APPRAISE 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 of the General Data Protection Regulation (''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 APPRAISE responsible for collection of data from online sources.

Data will be collected from:

i. Public social media posts from Twitter and YouTube, the content of which will be associated to imminent attacks against soft targets.
ii. Webpages (surface and dark web)

1. The Project

APPRAISE aims to build on the latest advances in big data analysis, artificial intelligence, and advanced visualisation to create an integral security framework that will improve both the cyber/physical security and safety of public spaces by enabling a proactive, integrated, risk-based, and resilience-oriented approach. This framework will be designed to support the secured private-public collaboration and optimise the coordination of operations involving private security staff, private operators, and law enforcement agencies. APPRAISE will offer unprecedented capabilities to predict and identify criminal and terrorist acts and enhance the operational collaboration of security actors before, during, and after an incident occurs. Social, Ethical, Legal, and Privacy observatories bringing together LEAs, private operators, technology experts, psychologists, sociologists, and society representatives will ensure full conformity of the developed tools with current EU legislation and citizens' acceptance, preparing the ground for successful exploitation.

2. Data Controller

[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.

The Centre of Research & Technology – Hellas (6th km Harilaou - Thermi, 57001, Thermi-Thessaloniki, Greece) is the Data Controller.

3. Data Processing

APPRAISE in general aims to deliver tools to automatically acquire, process and analyse vast quantities of data from online, sources like social networks, surface web and darknet to capture the contextual risks for soft targets. The purpose of data collection in this project is to extract useful information by citizens observations though social media platforms, around imminent attacks against soft targets. 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.

What personal data is being processed? –

The processed 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 found within the textual content.
- Social media account information, including the username, description (if any from the user), location, as well as the number of friends, followers and favourites.
- Social media posts including comments, textual and multimedia content uploaded by social media users, together with relevant metadata, hashtags, multimedia data (image links, linked to articles, posts, etc. found on the surface web).
- Social media account interactions (i.e., user mentions, replies)

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). 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 (Twitter/YouTube) 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, while mentioned users will be left as is, for research purposes. 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?

Collection and further processing of those data will support Law Enforcement Agencies during investigations in cybercrime or counterterrorism areas, by allowing analysis of large volumes of data, recommending similarities, recurrent trends and activities, and hidden connections within collected data in less time than a human usually spends.

Data security

The APPRAISE 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 in accordance with the licenses and terms & conditions of the data providers. All data will be gathered only from public accounts, with the permission defined by the web/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 EU cloud-based 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 pseudonymized 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/stfp 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 be also stored in a local database that is secured (authentication mechanisms are enabled) and is also IP protected. In case of data breach Art. 33 and 34 of GDPR are applicable.

Will the collected data be shared?

The collected personal data (in their pseudonymised form) may be disclosed: (1) to all partners of the Consortium, through a password protected system; and (2) if this is required to third parties 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. 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. It is also highlighted that we will share specific data from web page crawling (raw data) with CENTRIC (UK). Any data transfer to CENTRIC (UK) complies with art. 45 GDPR, as the European Commission has adopted an adequacy decision for transfers of personal data to the United Kingdom, under the General Data Protection Regulation (C (2021) 4800 final).

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., February 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 defense of legal claims.

Will the collected personal data be used for other purposes?

All personal data collected in APPRAISE 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?

Your data will be used for (i) for scientific research purposes, (ii) to facilitate the functionality of other modules of the project, and (iii) for demo purposes. Data collected from you will only be used to test the capabilities of the APPRAISE 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?

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*: 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 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