

Instant Messaging Groups Privacy Statement

Table of Contents

Controller	1
Contact person for the registry	1
Purpose and legality of the processing of personal data	2
Data content of registers	2
Regular data sources	2
Regular disclosures and transfer of data outside the EU or the EEA	2
Storage period of personal data	2
Register protection principles	3
Duty to inform	3
Right to inspect and to demand rectification	3

This privacy statement applies to the personal data register of Suuri Armo ry called Instant Messaging Groups.

Created 23.2.2020, updated 18.1.2025 RH, updated 19.8.2026 RH, KH, translated from Finnish 19.8.2026 KH

Version: 19.8.2026

Suuri Armo (registered association) collects and maintains personal data registers in order to carry out the task defined in its rules and related services in the churches it maintains. This privacy statement is a register and data protection statement in accordance with the EU General Data Protection Regulation 2016/679. By 'register' we mean an information system in which personal data are processed.

Controller

Suuri Armo ry, Business ID 0609764-0 Privacy Officer Riitta Holm riitta.holm@armossa.fi	Domicile of Turku Hämeenkatu 28, 20700 Turku www.raamattupuhuuturku.fi
---	--

Contact person for the registry

Enquiries and requests concerning personal data are answered by Maaret Severinkangas, tel. 045 279 8009, maaret.severinkangas@armossa.fi, Hämeenkatu 28, 20700 Turku.

Purpose and legality of the processing of personal data

The purpose of the processing is to carry out internal communication.

Legality is based on the person's request to join the group.

Personal data is not used for direct marketing. The processing does not involve data profiling or automated decision-making.

Data content of registers

According to the instructions shared by the association, the person's phone number and a recognizable name are required to join the groups; a first name alone is usually enough. You can also hide your phone number. Everyone agrees to the privacy policies of that application, such as Signal and WhatsApp, when joining the service, and group settings when joining the group.

Regular data sources

The source of data is the group member himself. In several groups, group members can send messages to the group. Members are responsible for their own profile and the messages they publish. A new member shall be added to the group only after expressing his or her consent. A member may choose to leave the group. Signal and WhatsApp communication groups operate on an external platform.

Regular disclosures and transfer of data outside the EU or the EEA

By joining an instant messaging group, a person demonstrates that they accept the disclosure of their information (at least an identifiable name) to the group membership list, from which it is visible to other group members, and the disclosure of their own messages to the members of the group. In addition, he agrees to the privacy policies of the platform he uses. The disclosure of data outside the groups cannot be monitored.

Storage period of personal data

A member of the group can leave the group at any time, but as a rule, they cannot delete their messages or attachments from the group members. Other members of the group may have copied their name and the other information they have provided about themselves.

Register protection principles

Large groups have a member of the administration as an administrator. They observe the messages and give instructions concerning personal data if needed. Messages published in the group are available to all members of the group. Guidelines for good practice, approved by the association, are distributed. Administrators cannot prevent group members from using the information in violation of the good practice.

Duty to inform

The privacy statement is published on the website www.raamattupuhuuturku.fi and in connection with the collection of personal data.

The data subject shall be informed without delay if the confidentiality, integrity, or availability of the register has been compromised so that it is likely to pose a high risk to the rights and freedoms of the data subject, for example in the form of identity theft, payment fraud, or other criminal activity. The necessary authorities are informed already when the data breach is detected.

Right to inspect and to demand rectification

Data subjects have the right to check their data stored in the personal data register, to correct any incorrect data, and to request the deletion of their data. The request must be made in writing to the controller's contact person. The applicant must prove his or her identity. The data subject has the right to lodge a complaint about the processing of their personal data with the Data Protection Ombudsman, P.O. Box 800, P.O. Box, 00521 Helsinki, Finland, tel. +358 29 566 6700.