UK General Data Protection Regulations (GDPR) Policy

Introduction

Radiocoms Systems Ltd (Radiocoms) respects your privacy and is committed to protecting your personal data. This privacy notice will inform you as to how Radiocoms looks after your personal data when you visit our website (regardless of where you visit it from), or when you engage with Radiocoms via other means, and to tell you about your privacy rights and how the law protects you.

Purpose of this privacy notice

This privacy notice aims to give you information on how Radiocoms collects and processes your personal data through your use of this website, including any data you may provide through this website when you make an enquiry, apply for a position, or purchase a product or service from Radiocoms, or when you engage with the company by any other means to make an enquiry or purchase a product or service.

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

It is important that you read this privacy notice, so you are fully aware of how and why your data is being used. This privacy notice supplements the other notices and is not intended to override them.

Controller

Radiocoms is the controller and responsible for your personal data (collectively referred to as "Radiocoms", "we", "us" or "our" in this privacy notice).

We have appointed a data privacy manager who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact the data privacy manager using the details set out below.

- Full name of legal entity: Radiocoms Systems Ltd
- Name or title of data privacy manager: Mr Bhupinder Sidhu
- Registered address: Units 2&3 The Chase Centre, 8 Chase Road, London NW10 6QD.
- Telephone number: 0844 5675670

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

Changes to the privacy notice and your duty to inform us of changes

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.

Third-party links from our website

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. When you leave our website, we encourage you to read the privacy notice of every website you visit.

The data we collect about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

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

- **Identity Data** includes first name, last name, username or similar identifier
- **Contact Data** includes billing address, delivery address, email address and telephone numbers.
- **Financial Data** includes bank account and payment details.
- **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, browser type and version, time zone setting and location, and other technical data that may be collected through the use of cookies.
- **Usage Data** includes information about how you use our website, products and services.
- **Marketing and Communications Data** includes your preferences in receiving marketing from us and your communication preferences where applicable.

We may also collect, use and share **Aggregated Data** such as statistical or demographic data for any purpose. Aggregated Data may be derived from your personal data but is not considered personal data in law as this data does **not** directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy notice.

We do not collect any **Special Categories of Personal Data** about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of a contract we have with you and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with goods or services). In this case, we may have to cancel a product or service you have with us but we will notify you if this is the case at the time.

How is your personal data collected?

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

- **Direct interactions.** You may give us your Identity, Contact and Financial Data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:
- apply for our products or services;
- subscribe to our service;
- request marketing to be sent to you;
- give us some feedback.
- **Automated technologies or interactions.** As you interact with our website, we may automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies.
- **Third parties or publicly available sources.** We may receive personal data about you from various third parties [and public sources] as set out below:
- Technical Data from analytics providers such as Google based outside the EU;

How we use your personal data

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with you.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal or regulatory obligation.

Generally we do not rely on consent as a legal basis for processing your personal data other than in relation to sending third party direct marketing communications to you via email. You have the right to withdraw consent to marketing at any time by using the 'unsubscribe' function or by contacting us directly.

Purposes for which we will use your personal data

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

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To register you as a new customer	(a) Identity (b) Contact	Performance of a contract with you
To process and deliver your order/services including: (a) Manage payments, fees and charges (b) Collect and recover money owed to us	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to recover debts due to us)
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy (b) Asking you to leave a review or take a survey	(a) Identity (b) Contact (c) Profile (d) Marketing and Communications	(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 to study how customers use our products/services)
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 deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications (f) Technical	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our website, products/services, marketing, 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 and to inform our marketing strategy)

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To make suggestions and recommendations to you about goods or services that may be of interest to you	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile	Necessary for our legitimate interests (to develop our products/services and grow our business)

Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising. We have established the following personal data control mechanisms:

Promotional offers from us

We may use your Identity, Contact, Technical, Usage and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you (we call this marketing).

You may receive marketing communications from us if you have requested information from us or purchased services from us or if you provided us with your details when you entered a competition or registered for a promotion and, in each case, you have not opted out of receiving that marketing.

Third-party marketing

We do not share your personal data with any company outside of Radiocoms for marketing purposes.

Opting out

You can ask us to stop sending you marketing messages at any time by following the opt-out links on any marketing message sent to you or by contacting us at any time.

Where you opt out of receiving these marketing messages, this will not apply to personal data provided to us as a result of a product/service purchase, product/service experience or other transactions.

Cookies

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies.

Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Disclosures of your personal data

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

- External Third Parties as set out in the Glossary.
- 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 notice.

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.

International transfers

We do not transfer your personal data outside the European Economic Area (**EEA**).

If, in the future, there arises a requirement to transfer your personal data out of the EEA, we will ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission. For further details, see European Commission: Adequacy of the protection of personal data in non-EU countries.
- Where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe. For further details, see European Commission: Model contracts for the transfer of personal data to third countries.
- Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between the Europe and the US. For further details, see European Commission: EU-US Privacy Shield.

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.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

Data retention

STATEMENT OF RECOGNITION

Radiocoms recognises the importance of effective file keeping records and data management to enable it to discharge its functions. In addition, there are a number of regulatory requirements to consider, for instance the 2018 UK Data Protection Act. This requires, amongst other things, a Data Retention System Security Policy.

BASIS OF RETENTION

To comply with UK GDPR, EU GDPR and the principles of the Data Protection Act 2018, records containing personal data must be:

- Stored appropriately having regard to the sensitivity and confidentiality of the material recorded
- Retrievable and easily traced
- Retained for only as long as necessary
- Disposed of appropriately to ensure that personal confidentiality and copyrights are not breached and to prevent them falling into the hands of unauthorised personnel

APPLICATION OF THE DATA & RECORD RETENTION POLICY

This policy applies equally to photographic, microform and electronic media that are used to store records as well as more traditional paper or card records. The period of retention only commences when the record is closed. The procedure for backing up of electronic media can be found in the Backup System Operating Procedure.

STORAGE OF DATA & RECORDS STATEMENT

All data and records should be stored as securely as possible in order to avoid potential misuse or loss. All data and records will be stored in the most convenient and appropriate location having regard to the period of retention required and the frequency with which access will be made to the record.

Data and records which are active should be stored in the most appropriate place for their purpose.

Data and records which are no longer active, due to their age or subject, should be stored in the most appropriate place for their purpose.

The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded.

Any data file or record which contains personal data of any form can be considered as confidential in nature.

Personally identifiable data storage must be limited to the amount and retention time to that which is required for legal, regulatory, and/or business requirements.

RETENTION STATEMENT

Data and records should not be kept for longer than is necessary. This principle finds statutory form in the Data Protection Act 2018, which requires “Personal data which is kept in a form which permits identification of data subjects must be kept for no longer than is necessary for the purposes for which the data is processed.”.

DESTRUCTION AND DISPOSAL STATEMENT

All information of a confidential or sensitive nature on paper, card, microfiche, or electronic media must be securely destroyed when it is no longer required.

This ensures compliance with the Data Protection Act 2018, Requirement and the duty of confidentiality owed to Radiocoms employees, clients, and customers.

DESTRUCTION AND DISPOSAL PROCEDURES

All information, in any format, destroyed from any location must have due regard to confidentiality of our employees, clients and customers.

When records or data files are identified for disposal in the Policy are destroyed, a register of such records needs to be kept.

The procedure for the destruction of Confidential or Sensitive Waste on paper, card or microfiche is as follows:

All office quality white or coloured paper should be mechanically shredded if the content is in any way sensitive.

If you dispose of waste by using a shredder, ensure that it is used safely in accordance with its operating instructions, and that waste is shredded in such a way that it cannot be put back together again, and made comprehensible.

The procedure for the destruction of Confidential or Sensitive Waste on electronic media such as tape, disk, cassette/cartridge, hard drives, CD-ROM, DVD, ZIP, USB hard or flash drive is as follows:

- Media that are being destroyed because they are showing signs of damage or are obsolete should be physically destroyed by being cut into pieces or other ways prior to disposal. A certificate of destruction must be completed.
- Where electronic media, such as disks, tapes, DVD, CD-ROM, USB hard or flash drives are being used to supply data to third parties they should, at the very least, be reformatted before the files are saved on to it. The process of saving files to the disk may overwrite areas of the disk previously used, but this is no guarantee of preventing retrieval of previously stored files. The most effective way to ensure that media are cleaned of all previous data is to use a utility package to perform a "secure wipe", and this method must be used if any non-public data may have been stored on this media previously.
- Destruction of back-up copies of such data also needs to be dealt with either by physical destruction as per the first paragraph, or by securely wiping as per the previous paragraph.

The procedure for the destruction of Confidential or Sensitive Waste on electronic media that is not being removed such as hard drives and SSD drives is as follows:

- Use a utility package to perform a "secure wipe" using software such as Blancco File Eraser.

Your legal rights

Under certain circumstances, you have 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 "data 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. 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) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.
- **Request restriction of processing** of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) 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 (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
- **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.
- **Withdraw consent at any time** where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

If you wish to exercise any of the rights set out above, please contact us.

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 may 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 may 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.

Glossary

LAWFUL BASIS

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure

we consider and balance any potential impact on you (both positive and negative) and your rights 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). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

Performance of Contract means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Comply with a legal or regulatory obligation means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

THIRD PARTIES

External Third Parties

- Service providers acting as processors based in the UK, EEA or EU who provide IT and system administration services.
- Professional advisers acting as processors or joint controllers including lawyers, bankers, auditors and insurers based in the UK, EEA or EU who provide consultancy, banking, legal, insurance and accounting services.
- HM Revenue & Customs, regulators and other authorities acting as processors or joint controllers based in the United Kingdom who require reporting of processing activities in certain circumstances.

Bhupinder Sidhu
Operations Director
Radiocoms Systems Ltd