

Privacy Policy

This privacy policy sets out how Radius Systems Limited, its UK and EU subsidiaries (Radius Subterra Limited, Radius Plastics Limited and Aeon International (Europe) Sp. z o.o.) and parent company (Radius Group Holdings Limited) (together, the “**Radius Group**”) collect, use and protect your personal data.

The Radius Group fully respects and is committed to protecting your privacy and follows strict security procedures for storing and disclosing information you provide to us.

1. Important information and who we are

Scope and territorial application

This privacy policy applies to the processing of personal data by Radius Group companies where UK data protection law applies, including processing carried out by our UK-based entities (Radius Group Holdings Limited, Radius Systems Limited, Radius Subterra Limited and Radius Plastics Limited) and processing undertaken in connection with our UK-centred business operations.

Where personal data is processed by Aeon International (Europe) Sp. z o.o. established in Poland, the processing will also be subject to the EU General Data Protection Regulation (EU GDPR). In such cases, references in this privacy policy to the UK GDPR shall be read, where appropriate, as references to the equivalent provisions of the EU GDPR.

This privacy policy gives you information about how the Radius Group collects and uses your personal data through your use of their websites, including any data you may provide when you complete forms to receive product information or otherwise engage with us.

This website is not intended for children and we do not knowingly collect data relating to children.

Controller

Each Radius Group company acts as an independent controller in respect of its own business activities, even where it is a subsidiary of a UK parent company, unless expressly stated otherwise:

UK

- Radius Group Holdings Limited (CRN: 09462842)
- Radius Systems Limited (CRN: 01585669)
- Radius Subterra Limited (CRN: 01147475)
- Radius Plastics Limited (CRN: NI013308)

Poland

- Aeon International (Europe) Sp. z o.o. (KRS: 0000283998)

Each company within the Radius Group acts as the controller of personal data in respect of its own website and business activities.

Accordingly:

- Radius Systems Limited is the controller responsible for the Radius Systems Limited, Radius Group Holdings Limited and the Radius Aeon websites. Where you receive products or services from a local Radius Group company, that company will act as the data controller in relation to such supply;
- Radius Plastics Limited is the controller responsible for the Radius CTS website; and
- Radius Subterra Limited is the controller responsible for the Radius Subterra Limited website.

This privacy policy is issued on behalf of the Radius Group. When we use the terms “Radius”, “we”, “us” or “our” in this privacy policy, we are referring to the relevant Radius Group company responsible for processing your personal data in the context in which it is collected.

In certain circumstances, another Radius Group entity may act as a processor (or joint controller where applicable) in relation to specific business relationships, communications or contractual arrangements.

If you have any questions about this privacy policy, including any requests to exercise your legal rights (**paragraph 9**), please contact us using the information set out in the contact details section (**paragraph 10**). If you wish to make a complaint about how a relevant Radius Group company processes your data, please refer to **paragraph 11**.

2. The types of personal data we collect about you

Personal data means any information about an individual from which that person can be identified.

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

- **Identity Data** includes first name, last name, username or similar identifier, title and date of birth.
- **Contact Data** includes billing address, delivery address, email address and telephone numbers.
- **Financial Data** includes bank account details.
- **Marketing and Communications Data** includes your preferences in receiving marketing from us and our third parties and your communication preferences
- **Transaction Data** includes details about payments to and from you and other details of products and services you have purchased from us.
- **Technical Data** includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, device ID and other technology on the devices you use to access the relevant website.
- **Usage Data** includes information about how you interact with and use our website, products and services.

We also collect, use and share aggregated data such as statistical or demographic data which is not personal data as it does not directly (or indirectly) reveal your identity. For example, we may aggregate individuals' Usage Data to calculate the percentage of users accessing a specific website feature in order to analyse general trends in how users are interacting with our website to help improve the website and our service offering.

3. How is your personal data collected?

We use different methods to collect data from and about you including through:

- **Your interactions with us.** You may give us your personal data by filling in online forms (including Microsoft forms) and other electronic means or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you request product data sheets to be sent to you and when you contact us or when you provide supplier and business partner information for onboarding, compliance and procurement purposes.

- **Automated technologies or interactions.** As you interact with our website, we will automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies.
- **Third parties or publicly available sources.** We will receive personal data about you from various third parties as set out below. We may also receive personal data from third-party due diligence and compliance providers, including CreditSafe, and from publicly available sources such as Companies House and sanctions registers, in connection with supplier onboarding, know-your-customer (KYC), fraud prevention, supplier verification, sanctions screening, business integrity assessments and compliance with applicable legal and regulatory requirements. Technical Data is collected from analytics providers, such as Google based outside the UK.

4. How we use your personal data

Legal basis - The law requires us to have a legal basis for collecting and using your personal data. We rely on one or more of the following legal bases:

- **Performance of a contract with you:** Where we need to perform the contract we are about to enter into or have entered into with you.
- **Legitimate interests:** We may use your personal data where it is necessary to conduct our business and pursue our legitimate interests, for example to prevent fraud and enable us to give you the best and most secure customer experience. We make sure we consider and balance any potential impact on you and your rights (both positive and negative) before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).
- **Legal obligation:** We may use your personal data where it is necessary for compliance with a legal obligation that we are subject to. We will identify the relevant legal obligation when we rely on this legal basis.
- **Consent:** We rely on consent only where we have obtained your active agreement to use your personal data for a specified purpose, for example if you subscribe to an email newsletter.

Purposes for which we will use your personal data

We have set out below a description of all the ways we plan to use the various categories of your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Purpose/Use	Type of data	Legal basis
To provide you with product data sheets	(a) Identity (b) Contact	Performance of a contract with you
To manage our relationship with you which will include: (a) Notifying you about changes to our privacy policy (b) Dealing with your requests, complaints and queries	(a) Identity (b) Contact (c) Marketing and Communications Data	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and manage our relationship with you)

(c) Administration of promotions, discounts and special offers.		
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) (b) Necessary to comply with a legal obligation
To enable you to partake in a competition or complete a survey	(a) Identity (b) Contact (c) Usage (d) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to study how customers use our products/services, to develop them and grow our business)
To deliver relevant website content and online advertisements and to use cookies and similar technologies to analyse usage and improve our website	(a) Identity (b) Contact (c) Usage (d) Marketing and Communications (e) Technical	(a) Consent (in relation to cookies, tracking technologies and personalised advertising, where required under applicable law). Non-essential cookies (including analytics and advertising cookies) will only be placed on your device with your consent, which you may withdraw at any time. (b) Necessary for our legitimate interests (for general website improvement and non-intrusive analytics where permitted)
To use data analytics to improve our website, products/services, customer relationships and experiences.	(a) Technical (b) Usage	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business)
To send marketing e-mails	(a) Identity (b) Contact	Necessary for our legitimate interests (to promote our products and services to existing corporate customers, suppliers and business contacts to develop business). You have the absolute right to object at any time to receiving direct marketing communications from us. You can do this by (a) clicking the unsubscribe link in any marketing email we send; or (b) contacting us using the details set out in paragraph 10 (Contact details). If you object, we will stop using your personal data for marketing purposes without delay.

To onboard, assess and manage suppliers, contractors, customers and other business partners, including directors, officers or beneficial owners, including the collection of information through online forms, carrying out know-your-customer (KYC), anti-fraud, sanctions, compliance and due diligence checks, maintaining records of such checks, and managing ongoing business relationships.	(a) Identity (b) Contact (c) Financial	(a) Necessary for our legitimate interests (to assess and manage business risk, prevent fraud, comply with internal governance requirements and protect our business) (b) Necessary to comply with legal obligations where applicable
To operate AI-assisted business systems, workflow automation tools and document processing platforms, including generating summaries, classifications, recommendations, workflow outputs and analytical insights.	(a) Identity (b) Contact (c) Usage (d) Transaction	(a) Legitimate interests (improving operational efficiency, productivity, information management and business processes); (b) Contract; (c) Legal obligation where applicable

Use of AI and automated technologies

We may use artificial intelligence (AI) and workflow automation technologies to support document processing, information retrieval, data analysis and operational efficiency.

These systems may process personal data contained within documents, records, correspondence and other information submitted to the platform.

AI-generated outputs are used to support human decision-making and are subject to human review. We do not use these systems to make solely automated decisions that produce legal or similarly significant effects on individuals.

Personal data submitted to AI-assisted systems is used solely for the provision of the relevant services and is not used to train public or shared AI models unless expressly stated otherwise. AI outputs are reviewed by appropriately authorised personnel before they are relied upon.

Use of cookies

For more information about the cookies we use and how to change your cookie preferences, please see our [Cookie Policy](#).

5. Disclosures of your personal data

We may share your personal data where necessary with the parties set out below for the purposes set out in the table in **paragraph 4** above.

- External third parties: We use third-party service providers as follows:
 - Craft CMS – our website platform, which processes basic technical data (like IP address and browser type) for functionality and security.

- Formie – manages our contact forms and securely stores the information you submit so we can respond to your enquiries.
- HubSpot – used for customer relationship management, including communications. It may process contact and interaction data in line with its privacy practices.
- Cloudflare – provides website security and performance services, processing limited technical data (such as IP addresses) to protect against attacks and optimize delivery.
- Microsoft Forms – used to collect information from suppliers, customers, contractors and other business contacts, including onboarding, procurement and compliance information submitted through electronic forms.
- CreditSafe – used for compliance with applicable legal and regulatory obligations; and/or legitimate interests in preventing fraud and managing business risk.
- Lleverage B.V. – used for AI-assisted document processing, workflow automation and business analysis.

These service providers may process limited personal or technical data to operate our site, manage communications, and keep everything secure. All providers follow strict data protection and security standards. We encourage you to review the privacy notices of these third parties to understand how they process your data. You should contact them directly to exercise your data protection rights in relation to their processing activities.

Sub-processors – these third-party service providers may in turn engage their own sub-processors to support the delivery of their services. We require our service providers to ensure that any sub-processors they use offer equivalent levels of data protection and comply with applicable privacy laws.

- Third parties to whom we may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy policy.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

6. International transfers

Whenever we transfer your personal data out of the UK to countries which have laws that do not provide the same level of data protection as the UK law, we always ensure that a similar degree of protection is afforded to it by ensuring that the following safeguards are implemented

We may transfer your personal data to service providers that carry out certain functions on our behalf. This may involve transferring personal data outside the UK to countries which have laws that do not provide the same level of data protection as the UK law.

Whenever we transfer your personal data out of the UK to service providers, we ensure a similar degree of protection is afforded to it by ensuring that the following safeguards are in place:

- We will only transfer your personal data to countries that have been deemed by the UK to provide an adequate level of protection for personal data under the UK GDPR, including EEA countries.

- For transfers to the United States, we may use the UK-approved standard contractual clauses, including the International Data Transfer Addendum, which ensure that your personal data receives the same level of protection as under UK data protection law.

7. Data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

8. Data retention

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of managing business relationships, satisfying any legal, regulatory, audit, tax, accounting, compliance or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

Detailed retention periods for different categories of personal data are set out in our Data Retention Policy. You can request further information about retention periods by contacting us.

In some circumstances you can ask us to delete your data: see **paragraph 9** below for further information.

9. Your legal rights

You have a number of rights under data protection laws in relation to your personal data.

You have the right to:

- Request access to your personal data (commonly known as a "subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
- Request erasure of your personal data in certain circumstances. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
- Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) as the legal basis for that particular use of your data (including carrying out profiling based on our legitimate interests). In some cases, we may demonstrate

that we have compelling legitimate grounds to process your information which override your right to object.

- You also have the absolute right to object at any time to the processing of your personal data for direct marketing purposes.
- Withdraw consent at any time where we rely on consent to process your personal data. This will not affect the lawfulness of processing carried out before withdrawal.
- Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
- Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in one of the following scenarios:
 - If you want us to establish the data's accuracy;
 - Where our use of the data is unlawful but you do not want us to erase it;
 - Where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
 - You have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

If you wish to exercise any of the rights set out above, please see Contact details in **paragraph 10**.

We do not carry out automated decision-making or profiling that produces legal or similarly significant effects on individuals.

No fee usually required - You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

What we may need from you - We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond - We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

10. Contact details

If you have any questions about this privacy policy or about the use of your personal data or you want to exercise your privacy rights, please contact us in the following ways:

e-mail: privacymatters@radius-systems.com

Postal address: Privacy Matters, Radius, Radius House Berristow Lane, South Normanton, Alfreton, Derbyshire, DE55 2JJ

11. How to make a data protection complaint

If you have any concerns about how we process your personal data, you have the right to make a complaint directly to us. We encourage you to raise any issues with us first so that we can try to resolve them promptly and fairly.

You can make a complaint using the above Contact Details (**paragraph 10**) or completing and submitting this [Complaint Form](#).

What Happens Next

- We will acknowledge your data protection complaint promptly, usually within 7 days.
- We will investigate your complaint without undue delay, making appropriate enquiries as necessary, and will keep you informed of its progress.
- We aim to provide a written outcome within one month, unless the complaint is particularly complex or exceptional circumstances apply, in which case we will explain the reasons for any delay.

If you remain dissatisfied after we have completed our internal complaints process, you may escalate your complaint as follows:

- In the UK, to the [Information Commission's Office](#), the UK regulator for data protection issues.
- In Poland, to the [Office for Personal Data Protection](#), the Polish regulator for data protection issues.

12. Changes to the privacy policy and your duty to inform us of changes

We keep our privacy policy under regular review.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us, for example a new address or email address.

13. Third-party links

This website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. We encourage you to read the privacy policy of every website you visit.

14. CCTV Images

Radius uses closed circuit television (CCTV) to provide a safe and secure environment for employees and for visitors to the company's premises and to protect company property. The legal basis for this processing is our legitimate interests in ensuring the safety and security of our employees, visitors and property. CCTV signage is displayed at relevant locations. The company's CCTV facility records images only. There is no audio recording. Images that are stored on media are erased or destroyed once the purpose of the recording is no longer relevant. In normal circumstances, this will be a period of 31 days. Where a law enforcement agency is investigating a crime, images may need to be retained for a longer period. Access to, and disclosure of, images recorded on CCTV is restricted. This ensures that the rights of individuals are retained. Images can only be disclosed in accordance with the purposes for which they were originally collected. The CCTV policy for the UK-centred business operations is available upon request.