TIOS.TRAINING

PRIVACY NOTICE

Controller: Counter-Terrorism Information and Criminal Analysis Centre (registered office: H-1117 Budapest, Fehérvári út 70, tax number: 15834577-1-51, represented by: dr. Tibor Takács, Lt. General, Director General)

Contact details of the Data Protection Officer: adatvedelem@tibek.gov.hu

Operator of the website, contact information: Computer and Automation Research Institute (registered office: H-1111 Budapest, Kende utca 13-17., tax number: 15300399-2-43, represented by: dr. László Monostori, Director)

I. GENERAL PROVISIONS

Definitions

Definitionsare based on those contained in the General Data Protection Regulation (GDPR).

1. Personal data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

2. 'processing': any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transfer, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

3. Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

4. 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

5. Recipient: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. Public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

6. consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

7. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transferred, stored or otherwise processed.

Principles relating to processing of personal data

Personal data:

1. are processed lawfully, fairly and in a transparent manner in relation to the data subject („lawfulness, fairness and transparency”);

2. may be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) of the GDPR, not be considered to be incompatible with the initial purposes („purpose limitation”);

3. must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed („data minimisation”);

4. must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay („accuracy”);

5. must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of GDPR subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject („storage limitation”);

6. must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality’)

7. The Controller shall be responsible for, and be able to demonstrate compliance with the above („accountability”).

The Controller declares that its processing is in accordance with the principles set out in the above points.

II. PROCESSING

II.1. ***Contact/ Registration, Information***

1. Collection of personal data, processed data and purpose and legal basisfor data processing

Personal data	Purpose of the processing	Definition of legal ground
Name	Identification	Article 6 (1) a)
E-mail address	Contact and sending of reply messages	Article 6 (1) a)
Telephone number	Contact	Article 6 (1) a)
If you register on the website:		
Date and time of contact	To participate in a training course	Article 6 (1) a)
IP address at the time of contact	To participate in a training course	Article 6 (1) a)

2. Data subjects: users who register on the tios.training website.

3. Duration of data processing, deadline for erasing data: Immediately after participation in the training, except where the data subjects consent to further processing them for the purpose of informing them about future trainings, in which case the processing will continue until their consent is withdrawn.

4. Potential Controllers entitled to access the data, recipients of the personal data: Personal data may only and exclusively be processed by the Controller's authorised staff and will not be transferred.

5. Description of the data subjects' rights regarding data processing:

Datasubject may request the Controller to access, rectify, erase or restrict the processing of personal data relating tohim/her.

Datasubject has the right to withdraw his/herconsent at any time.

6. Data subject may request access to, erasure, rectification or restriction of the processing of personal data by sending an e-mail to tios.training@tibek.gov.hu.

7. Please note, that the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

II.2. Processor used:

1. Activity performed by the Processor: system operation and webpage management

2. Name and contact details of the Processor: Computer and Automation Research Institute (registered office: H-1111 Budapest, Kende utca 13-17., tax number: 15300399-2-43,

represented by: dr. László Monostori, Director, contact details of the data protection officer)

3. The fact of data processing, the scope of processed data: All personal data provided by the data subject in the course of the operation of the tios.training website: name, telephone number, e-mail address

4. Data subjects: All data subjects using the website.

5. The purpose of processing: Operates the website for training purposes; make the website available and to ensure its proper functioning.

6. Duration of data processing, deadline for erasing data: Until the end of the training, except where the data subjects consent to further processing them for the purpose of informing them about future trainings, in which case the processing will continue until their consent is withdrawn except where the data subject has consented to the processing of their data after the training, until the withdrawal of the data subject's consent, but no later than the termination of the agreement to operate the website.

7. Legal ground for the processing of the data: Article 6(1)(c) and Section 13/A (3) of Act CVIII of 2001 on Certain Aspects of Electronic Commerce and Information Society Services. Based on a contract for the proper operation of the website, protection against attacks and fraud.

III. DATA SUBJECTS' RIGHTS

1. Access right:

You have the right to receive notification from the Controller regarding whether or not their personal data are beingprocessed, and if they are, Data Subject has the right to access his/herpersonal data and the following information in accordance with appointed references of the GDPR:

2. Right to rectification

You shall have the right to obtain from the Controller, without undue delay, the rectification of inaccurate personal data concerning you.

You shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

3. Right to erasure

You have the right to request the Controller the immediate erasure of your personal data and, upon receiving such a request, the Controller shall immediately perform the requested erasure in case of the following conditions:

a)the personal data requested to be erased are no longer needed for the purpose they were obtained for and otherwise processed;

b)the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

c)the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

d) the personal data have been processed unlawfully;

e)the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the Controller is subject;

f)the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

5. Right to the restriction of processing

You shall have the right to request the Controller to limit processing when any of the following conditions are fulfilled:

a) You dispute the accuracy of the personal data, in which case the restriction applies to the period of time that allows the Data Controller to verify the accuracy of the personal data;
b) the processing is unlawful and you oppose the erasure of the personal data and request the restriction of their use instead;
c) the Data Controller no longer needs the personal data for the purpose of data processing, but you require their retention in order to submit, enforce or protect legal claims
d) You have objected to the data processing; in this case, the restriction applies for the period until it is established that the legitimate interest of the Data Controller is override your legitimate interest.

6. Right to data portability

You have the right to receive the personal data concerning you, which they have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Controller without hindrance from the Controller to which the personal data have been provided, where:

7. Automated individual decision-making, including profiling

You have the right not to be covered by a decision based solely on automated data processing, including profiling, which would have legal effect on you or would have other significant effect on you.

The previous paragraph shall not apply if the decision:

a) Is necessary for entering into, or performance of, a contract between you and the Controller;
b) is authorised by Union or Member State law to which the Controller is subject and which also lays down suitable measures to safeguard your rights and freedoms and legitimate interests; or
c) is based on your expressed consent.

6. Deadline for taking action

The Controller shall, without undue delay, but by **no later than within 1 month** of the receipt of the request, inform you in accordance with the above requests, of the action taken in response to the request. **If necessary, this deadlinemay be extended by 2 months.** The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. . If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

V. SECURITY OF PROCESSING

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Controller and the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

2. ensuring the ongoing confidentiality, integrity, availability and resilience of the systems (http, https systems, ssl encryption) used to process personal data;

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

4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

5. The storage of the processed data in such a way that unauthorised persons do not have access to them.

6. The method of storing the data by computerised means must be chosen in such a way that they can be erased, also taking into account any different erasure deadline, at the end of the deadline for erasure or if otherwise necessary. Erasure shall be irreversible.

7. Paper-based data media shall be destroyed by shredding or persona data shall be removed from them by using an external organisation specialised in shredding. In case of electronic data media, physical destruction and, where necessary, prior secure and irretrievable erasure of the data shall be ensured in accordance with the rules on the disposal of electronic data media.

Physical Protection

1. Paper documents shall be stored in a secure, lockable dry room.

2. In the course of their work, the Controller's processing employee may leave the room where the processing takes place only by locking away the data carriers entrusted to them or by locking the room concerned;

3. The personal data can only be accessed by authorised persons, with no third parties having access thereto.

4. The Controller's building and premises are equipped with fire and property protection equipment.

IT Protection

1. The website used by the Controller and operated by the Processor is a hhtp, https system with ssl encryption.

3. To ensure the security of the digitally stored data, the Processor uses data backups and archives every week, both remote (Sundays at 0:00) and local (Saturdays at 0:00).

4. Access to the website is only granted to authorised persons and is recorded on the tios.training platform.

5. Data stored on the computers can only be assessed with a user name and password.

VI. INFORMATION OF THE DATA SUBJECT ON THE PERSONAL DATA BREACH

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall communicate to the data subject without undue delay.

The information provided to the data subject shall clearly and prominently describe the nature of the personal data breach and communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; it shall describe the likely consequences of the personal data breach; describe the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The communication to the data subject shall not be required if any of the following conditions are met:

a) the Controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

b) the Controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
d) If the controller has not yet communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so.

Notification of a personal data breach to the authority

In the case of a personal data breach, the Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority (NAIH) competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

VII. COMPLAINT

The data subject may lodge a complaint against a possible infringement by the Controller tothe National Authority for Data Protection and Freedom of Information at the following contact details:

National Authority for Data Protection and Freedom of Information
1055 Budapest, Falk Miksa utca 9-11.
Correspondence address: 1363 Budapest, PO Box 9.
Phone: +36 -1-391-1400
Fax: +36-1-391-1410
E-mail: ugyfelszolgalat@naih.hu