ePrivacyseal

# C E R T I F I C A T E

**no. 354/21**

ePrivacyseal GmbH
Große Bleichen 21, 20354 Hamburg, Germany

hereby certifies* that

as determined in the certification decision of 09 June 2021

**Roq.ad GmbH**
Taubenstrasse 26, 10117 Berlin, Germany
as a processor in the sense of art. 4(8) GDPR

operates its product or service
**„Roq.ad cross-device platform“**
version 26/05/2021
as defined in annex 1 and to the exclusion of the processing activities in annex 2 to this certificate

in conformity with the criteria catalogue of ePrivacyseal GmbH, version 2.1. of May 2018.

final audit day: 06/06/2021
next planned monitoring by 21/06/23
period of validity: 22/06/2021 – 21/06/2023

*ePrivacyseal GmbH is not an accredited certification body within the meaning of art. 42(5) GDPR.

**Annex 1 to certificate no. 354/21**

**Definition of processing activities**

Roq.ad provides a cross device user recognition technology. The devices on which users are recognized are PCs, tablets, and smartphones. Using a tracking pixel and third-party data, users can be served targeted advertising across multiple devices (cross-device user recognition), and customers are provided with analytics and attribution data (probabilistic mapping of device identifiers).

The process of Roq.ad's services can be described in following steps:

1. A user's activity in internet is tracked with:
    a. tracking pixels placed on Roq.ad's partner websites (all device types)
    b. tracking pixel placed in online ads (all devices)
    c. data obtained from partners
2. When an user visits websites and launches mobile applications mentioned above, events are sent to Roq.ad's tracking server.
3. Roq.ad collects only data from users that have given their consent. Consent is managed using the IAB consent framework. All data sets contain an IAB TCF-compliant consent string, or the data partner is contractually required consent from the user in question.
4. Based on these events, Roq.ad is able to:
    a. deterministically connect different browsers and devices based on some common factors sent by a tracking code (like hashed e-mail or hashed login)
    b. probabilitically connect browsers and devices based on different sets of attributes (like hashes of IP addresses changing over time, user agents, behavioural data)
5. In parallel with this tracking process, Roq.ad's code performs a cookie-matching procedure (exchange of an anonymous user ID with other internet companies) with:
    a. DSPs (demand-side platforms)
    b. DMPs (data management platforms)
6. With these external DSP IDs, Roq.ad is able to run campaigns on these platforms targeting different audience groups.
7. After an user accesses a website using a mobile device, and the website is part of Roq.ad's network of publishers (hereinafter also referred to as "partners"), a cookie is set in the web browser of the user by the tracking pixel.
8. If the same user has a second device, a matching can take place because of a similar IP address and other methods of Roq.ad's algorithm like similar user behaviour, similar user features, etc. This enables Roq.ad to conclude that the two devices probably belong to the same person.
9. The matching also can be carried out using login data (user name or email address). If a user uses a service on multiple devices (e.g. social networks, email clients), these login data are hashed via SHA256 before Roq.ad receives them from its partners, and if the hash value matches, the chance that multiple devices belong to one person is high.

**Annex 2 to certificate no. 354/21**

**Excluded processing activities**

This evaluation refers only to the product mentioned above and therefore only to the processes in which roq.ad is involved with its customers. B2B processes between the company and its customers have not been taken into account in this evaluation.