

CESAGRAM 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 CESAGRAM responsible for collection of data from online sources.

Data will be collected from social media accounts which will be publicly available as well as from the web forums, the content of which will be associated to grooming activities.

1. The Project

CESAGRAM aims to enhance the understanding of the process of grooming, and more particularly how it is facilitated by technology and how it can lead to child sexual abuse and missing children, in order to, based on this better understanding: (a) ensure that grooming for sexual abuse and potentially leading to going missing is prevented insofar possible, and (b) ensure that victims of grooming are identified and receive appropriate support before, during and after a disappearance. The proposed project will mainly target young people 11-14 who are at risk of grooming or are victims of grooming themselves and are at risk of missing, carers and teachers, frontline professionals (social workers, NGOs, law enforcement) as well as policy makers. It will support the implementation of the existing legislation on child sexual abuse along with the European Commission's Child Sexual Abuse Prevention Network (CSAPN) and the future European Centre against Child Sexual Abuse, as well as the relevant strategies developed by the European Commission (Child Rights Strategy, EU Child Sexual Abuse strategy, European Strategy for a Better Internet for Children).

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: EUROPEAN FEDERATION FOR MISSING AND SEXUALLY EXPLOITED CHILDREN AISBL (MCE), RUE DE L INDUSTRIE 10, BRUXELLES 1000, Belgium.

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.

It is foreseen that through the processing of the collected data from various sources useful intelligence will be generated to combat child grooming. With respect to the processing of personal data, the applicable legal ground for such processing activities carried out through the CTI tool is the legitimate interest of the data controller (CERTH/ITI) pursuant to 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.

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:

- Social media and forum posts including the language, textual content, hashtags, images/videos (their urls), whether the post is a reply to another post, timestamps;
- Social media account information including the username, the names and surnames, other info voluntarily disclosed in posts, as well as the number of friends, followers and favourites;
- 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) 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 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 and names will be replaced by a randomly generated ID, to achieve 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. In accordance with the data minimisation principle, only personal data that are deemed necessary for the project will be processed adhering to privacy-by-design principles, while the majority will be deleted immediately, prior to storage. Further, details are provided in the "What is the purpose of the processing" section.

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. This might be done with the help of a relevant NGO or agency with appropriate expertise who can provide support

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.

The collected pseudonymised (or anonymised where possible) 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. Please be also informed that the consortium is mostly composed of EU-based entities, except for one non-EU partner (Marie Collins Foundation), based in the United Kingdom (UK). However, while no longer an EU Member State, UK's legal framework is very much in line with EU standards, as illustrated by the adequacy decision on data protection by the European Commission (Commission Implementing Decision (EU) 2021/1772 of 28 June 2021, C(2021)4800).

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. This might be done with the help of a relevant NGO or agency with appropriate expertise who can provide support.

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 anonymised or pseudonymised form will be the duration of the project plus five (5) years after the end of the project [i.e., December 2024], 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 CESAGRAM 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 CESAGRAM 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. 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 Article 17 GDPR, 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 Article 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. Article 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