personal data to detect VAT loss/VAT circumvention, in particular potential cross-border e-commerce VAT risks and VAT fraud, and to take necessary measures to fight any kind of illegal action in this regard.

All information in CESOP is made available to Member States' anti-fraud experts via Eurofisc in full compliance with the principles set out in Regulation (EU) 2016/679 (GDPR). This also includes automated decision-making, where applicable.

Data sent to the Member States may be stored and processed by the respective Member States outside the Central Electronic System of Payment Information according to respective national legislation and based on the national privacy statements.

3. Which personal data do we collect and process?

Personal data means any information relating to you, as an identified or identifiable **natural person** (payees do not need to be confirmed in this regard).

The following (categories of) personal data are being processed:

1. Payee name
2. Payee VAT number/TIN/other identification number
3. Payee Address¹

To execute our activities, we request and obtain your personal data from PSPs, including variations of such personally identifiable data stored for data subjects. Such variations need to be provided in the event of a data access request.

a. Lawfulness of the processing operation

The processing is lawful and necessary for compliance with a legal obligation to which we, the competent authorities of Member States, are subject or where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body. The legal basis for providing confirmation of the validity of a VAT identification number as well as the associated name and address is Chapter V of Council Regulation (EU) 904/2010.

4. How long do we keep your data?

For the purpose of CESOP and according to Article 1(2)(c) of Council Regulation (EU) 2020/283 as well as Article 24c of Council Regulation (EU) 904/2010, the Commission, on behalf of the Member States, stores your data for a retention period of 5 years from the end of the year in which the information was transmitted to it.

¹ Payee address incl. all variations of such personally identifiable data stored for data subjects.

5. How do we protect your data?

The Commission guarantees that 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-authorised access, alteration or transmission.

We have implemented the following security measures:

- secure communication channels to protect data in transit;
- encryption of data by the Commission to protect data collected at CESOP central system level;
- defined procedures for user access management;
- user access control mechanisms to prevent unauthorised access to CESOP central data;
- central monitoring and audit of data quality aspects by the CESOP Operational Team;
- automated mechanisms to ensure data storage in the system is compliant with data retention policies.

The above list is not exhaustive.

The usage of the central CESOP service is closely monitored and analysed by the European Commission, i.e. its contractors, on a daily basis to block abusive use of CESOP. In circumstances where certain actions would be recognised as abusive use of the service, the originator of the request (specific IP addresses) will be blocked, and appropriate action will be taken.

The systems of the European Commission or its contractors carrying out processing operations on behalf of the European Commission abide by the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 concerning the security of communication and information 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.

For the development and maintenance of the IT system, the Commission contracts external service providers (contractors). These contractors have a designated security officer whose role is to ensure adequate security implementation. Compliance with the data protection regulation is required by individual contracts.

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

According to Article 24d of Council Regulation (EU) No 904/2010, access to CESOP is only granted to Eurofisc Liaison Officials who hold a personal user identification for CESOP and where that access is in connection with an investigation into suspected VAT risks or is intended to detect VAT fraud.

The Commission has the necessary safeguards and agreements in place with its partners to ensure that the adequate level of protection of your personal data is not undermined.

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

a. Right of access by the data subject

You are, at any given moment, entitled to the access and rectification of your personal data received from PSPs according to Article 15 et seq. of Regulation (EU) 2016/679, and/or in case the data is inaccurate or incomplete. According to national legislation and as explained in section 7.3, you may have the rights of access, to be informed and to rectification. However, the scope of your rights might be restricted, in accordance with Article 55 of Council Regulation (EU) No 904/2010, to what is strictly necessary in order to safeguard the interests referred to under point (e) of Article 23(1) of Regulation (EU) 2016/679.

b. Exercising your rights

You can exercise your rights by contacting any or all Member States as Data Controllers. The list of [national CESOP portals](#) serves to facilitate addressing the relevant point of contact based on the country code of your IBAN account.

If you feel that your rights are violated in any way, you are entitled to file a complaint with the [National Authority responsible in the jurisdiction in which your rights might have been infringed](#) and also with the competent national authority that has issued the VAT identification number, following the applicable national procedure.

c. Restrictions to your rights

You also have the right to object to the processing of your personal data on legitimate compelling grounds except when

- personal data are collected in order to comply with a legal obligation, or
- processing is necessary for the performance of a contract to which you are a party, or
- personal data are to be used for a purpose for which you gave unambiguous consent.

d. What will be done in case of data breaches

In case of a data breach we will handle the incident in compliance with the GDPR and our national laws.

Where that personal data breach is likely to result in a high risk to your rights and freedoms, we will inform you promptly in order to allow you to take the necessary precautions.

8. Contact information

If you have comments or questions, any concerns or a complaint regarding the collection and use of your personal data, please feel free to contact the respective competent national authority.

A summary of the contact details:

Type of contact	Reference
National Tax Administrations	https://ec.europa.eu/taxation_customs/taxation-1/national-tax-administrations_en
National contact points	https://taxation-customs.ec.europa.eu/national-tax-websites_en
CESOP - List of National Portals	https://taxation-customs.ec.europa.eu/document/download/a6ba92c0-f6ba-4494-9b7f-3d54725f3d4a_en?filename=CESOP_National_Portal_2024-02-16.pdf
National Authority responsible for data protection (GDPR)	https://edpb.europa.eu/about-edpb/about-edpb/members_en