# CTC Data Protection Notice

## Information for the processing of personal data in accordance with art. 14 GDPR

The purpose of this data protection notice is to inform data subjects about the processing of their personal data. Considering the technical nature of the module and limitations imposed by the research design (i.e., scale), it is considered that informing those data subjects directly would involve a disproportionate effort. For this reason, this information is made publicly available via the project's website in accordance with art. 14 GDPR and with its potentially applicable derogations (art. 14 (5) (b) GDPR[1]), as an effort of enabling the data subjects to be informed about the data processing and to exercise their rights. This notice refers to the specific module of the CTC responsible for collection of data from online sources.

Data will be collected from social media accounts which will be publicly available as well as from the surface and dark websites, the content of which will be associated to terrorist financing

### 1. The Project

Cut The Cord (CTC, GA: 101036276) project aims to strengthen the EU's capacity to understand and counter terrorist financing by exploring the use of new payment methods (e.g., cryptocurrencies) and internet-based communication platforms (e.g., social media, darknet forums) for such purposes. It aims to enhance the public-private cooperation through the establishment of a wide stakeholder community, with the vision to sustain it beyond the end of the project. Joint training exercises (theoretical and hands-on) will be organised to build capacity of the Counter-Terrorism Financing end-users (law enforcement agencies, Financial Authorities and payment Services, Cryptocurrency Anti Money Laundering organisations, Financial Information Units etc.) in emerging terrorism financing risks and to enhance the preparedness end-users to tackle the financial activities of terrorist organisations. Finally, CTC aims to provide technical solutions based on Artificial Intelligence tools for data acquisition and analysis of financial transactions (e.g., cryptocurrency transactions), as well as an information exchange mechanism based on decentralized technologies, to ensure secure and levelled information and intelligence sharing, along with digital evidence exchange in a timely manner. As a result, it will develop an appropriate framework for sharing financial data to model suspicious transactional behaviour at the points of ingress and egress between traditional and digital economy, track the audit trail that has been followed by the criminals, improve the investigation capabilities of law

[1] Paragraph 5 (b) of this Article provides for an exemption if such information proves impossible or would involve a disproportionate effort, for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In this case, subject to the conditions and safeguards referred to in Article 89(1) GDPR, the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.

enforcement agencies, and enhance the cooperation between different stakeholders involved in the "investigation supply chain.

**2. Data Controller and Key Contacts**

The Centre of Research & Technology – Hellas (6th km Harilaou - Thermi, 57001, Thermi-Thessaloniki, Greece) is the Data Controller. You can ask any questions and exercise your rights related to data protection by using the following contacts:

| Name | Organisation | e-mail | Role |
|---|---|---|---|
| Dimitrios Kavallieros | CERTH/ITI | dim.kavallieros@iti.gr | Contact Person |
| Theoni Spathi | CERTH/ITI | tspathi@iti.gr | Contact Person |
| Theodora Tsikrika | CERTH/ITI | theodora.tsikrika@iti.gr | Contact Person |
| Stefanos Vrochidis | CERTH/ITI | stefanos@iti.gr | Contact Person |

**3. Data Processing**

Data will be collected from social media accounts which will be publicly available as well as from the surface and dark websites, the content of which will be associated to terrorist financing, thus uncovering links to online marketplaces, darknet and hidden services. Parallel to that, an AI-based tool to detect patterns of suspicious events will be developed, along with an AI-based cross-modal correlation among multimodal datasets, thus further enabling the detection of potentially illegal financial activities and enhancing in that way security. The legal basis under which the data shall be processed is article 6(1)(f) GDPR. The legitimate interest of the controllers lies with the pursuit of scientific research purposes confirmed by the European Commission. Such data will be collected by the web and social media crawling that will be tested in the context of the CTC pilots.

Within this Data Protection Notice you have been given the contact details of the relevant project representatives (see Section 2) should you have any questions regarding the processing of your personal data.

**What personal data is being processed?**

The following categories of personal data publicly available on social media and/or the surface and dark web will be collected and processed:

- IP addresses
- E-mail addresses

- Social media and forum posts including the language, textual content, hashtags, images/videos, whether the post is a reply to another post, as well as the number of retweets (in case of twitter) and the number of likes;
- Social media and forum account information, including the username, the names and surnames, birth dates, birth places, marital status, addresses, tax information, and phone numbers, username, description (if any from the user), location, as well as the number of friends, followers and favourites;
- Social media account interactions, including user mentions;

No special categories of personal data (art. 9(1) GDPR) will be collected, nor data relating to criminal convictions (art. 10 GDPR). All data will be collected in accordance with the licences and terms & conditions of the data providers. All data will be gathered only from public accounts, with the permission defined by the social media platforms and in compliance with the respective terms of use, including the ones referred explicitly to the terms of use on behalf of minors, thus in accordance with user expectation of privacy. All collected data will be pseudonymised. The names of users that posted a tweet or are mentioned inside a tweet are all encrypted with a cryptographic cipher and replaced with alphanumeric characters. Data minimisation will also be applied, as the content of the stored posts will be limited only to the relevant information with no reference to personal data. In accordance with the data minimisation principle, only the parts that are deemed necessary for the project's objectives will be processed subject to a privacy-by-design technique, while the majority will be deleted immediately. Further, details are provided in the "What is the purpose of the processing" section.

**What is the purpose of the processing?**

CTC aims on the identification and analysis of the modus operandi of terrorist organisations (and sympathisers) regarding their online financial activities. The purpose of data collection in this project is to monitor and analyse Surface, Dark Web and Social Media data (Internet monitoring) as well as to discover relevant links to darknets. Special focus will be given in the use of new payment methods (e.g., cryptocurrencies) to provide meaningful insights on the employment of technological advancements from terrorist organisations. The additional multilingual text analysis will aim to detect communities of users involved in closely associated transactions, as well as the users with a key role within such communities, find further linkages with crypto/fiat exchangers (e.g., virtual criminal 'shops', cryptocurrencies suggested as payment methods, wallets and crypto addresses, emails, etc.), track potential money flows, or transitions from Surface to Deep or Dark websites, thus further enabling the detection of potentially illegal financial activities and enhancing in that way security. Individuals will have long-term effects from the outcomes of CTC project, as its main aim is to prevent and disrupt terrorism financing, enhancing the preparedness of relevant end-users to tackle the financial activities of terrorist organisations. In that way it will support the socioeconomic stability and feelings of security of the society in general. The minimum of the aforementioned data that is necessary for the CTC research, in their anonymised or pseudonymised form (see below "Data security"), will be

processed for scientific research purposes related to the CTC project (i) to facilitate the functionality of other modules of the project, and (ii) for demonstration purposes..

**Data security**

A Data Protection Impact Assessment has been conducted by the controller. The CTC project implements appropriate technical and organizational measures in accordance with Article 89 par.1 GDPR and security measures against the risks arising from the processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access .

Examples include rule-based anonymisation techniques and machine learning based techniques that will be applied to the recognised names that may correspond to personal data. Personal data considered useful for the project will be either pseudonymised and deleted or encrypted and stored in a password-protected database. IPs and email addresses will be pseudonymised on the fly (IPs are replaced with the expression “rectified_IP'' while emails are replaced with the expression “rectified_email”). The retrieved text will be stored encrypted using the AES256 encryption algorithm. The key will be securely stored in the machine that hosts the information gathering module. All the personal identifiers (if any) from all the other data sources (surface web) will be removed (e.g., Photos blurring etc.) before being further processed, so that access to raw data with further links to personal data will not be possible. For any interaction with the server (e.g., remote control or data transfer), secure protocols such as ssh/stfp will be used. Additionally, only authorised personnel will have access to this machine. Parallel to that, all crawling activities will adhere to the terms of the official APIs of the social media platforms as well as to the robots.txt protocols. All data will be gathered only from public accounts, with the permission defined by the social media platforms and in compliance with the respective terms of use, thus in accordance with user expectation of privacy. In accordance with the data minimisation principle, only the parts of the social media posts that are deemed necessary for the project’s objectives will be processed subject to a privacy-by-design technique, while the majority will be deleted immediately. The server hosting this database is accessible only by authorised users through authentication (using passwords of high complexity). A firewall will also be in place to allow only specific (whitelisted) IPs to access the server and to restrict the access of each whitelisted IP only to specific ports/services. Different access privileges to the data are available to ensure that the authorised users will only have access to the stored data on a need-to-know basis, i.e., that the authorised users will have access only to the stored anonymised/pseudonymised data needed to fulfil their tasksIn case of data breach Art. 33 and 34 of GDPR are applicable. After the end of the project (October 2023), secure deletion tools will be applied by CERTH, that will make the data irretrievable.

**Will the collected data be shared and who will be responsible for all the data when this study is over?**

The collected personal data may be disclosed to third parties, if this is required for the fulfilment of our legal obligations or is necessary for the fulfilment of the above data processing purposes, in compliance with the applicable legal framework. It is also highlighted that no personal data will be transferred outside the European Union (EU) or the European Economic Area (EEA).
When this study is over, CERTH/ITI will be the only one responsible for the information collected.

**How long will data be stored?**

The storage duration of the data in their anonymised or pseudonymised form will be the duration of the project plus five (5) years after the end of the project [i.e., October 2023], to be available for demonstration in case of an inspection or an audit.

**Will the collected personal data be used for other purposes?**

All personal data collected in CTC (*see section 3: What personal data is being processed?*) will not be processed for any other purposes outside of those specified in this document.

**Will the collected data be processed by automated tools supporting decision-making?**

The minimum of the aforementioned data that is necessary for the CTC research, in their anonymised or pseudonymised form (see below "Data security"), will be processed for scientific research purposes related to the CTC project (i) to facilitate the functionality of other modules of the project, and (ii) for demonstration purposes. Data collected from you will only be used to test the capabilities of the CTC tools and you will not suffer any consequences of automated processing supporting decision-making. After hashing of your account information, the researchers will not be able to trace back your data back to you.

**What are your rights?**

**According to Articles 15-21 and Article 77 GDPR:**

- *Right to information:* you may request information about whether we hold personal information about you, and, if so, what that information is and why we are holding it. This information shall be provided within a reasonable period after obtaining the personal data, but at the latest within one month.
- *Right to access:* you may request to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- *Right to rectification*: you may ask us to rectify the information that we hold about you in case you consider that something is missing or is incorrect.
- *Right to erasure*: you may ask us to erase your personal data at any given moment without a specific reason
- *Right to object*: you may request to stop processing delete or remove your personal data at any desired moment where there is no good reason for us continuing to process it
- *Right to data portability*: you have the right to request the transfer of your personal data in an electronic and structured form to another party or directly to you. This enables you to take your data from us in an electronically usable format and to be able to transfer your data to another party in an electronically usable format.
- Lodge a complaint with the Hellenic Data Protection Authority (https://www.dpa.gr).

Please note that some of the aforementioned rights may be restricted in the light of the GDPR (art.89 par.2) and the applicable national data protection legislation .

For the exercise of your rights and for any other data-related information you may contact the contacts mentioned above or CERTH's DPO at dpo@certh.gr