PRIVACY STATEMENT PUBLICROAM

First of all, we would like to thank you for choosing to use our service, called “publicroam”. In this document, which we have named the “Privacy Statement”, we explain which data we process about you when you use publicroam, what we do with this data, how we ensure the security of your data, and which rights you have in relation to your privacy.

Our identity

We are Publicroam B.V., located in Zeist at Driebergseweg 2, The Netherlands, and registered with the Dutch Chamber of Commerce under number 70318433.

The service “publicroam”

Publicroam is an authentication service for Wi-Fi networks. By using publicroam for the first time, you create a “publicroam account” (to be regarded as a virtual identity) which enables you to connect safely and easily to Wi-Fi networks of organisations that use publicroam (hereinafter referred to as “host organisations” and their Wi-Fi networks as “Wi-Fi guest networks”).

It is important to understand that publicroam is not an internet access service or any other (tele)communications service. The publicroam service only verifies your virtual identity (by means of your “publicroam account”) so that you, as a user, can be authenticated to access the Wi-Fi guest network of the host organisation.

Publicroam and privacy

Publicroam provides access to Wi-Fi guest networks; we do not trade in data. This means that we do not collect and resell personal data, and we do not track you. And this will never happen. The data that is collected is only needed for authentication and to ensure the service functions properly. So no user profiles, no personalised advertising, and no covert practices.

Our policy is that personal data is processed and secured with care. This means that:

- it is clearly stated for which purposes your personal data is processed;
- your explicit consent is requested for processing your personal data in cases where consent is required;
- the collection of personal data is limited solely to what is necessary for the purposes for which it is processed;
- personal data is not passed on to third parties, unless necessary to provide the requested service or where there is a legal obligation to do so;
- where personal data is shared with third parties, agreements are made to ensure that such data is not used for other purposes;
- appropriate security measures are taken to protect personal data.

Publicroam has agreed with host organisations that they will carry out their processing activities in line with Publicroam’s policy on processing and securing personal data, as described in this Privacy Statement.

Why using publicroam enhances your security

Publicroam helps safeguard your security, as well as that of other users of the Wi-Fi guest network and the host organisation. Security experts generally advise against the use of public Wi-Fi networks without such protection, as unauthorised parties may otherwise gain access too easily to your device (for example, your laptop, smartphone, or tablet) and the data you store on it.

For your own safety, it is therefore recommended to use public Wi-Fi networks only if they employ publicroam or a similar form of protection. If you would like to know more about the security of publicroam, please refer to the section “Security”.

Applicability of this Privacy Statement

This Privacy Statement applies to our processing of your data when using publicroam. In this declaration, we wish to provide insight into how personal data is processed when using publicroam, and therefore also explain aspects of the processing carried out by the host organisation. The host organisation may provide further information on how it processes your data in its own privacy statement. Any such privacy statement must always be in line with Publicroam’s policy and the agreements made regarding the processing and security of personal data.

Roles, responsibilities, processed data and retention periods

Data we are responsible for

Publicroam account

If you register an account with publicroam in order to connect to a Wi-Fi guest network of a host organisation, we are responsible for processing the data in your publicroam account, for the purpose of authentication.

This concerns the following data:

- Publicroam username and password
- Email address
- Mobile phone number
- The MAC address of the device you use to connect to a Wi-Fi guest network
- Timestamps of request and activation of the publicroam account
- Organisation(s) where the publicroam account was requested and activated
- Data about the Wi-Fi guest network to which you are connected
- Content and traffic data of SMS messages used to request a publicroam account

Retention period of publicroam account data:

Your publicroam username and password, email address, mobile phone number, and location/time of account request and activation are retained for as long as your publicroam account remains active. You may cancel your publicroam account at any time. If you do not use publicroam for 12 months, your account will be terminated automatically. Your data will be deleted no later than six months after cancellation or termination. Other data, including the MAC address and data about the Wi-Fi guest network you connected to or attempted to connect to, will be retained for a maximum of three months. If we are legally obliged to retain data for longer, we will comply with this obligation. Data flagged due to misuse or suspected misuse may be retained for as long as necessary to determine definitively whether misuse occurred and to take any legal action in response.

Support

We are also responsible for processing your data if you contact our support. This may include your email address, first and last name, phone number, and other personal data you provide to us. This data will be deleted within 3 months after we consider your query to be fully resolved.

Service messages

If you have a publicroam account, we process data to send you service messages, such as security updates. This may include your email address and phone number. This data is retained for as long as your publicroam account remains active. You may cancel your publicroam account at any time. Your data will be deleted no later than six months after cancellation.

Newsletter

If you choose to receive the publicroam newsletter, we process your email address. This will be retained for as long as you are subscribed to our newsletter. You may unsubscribe at any time via the link in the newsletter.

Data the host organisation is responsible for

Authentication data for access to the Wi-Fi guest network

The host organisation is responsible for processing all authentication data that the Wi-Fi access point (the device that transmits and receives the signals of the guest network) must technically process in order to allow you to use the Wi-Fi guest network. This may include the following data:

- Your Publicroam username
- The MAC address of the device you use to connect to a Wi-Fi guest network
- The time and duration of your connection with the host organisation's Wi-Fi guest network
- Data about the host organisation's Wi-Fi guest network you connected to or attempted to connect to

Publicroam and the host organisation have mutual agreements regarding the processing of authentication data that publicroam receives from a host organisation. This may include the following data:

- Your Publicroam username
- Time of your connection with the host organisation's Wi-Fi guest network
- Data about the host organisation's Wi-Fi guest network you connected to or attempted to connect to

Retention period

Authentication data is retained for a maximum of 3 months after the termination of the connection with the Wi-Fi guest network, unless the data must be retained longer to combat misuse or where there is a legal obligation to retain the data longer. If data must be retained longer to combat misuse, it will be kept for as long as necessary to address the detected misuse, and otherwise for a maximum of 3 months.

Purposes and legal grounds for processing

We process your data solely to enable you to connect safely and conveniently to Wi-Fi guest networks of our host organisations. The legal basis for processing is primarily the performance of a contract with you (Article 6(1)(b) GDPR). By using publicroam, you also give your consent for your data to be processed in accordance with this Privacy Statement (Article 6(1)(a) GDPR). Additionally, we process data on the basis of our legitimate interest in offering publicroam and in protecting our services and the connected Wi-Fi guest networks against unauthorised access and misuse (Article 6(1)(f) GDPR). If we are required by competent authorities or by law to retain data (Article 6(1)(c) GDPR), we will comply with that obligation.

We will never sell your data

We do not use your personal data for any purposes other than enabling you to use publicroam and the connected Wi-Fi guest networks. We never sell your data to third parties.

Engaged third parties and confidentiality of your data

All employees of publicroam must comply with this Privacy Statement and treat your data confidentially. If we engage third parties to process your personal data on our behalf, we enter into an agreement (known as a 'data processing agreement') to ensure the confidentiality of your data. Third parties we engage who may receive your personal data to process it confidentially on our behalf may include, for example, a telecom provider used to send you SMS messages from publicroam, or a provider of highly secure hosting or data centre services.

Anonymous statistics

We may process fully anonymous data to map the general use of publicroam and the Wi-Fi guest networks (at an aggregated level) and to improve these services. Such aggregated data, for example the average number of users connected during a given period, may also be used in communication with third parties, such as potential customers and the media. This anonymous data can never be traced back to you or any other individual user.

Storage and security of data

We take appropriate measures to secure your use of the Wi-Fi guest networks as effectively as possible. Only employees who need access to your data for the performance of their duties are granted access. Among other things, we implement the following security measures:

- Technical, organisational, and physical security measures for access to our own systems, including:
  - Restrictive access policy based on need-to-know or need-to-process;
  - Logical access control of our systems using passwords;
  - Locks, CCTV surveillance, and other physical security measures for areas where personal data is processed;
- Technical measures for the security of Wi-Fi guest networks, including:
  - WPA2-Enterprise and AES support;
  - IEEE 802.1X with the Extensible Authentication Protocol (EAP);
  - Routable IP addresses;
  - VLAN separation.

Access, rectification and right to object

If you wish to know which data we have stored about you, please contact us using the options listed under 'Contact'. Please include your mobile phone number linked to your account. We will contact you within 2 weeks. If the overview we provide contains inaccuracies, you may submit a written request to have the data corrected or deleted.

We handle requests or complaints on behalf of the host organisation, unless they concern an account flagged for misuse or suspected misuse. In such cases, the host organisation itself may handle the request or complaint.

Complaints – Dutch Data Protection Authority

Should you have a complaint, you can always contact us via the details listed at the end of this document. Under privacy legislation, you also always have the right to lodge a complaint with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) about our processing of your personal data. You can contact the Dutch Data Protection Authority via https://autoriteitpersoonsgegevens.nl.

Amendments to the Privacy Statement

We may amend this Privacy Statement if necessary. The latest version will always be available on our website. If you wish to stay informed about changes, please visit our website regularly. Should we wish to make a change requiring your consent, we will of course request your consent in advance.

Contact

You can contact us by email or telephone:

support@publicroam.nl
+31 30 307 44 99