

Privacy Policy

In **Roivenue s.r.o.**, with its registered office at Milady Horákové 116/109, Hradčany, 160 00 Praha 6, Czech Republic, registered with the Commercial Register kept by the Municipal Court in Prague under file no. C 289445, CRN: 06812279, VAT ID: CZ06812279, a member of the ScanmarQED group (**Roivenue**”, “**we**” or “**us**”), we, as a data controller, pay great attention to protecting your personal data.

This Privacy Policy describes how we process personal data in connection with (i) our website at www.roivenue.com (“**Website**”), (ii) the **Roivenue Platform** (“**Platform**”), our cloud-based marketing-attribution and marketing-data integration Software-as-a-Service offering and (iii) the **Roivenue MCP Connector** (“**MCP Connector**”), our official Model Context Protocol connector that lets authenticated Clients and Platform users query their own Roivenue Platform data from within MCP-compatible AI assistants, including Anthropic’s Claude, OpenAI’s ChatGPT and Microsoft Copilot, using natural language.

It explains for what purposes we process your personal data, from which sources we obtain this data, who processes your personal data on our behalf, to whom we transfer it, and how we ensure the security of your data. In the last sections, we set out what rights you have when we process your personal data and how you can exercise them.

This Privacy Policy may be amended from time to time to reflect changes to our services, applicable law or our processing activities. The latest version of this Privacy Policy shall always apply and will be made available on the Website.

THIS VERSION OF PRIVACY POLICY HAS BEEN EFFECTIVE SINCE 1ST AUGUST 2026.

Note on client model and attribution data. When we process personal data on behalf of our Clients in connection with the provision of the Roivenue Platform or when you are operating with the MCP Connector regarding Platform data (for example, marketing-performance datasets, CRM exports or advertising-platform feeds that the Client provides to us or that we ingest on the Client’s behalf), we act as a **data processor** and the processing is governed by the Data Processing Agreement that forms part of our Terms and Conditions, not by this Privacy Policy.

A. CATEGORIES OF PERSONAL DATA WE PROCESS

Below are the categories of personal data, including examples that we process for the purposes set out in the following section. We refer to these categories in other parts of this Privacy Policy.

- A.1. **Identification data.** Name and surname (and, where relevant, job title), so we can identify you while concluding or fulfilling a contract with you or the entity you represent, or while you are using the Platform.
- A.2. **Contact details.** Business e-mail address, business telephone number and the company you represent, so we can make the Platform available to you and communicate with you.
- A.3. **Account and login data.** Username, hashed password, multi-factor authentication factors, single sign-on identifiers, role and permission attributes within the Platform, API tokens, and the timestamp of your last login, OAuth 2.0 access and refresh tokens, granted scopes and token expiry, and the account/workspace identifier used to authenticate you to the Platform from a third-party AI software.
- A.4. **Payment and billing details.** Client entity details, billing contact, purchase order references and invoice records, processed to manage and account for your subscription.
- A.5. **Records of our mutual communication.** Any personal data contained in e-mails, support tickets, in-app chat, calls and meeting notes that you exchange with us, including any attachments.
- A.6. **Information about Platform usage and telemetry.** Pages and features used, session timestamps, configuration changes, data-connector activity, IP address, device type, operating system and browser, and security and audit logs that record actions performed within the Platform. We use this data to operate the Platform, monitor and improve performance, ensure security and integrity, and detect and prevent abuse.
- A.7. **Information about Website usage.** When you visit www.roivenu.com we automatically receive your IP address and information your browser sends, such as the pages you visit, time spent, referring URL, and operating system and browser version.
- A.8. **Information from cookies and other tracking technologies.** If you have enabled the storage of cookies in your browser, they send us additional information, for example about the pages you visit and your preferences. For more information on the use of cookies and similar technologies, please see Section D “Cookies and other digital identifiers” below.

B. PURPOSES OF PROCESSING

- B.1. **For our Clients and Platform users.** If you are our Client or you use the Platform under a contract concluded between us and the entity you represent, your personal data, and where applicable personal data of your employees or contractors, will be processed for the following purposes:
 - B.1.i) **Provision of the Platform and performance of our contract.** We process your personal data to make the Platform available to you, manage your account, authenticate you, deliver the attribution, reporting and data-integration outputs agreed under the contract, and provide Client support. For this purpose, we process Identification data, Contact details, Account and login data, Records of our mutual communication and Information about Platform usage and telemetry. The legal basis is the performance of a contract or our legitimate interest in administering the contractual relationship with the entity you represent.
 - B.1.ii) **Billing, accounting and protection of our rights and claims.** We process your personal data to invoice you, collect payment, keep statutory accounting records, and to establish, exercise or

defend legal claims (in judicial, extrajudicial, enforcement or similar proceedings). For this purpose, we process Identification data, Contact details, Payment and billing details and Records of our mutual communication. The legal basis is compliance with our legal obligations under Czech accounting and tax law and our legitimate interest.

- B.1.iii) **Security, integrity and abuse prevention.** We process Account and login data and Information about Platform usage and telemetry to monitor and protect the Platform, detect and prevent fraud, unauthorised access and other security incidents, and to investigate and respond to incidents. The legal basis is our legitimate interest in operating a secure service and, where applicable, compliance with our legal obligations.
- B.1.iv) **Improvement of the Platform.** We process Information about Platform usage and telemetry on an aggregated and pseudonymised basis to understand how the Platform is used, fix issues and improve features. The legal basis is our legitimate interest. This processing does not constitute automated decision-making producing legal effects on you.
- B.1.v) **Compliance with legal obligations.** We process personal data to comply with legal obligations imposed on us, including tax, accounting, anti-money-laundering, sanctions screening and similar requirements under Czech and EU law. The legal basis is compliance with our legal obligations.
- B.1.vi) **Marketing communication and promotion of our services.** We may send our newsletter and other marketing communication, or process your personal data to promote our services. For this purpose we mainly process Identification data and Contact details. If you are our Client, we are entitled to offer you similar services to those already provided on the basis of our legitimate interest. Otherwise, we will only send you marketing communication on the basis of your consent. You can withdraw your consent or object to this processing at any time, including via the unsubscribe link in any marketing message or by writing to privacy@scanmarqed.com. Withdrawal of consent does not affect the lawfulness of processing prior to such withdrawal.

B.2. **For Website visitors.** If you visit www.roivenu.com and subsequent subdomains, your personal data will be processed for the following purposes:

- B.2.i) **Operation and security of the Website.** We process Information about Website usage and strictly necessary cookies to operate the Website, deliver the content you request, and ensure its security and integrity. The legal basis is our legitimate interest. We generally retain this data for up to 24 months after your visit.
- B.2.ii) **Analytics and measurement.** Subject to your consent given through the cookie consent banner, we use cookies and similar technologies to understand how visitors use the Website (for example, which pages are most viewed and how visitors navigate between them) so we can improve and optimise it. We retain this data for the duration of your consent and in any case no longer than 24 months. The legal basis is your consent.
- B.2.iii) **Marketing and promotion on the Website.** Subject to your consent given through the cookie consent banner, we and our advertising partners use cookies and similar technologies to show you relevant content and advertising on the Website and on third-party platforms, and to measure the effectiveness of our marketing. The legal basis is your consent. You can withdraw your consent at any time via the cookie preferences link on the Website.

B.3. For users of the MCP Connector. If you access your Platform data through the MCP Connector, we will process your personal data for following purposes:

- B.3.i) Provision of the Platform and performance of our contract.** We process your personal data to authenticate you to the Platform from your AI assistant, authorise access to the account and data scope you are permitted to use, execute the queries you make and return the corresponding results. For this purpose, we process Identification data, Contact details, Account and login data, including the Connector authentication data described here and Information about Platform usage and telemetry. The legal basis is the performance of a contract or our legitimate interest in administering the contractual relationship with the entity you represent.
- B.3.ii) Security, integrity and abuse prevention.** We process Account and login data and Information about Platform usage and telemetry to secure the Connector, detect and prevent unauthorised access and other abuse, and to investigate and respond to incidents. The legal basis is our legitimate interest in operating a secure service and, where applicable, compliance with our legal obligations.
- B.3.iii) Compliance with legal obligations and protection of our rights and claims.** We process personal data relating to MCP Connector use to comply with legal obligations imposed on us and to establish, exercise or defend legal claims. The legal basis is compliance with our legal obligations and our legitimate interest.

C. SOURCES OF PERSONAL DATA

We process the personal data that you (or the entity you represent) provide to us when concluding a contract, when registering on the Platform, when contacting us, and when visiting the Website.

We may also collect personal data automatically when you use the Platform or visit the Website (such as Account and login data, Information about Platform usage and telemetry, Information about Website usage and Information from cookies and other tracking technologies). We may derive other data from the data set out above.

We may also receive personal data from our partners, including resellers, identity providers (where you authenticate via single sign-on) and integration partners (including advertising, web-analytics and CRM platforms) that pass data to us based on your or your organisation's instructions.

Where you use the MCP Connector, we also receive the authentication data and the query parameters transmitted from the AI assistant you use, on your instruction; the corresponding results are retrieved from your Platform account.

D. COOKIES AND OTHER DIGITAL IDENTIFIERS

Each time you visit the Website, we may store cookies – small files containing information about your visit – on your device and read them on subsequent visits. We use both session cookies (deleted after your visit) and persistent cookies that remain on your device for a set period, but no longer than 24 months. In addition to cookies, we use other similar technologies, such as web beacons and pixel tags, that have a similar function to cookies.

We use four categories of cookies and similar technologies on the Website: (i) strictly necessary (required for the Website to function and to keep it secure), (ii) preferences (remember your settings, such as language), (iii) analytics (help us understand how the Website is used), and (iv) marketing (used by us and our partners to deliver and measure relevant advertising). All categories other than strictly necessary cookies are activated only with your consent given through the cookie consent banner. You can withdraw or change your consent at any time using the cookie preferences link on the Website.

Where cookies cause your data to be transferred to processors or third parties, those recipients are listed in Section E and, where applicable, in the cookie consent banner.

E. PROCESSORS AND OTHER PERSONAL DATA RECIPIENTS

The processing of your personal data involves processors who always act on our documented instructions and for the purposes set out in this Privacy Policy. The current categories of processors involved in the operation of the Website and the Platform include:

- E.1. Cloud infrastructure and data hosting providers;
- E.2. Identity, authentication and single sign-on providers;
- E.3. Product analytics, error monitoring and observability providers used in connection with the Platform;
- E.4. Website analytics, marketing-automation and advertising providers (only where you have given consent through the cookie banner);
- E.5. Client-relationship-management, support and communication tools used to manage our interactions with you;
- E.6. Payment processing and billing providers (we do not receive or store payment card numbers);
- E.7. Other companies within the ScanmarQED group that provide shared services (such as IT, security, finance and Client support) on our behalf;

- E.8. Professional advisers, including auditors and legal counsel where necessary.
- E.9. Third-party AI assistant platforms through which you access the MCP Connector, which may include Anthropic – Claude, OpenAI – ChatGPT, and Microsoft – Copilot. As you invoke the MCP Connector from within such a platform on your own initiative, the query parameters you provide and the results returned pass through, and are displayed in, that platform, which processes them under its own terms and privacy policy and acts as an independent controller for its own services, not as our processor.

F. INTERNATIONAL TRANSFERS OF PERSONAL DATA

We seek to keep personal data within the European Economic Area (“EEA”). Where we need to use processors that store or process personal data outside the EEA, we ensure that an appropriate safeguard is in place, in particular:

- F.1. an adequacy decision adopted by the European Commission, or
- F.2. the Standard Contractual Clauses adopted by the European Commission, supplemented by additional technical and organisational measures where necessary, available at https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

These safeguards apply equally to any transfer by our processors arising from your use of the MCP Connector. Where you choose to use a third-party AI assistant platform as per Section E.9, that platform may process and transfer data under its own transfer mechanisms, outside our control.

G. MEASURES FOR DATA PROTECTION

Protecting your data is our priority. For this reason, we have adopted, maintain and continuously improve technical and organisational measures to protect personal data against unauthorised or unlawful processing, accidental loss, destruction, damage or disclosure. We are also ISO 27001:2022 certified.

These measures include role-based access controls and the principle of least privilege; encryption of data in transit and at rest; multi-factor authentication for administrative access; centralised logging and monitoring; vulnerability management, secure development practices and regular penetration testing; vendor and sub-processor risk assessment; documented incident-response and business-continuity procedures; and confidentiality obligations imposed on all personnel and processors with access to personal data.

For MCP Connector specifically, authentication uses OAuth 2.0 with TLS certificates issued by recognised authorities and no password is shared with the AI assistant and personal data that could appear in Connector logs is redacted or pseudonymized.

All security vulnerabilities can be reported to privacy@roivenu.com, while we will follow our regular adopted security processes investigate with a reasonable standard of care.

H. RETENTION OF PERSONAL DATA

We retain personal data only for as long as necessary for the purposes for which it was collected, and in particular:

- H.1. **Client relationship and Platform use:** for the duration of the contractual relationship with the entity you represent and for the duration of the applicable statutory limitation period thereafter (typically up to ten (10) years after termination of the contract under the Czech Civil Code, or longer where required by other applicable law).
- H.2. **Accounting and tax records:** for the period required by Czech accounting and tax law (five (5) years under the Czech Accounting Act, and ten (10) years for VAT-related records under the VAT Act).
- H.3. **Marketing communication:** for the duration of the Client relationship and up to two (2) years thereafter, or until you withdraw your consent or object to the processing, whichever is earlier.
- H.4. **Website analytics and marketing cookies:** for the duration of your consent, and in any case no longer than twenty-four (24) months.

- H.5. **Security and audit logs:** for as long as necessary to ensure the security and integrity of the Platform, typically not longer than twelve (12) months, unless a longer period is required to investigate an incident or comply with a legal obligation.
- H.6. **MCP Connector data:** authentication tokens are retained only for the lifetime of your session or their validity and are deleted or invalidated on disconnection, revocation or expiry; results returned to a query are not persisted by the MCP Connector beyond what is needed to return the response (they reside in your Platform account and in your AI-assistant conversation). MCP Connector operational and security logs follow H.5.

I. YOUR RIGHTS RELATED TO PROCESSED PERSONAL DATA

You have the following rights under the General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR") in relation to the processing of your personal data, which you can exercise by contacting us at privacy@scanmarged.com. We will respond as soon as possible and, in any event, within one (1) month of receipt of your request. In exceptional cases, we may extend this period by a further two (2) months and will inform you of any such extension.

- I.1. **Right of access.** You have the right to obtain confirmation as to whether we are processing your personal data and, where we are, access to that data and to information about the purposes and scope of the processing, the recipients of the data, the duration of the processing, your rights, the right to lodge a complaint with a supervisory authority and the sources of the personal data. You can also ask us for a copy of the personal data we process; the first copy is free of charge, further copies may be subject to a reasonable fee.
- I.2. **Right to rectification.** You have the right to request that we correct inaccurate personal data concerning you and, where relevant, complete incomplete personal data.
- I.3. **Right to erasure ("right to be forgotten").** You have the right to request the erasure of your personal data where one of the grounds set out in Article 17 GDPR applies. This right does not apply where processing is necessary for compliance with a legal obligation to which we are subject, or for the establishment, exercise or defense of legal claims.
- I.4. **Right to restriction of processing.** You have the right to request that we restrict the processing of your personal data in the cases set out in Article 18 GDPR.
- I.5. **Right to data portability.** You have the right to receive the personal data you have provided to us in a structured, commonly used and machine-readable format, and to transmit that data to another controller, where the processing is based on your consent or on a contract and is carried out by automated means.
- I.6. **Right to object.** You have the right to object, on grounds relating to your situation, to processing of your personal data based on our legitimate interest. You also have the right to object at any time to processing for direct-marketing purposes; we will stop such processing on receipt of your objection.
- I.7. **Right to withdraw consent.** Where processing is based on your consent, you can withdraw that consent at any time. Withdrawal of consent does not affect the lawfulness of processing prior to such withdrawal.
- I.8. **Right not to be subject to automated decision-making.** You have the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects concerning you or similarly significantly affects you. We do not carry out such processing in the operation of the Website, the Platform or the Connector.

- I.9. **Right to lodge a complaint.** In addition to exercising your rights with us, you have the right to lodge a complaint with a supervisory authority, in the Member State of your habitual residence, place of work or the alleged infringement. For the Czech Republic, this is the Úřad pro ochranu osobních údajů (Czech Office for Personal Data Protection), Pplk. Sochora 27, 170 00 Prague 7, Czech Republic (<https://www.uoou.gov.cz>).