

Privacy statement

This is the Data Protection Act and the General Data Protection Regulation of the European Union (2016/679/EU) combined Data Protection Statement and information document.

Registrar

Terra Patris Oy

Visiting address

Technopolis Asemakeskus

Peltokatu 27

33100 Tampere

Subsidiaries

Movax Oy

Tölkkimäentie 10,

13130 Hämeenlinna

Metalpower Oy

Ketolantie 9,

91800 Tyrnävä

TP Silva Oy

Valimotie 1

85800 Haapajärvi

Finnmaster Boats Oy

Lahdenperäntie 10,

67900 Kokkola

CEO Turkka Hirvonen

Terra Patris Oy

050 312 0132

turkka.hirvonen@terrapatris.fi

Registry name

Terra Patris Oy and its subsidiaries' Privacy Statement and the register of the notification channel (hereinafter "notification channel register", "register").

The legal basis for processing personal data, i.e. why do we collect personal data?

Data collection is based on the European Union's 23 October 2019 approved directive on Union law on the protection of persons reporting violations (EU 2019/1937). The directive obliges companies to offer, for example, a reliable reporting channel to their employees, which enables reporting of abuses and unethical activities. Personal data processing is necessary to fulfil the obligations set by the directive.

Explanation of personal data processing and purpose

Data processing is related to the maintenance of the group's whistleblowing notification channel. We use a third party operated notification channel platform service. Terra Patris Oy is the data controller (hereinafter "data controller") and the provider of the service Keskuskauppakamari (hereinafter "the provider of the service") is the personal data handler.

The reporting person can make the report anonymously and so that the report does not include their personal data. Should the reporting person leave their personal information in the notification form, the processing of personal data is based on the data subject consent.

To the extent that the notification channel register contains identifiable personal data, their processing complies with the Data Protection Act and other laws, decrees, regulations and official instructions concerning the processing of personal data. Personal data refers to information that can be connected to a specific person.

Data content of the register

How is personal data collected?

The reporting person provides information when making a report about possible unethical activity. The notification does not contain personal information about the person making the notification unless the informant expressly decides to give them. The instructions regarding the notification state that leaving a notification does not require providing personal information.

The notice may contain personal information about a third person. This is the case, for example, when the notification contains an image file of a third person.

Personal data is not collected in other ways.

How is personal data processed?

Personal data is processed to process whistleblowing reports. By going through these reports, the data controller begins due measures. These obligations derive from legislation.

Where is the collected personal data stored?

Notification information is stored encrypted in the database. The personal data processor does not have access to the stored data and data only belong to the notification handlers designated by the data controller in use. The registrar can limit access to notifications based on different notification types.

Scope of personal data processing

No personal data is collected from those who submit notifications, but the notifiers themselves may include their own data or other persons' data as part of their report or through the metadata of attached files.

Principles of registry protection

The information contained in the electronically processed notification channel register is protected by firewalls, with passwords, providing two-step authentication for notification handlers and others with generally acceptable technical means in the information security industry. Data transmission is encrypted with

SSL (Secure Socket Layer) technology, or another solution generally classified as information security. Secure email solutions are used in e-mail communication dealing with confidential materials (e.g. Deltagon's SecGW).

Notifications and attachments submitted to the service are encrypted at the time of submitting the notification. Encryption is done with symmetric and asymmetric strong encryption algorithms (XSalsa20 and Poly1305 algorithms combination). Decryption and plain language reading of notifications are only successful with the identifiers of the controller's predefined authorized processors. The service provider does not decrypt even at the request of the data controller.

The service provider carries out internal and third-party evaluations that cover both the technical security of critical information systems and administrative information security and data protection processes and guidelines. The platform called GlobaLeaks is used as the technical platform of the notification channel. The development of the application takes place together with an active user community by the service provider (subcontractors Haltu Oy and Silverskin Information Security Oy).

Data retention period

The law obliges the registrar to keep the information about the notification for five years. The registrar is stored in Terra Patris Oy's centralized data centre in a secure location in the disk system section, which can only be accessed with the credentials of pre-defined authorized handlers. Delegated handlers copy the notices to the target address as indicated by the service provider.

Data transfer outside the EU

The controller does not transfer data outside the EU, to third countries or to international organizations.

Rights of the registrant

When the basis for processing data is the controller's statutory obligation, the data subject has the right to receive information about the processing of personal data. If desired, the registered person has the right to receive the right to receive access the information about them, the right to correct the information, the right to limit the processing of the information or to demand correction of personal data. The registrant has the obligation to notify the processing of personal data restrictions. The registered person has the right not to be subject to automatic decision-making without legal basis. It is possible to make a notification in the notification register anonymously, in which case the notifier accepts that if he wants to invoke his rights, he must submit his personal data to the controller information.

The registered person must submit their request to the controller in writing.