Introduction

The European Commission is committed to protecting and respecting your privacy.

As the download portal in the Europa website processes personal data, 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 Text with EEA relevance, is applicable.

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

- The personal data processed;
- How personal data are used;
- For how long personal data are preserved/stored;
- Who has access to the personal data;
- What are your rights as the data owner; and
- How you can exercise them.

The processing of personal data occurs by *DG TAXUD*, acting as the *Controller*, hereafter referred to as "we".

1. What do we do?

The download portal is a section in the Europa website where the user can download eLearning material (available in more than 22 languages).

The users of the download portal are citizens, academia, companies or public administrations that want to download the training material for their private use.

2. Why do we process your personal data?rsonal data?

2.1 PURPOSE OF PERSONAL DATA PROCESSING IN LINE WITH THE LEGAL BASE

Your personal data are processed on the basis of the Regulation (EU) 2018/1725, Art. 5.1 point d):

"*The data subject has given consent to the processing of his or her personal data for one or more specific purposes* ".

2.2 PURPOSE OF PROCESSING EXPLAINED

The Commission acts as a controller and decides 'why' and 'how' the personal data included in the download form is used.

We process your personal data for the following purposes:

1. to draft yearly reports in the use of the training material for statistical purposes;
2. to ensure that the anonymous survey on the evaluation of the eLearning material downloaded is filled (also to reply to statistical purposes).

2.3 LAWFULNESS OF PROCESSING

The processing is lawful: the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

3. Which personal data we collect and process?

Personal data in this context means any information relating to an identified or identifiable natural person. The following (categories of) personal data are being processed:

1. Company name
2. E-mail address
3. Country

4. How do we obtain your personal data?

4.1 DIRECTLY

To execute our activity, your personal data are directly requested and obtained from the data subject (from "you"): the data subject is able to validly perform a ´clear affirmative act´ to consent to

the processing by actively ticking an optional box stating "By checking this box, you acknowledge that you have read and understood the privacy statement".

5. To whom does the personal data that we process belong?

The personal data belongs to the following (categories of) data subjects:

- Officials (of the competent authorities)
- Citizens

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

Recipients within the EU organisation: EC officials.

Recipients outside the EU organisation: DG TAXUD contractor in charge of preparing the data for statistical use.

6.1 INTERNALLY

Access to your data is provided to authorised employees according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

The databases are under DIGIT's management. Access to the data is done by a limited number of authorized users and on a need-to know basis (access needed in order to provide the services, for example to investigate and fix possible issues). All persons are either EC employees or working under an NDA agreement with EC.

6.2 EXTERNALLY

Transfer of personal data inside the EU:

We have the necessary safeguards and agreements in place with our partners to ensure that the adequate level of protection of your personal data is not undermined.

Only EC contractor can have access to the data and therefore can see email address, but cannot delete or modify.

7. How do we protect your data?

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

We implemented, amongst other, but not limited to, the following **security measures:**

Organisational:

- Risk Assessment and Risk management standardized processes are in place for all layers;
- Corporate IT Security Risk Management is defined and used on a consistent basis;
- Security incident management processes are in place, including management of the notifications according to data privacy regulations.

Personal data breach handling:

- On hosting side, it is included into the existing Security incident management process, involving CSIRC and DPC as well as IS owner and LISO of the DG;
- Actions needed are decided in collaboration with involved actors and based on the analysis of the incident.

Technical measures:

Physical:

- Access to the EC buildings is restricted, using an authentication and authorization system. Access on premises is centrally logged and security guards are monitoring the premises 24/7;
- Physical access to individual elements of EC is restricted, using additional authentication and authorization systems with segregation of authorized access per type of asset (network, processing, storage) with central logging of accesses and changes.

Cybersecurity:

- WAF for protecting the web applications;
- Firewall for segregating the network from internet access, with identification of the authorized connections;
- Intrusion Detection applications for identification of possible intrusion;
- Vulnerability and patch management at the level of all elements (firewall, WAF, physical devices, virtualization servers, Linux OS, application servers, application code dependencies);
- Solid authentication and authorization mechanism in place for the application itself (using EU Login and user roles with minimal access as defined by the owner of the web application);
- Logging, monitoring and regular analysis of the aggregated logs in order to identify unexpected behaviours and identify early possible security incidents.

All data in electronic format (e-mails, documents, uploaded batches of data etc.) are stored either on the servers of the European Commission or of 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 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 the Commission, and by the confidentiality obligations deriving from the transposition of Regulation (EU) 2018/1725.

Standard security measures implemented in the EC DC are in place for protecting the information.

A Security Plan was prepared by DIGIT DC and identified relevant security risks with implementation of following main security controls in order to address infrastructure related risks:

- DC network is segregated from internet; a firewall verifies that all connections are authorized in advance based on a specific DG HR.DS approval (active security convention);

- Web Application Firewall protect web applications, imposing various security controls (blacklist of suspect IPs or known malicious IPs, block of malicious activities such as SQL injection/XSS or similar, throttling of number of web requests for DOS/DDOS prevention);

- VMs used for hosting the application are maintained up to date with relevant security patches applied by DC colleagues on a regular basis and base on the assessed vulnerability risk/impact;

- Application servers are maintained up to date with relevant security patches on a regular basis;

- Compliance tools are used in order to detect deviations and identify possible vulnerabilities not fixed correctly.

Web application security measures are implemented by our Next Europa team:

- Web application code is maintained and regularly updated to recent version or patched with relevant fixes, based on a weekly analysis of all security vulnerabilities and their evaluation using a defined security assessment process. Follow up is done by a Security Manager in order to ensure fixes are deployed in a timely manner based on the assessed vulnerability risk/impact. Vulnerabilities are classified into CRITICAL and SEVERE (temporary fix applied ASAP, final fix based new risk/impact with the temporary fix in place), MODERATE (fix in 1 month), COMMODITY (fix in 3 months) and assignment is done using an adapted version of the corporate vulnerability assessment process.

- All code passes through a QA team, which evaluates various elements before allowing deployment of code into production. Security vulnerabilities are included in the check and a manual code review ensures the highest code quality

Supporting documentation for the security measures applied:

- Vulnerability assessment done in Next Europa
- Security Plan of Next Europa

FORMTOOLS PLATFORM security measures

Description:

• The database is only available from the internal EC network and is protected by user/password.

• The database is backed up every day on a dedicated server (access to this server restricted to DIGIT's Devops team in the internal network).

• The data controller only has access to submissions conveyed to his/her instance of the implementation but is able to provide 3rd-parties with access.

Cybersecurity:

All instances of the FormTools system are available via a secured encrypted connection only.

Encryption and/or pseudonymisation of personal data:

FormTools does not store the IP address of the end-user that submits a form (all IPs replaced by 127.0.0.1).

Other:

The data is hosted on infrastructure that is owned by DG DIGIT and hence meets DG DIGIT's security standards.

Thereby, measures are in place to

• aim for using privacy-enhancing technologies (PETs);

• ensure confidentiality, integrity, availability and resilience of processing systems and services;

• to restore availability and access to personal data in a timely manner in the event of physical or technical incident.

8. How long do we keep your data?

We only store your data as long as is necessary for the predefined purpose of the processing.

Time limit

Each user should take contact with functional mailbox: TAXUD-ELEARNING@ec.europa.eu to request the deletion of the data when he/she considers appropriate.

Personal data (country and company name) is deleted 18 months after the download form was filled online by the user. Specifically for the email address the deletion is after 12 months.

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

9.1 YOUR RIGHTS

You are at any given moment 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.

9.2 EXERCISING YOUR RIGHTS

The users have the possibility to delete immediately their data from our database by writing to functional mailbox: TAXUD-ELEARNING@ec.europa.eu;

9.3 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 the 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 you to take the necessary precautions.

10. 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 Data Controller using the following contact information:

The Data Controller:

- *DG TAXUD E3*
- *+32 4 2952451*
- *TAXUD UNIT E3 TAXUD-UNIT-E3@ec.europa.eu;*
- *TAXUD-ELEARNING <TAXUD-ELEARNING@ec.europa.eu>*

The Data Protection Officer (DPO) of the Commission: DATA-PROTECTION-OFFICER@ec.europa.eu

11. Recourse

Complaints can be addressed to the European Data Protection Supervisor. All details can be found at: https://edps.europa.eu/data-protection/our-role-supervisor/complaints_en.

12.Where to find more detailed information?

The Commission Data Protection Officer publishes the register of all operations processing personal data. You can access the register through the following link: http://ec.europa.eu/dpo-register.