

# Privacy Policy of auth.fi authentication service

V1.6, 23.2.2021

## Data Controller

Radiator Software Oy (1806724-6) ("Radiator Software")

Varastokatu 3 A

33100 Tampere

Finland

[support@radiatorsoftware.com](mailto:support@radiatorsoftware.com)

## Contact Person in Personal Data Matters

Karri Huhtanen

Varastokatu 3 A

33100 Tampere

Finland

[support@radiatorsoftware.com](mailto:support@radiatorsoftware.com)

## Name of the Register

auth.fi identification service

## Purposes of Processing and Legal Basis for Processing

For user account verification, the auth.fi authentication service uses an email address or a phone number. This email address or a phone number used for the user account verification may be the user's personal email address or phone number. The user account, or the email address or phone number connected to the account, is used for authenticating the user and for authenticating and logging user's actions within the service (such as user account registration and renewal). The user account and the email address or the phone number connected to the account is used also for error diagnostics and solving of errors of the service, and for diagnosing the error in the user's authentication session as well as for diagnosing the abuse and suspected abuse cases. The auth.fi authentication service provides interfaces for service integration. To limit, oversee or diagnose the functionality of these interfaces, personal information (such as user account, phone number or email address) of persons authorized to use interfaces may be used.

When the person is from Radiator Software's customer organization, the personal data may be processed also for the purpose of offering Radiator Software's products and services, fulfilling contractual obligations or to conduct actions prior to entering into a contract and for using Radiator Software's contractual rights.

In addition, statistics may be created on the usage of the service. Personal data may be processed also for the purpose of developing Radiator Software's products, services and business (such as for investigating and correcting errors). After anonymization of personal data, the data is no longer personal data.

Personal data may be processed for the purpose of taking care of data security and to prevent fraud. Compliance with a legal obligation and Radiator Software's legitimate interests are the legal basis for processing of personal data for these purposes.

Personal data may also be processed for the purpose of providing notifications regarding Radiator Software's service.

Based on a person's consent, personal data may also be processed for the purpose of direct marketing of Radiator Software's products and services and for the purpose of delivering newsletters.

Unless otherwise stated above, Radiator Software's legitimate interests are the legal basis for processing of personal data.

In situations where the processing is based on a person's consent, the person has the right to withdraw his/her consent for the processing. The withdrawal of the consent does not affect the lawfulness of the processing based on the consent before the withdrawal.

To the extent the processing is based on Radiator Software's legitimate interests, a legitimate interest is e.g. a customer or a user relationship with Radiator Software, or the person may otherwise expect the processing. The person's interests or fundamental rights and freedoms for the protection of personal data do not override such legitimate interests.

## Content of Register

- User account:
  - Email address for those using organization specific authentication
  - Completely or partially randomized guest username
- The latest randomized password set for user account
- The latest IP address used in requesting or creating the user account
- The latest IP address from which the user account has been verified
- The latest IP address from which the user account had been requested for renewal
- The email address or phone number, which has verified the user account
- The information provided by a possible 3<sup>rd</sup> party authentication service that is necessary for network access or the user account verification
- From each authentication event ending up into service, if user's device or home organization's configuration provide this information:
  - User account
  - IP and MAC addresses of the device performing the authentication, possibly the network name
  - IP and MAC addresses of the user device authenticated

- The start and end time of user's session
- The amount of data transferred in the user's session
- The reason for ending or aborting user's session or authentication
- Other information relating to the user's session provided and relayed by the device performing authentication
- From each authentication event, if the network devices or authentication servers participating to the authentication event provide this information:
  - User account
  - IP and MAC addresses of the device performing authentication, network name
  - IP and MAC addresses of the user device authenticated
  - The start and end time of user's session
  - The amount of data transferred in the user's session
  - The reason for ending or aborting user's session or authentication
  - Other information relating to the user's session provided and relayed by the device performing authentication
- Information provided by user's WWW browser regarding the user device and the browser when the user is using the service or service interfaces
- The MAC addresses and/or user accounts added to service's allow and deny lists, and the user or interface accounts used to add, modify and delete this information
- The information provided via service interfaces (such as allow/deny list information, end user's user account, MAC address, interface user's IP address, interface user's user account, email address or API token) and the logs of interface use created by the WWW server software

Home organization is the organization providing the Wi-Fi or other network to which the user is requesting access or to which the user receives access, or the organization, which authenticates the user or on whose behalf the user is authenticated.

## Regular Sources of Data

The user registers, without or with the help of the home organization's IT administration, the user's email address as a user account to the service, or verifies an automatically generated user account with an email address, phone number or external authentication service. By accessing a network with the user account, the user uses the authentication service to get access to the network. The user of a service interface may provide, via the service interfaces, additional information (such as allow/deny list information, end user account, MAC address, interface user's IP address, interface user's user account/email address/API token).

## Regular Transfers of Personal Data

Personal data may be transferred to the service's home organization. In such a case the home organization is another controller of the personal data regarding the personal data it has received, in accordance with its own privacy policies and practices. Personal data may be also transferred to authorities, if the authority is entitled to receive the personal data

pursuant to law. Radiator Software is not responsible for the processing or transfers of personal data by the home organization or authorities.

## Transferring Personal Data outside of EU or EEA and Suppliers

Radiator Software and/or its suppliers and/or its suppliers' subcontractors may transfer personal data outside of the European Economic Area (EEA) and European Union (EU). In such cases the applicable legislation (such as EU's General Data Protection Regulation) and the requirements stipulated therein are followed.

***There may be differences in fulfilling a person's rights set forth in this Privacy Policy depending on who is the supplier of Radiator Software, to whom e.g. the request for access or rectification is made.***

Radiator Software's current suppliers and how they process personal data is described e.g. in the following:

<https://radiatorsoftware.com/gdpr/>

<https://www.salesforce.com/uk/company/privacy/>

<https://www.mailgun.com/gdpr/>

<https://www.clockworksms.com/blog/gdpr-update/>

<https://cloud.google.com/terms/data-processing-terms>

Between Radiator Software and its suppliers, the data protection agreement between Radiator Software and the relevant supplier is applied.

The verification email may, e.g. depending on the user's or home organization's email service provider, be transmitted without encryption via or to the countries outside of the EU or EEA. The verification email is sent to the email address provided by the user and contains (in addition to general instructions) also a verification link with respect to the user account. The user account and the network access can be verified also by a confirmation link sent by SMS, and the SMS and the verification may be transmitted via or to the countries outside of the EU or EEA.

If the user chooses to use an external authentication service to verify the access to network or to verify the user account, these 3<sup>rd</sup> party servers may reside outside of the EU or EEA or the external service provider may process the data outside of the EU or EEA. The service provider can select the authentication and verification methods available to the user.

## Retention Period of Personal Data

Personal data is processed by Radiator Software as long as it is necessary to fulfill the purposes stated above in "Purposes of Processing and Legal Basis for Processing" pursuant to applicable legislation in force from time to time. For instance, the personal data of customers' representatives may need to be processed until liabilities related to the personal data have expired and claims can no longer be made against Radiator Software. For instance, the main rule for expiry of debt is three (3) years, and it may be necessary to store evidence on fulfilling the person's rights even for a longer time period.

The network log-in information is stored by Radiator Software usually approximately for 390 days.

## Right of Access

A person has the right to obtain confirmation from Radiator Software as to whether or not personal data concerning him or her is being processed.

If the person's personal data is being processed by Radiator Software, Radiator Software provides, upon request, to the person a copy of the personal data undergoing processing as well as the information required to be given pursuant to personal data legislation.

If the person asks for any further copies, Radiator Software may charge a reasonable lawful fee.

## Right to Request Rectification

A person is entitled to require that Radiator Software rectifies without undue delay inaccurate and incorrect personal data regarding the person. Taking into account the purposes for which the data was processed, the person has a right to have incomplete personal data completed.

## Right to Request Erasure

Radiator Software will erase, upon a person's request, the personal data regarding him or her, if any of the following conditions is fulfilled:

- (a) the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- (b) the person withdraws the consent on which the processing was based, and there is no other legal ground for the processing;
- (c) the person objects to the processing and there are no overriding legitimate grounds for the processing;
- (d) the personal data has been unlawfully processed;
- (e) the personal data has to be erased in order to comply with a legal obligation applicable to Radiator Software; or
- (f) the personal data has been collected in connection with offering information society services.

However, Radiator Software is not obliged to erase the personal data, in case processing of the personal data is necessary for:

- (a) for exercising the right of freedom of expression and information;
- (b) for compliance with a legal obligation which requires processing by law to which Radiator Software is subject or for the performance of a task carried out in the public interest;

- (c) for reasons of public interest in the area of public health;
- (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or
- (e) for the establishment, exercise or defence of legal claims.

## Right to Restriction of Processing

“Restriction of processing” means the marking of personal data so that its use will be limited in the future.

Radiator Software limits the processing of personal data upon the person’s request in the following situations:

- (a) the person contests the accuracy of the personal data, for a period enabling Radiator Software to verify the accuracy of the personal data;
- (b) the processing is unlawful and the person opposes to the erasure of the personal data and requests the restriction of their use instead;
- (c) Radiator Software no longer needs the personal data for the purposes of the processing, but the personal data is required by the person for the establishment, exercise or defence of legal claims;
- (d) the person has objected to processing, but verification whether the legitimate grounds of Radiator Software override those of the person is still ongoing.

In the above-stated situations Radiator Software processes the personal data only in the following situations:

- (a) based on the person’s consent;
- (b) for the establishment, exercise or defence of legal claims;
- (c) to protect another natural or legal person’s rights; or
- (d) for reasons of important public interest of the European Union or of a European Union member state.

## Right to Object

A person has the right to object, on grounds relating to his or her particular situation, to processing of personal data concerning him or her in case the processing is based on any of the following: (i) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Radiator Software, or ii) the processing is necessary for the purposes of the legitimate interests pursued by Radiator Software or a third party. In such a case, Radiator Software is not allowed to process the personal data, unless Radiator Software can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the person or for the establishment, exercise or defence of legal claims.

## Right to Data Portability

If the processing of personal data is based on the person's consent or a contract with the person and if the processing is carried out by automated means, the person is entitled to, upon request:

- (a) to receive the personal data concerning him or her which he or she has provided to Radiator Software, in a structured, commonly used and machine-readable format; and
- (b) if technically feasible, to have the personal data transmitted to another controller.

## Right to Lodge Complaint with a Supervisory Authority

If a person considers that Radiator Software processes personal data in violation of data protection legislation, the person may lodge a complaint with the Office of the Data Protection Ombudsman in Finland or other competent supervisory authority of a EU country.

The contact information of the Office of the Data Protection Ombudsman in Finland is:

<https://tietosuoja.fi/en/office-of-the-data-protection-ombudsman>

## Automated Decision-Making

Radiator Software does not process personal data in automated-decision making meant by the EU's General Data Protection Regulation.

## Methods How Register is Secured

### Manual material

As a main rule, there is no manual material.

### Information processed automatically

The connections to the service are encrypted with HTTPS protocol. The email service between the service and the user's home organization may be encrypted depending on the service settings of the sending and the receiving end. In Radiator Software's systems, data saved in electronic format is stored in systems which are protected with firewalls from contacts coming outside of the service provider and the home organization. The administrators at Radiator Software have been defined their own limited user rights and accesses to the data included in the service, and these are protected at least with user names and passwords. Logs of service usage are saved (maintenance use, user account registration and verification, authentication events). Home organization, its service providers, telecom operators and similar operators may see personal data contained in the service. Each administrator of Radiator Software has maintenance and/or browsing right only to such data which is necessary for the user's role. Radiator Software's information system is protected and only named users with personal user names and passwords may access it.

Each employee processing the register and identification event data on behalf of Radiator Software has committed to confidentiality.