

# Privacy Policy (Data Management Information)

for Users of the Trinity Guard Software Application

Effective from December 15, 2022.

## 1. Introduction

During the operation of the software application, the service provider / data controller processes the data of the users in order to provide them with appropriate services.

The service provider aims to fully comply with the legal requirements regarding the processing of personal data, in particular the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council.

This data management notice is based on Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of personal data of natural persons and on the free flow of data, taking into account the contents of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (the two Acts altogether shall be referred to as “Privacy Act”).

## 2. Name of Service Provider and Data Controller

**Company Name:** Trinity Security Kft.

**Registered Address:** 4172 Biharnagybajom, Rákóczi út 38.

**Tax Number:** 32028452-2-09

**National Authority for Data Protection and Freedom of Information Registration Number (NAIH):**

-

**Name of the website, address:**

www.trinity-guard.com

**Availability of Privacy Policy (Data Management Information):**

<https://trinity-guard.com/privacy-policy>

**3. Contact Details of Data Controller:**

**Company Name:** Trinity Security Kft.

**Registered Address:** 4172 Biharnagybajom, Rákóczi út 38.

**Postal Address:** 4172 Biharnagybajom, Rákóczi út 38.

**E-mail:** info@trinityguard.hu

**Phone:** +36 70 324 7525

## 4. Definitions

**GDPR** (General Data Protection Regulation) is the new data protection regulation of the European Union.

**data processing**: any operation or set of operations performed on personal data or datasets in an automated or non-automated manner, including by means of collection, recording, systematization, sorting, storage, transformation or modification, consultation, access, use, communication, transmission, distribution or otherwise making available, coordination or linking, limitation, deletion or destruction;

**data processor**: the natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller;

**personal data**: any information relating to an identified or identifiable natural person (the person concerned, the data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

**data controller**: the natural or legal person, public authority, agency or any other body that determines the purposes and means of the processing of personal data, alone or in conjunction with others; where the objectives and means for processing are specified in Union or Member State law, the data controller or the specific criteria for the designation of the controller may also be specified by Union or Member State law;

**consent of the data subject**: a voluntary, specific and appropriate informed and unambiguous declaration of the will of the person concerned by means of a declaration or an act of confirmation that he or she agrees to the processing of personal data concerning him or her;

**data breach**: a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access to personal data transmitted, stored or otherwise processed.

**recipient**: the natural or legal person, public authority, agency or any other body to whom or to which personal data is disclosed, regardless of whether it is a third party. Public authorities which have access to personal data in accordance with Union or Member State law in the context of an individual investigation shall not be considered as recipients;

the processing of such data by those public authorities shall comply with applicable data protection rules in line with the purposes of the data processing;

**third party:** a natural or legal person, public authority, agency or any other body that is not the same as the data subject, the data controller, the processor or those persons who have been authorised to process personal data under the direct control of the controller or processor.

## 5. Directives on Data Management

The Data Controller declares that the processing of personal data is carried out in accordance with the data management information and complies with the provisions of the applicable legislation, taking into account the following:

The processing of personal data shall be lawful, fair and transparent to the data subject.

Personal data may only be collected for specified, clear and legitimate purposes.

The purpose of the processing of personal data must be appropriate and relevant and only to the extent necessary.

Personal data must be accurate and up-to-date. Inaccurate personal data must be deleted immediately.

Personal data should be stored in such a form that the identification of the data subjects is possible only for the time necessary. Personal data may be stored for a longer period only if the storage is carried out for archiving purposes in the public interest, for scientific and historical research or for statistical purposes.

Personal data shall be processed in such a way as to ensure adequate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, by applying appropriate technical or organisational measures.

The principles of data protection should apply to all information relating to an identified or identifiable natural person.

## 6. Important Data Management Information

The purpose of data processing is to enable the service provider/data controller to provide appropriate additional services to individuals interested in the application while operating the application.

The legal basis for data processing is the consent of the person concerned.

Those involved in the data management are the users of the application.

Duration of data processing and deletion of data. The duration of data processing always depends on the specific purpose of the user, but the data should be deleted immediately when the originally envisaged purpose has already been achieved. The data subject may withdraw his consent to data processing at any time by sending a letter to the contact e-mail address. If there is no legal obstacle to deletion, your data will be deleted.

The data controller and its employees are entitled to access the data.

The data subject may request from the controller access to, correction, deletion or restriction of the processing of personal data concerning him/her and may object to such personal data processing and to his/her right to data portability.

The data subject may withdraw his/her consent to the processing at any time, but this does not affect the lawfulness of the data processing carried out on the basis of the consent prior to the revocation.

The person concerned may exercise the right to lodge a complaint with the supervisory authority.

If the person concerned wishes to use the application, it is necessary to provide the requested personal data. It is not possible to use the application without providing the data.

The data subject has the right, at the request of the data controller, to correct or supplement inaccurate personal data relating to him or her without undue delay.

The data subject has the right, at the request of the data controller, to delete inaccurate personal data relating to him/her without undue delay, and the controller is obliged to erase the personal data concerning the data subject without unjustified delay if there is no other legal basis for the data processing.

Modification or deletion of personal data may be initiated by e-mail, telephone or mail through the contact options provided above.

## 7. Data Processors

The hosting provider:

**Company Name:** Rackforest Kft.

**Registered Address:** 1132 Budapest, Victor Hugo utca 11. 5. em.

**Phone:** +36 1 211 0044

**E-mail:** info@rackforest.com

The data you provide is stored on the server operated by the hosting service provider. Only our employees and the staff who operate the server have access to the data, but they are all responsible for the safe handling of the data.

Name of activity: hosting service, server service.

The purpose of data management is to ensure the operation of the application.

The duration of data processing and the deadline for deletion of data. Data management is carried out until the end of the operation of the application or according to a contractual agreement between the operator of the app and the hosting service provider. The person concerned may, if necessary, request the deletion of his data by contacting the hosting provider.

The legal basis for the data processing is the consent of the data subject or data processing based on applicable legislation.

## 8. Data Used In The Application

**The data used will be stored until the termination of the contract with the respective company, unless otherwise provided in this contract for the specific data type.**

**Name:** Users' names are seen by the company's own employees for identification purposes only.

**E-mail address:** Required for login and sending a password reminder e-mail.

**GPS coordinates:** Location data from the user's phone is saved every 5 seconds during task execution. These are stored on the server and are accessible to the employing company upon completion of the task.

**Chat-shared content:** Messages sent in the form of text, image and voice messages that are stored on the server and can only be seen by the participants in the chat group.

**Incidents:** Users can report incidents, which may include images and text. Only the employees of the company can see it.

**Services, Tasks:** Their performance can be checked by the respective superior of the employee.

**Language:** The language selected by the user in which the text of the application is displayed.

**Error Logs:** When an application receives an error code from the server, it logs the data of the request and sends it to the server to store it. It contains no other data except the user ID and is intended solely for troubleshooting and correction purposes. These logs are only accessible to developers and will be deleted once the errors have been corrected.

## 9. Rights Relating To Data Management

### Right to request information

Through the contact details provided, you have the right to request information from us regarding the data that our company processes about you, including the legal basis for processing, the purpose of processing, the source of the data, and how long we will keep it. We will promptly provide you with the requested information, but no later than 30 days after receipt of your request, and will send it to the e-mail address you provide.

### **Right to correction**

You can request us to change some of your data through the contact details provided. At your request, we will act immediately, but not later than within 30 days, sending information to the contact information provided by you by e-mail.

### **Right to erasure**

You can request that we delete your data by contacting us at the provided contact information. We will promptly take action on your request, but no later than 30 days after receipt of your request, and will send a notification to the email address you provide.

### **The right to restriction of processing**

You can request us to restrict the processing of your data through the contact details provided. The restriction will continue for as long as the reason indicated by you requires the data to be stored. At your request, we will do so immediately, but not later than within 30 days after receipt of your request, sending information to the contact information provided by you by e-mail.

### **The right to object**

You can object to data processing through the contact information provided. We will examine the objection as soon as possible, but not later than 15 days from the date of submission of the request, make a decision on its validity and inform you by e-mail.



## **The right to seek legal remedy related to data processing**

If you believe that we have processed your data illegally, please inform us so that we can take steps to restore legal compliance as soon as possible. We will do everything we can to resolve the issue. If you believe that legal compliance cannot be restored, you may contact the National Authority for Data Protection and Freedom of Information at the following address:

National Authority for Data Protection and Freedom of Information

Postal address: 1530 Budapest, Pf.: 5.

Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c

Phone: +36 (1) 391-1400

Fax: +36 (1) 391-1410

E-mail: [ugyfelszolgalat \(kukac\) naih.hu](mailto:ugyfelszolgalat (kukac) naih.hu)

URL: <https://naih.hu>

Coordinates: N 47°30'56"; E 18°59'57"

## **10. Legislation on which data processing is based**

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Regulation (EC) No 95/46 (General Data Protection Regulation)

Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (the two Acts altogether shall be referred to as "Privacy Act").

Act LXVI of 1995 on Public Records, Public Archives and the Protection of Private Archives Materials.

Government Decree 335/2005 (XII. and 29.) on the General Requirements for the Handling of Documents by Public Entities

Act CVIII of 2001 on Electronic Commerce Services and Specific Issues of Services Related to Information Society ("Electronic Commerce Act").

Act C of 2003 on Electronic Communications.