ODYSSEUS Data Protection Notice

Information for the processing of personal data in accordance with Article 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 Article 14 GDPR and with its potentially applicable derogations (Article 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 ODYSSEUS responsible for collection of data from online sources, as described below.

Data will be collected from:

i. Public social media posts, the content of which will be associated to online homemade explosives (HME) recipes.
ii. Forum Posts on the Surface Web.
iii. Webpages.

1. The Project

ODYSSEUS aims to increase the knowledge on homemade explosives (HMEs) and explosive precursors, including precursors not previously studied, and develop effective and efficient prognostic, detection, and forensic tools to improve the capabilities of Law Enforcement Agencies (LEAs) towards the prevention, countering, and investigation of terrorist incidents involving HMEs. To discover potentially hitherto unknown information, online HMEs recipes will be collected, and their content will be analysed to extract knowledge about (possibly unknown) precursors and HMEs. Selected precursors will then be characterised and analysed for determining their explosive properties, feasibility, and potential for becoming a threat. This knowledge will be leveraged for developing (i) tools for chemical supply chain monitoring for irregularity detection to enable prediction and localisation of potential threats; (ii) advanced sensors for detecting in (near) real-time explosive precursors through air emissions and sewerage networks; (iii) robotised tools for improved mobile detection and in-situ forensic support; and (iv) tools for automated threat detection, localisation, and assessment; these tools and the sensors' outputs will be integrated into a configurable platform that will assist Law Enforcement Agencies' operations in diverse scenarios.

[1] Paragraph 5 (b) of this Article provides for an exemption if the provision of 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.

2. Data Controller

Data Controller: Centre for Research & Technology – Hellas (CERTH)/Information Technologies Institute (ITI), 6th km Harilaou - Thermi, 57001, Thermi - Thessaloniki, Greece.

Project Coordinator: INSTITUT PO OTBRANA BDI Bulgaria, Professor Tzvetan Lazarov 2 Blvd., 1592, Sofia, Bulgaria

3. Data Processing

The purpose of data collection in this project is to extract useful information related to the online HME recipes, posted explicitly both by malicious actors and by explosive enthusiasts (e.g., pyrotechnics) that may unwittingly make information available to terrorist actors. With respect to the processing of personal data, the applicable legal ground for such processing activities is the legitimate interest of the data controller (CERTH/ITI) (Article 6(1)(f) GDPR and Article 14(2)(b)); *the processing is necessary for the scientific purposes described in Section 3.2*.

3.1. What personal data is being processed?

The processed personal data stemming from the social media posts and webpages, with publicly available accounts and with full respect of the terms and conditions of the relevant websites/social media platforms will include:

- E-mail addresses;
- Social media and forum posts including comments, textual content uploaded by social media users, together with relevant metadata;
- Social media account interactions, including user mentions.

No special categories of personal data (Article 9(1) GDPR) are foreseen to be collected (at least not intentionally), nor data relating to criminal convictions (Article 10 GDPR)[2]. In case that such an unintentional data processing happens, 9(2)(j) and 89(1) GDPR apply due to the scientific purpose of such a processing. Also, 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 kept and will be secondary/ further processed subject to a privacy-by-design technique, while the majority will be deleted immediately, prior to storage. All data will be collected in accordance with the licences and terms & conditions of the data providers (adherence to the robots.txt protocol during the web crawling activity and to the terms of the official Application Programming Interface (APIs) of the social media platforms). 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. Usernames will be replaced by a randomly generated ID, to achieve pseudonymity, while

[2] In case any criminal activity is witnessed or uncovered during this research activity, the research team will be required to share this information and all necessary (pseudonymised) data with the appropriate and responsible authorities.

the personal data will be encrypted and stored in their pseudonymous form in a secure database, or they will be deleted at the moment of the collection. Further, details are provided in Section 5 below.

3.2. What is the purpose of the processing?

In particular, the data will be used for the following specific purposes (i) to enhance the current capabilities of the tools created during the ODYSSEUS project on behalf of CERTH, with respect to social networking analysis, textual analysis (i.e., classification, entity recognition, clustering, and topic detection) and (ii) for training purposes (of the AI models).

4. Data security

CERTH, as Consortium partner in the ODYSSEUS project, implements appropriate technical and organizational measures to ensure an appropriate level of protection against the risks arising from processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access. All data will be collected taking into consideration all the safeguards as described in Section 4. 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) Internet Protocol address (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., to the stored pseudonymised data needed to fulfil their tasks. Devices that will store a backup of the data will follow the same security procedures as the main server. For any remote interactions with the server (e.g., remote control or data transfer), secure protocols such as ssh/sftp are used. Any processing of the data is performed on that server. In case processing will be needed on other machines, the same security measures of the server will be applied to the respective machine. The metadata of the social media and the webpages will also be stored in a local database that is secured (authentication mechanisms are enabled) and is also IP protected.

4.1. Will the collected personal data be shared?

The collected personal data (in their pseudonymised form) may be disclosed: (1) to relevant partners of the Consortium, according to a need-to know principle, through a password protected system; and (2) if this is required to third parties for the fulfilment of our legal obligations or if necessary for the fulfilment of the above data processing purposes and is in compliance with the applicable legal framework. The information collected will be also used to contribute towards several journal and conference publications as well as scientific contests, in line with social media/Web Policy.

4.2. Who will be responsible for all the personal data when this study is over?

When this study is over, CERTH/ITI will be the only one responsible for the personal data collected.

4.3. How long will personal data be stored?

The storage duration of the personal 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., September 2029], to be available for demonstration in case of an inspection or an audit, as long as required to achieve the

above purposes of processing, unless a longer retention period is required by law or for the establishment, exercise or defence of legal claims.

4.4. Will the collected personal data be used for other purposes?

All personal data collected in ODYSSEUS will not be processed for any other purposes outside of those specified in this document.

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

The collected data will not be processed by automated tools supporting decision-making. After hashing of any account information, the researchers will not be able to trace back the data back to the original owner.

4.5. What are the rights of the data subject?

The data subject rights under GDPR are contained within articles 12-23 and 77. Some of the most important rights include:

- *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 of receipt of the request.
- *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.
- *Right to lodge a complaint* with the Hellenic Data Protection Authority (https://www.dpa.gr).

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

For the exercise of the rights and for any other data-related information, data subjects may contact us at m4d_ethics@iti.gr