

TREEADS 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) GDPR¹), 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 TREEADS responsible for collection of data from online sources.

Data will be collected from:

- Public social media posts from X (former Twitter), the content of which will be associated to possible fire incidents.

1. The Project

Wildfires are a severe threat across Europe, causing significant environmental and economic damage. They are becoming more intense and widespread because of climate change, particular forestry practices, ecosystem deterioration, and rural depopulation. Extreme wildfire events, in addition to their devastating ecological impact, have an unparalleled social cost in terms of both human life and economic losses. [TREEADS](#) (A Holistic Fire Management Ecosystem for Prevention, Detection and Restoration of Environmental Disasters), aims to tackle several major challenges that wildfires pose by building upon state-of-the-art high TRL products and unite them in a holistic Fire Management Ecosystem consisting of various innovative technologies and systems to optimize and reuse the available Socio-technological Resources in all three main phases of Wildfires. By adopting a multi-stakeholder, multi-actor approach at its core, the TREEADS solutions will contribute to sustainable development as an inclusive societal process and secure sustainability and resilience of natural environment, as well as local human societies.

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: RISE Fire Research AS (FRN), Tillerbruvegen 202, 7092 Tiller, Norway.

3. Data Processing

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.

TREADS aims to systematically collect data on potential fire incidents reported by citizens through social media platforms such as X (formerly Twitter). The collected data is processed by several analytical modules designed to extract critical information, including geographical locations, key visual content concepts, and relevance to fire incidents. These analyses provide comprehensive insights into emerging fire events. The Fire Events Detection module identifies fire incidents reported on social media and stores them within a MongoDB database. The processed information is visualized through an intuitive WebGIS Dashboard. This valuable tool helps users understand and analyse fire-related data from social media. By organizing and displaying the data (i.e., social media post text, images, visual and textual analysis, and other metadata) in an intuitive and user-friendly way, the platform helps users better understand the scope and impact of fire incidents and can ultimately aid in the prevention and mitigation of future fires. The legal basis under which the data shall be processed is Article 6(1)(f) GDPR. The processing is in fact necessary for scientific purposes and for the purposes of enhancing the understanding of the process of grooming, in accordance with recitals 49 and 50 GDPR. The legitimate interest of the controllers lies in the pursuit of scientific research purposes confirmed by the European Commission.

What personal data is being processed?

The following categories of personal data publicly available in social media posts/web forums etc. are foreseen to be collected/processed:

- X (former Twitter) posts including comments, textual and multimedia content uploaded by the relevant users, together with relevant metadata, hashtags, multimedia data (image links, linked to articles, posts, etc. found on the surface web).

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). In case that such an unintentional data processing happens, 9(2)(j) and 89(1) 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 terms of the official APIs of the X (former Twitter) platform. 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 and names will be replaced by a randomly generated ID, to achieve (pseudo)anonymity, while the tweets will be encrypted and stored in their pseudonymous form in a secure database. Any other personal data considered necessary for the project will be pseudonymised, encrypted and stored in a password-protected database.

What is the purpose of the processing?

As aforementioned, the data will be used for (i) scientific research purposes, (ii) to facilitate the functionality of other modules of the project, and (iii) for demo purposes.

Data security

Appropriate technical and organisational measures will be implemented in accordance with Article 89 (1) GDPR and security measures against the risks arising from the processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access. More in particular: (a) In accordance with data minimization principle, only personal data considered necessary for the project will be maintained after being pseudonymised or encrypted and stored in a password-protected database; A total anonymization isn't feasible, because in the public social media accounts, the content of social media posts can lead to the user id (b) A dedicated server hosting this database will be accessible only by authorised users through authentication (using passwords of high complexity); (c) A firewall will be in place to allow only specific (whitelisted) IPs to access the server and restrict the access of each whitelisted IP only to specific ports/services; (d) The server will be located inside a locked room, accessible only by authorised personnel; (e) Devices that will store a backup of the data (if any) will follow the same security procedures as the main server; (f) For any remote interactions with the server (e.g., remote control or data transfer), secure protocols such as ssh/stfp will be used; (g) Any processing of the data will be performed on the relevant server. In case processing will be needed on other machines, the same security measures of the server will be applied to the respective machine; (h) In case of a data breach, CERTH/ITI adopts a procedure in accordance with the provisions of Article 33 and 34 GDPR.

Will the collected data be shared?

The collected (pseudonymised) 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 (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 follows 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). 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.

Who will be responsible for all 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 anonymised or pseudonymised form will be the duration of the project plus five (5) years after the end of the project [i.e., May 2030], 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?

All personal 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?

All the relevant collected data will be processed for scientific research purposes related to the TREEADS 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 TREEADS 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 GDPR. 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.
- *Right to access:* you may request to receive a copy of any personal information we may hold about you, if any, 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. We will reply to your request within (1) one month after receiving it and without any cost for you. The above period might be extended for two (2) more months, due to the complexity or the number of the requests. In such a case you will be informed for the time extension and the reasons for it, as soon as possible.