SAFEGUARD 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 SAFEGUARD project responsible for collection of data from online sources.

Data (only textual) will be collected from public social media posts (X, YouTube) as well as content from the surface and dark Web, the content of which will be associated to the protection of public spaces for supporting LEA operations.

1. The Project

SAFEGUARD aims at developing a next-generation holistic suite of tools that significantly improve LEA capabilities to protect public spaces against terrorist attacks through the entire lifecycle of their operations. The project equips LEAs with a powerful OSINT platform gathering and analysing data from online resources based on advanced AI methods, including Web and social media crawling, multimodal analytics, visual analytics, and threat assessment, for monitoring and detecting threats targeting public areas, supporting pre-occurrence terrorism prediction and prevention. Additionally, it supports LEA operations in public spaces through a Command & Control dashboard leveraging modern technologies, including UAVs for dynamic coverage of the protected area, IoT sensors (fixed, mobile or drone-carried cameras) for situational awareness, computer vision for visual monitoring, intelligent threat assessment for early warnings, Augmented Reality for the delivery of pertinent information, as well as 3D reconstruction and Virtual Reality for operational planning and training.

2. Data Controller

Data Controller and project coordinator: Centre of Research & Technology – Hellas (6th km Harilaou - Thermi, 57001, Thermi- Thessaloniki, Greece)

[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.

3. Data Processing

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) pursuant to Article 6(1)(f) GDPR and Article 14(2)(b); the processing is necessary for the scientific purposes described in Section "*What is the purpose of the processing?".*

What personal data is being processed?

The following categories of personal data publicly available

- E-mail addresses
- Social media posts (i.e., tweets in case of X), including the language, textual content, hashtags, whether the post is a reply to another post, as well as the number of retweets (in case of X)
- Social media account information, including the username, 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) are foreseen to be collected (at least not intentionally), nor data relating to criminal convictions (art. 10 GDPR). In any case and 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. 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/Web forum communities 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. For any personal data, processed, advanced pseudonymisation will take place to the extent possible without compromising the usability of the collected data/datasets. In particular, hashing algorithms, such as SHA512, will be used to pseudonymise personal data (e.g., usernames) derived from crawling of social media before the data is stored. Data minimisation will also be applied, i.e., only data that are necessary for the purposes of the project will be processed. Further, details are provided in the "*What is the purpose of the processing"* section.

What is the purpose of the processing?

The purpose of data collection in this project is to extract useful information related to the protection of public spaces, posted in publicly available online sources by potentially malicious actors. The above data will be required for the duration of the project: (i) for scientific research purposes, (ii) to facilitate the functionality of other modules of the project, and (iii) for demonstration purposes.

Data security

CERTH, 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 herein. 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.

Will the collected data be shared?

The collected personal data (only in their pseudonymised form) may be disclosed: (1) to relevant partners of the Consortium, according to a need-to know principle, through an authorization and authentication mechanism (i.e., password protected system); and (2) if this is required to third parties (including data processors if exist) for the fulfilment of our legal obligations or is necessary for the fulfilment of the above data processing purposes and is 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).

Who will be responsible for all of the data when this study is over?

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 pseudonymised form will be the duration of the project plus five (5) years after the end of the project [i.e., June 2031], 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

Will the collected personal data be used for other purposes?

No, the data 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?

Data collected from you will only be used to test the capabilities of the SAFEGUARD solutions with no automated support decision, thus you will not suffer any relevant consequences.

What are your rights?

Your rights under GDPR are contained within articles 12-23 and 77. Some of your 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:* based on the grounds laid out in Art 17, you may ask us to erase your personal data at any given moment.
- *Right to object*: you may request us to stop processing their personal data based on the legal ground stated in Art 21 GDPR
- *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 the aforementioned rights may be restricted in the light of the GDPR (e.g. 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 us at m4d_ethics@iti.gr