Personal data processing in the Secapp service

This is a record of data processing activities, in accordance with the EU General Data Protection Regulation (GDPR), to describe how Secapp Oy processes personal information in the Secapp service on behalf of its different customers.

Prepared on November 25th 2020. Last modified on **December 13, 2023**. Secapp Oy follows changes in legislation and regulator instructions and develops the service further, and therefore we may update the policy to reflect the changes. We recommend to check the current policy on our website.

DEFINITIONS

“Service” or “Secapp Service” is a SaaS service, produced by Secapp Oy, for critical communications, alerting and documentation.

“System” or “Secapp System” is the system by Secapp Oy, where End Customers log in and create an End Customer Account in order to use the Service.

“End Customer” is an organization, which uses the Service based on an agreement with either Secapp Oy or a Distributor of Secapp Oy.

“End Customer Agreement” is an agreement between Secapp Oy and each customer organization of Secapp Oy (“End Customer”) for the provision of the Service related to the Secapp System.

“End Customer Account” is an entity within the Secapp System, which is controlled by End Customer as the personal data controller, and which contains data of the End Customer, including personal data of Users.

“Distributor” is a distributor authorized by Secapp Oy, which can resell the Service to End Customers. If Distributor itself uses the Secapp System on their own End Customer Account, the Distributor itself is additionally considered as an End Customer as described in this record document.

“Distributor Agreement” is an agreement between Secapp Oy and Distributor for provisioning of the Service related to the Secapp System and for representing and delivering the Service to the Distributor or to an End Customer defined by the Distributor.

“Users” are end users of the Secapp System, defined by each End Customer. Their personal data is processed to provide the service and they typically have a personal user account to the System, unless End Customer uses common accounts shared by several Users.

SUMMARY

The Secapp System is used by various End Customer organizations, for example for communications and managing operations. The data is stored in an End Customer specific End Customer Account in the System, and the End Customer defines which Users have access to the data on the End Customer Account and to what extent.

The processing of personal data is always based on an End Customer Agreement or Distributor Agreement. As a general principle, the following applies in the agreements: The End Customer is the personal data controller and is therefore responsible for the collection of the personal data and any other data and for the related obligations, including the possibly related consents, and the maintenance of the personal data. The control on the personal data is always with the End Customer and Secapp Oy acts either as a personal data processor or subprocessor on behalf of its own customer, which is, depending on the circumstances, the End Customer or the Distributor. Secapp Oy shall process personal data for as long as the provision of the agreed Service to the End Customer or Distributor requires it. Personal data will not be transferred to third parties, unless separately agreed with the End Customer or Distributor.

The purpose of this record document is to serve as a basis for the End Customer and Distributor organizations’ own privacy policies or data processing agreements and to describe the general data protection principles of the Service to Users.

This document is an integral part of each agreement between Secapp Oy and its customer organizations about personal data processing, together with the other content of each such agreement containing the details required by paragraphs 3 and 4 of the Article 28 ("Processor") of the GDPR.

DATA CONTROLLER

The customer organization (End Customer) of either Secapp Oy or of Distributor of Secapp Oy, which has acquired the right for its named Users to use the Secapp System, acts as the personal data controller of the Users’ personal data in the System. Secapp Oy (Finnish business ID 2411828-1), Viitaniementie 21 E 47, 40720 JYVÄSKYLÄ, Finland, acts as the personal data processor or subprocessor based on an agreement with its customer organization or Distributor.

CONTACT PERSON REGARDING PERSONAL DATA

Regarding the processing of personal data related to the Service, the User should primarily contact their own organization (End Customer), which acts as the personal data controller. For End Customer organizations using the Secapp Service, the contact person should be verified from the person in the User's organization who is responsible for administering the Secapp Service, such as the nearest supervisor or manager.

In the Secapp System, each End Customer Account may be divided to several organizations ("companies") with different names, and the End Customer acts as the data controller for all of them. The User may be connected to one or several of such organizations.

If the User has been connected to several End Customer Accounts, or participates in communications of another End Customer, such as group discussions, each End Customer is responsible for the data of their organization and therefore the User's personal data may have several personal data controllers.

The Secapp contact person of Secapp Oy's customer may ask Secapp Oy for more information about the personal data processing, if necessary. The information security officer responsible for providing information to the Secapp contact person is Antti Hämäläinen, tietosuoja@secapp.fi.

LEGAL BASIS AND PURPOSE OF PROCESSING OF PERSONAL DATA

The purpose of processing personal data on behalf of the customers is to deliver, provide and improve the Secapp Service and provide the related customer communication. The service includes, for example, User specific messaging functionality and functionality for managing operations, and for these purposes names of Users, contact information and messages and information sent or received by Users are stored in the System.

Secapp Oy only processes information provided by the User, the End Customer or Distributor themselves or which are created through the use of the System.

The legal basis for the processing of personal data, in accordance with the EU General Data Protection Regulation, is the fulfilling of the agreement between Secapp Oy and its End Customer or Distributor.

CATEGORIES OF PERSONAL DATA

The categories of personal data of Users are as follows:

- User accounts and other authentication information
- Basic information including, but not limited to name, telephone number, email, address, and the company/organization or organizations using Secapp where the person works or operates
- User's group, skill and qualification information
- System usage settings, such as permissions or restrictions to collect and store location information and history
- User groups and user permissions
- Possibly User's location information to be used to target messages to users based on geofencing and to locate the user if the situation requires so.
- Operating system information of the smart telephone for message delivery
- Content of messages between Users, which may include for example text and images, video and audio recordings, location information and various files.
- Database content defined by the End Customer in the documentation component of the System, as well as attachment files such as for example text documents, spreadsheets, images or video files
- Information about the usage of the Service, such as for example log and audit trail information
- Actions related to messages or message material, such as reception confirmations or choices
- Log data of possibly voice or video connections between Users. Note: Any content of such voice or video connections is not stored, and therefore no personal data is created from them.
- Other significant data entered in the System by End Customer or User.

USE OF LOCATION INFORMATION

In some cases, if User is using the Secapp Service on a mobile application, User's mobile device based location information can be used to target messages or locate the User. This happens only if 1) User's End Customer Organization is using the location functionalities, 2) location settings are active in User's settings, 3) User has given the mobile app the required permissions to location information. When used, the location information may be based on the mobile device operating system's location features, which may be based on for example GPS or information from different kinds of other

wireless connections, depending on the device hardware and settings, and which may vary in its accuracy accordingly.

The location settings can at any time be disabled by the User and the Service will then otherwise work normally. This may, however, reduce the usability of the Service for the intended purpose of the End Customer and for example location based messages may not reach all intended Users, depending on the scenario. Users may, however, set their location manually in the app settings to receive some location based messages.

Each End Customer organization may have their own reasons for using location information, such as for example the ability to send messages or alerts to Users in a specific area, or the need to receive location information from employees in different ways when they work alone in dangerous situations. To ensure correct delivery of alerts, a User may need to give the mobile application the permission to always access location information ("location access in the background") including when not using Secapp.

If the location use is enabled in an organization, all of its Users can still disable or restrict the use of location information in different ways, which depending on the End Customer organization may include settings related to collection and storing of data and restricting location information use to specific times, such as work time, or to specific colleagues.

The organization (End Customer) should inform Users of the location features used in their organization as a part of their personal data controller responsibilities. If Users do not know why the location is required, they may always disable the location features in their Secapp user account settings and reject the location permission for the Secapp mobile app. The organization administrators should ensure that Users are aware of the required location settings, so that turning location features off does not result, for example, in missing alerts related to dangerous situations.

REGULAR SOURCES OF INFORMATION

Personal information is primarily collected directly from the Users (data subjects themselves or the main users of End Customer) when they are using the Service.

Personal information is additionally stored at the beginning of the customer relationship and registration. The initial basic information about the Users stored in the System is obtained from the End Customer or Distributor via e.g. web forms, e-mail, telephone, contracts, customer meetings and other situations in which the End Customer or

Distributor transfers the information for processing. Personal data can also be collected and updated directly from the End Customer's own corresponding systems, such as for example by a technical integration with End Customer's user management software. When using the Service, some information may be collected from other systems related to the Service, such as for example when Users send information with a telephone text message (SMS).

Secapp Oy does not obtain personal data to the Secapp System from a commercial or third party.

TRANSFER OF INFORMATION

Secapp Oy does not transfer personal information in the System to third parties unless:

1) separately agreed with End Customer or Distributor,
2) it is necessary for the functionality of the service as agreed with End Customer or Distributor, for example by relaying text message alerts or public authority network messages (TETRA) to Users through a telecommunications carrier,
3) if separately agreed with End Customer or Distributor, limited data may also be transferred automatically to systems used by End Customer or Distributor through a technical integration, or to third parties, such as to suppliers of optional additional services to the Service.
If needed, the User may ask End Customer or Distributor for more detailed information about the agreed information location and possible transfers.

Furthermore, Secapp Oy acts within the limits permitted and required by the applicable legislation e.g. when responding to requests for information from the authorities.

In the Secapp System it is possible to join a single User (account) to several End Customer Accounts, if none of the End Customer Accounts, managed by End Customers, to which the User belongs have restricted this in the settings and both End Customer Accounts are in the same server environment. In such case, the main user of another End Customer may add the User to their End Customer Account based on the individual User account communicated by that User. In such case, the basic information of the user account (name, and if the account has not restricted this and such information is registered, the email address and phone number) will be transferred to the other End Customer. In such case, both End Customers will have the data controller rights to control the basic information of the user account, but no other rights or access to another End Customer's data. Each End Customer will otherwise act as the personal data controller for End Customer Account specific messages and other information.

In some cases, the User of an End Customer may create group messaging functionalities belonging to a particular End Customer Account, between Users of different End Customer Accounts, and in such case the content of each message is sent (transferred) from their End Customer to the Users from other End Customers who belong to the same group, and the content will be visible to them, as well as the names of all members of the group. Each group discussion belongs to a particular organization, and the End Customer managing that organization acts as the data controller for that group discussion. There may be customer specific agreed restrictions to group discussions and joining Users to another End Customer's account.

The data will not be processed or transferred outside the European Union or the European Economic Area, unless agreed with the Customer. The Customer and Users may, however, use the System with an Internet connection or message delivery connections from anywhere, and information will then be transferred between the used terminal device and Secapp System.

PROTECTION OF THE PERSONAL DATA AND DATA RETENTION PERIOD

The data stored in the service is protected by technical and organizational methods. The data is collected using telecommunication connections to the databases and file systems of the Service. The telecommunication connections required to use the System are encrypted and the System is generally protected by firewalls and other technical means. The servers used by the Secapp System are located in locked and guarded premises, where the data can only be accessed by certain predefined persons responsible for the maintenance of the servers, or in premises defined by the End Customer or Distributor in special cases. The information security is described in more detail in each agreement between Secapp Oy and the End Customer or Distributor. The customer of Secapp Oy may also request additional information about the information security.

Access to the Secapp System requires at minimum entering a username and password and, optionally upon End Customer decision, two-way authentication using for example an SMS (mobile phone text message). Each End Customer or Distributor defines the Users, who are given a user account to the End Customer Account of that data controller (End Customer) within the limits of their user permissions, or whose user account, which is already used at another End Customer in the Secapp System, is added to the account of the End Customer.

Everyone who processes the personal data on behalf of the Secapp Oy has signed a personal non-disclosure agreement. The personnel of Secapp Oy has been instructed

about the legislation related to personal data processing and ensuring information security and only those have access to the data, who require the data in their work in order to deliver the Service.

The object and duration of the processing of personal data is defined as follows: Secapp Oy shall process personal data only as long as the providing service pursuant to the Agreement to the Customer requires it.

The personal data controller (End Customer) or Distributor defines the retention period for the data processing and can erase personal data from their End Customer Account. Secapp Oy will process personal data as long as required for delivering the Service to the customer based on the End Customer Agreement or Distributor Agreement, and will agree about the processing and erasure of data with their agreement party. Typically the personal data will be erased latest after a period of time, specified in the agreement or agreed upon ending the Service, after the agreement about the Service has ended and the customer has stopped using the service. Some data, such as different kinds of log data and audit trail data regarding the use of the Service, may have a different, data type specific retention time, so that for example events related to information security can be investigated afterwards using that data if necessary.

RIGHTS OF THE DATA SUBJECT

If the End Customer (personal data controller) operates in the EU area, the data subject (User) has the right to inspect the personal data stored in the System and the right to request the rectification and deletion of the data (“right to be forgotten”) or the right to restrict the processing in certain situations. Relevant requests should be addressed to the data controller, which is the Customer organization. The data subject also has the right to lodge a complaint about the processing of personal data with the competent supervisory authority.