DYNAMO 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 DYNAMO responsible for collection of data from online sources.

Data will be collected from:

i. Webpages (surface and dark web)

1. The Project

DYNAMO aims to combine the two fields of business continuity management (BCM) and cyber threat intelligence (CTI) to generate a situational awareness picture for decision support across all stages of the resilience cycle (prepare, prevent, protect, response, recover). Professionals of different backgrounds will work together with end-users to develop, refine, and combine selected tools into a single platform. In alignment to end-user needs, human factors, high ethical standards and societal impacts, DYNAMO includes the following goals:

Resilience assessment as basis for BCM

- An assessment with different levels of detail offers with varying existent data a fast or detailed evaluation of the investigated sector and helps to identify critical processes.
- End-user data will be integrated to measure determined performance targets. With respect to the functional description, AI-based approaches will be used for a deeper understanding and potential self-learning of the interconnected process.
- The results generate knowledge concerning susceptibility and vulnerability of the investigated sector.
- The solutions support the BCM with respect to the five resilience phases.

[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.

Leveraging CTI

– CTI will be improved with respect to existing solutions and will be extended and integrated in DYNAMO.
– The CTI approach deliver data that will be integrated into the resilience and BCM approach. The use of AI will support the development. Solutions will be integrated with the Cyber Knowledge Graph to visualize the analysis of threat intelligence.

The DYNAMO platform will be able to collect organization's skills data, elaborate and create custom tailored organisational training to improve organisational resilience which will be demonstrated within three different (cross-)sectoral use-cases.

2. Data Controller

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

3. Data Processing

DYNAMO in general aims to deliver tools to automatically acquire, process and analyse quantities of data from online, sources like surface web and darknet to capture the contextual risks for soft targets. The information will be fed to the DYNAMO platform to create tailored organisation training to improve organisational resilience in critical sectors, increasing situational awareness and ensuring critical risk assessment.

What personal data is being processed?

The processed data stemming from the webpages, with publicly available accounts and with full respect of the terms and conditions of the relevant websites will include:

- IP addresses

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 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. 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 use of personal data included in the collected data (i.e., IPs) enables the data controller to correlate the gathered data to extract more advanced intelligence about cyber threats and produce policies to support effective BCM and Business Continuity Plans (BCP). The purpose of the data controller is not to collect personal data, but to use this data to enrich the collected intelligence and utilise it for BCM. This will facilitate the generation of more realistic scenarios that are based on identified and forecasted trends of cyber-attacks and vulnerabilities which will result in the better education of the users of the DYNAMO platform against cyber-attacks. The main sources of interest to be processed should primarily include information about cyber threats and their purpose should be to educate people and organisations against cyber threats and how to implement and utilise BCM. This is in line with the aim of the DYNAMO project, which is to develop a federated cyber-range. Some of the sources that will be monitored (e.g., specific web pages from the Dark Web) can have different uses in the framework of the scientific research (DYNAMO is a research program) for collecting or sharing data, such as Dark Web forums that sell new vulnerabilities (i.e., 0-days). This information can be used by the DYNAMO project to inform and educate its users about those new vulnerabilities to increase their security. The project is interested neither in the collection nor in any other type of personal data processing made by this tool and considers it a by-product. The IPs that will be collected will be encrypted by design.

Data security

The DYNAMO 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 licences and terms & conditions of the data providers. All data will be gathered only from public accounts, with permission defined by the web 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 posts/content 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. 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 is needed on other machines, the same security measures of the server will be applied to the respective machine. The metadata of 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 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 Web Policy. 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 form will be the duration of the project plus five (5) years after the end of the project [i.e., 1/10/2027], to be available for demonstration in case of an inspection or an audit, 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 DYNAMO 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 DYNAMO tools and you will not suffer any consequences of automated processing supporting decision-making.

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