

RENOLD WEAR APPLICATION PRIVACY STATEMENT

Introduction

This Privacy Statement explains in detail the types of personal data ("information") we collect about you when you interact with us through our mobile phone application ("Wear app" or "app"). It also sets out the basis on which we process the information which you provide to us, or we collect from you in connection with the app.

The Wear app is intended for use only by residents of Europe and Asia. The Wear app is not intended for distribution to, or use by, any person or entity in the United States of America, Canada, or any jurisdiction or country where such distribution or use would be contrary to law or regulation, or which would subject Renold or the corporate group to which it belongs ("Renold Group") to any registration requirement within such jurisdiction or country.

Please read the following carefully to understand how we handle your information.

Data Controller

Renold Plc is the controller and is responsible for this app. Renold Plc is a company registered in the United Kingdom under company number 249688 and we have our registered office at Trident 2, Trident Business Park, Styal Road, Wythenshawe, Manchester, M22 5XB which is also our main trading address.

Changes to this Privacy Statement and changes to your data

From time to time, we may be required to make changes to this Statement, any such changes will be notified to you when you next access the app.

Third-party links

This app 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 information about you. We do not control these third-party websites, plug-ins and applications and are not responsible for their privacy statements. When you leave our app, we encourage you to read the privacy policy of every website, plug-in and application you visit.

Information we may collect from 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 as follows:

- **Identity Data** includes first name, last name, business/employer, username or similar identifier and title.

- **Contact Data** includes job title, email address and residing country.
- **Technical Data** includes internet protocol (IP) address, your login data, time zone setting and location, operating system and platform, and other technology on the devices you use to access the Wear app.
- **Profile Data** includes your username and password, your preferences, feedback and survey responses.
- **Usage Data** includes information about how you use the Wear app, for example time spent on certain pages, how you navigate between different parts of the Wear app and any errors or malfunctions of the Wear app during your use.
- **Report Data** includes information relating to the outcome of any tests you carry out using the Wear app and includes any Reports we produce (where linked to your Wear app account or other personal data we hold about you).
- **Marketing and Communications Data** includes your preferences in receiving marketing from us and our third parties and your communication preferences.

We also collect, use and share **Aggregated Data** such as statistical or demographic data. Aggregated Data could be derived from your personal data but is not considered personal data in law as this data will **not** directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific app 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 Statement.

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.

How we collect your personal information

We will only use the information we collect about you in connection with our app in the ways outlined below.

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

Information you give us – You may give us information about you by filling in forms on the Wear app (e.g. the registration form) or by corresponding with us by phone, e-mail or otherwise. This includes information you provide when you subscribe to receive email alerts or when you leave us feedback and/or report a problem with the Wear app. The information you give us may include your name, job title, e-mail address and residing country.

Information we collect about you – We may automatically collect information about you when you first download our app or register to use it and on each of your visits to our app. We

may also collect information from public sources or from your relationship with other parts of the Renold business to allow us to verify your right to use the app.

We will not contact your Internet Service Provider to personally identify you, unless permitted by law.

Information we receive from other sources – We may receive information about you if you use any of the other apps or websites we operate or deal with us in connection with the other goods or services we provide.

Our lawful basis for use of your personal information

Contractual obligations

In certain circumstances, we may need to collect and process your information to perform our obligations under a contract.

For example, to provide the app services requested by you.

Legal obligations

If we are required to by law, we may need to collect and process your information, and share it with the relevant authorities as applicable.

For example, we may pass on the details of people involved, or suspected to be involved, in fraudulent or other criminal activity affecting the Renold Group to the relevant authorities to assist with criminal or civil investigations.

Legitimate interests

In specific situations, we may collect and process your information to pursue our legitimate interests as part of running our business and operating our app, provided that this is in a way which you might reasonably expect and which will not materially impact your rights, freedoms or interests.

For example, we may also aggregate the Usage Data of multiple users to identify trends and ensure we can keep up with demand, or develop new products and services.

Consent

In specific situations, we may collect and process your information with your consent.

For example, when you tick a box to subscribe to email newsletters.

We will always make it clear to you what you are consenting to and what information is necessary for which services.

How we use your personal information

We have set out in this section how we may use the personal information collected about you, where we collect this personal information and our lawful basis for our processing activities:

How do we use your personal information	What personal information do we use?	Where do we collect this personal information?	What is our lawful basis for processing?
<p>To provide the Wear app and related services to you, including registering your account, providing our services to you, providing support services in connection with our app and corresponding with you where necessary in connection with your use of the Wear app.</p>	<p>First name, last name, business/employer, username or similar identifier, password and title; job title, email address and residing country; and information relating to the outcome of any tests you carry out using the Wear app (including any Reports we produce).</p>	<p>This personal information is collected directly from you or generated by us during your use of our app.</p>	<p>Processing this personal information is necessary for the performance of our contract to provide the Wear app to you.</p>
<p>To notify you about changes to the Wear app, our services, our terms and conditions or this Statement;</p>	<p>First name, last name, username and email address</p>	<p>This personal information is collected directly from you.</p>	<p>Processing this personal information is necessary for the performance of our contract to provide the Wear app to you.</p>
<p>To ensure that content from our app is presented in the most effective manner for you and for your device.</p>	<p>IP address, your login data, time zone setting and location, operating system and platform, and other technology on the devices you use to access the Wear app; and data relating to your use of the Wear app.</p>	<p>The personal information is collected by us when you use the Wear app.</p>	<p>Processing this personal information is necessary for our legitimate interests of improving the Wear app and the services we provide so we can improve user experience for existing users and attract new users.</p>

<p>To manage our app and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes. This may include anonymization and aggregation of your personal information so it is no longer personally identifiable.</p>	<p>IP address, your login data, time zone setting and location, operating system and platform, and other technology on the devices you use to access the Wear app; data relating to your use of the Wear app; and your responses to surveys and feedback requests we issue to you.</p>	<p>This personal information is collected directly from you or generated by us during your use of our app.</p>	<p>Processing this personal information is necessary for our legitimate interests of improving the Wear app and the services we provide so we can improve user experience for existing users and attract new users.</p>
<p>To keep our app safe and secure.</p>	<p>First name, last name, business/employer, username or similar identifier, password and title; job title, email address and residing country; IP address, your login data, time zone setting and location, operating system and platform, and other technology on the devices you use to access the Wear app; and data relating to your use of the Wear app.</p>	<p>This personal information is collected directly from you or generated by us during your use of our app.</p>	<p>Processing this personal information is necessary for our legitimate interests of improving the safety and security of the Wear app and the services we provide so we can improve user experience for existing users and attract new users. Processing of this personal information is also necessary for us to comply with our legal obligations of providing a safe and secure mobile application.</p>
<p>To send you marketing communications relating to our app and to analyse the effectiveness of such marketing communications</p>	<p>First name, last name, business/employer, username or similar identifier and title, job title, email address and residing country.</p>	<p>This personal information is collected directly from you.</p>	<p>We will only send you marketing communications with your consent.</p>

<p>As necessary for the establishment, exercise or defence of legal claims relating to the Wear app or the services provided via it.</p>	<p>First name, last name, business/employer, username or similar identifier, password and title; job title, email address and residing country; IP address, your login data, time zone setting and location, operating system and platform, and other technology on the devices you use to access the Wear app; data relating to your use of the Wear app; and information relating to the outcome of any tests you carry out using the Wear app (including any Reports we produce).</p>	<p>This personal information is collected directly from you or generated by us during your use of our app.</p>	<p>Processing this personal information is necessary for our legitimate interests of the establishment, exercise and defence of legal claims as necessary to protect the Renold business.</p>
------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Marketing purposes

We value your privacy and your rights as a data subject and we will only send you marketing communications with your prior consent. You will have the right to opt in or out of receiving such marketing communications at all times, and we will provide easy-to-follow instructions on how to do so in each communication.

Please note that your consent for marketing purposes is entirely voluntary and can be withdrawn at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

How long we keep your personal information

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 satisfying any legal, regulatory, tax, accounting or reporting requirements. For most of the personal information we process in connection with your use of our app, we will retain your personal information for up to 12 months following deletion of your account. We may retain your personal data for a longer period in the event of a complaint, if we reasonably believe there is a prospect of litigation in respect to our relationship with you or where required by law.

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.

At the end of that retention period, your information will either be deleted or anonymised, for example by aggregation with other data so that it can be used in a non-identifiable way for statistical analysis and other business purposes.

How we share your information

We may share your personal information with our carefully selected third party service providers who assist us in providing our app and processing your personal information as set out above. These third parties will not use your information for their own purposes and we will ensure they are subject to appropriate contractual obligations with regard to the processing of your information. Our service providers include:

- Other companies within the Renold Group for the purposes of improving the user experience, managing the functionality of the app and analytics;
- Analytics providers for the purpose of providing analytics services in connection with our app;
- Our app developers who assist us in the improvement and optimisation of our app and the running of our business; and
- Our app host who hosts the Wear app on our behalf.

In addition, we may disclose your personal information to third parties:

- In the event that we sell or buy any business or assets, in which case we may disclose your personal data to the prospective seller or buyer of such business or assets;
- If the Renold Group or substantially all of its assets are acquired by a third party, in which case personal data held by it about its customers will be one of the transferred assets; or
- If we are under a duty to disclose or share your personal data in order to comply with any legal or regulatory obligation, or in order to enforce or apply our terms of use or other agreements; or to protect the rights, property, or safety of the Renold Group, our customers, or others.

Transfers and security

International Transfers

This section applies only where you reside within the European Economic Area ("EEA") or UK.

We may be required to transfer your information to countries outside the UK and EEA in order to provide the Wear app. This may occur where our third party service providers (including a company within the Renold Group) are based outside of the EEA or UK. These countries may not have the same data protection laws as the country in which you initially provided the information and may not provide the same level of protection. Your personal information may be subject to the laws of such foreign jurisdiction and may be accessible without notice to you by the courts, law enforcement and national security authorities of such foreign jurisdiction.

If we transfer personal information to countries outside of the EEA or UK, we will ensure (in accordance with applicable laws) an adequate degree of protection is afforded to your personal information by ensuring at least one of the following safeguards is implemented:

- we may transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data;
- for transfers to the US, we may rely on the EU-US Data Privacy Framework or the UK Extension to the EU-US Data Privacy Framework (as applicable). Further information about the EU-US Data Privacy Framework can be found [here](#). Further information about the UK Extension to the EU-US Data Privacy Framework can be found [here](#);
- we may use specific contracts approved for use in the UK and EEA which give personal data the same protection it has in the UK. Further information regarding such contracts are available on the [European Commission's website](#) and the [ICO's website](#).

Security of Personal Information

We have in place appropriate policies, rules and technical and organisational measures to protect your personal information from unauthorised or unlawful processing, and against accidental loss, destruction or damage. In particular, we store your personal information on secure, encrypted servers to ensure maximum protection of your information. Access to this data is strictly limited to authorised personnel who have legitimate business needs to access it.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your information, we cannot guarantee the security of your information transmitted to our app; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features, in line with the standards set out in the UK GDPR, to try to prevent unauthorised access.

On occasion, links to third party sites may be posted on this app. We are not responsible for the content of websites which are outside of our control, and they are not covered by this Privacy Statement. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any information to these websites.

Your rights

Residents of the EU and UK have a range of rights over their personal information and (to the extent these rights apply to you) we will endeavour to respect any requests by you to exercise them.

Access

You may request access to the personal information we hold about you and we must provide it free of charge unless we deem the request to be manifestly unfounded or excessive. In this event, we will explain why we have decided not to action your request.

Correction

You may request that we correct the personal information we hold on you when it is incorrect, out of date or incomplete.

Erasure

You may (in certain circumstances) request that we destroy or delete the personal information we hold on you when it is no longer necessary for the purpose which we originally collected it for.

Restriction

You may (in certain circumstances) request that we stop processing your personal information when you contest its accuracy or the lawfulness of the processing.

Transfer

You may (in certain circumstances) request that we transfer the personal information we hold about you to you or a third party.

Withdrawing consent

Whenever we rely on your consent to use your information, you have the right to change your mind at any time and withdraw your consent by notifying us in writing using the details set out in this Statement.

Object to processing

In cases where we are processing your information on the basis of our legitimate interest, you can ask us to stop for reasons connected to your individual situation.

We will do so unless we believe we have a legitimate overriding reason to continue processing your information.

Marketing

You have the right to stop our use of your information for direct marketing activities through all channels, or selected channels. We must always comply with your request.

Click the 'unsubscribe' link in any email communication we send to you to notify us that you would like us to stop any further emails.

Submitting a request

You can request to exercise these rights at any time by contacting us at: dataprotection@renold.com.

No fee usually required

You will not have to pay a fee to access your personal information (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 information (or to exercise any of your other rights). This is a security measure to ensure that personal information 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.

Contacting the Regulator

If you feel that your personal information has not been handled correctly, or you are unhappy with our response to any requests you have made to us regarding the use of your personal data, you have the right to lodge a complaint with your local supervisory authority. In the UK, this will be the Information Commissioner's Office. In the EU, you will be able to find details of your supervisory authority [here](#).

You can contact the ICO by going online to www.ico.org.uk/concerns. For the EU, contact details for your supervisory authority are available at the above link. Please note these links open in a new window and we are not responsible for the content of external websites. We would, however, appreciate the opportunity to address your concerns first before you escalate matters to your supervisory authority

Contacting Us

In the event that you have any questions, comments or concerns regarding this Privacy Statement or privacy information requests, please [email: dataprotection@renold.com](mailto:dataprotection@renold.com).

If you have any questions regarding Renold, our products & services or general enquiries, please engage with your usual contact at Renold or go to the contact page on your relevant country website.