

SPACETALK Privacy Policy

Updated: 22 April 2021

We are Spacetalk Holdings Pty Ltd (**Spacetalk**) and its UK subsidiary SPACETALKWATCH UK Ltd (**STW**). We sell the Spacetalk Watch and associated services directly or indirectly through resellers and distributors in Australia, New Zealand, the United Kingdom and throughout the European Union. This Privacy Policy explains how we collect, use, disclose and protect information that applies to our services to Spacetalk Watch users, owners and visitors to our websites www.spacetalkwatch.com and www.spacetalkwatch.co.uk and users of our associated mobile and software application the Spacetalk app. When you use our products and services, we understand that you trust us with your information - we are committed to keeping that trust. That starts with helping you understand our privacy practices and your choices regarding this information, including for Spacetalk Watch users in the European Economic Area (EEA) the EU General Data Protection Regulation 2016/679 (**GDPR**), for users in the United Kingdom the UK-GDPR and for Australian users, in accordance with the *Privacy Act 1988* (Cth) (**Australian Privacy Act**) were applicable.

Nothing is more important to us than our customers' safety and privacy. We take all reasonable steps to ensure that data in our possession or control is kept secure and not misused. Making our customers aware of our Privacy Policy is part of our commitment to providing you with the best possible service, so please take a moment to read the following policy and learn how we handle personal data.

Holders of parental, guardian or other legal responsibility are responsible for considering privacy of the watch wearer or person in their care and providing consents as desired for them.

We maintain and regularly review this Privacy Policy and take reasonable steps to comply with the Australian Privacy Act, the UK-GDPR, the GDPR and other EU privacy legislation, all to the extent applicable and as far as is reasonably practical in the circumstances of managing our business. To ensure your personal information remains confidential, we communicate this Privacy Policy to all our employees and make this Privacy Policy readily available and accessible to all customers, clients and service providers.

Please note that italicised words and phrases in this Privacy Policy have the meanings ascribed to them in the Australian Privacy Act and/or the GDPR and UK-GDPR.

ABOUT SPACETALK'S SYSTEMS

Spacetalk™ App and Spacetalk™ are fully owned by Spacetalk Holdings Pty Ltd and this business is a fully owned subsidiary of Spacetalk Limited, a Public Company listed on the Australian Stock Exchange (ASX company code: SPA) ABN 93 091 351 530. For the purposes of this and related policies, STW and Spacetalk are joint *data controllers*.

WHAT PERSONAL DATA WE COLLECT, HOLD AND USE

We will only collect personal data from you if it is reasonably necessary to provide services to you. We will only collect personal data for the purposes for which we advised you we were collecting it for or a related purpose which would reasonably be expected or otherwise with your permission.

Personal data we may collect and hold includes:

1. Personal Information: first name, last name, date of birth, gender, username, or similar identifier and title

2. Contact Data: billing address, email address and telephone numbers
3. Third-Party Contact Data: name (or nickname), phone number and photo (optional)
4. Financial Data: payment card details
5. Transaction Data: details about payments to and from you and other details of products and services you have purchased from us
6. Device Data: Phone Number, IMSI, Device ID, network information, request logs and Chat Handles
7. Profile Data: username, password, security pin and preferences
8. Location Data: Geographical location data and safe zone parameters
(With some of our products, such as Spacetalk™, we collect the geographical location of a smartphone or smartwatch. This data can be used to locate the carrier or wearer of the device. Location Data is collected solely for the purposes of assisting parents and caregivers to determine the location of the wearer or carrier of the device, under the explicit or implicit consent of that person. The services deal with location, so in order to work, the services need to know your location. Whenever you open and use/interact with our services on a mobile device, watch or go to one of our sites, we use the location information from your mobile or watch or other tracking device to tailor the services experience to your current location (we'll show your location). The services may also use your mobile device's background location to provide the services. If you have background location turned on, the services will, from time to time, inform us about your device's location even if you are not directly interacting with the services. How we collect this data is detailed below. Where we collect user data in a service we will comply with the relevant Apple App Store and Google Play Store requirements.)
9. Health Information (*sensitive information*): weight, average activity levels, movement/physical ability, medical conditions, medication/prescriptions.
10. We will only collect *sensitive information* about you if it is considered reasonably necessary for us to collect such information for us to perform our functions or activities and you consent, or collection is required by law or another exception under the GDPR, UK-GDPR or Australian Privacy Act applies.

HOW WE COLLECT YOUR PERSONAL DATA

We will generally collect the above personal data from you directly. We collect personal data from you in various ways such as when you communicate with us, when you fill in an application or form or survey, if you apply for a job with us, if we provide a product or service to you, or when you participate in any of our activities. We may also retain any messages you send through the service. We may also retain fall reporting (time and velocity of fall events). We use this information to operate, maintain, and provide to you the features and functionality of the services. We may also use this information to correspond with you, and to address any issues you raise about the services.

We may also collect data and personal information about individual from third parties and automatically, including through Web Servers and Location Data (as further set out below):

Website Servers: When you access our website and online services the Web Server Data listed above is collected. We advise Google Analytics Demographic and Interest reporting may be used to develop specific offers or advertising from time to time.

Location Data: we may collect this data in a variety of ways, including:

- Global Positioning System (GPS);
- Nearby Wi-Fi networks;
- Mobile cell tower triangulation;

- Near Field Communication;
- RFID.

We send the location of the wearer's device to our servers when you pair the device with a Spacetalk app user account and grant the device access to location services. We take user location privacy seriously.

Please note that we store or transmit actual location data away from the device itself on our servers, the degree of accuracy that the location data is stored is the same as what is accessible to the holder of parental responsibility through the Spacetalk app.

WEBSITE COOKIES

When you use and access our websites, we may place a number of cookies files in your web browser. We use cookies to help us recognise you, to improve your experience, increase security and measure use of our Services. We may also use cookies to ensure that content from our websites is presented in the most effective manner for you and your computer or mobile device and to enable certain functions of the Service such as to enable advertisements delivery.

Our Cookies Policy details the types of Cookies we use to run our service and your options regarding Cookies. Our current Cookies Policy can be viewed and downloaded from our website www.spacetalkwatch.com.

If you have any questions about opting out of the collection of cookies and other tracking/recording tools, you can contact us directly at privacy@spacetalkwatch.com.

THE PURPOSES FOR WHICH WE COLLECT, HOLD, USE AND DISCLOSE PERSONAL DATA

We collect personal data which is reasonably necessary for one or more of our functions as noted above and including to:

- maintain your account and contact details;
- allow you to download and purchase our products and services;
- process transactions and end user related information, including confirmations and invoices;
- communicate with you;
- provide you with access to protected areas of the site;
- verify data for accuracy or completeness;
- improve the quality of our services and develop new ones;
- Help our services deliver more useful, customized content such as location tracking and children's reward programs;
- Keep you posted on software updates, technical updates, security alerts and support and administrative messages;
- send marketing communication to you;
- conduct surveys to determine use and satisfaction;
- detect, investigate and prevent potentially unlawful acts or omissions or acts or omissions with the potential to breach our Privacy Policy or any other policy;
- comply with our legal obligations;
- combine or aggregate your personal data with data we collect from third parties and use it for the purposes set out in this Privacy Policy;
- protect a person's rights, property or safety;
- credit reporting purposes; and
- any other purpose made known in this Privacy Policy or other policy.

We will not use or disclose this data for a secondary purpose unless you consent to us doing so, or under the circumstances involved we believe you would reasonably expect us to use or disclose the data for a secondary purpose and that that secondary purpose is related to the primary purpose.

In the event that we hold *sensitive data* about you, we will only disclose or use that data with your consent or if the use or disclosure is directly related to the primary purpose.

Please note that we will also use or disclose your personal data or *sensitive data* if we are required to do so by law or a court/tribunal order; or if we reasonably believes that the use or disclosure of the data is reasonably necessary for an enforcement related activity or on behalf of an enforcement body, in which case we will make a written note of the use or disclosure or another exception applies under the Australian Privacy Act, UK-GDPR, GDPR or relevant EU privacy legislation.

LAWFUL BASIS FOR PROCESSING PERSONAL DATA UNDER THE GDPR (for users in the EEA)

For users in the EEA, we will only use and process your personal data in the following circumstances:

- Where you have provided explicit consent. You have the right to withdraw consent you provided to us at any time by contacting us.
- Where we need to comply with a legal or regulatory obligation.
- 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. Depending on the situation you can withdraw your consent by emailing privacy@spacetalkwatch.com. Where we are using your information because of a legitimate interest to do so, you have the right to object to that use, however, if you do so it may mean that it is not possible for you to continue using the services.

ANONYMITY AND PSEUDONYMITY

Spacetalk will allow its customers to transact with it anonymously or by using a pseudonym, wherever that is reasonable and practicable. However, this will not be possible if Spacetalk is required or authorised by law or other instrument to deal with customers who have been appropriately identified; or where it is impracticable for us to deal with individuals who have not identified themselves or who would prefer to use a pseudonym.

WHO DO WE DISCLOSE YOUR PERSONAL DATA TO?

Because Spacetalk and STW are part of a global business and group of companies, information may be shared with other related business units around the world. Information will be treated confidentially and only disclosed on a need to know basis.

Data will be protected in accordance with this Privacy Policy. We will not rent or sell your information into third parties outside Spacetalk and its group companies (including any parent, subsidiaries and affiliates) without your consent, except as noted in this section:

We work with other companies that help us provide our systems and services to our customers, and we may provide data to these companies for the purpose of providing the services and products to you and to facility our interests as stated above. Those service providers will only be provided with access to your information as is reasonably necessary for the purpose that we have engaged the service provider, and we will require that such third parties comply with our Standards and all applicable laws.

To enable us to provide you with data about our products and services we may disclose your personal data to credit reporting agencies and other third parties. The data we may disclose for credit reporting purposes includes, amongst other things:

- the fact that you have applied for credit and the amount;
- the fact that we are a credit provider to you; and
- payments which become overdue and for which debt collection action has started.

We may also use your personal data to:

- obtain from a credit reporting agency a credit report containing personal data about you in relation to commercial credit provided by us;
- obtain a report containing information about your commercial activities or commercial creditworthiness from a business which provides information about the commercial creditworthiness of a person; and
- obtain a report from a credit reporting agency and other information in relation to your commercial credit activities.

We may also disclose your personal data to third parties to whom you expressly ask us to send the personal data to or to third parties you consent to us sharing your personal data with.

DEALING WITH UNSOLICITED PERSONAL DATA

If we happen to receive personal data about you from a source other than you, or it is data provided by you which we did not request, we undertake to determine, within a reasonable period, if we could have requested such personal information in accordance and where applicable the Australian Privacy Act, UK-GDPR or the GDPR and handle the unsolicited information accordingly.

WHERE WE STORE YOUR PERSONAL DATA

You have the right to know where your personal information is stored.

Individuals in the United Kingdom

All your personal data is stored in UK: The personal data we collect from you is stored on secure information technology systems located in the United Kingdom.

Individuals in the European Union and European Economic Area

All your personal data is stored in UK: The personal data we collect from you is stored on secure information technology systems located in the United Kingdom.

Individuals in the Australia and/or New Zealand

All your personal data is stored in Australia: The personal data we collect from you is stored on secure information technology systems located in Australia.

INTERNATIONAL TRANSFER OF PERSONAL DATA

We operate on a global scale – as such the international transfer of data is an essential element of our business operations, for example, we may store and process personal data in a cloud service hosted outside the EU or Australia in any country in which we or our partners maintain their data.

Individuals in the European Union, European Economic Area and United Kingdom

For the provision of customer support, or to troubleshoot issues, we may give incidental access to our systems to suppliers or individuals outside of Europe and the United Kingdom.

Where we do provide access, it will strictly be under the European data protection rules, namely GDPR and UK-GDPR and our suppliers are also contractually obliged to abide by these regulations.

We have a rigorous selection process and work only with affiliates and service providers that offer the same level of security and data protection as we do. We make sure to have a contract signed with each third party that guarantees their confidentiality and dedication to the safekeeping of your personal data in accordance with the applicable laws.

We may also transfer your personal data overseas, for example if we receive a legal or regulatory request from a foreign law enforcement body. We will always take steps to ensure that any international transfer of data is carefully managed to protect your rights and interests and only transfer your personal data utilising encryption and pseudonymisation activities.

You have the right to ask for more information about the safeguards we have put in place as mentioned above. Contact us as set out in the details below if you would like further information.

ADOPTION, USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS

As a general practice, we do not collect or use government related identifiers. In any event we will not use or disclose a government related identifier unless it is reasonably necessary for an enforcement related activity by or on behalf of an enforcement body. We may also use or disclose a government related identifier related to you if we are allowed or required by law or regulation to do so.

QUALITY OF PERSONAL DATA

We take all steps reasonable in the circumstances to ensure that the personal data we collect from you is accurate, up to date and complete. Where we collect data from you directly, we rely on you to supply accurate data and we may not consider that further steps are required. We will also ensure that all steps reasonable under the circumstances to ensure that the personal data we use or disclose is, when considered in relation to the purpose for which we are using or disclosing the data, accurate, up to date, complete and relevant.

PROTECTION OF PERSONAL DATA

We will take all reasonable steps to protect your personal data from misuse, interference, loss, unauthorised access, modification and unlawful disclosure. Personal data that is no longer needed will be deleted or anonymized.

How you can protect your data

We urge customers to take every precaution to protect their personal data and the watch user data by changing passwords often, using a combination of letters and numbers, and make sure a secure browser and internet connection is used.

How we protect your data

We safeguard the security of the data with physical, electronic, and managerial procedures. We use industry best practice encryption all our services including Devices, Applications, Websites and Communications

All data is stored and processed in infrastructure restricted centres. The environment utilises start-of-the-art network security electronic surveillance, physical security and multi-factor access control systems to protect client data. The data centres are staffed 24x7 by trained security teams.

Network Security

We use purpose-built, integrated firewall and virtual private network (VPN) security appliances and systems which ensures the highest level of protection.

Police Background Checks

A condition of engagement of all our employees, consultants, contractors and sub-contractors, communication service providers and advisors is that they successfully pass Police Background Checks for any prior child safety and/or sexual offences. Any child safety or related offence results in the immediate termination of our relationship with that individual or organisation.

NOTIFIABLE PERSONAL DATA BREACH

In the event that there is a personal data breach and we are required to comply with the notification of eligible data breaches provisions under Australian privacy laws, the GDPR and/or any other regulations or legislation, we will take all reasonable steps to contain the suspected or known breach where possible and follow the following process set out in this clause.

We will take immediate steps to limit any further access or distribution where possible. If we have reasonable grounds to suspect that the data breach is likely to result in serious harm to any individuals involved, then we will take all reasonable steps to ensure an assessment is completed within 30 days of the breach or sooner if possible.

In the case of a personal data breach in the EEA we will without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the ICO in accordance with the Data Protection Act 2018, UK-GDPR and the GDPR.

If we reasonably determine that the data breach is not likely to result in serious harm to any individuals involved or any remedial action we take is successful in making serious harm no longer likely, then no notification or statement will be made.

Where, following an assessment and undertaking remedial action (if any), we still have reasonable grounds to believe serious harm is likely, as soon as practicable, we will provide a statement to each of the individuals whose data was breached or who are at risk. The statement will contain details of the breach and recommendations of the steps each individual should take. We will also provide a copy of the statement to the relevant Supervisory Authority (for users in the EEA).

We will then review the incident and take action to prevent future breaches.

YOUR RIGHTS OF ACCESS TO, AND CORRECTION OF, PERSONAL DATA

The laws of some countries grant particular rights in respect of personal information. Users in those jurisdictions may have the right to:

- Request a copy of your information;
- Request that we correct inaccuracies relating to your information;
- Request that your information be deleted or that we restrict access to it;
- Request a structured electronic version of your information; and
- Object to our use of your information;

Should you wish to make a request in respect of your personal information please contact us at privacy@spacetalkwatch.com.

In some circumstances we may not be able to comply with a request that you make in respect of your personal data. For example, we may not be able to provide a copy of your information where it infringes on the rights of another User. We may also be required to retain certain information that you ask us to delete for various reasons, such as where there is a legal requirement to do so. In some cases, you may have shared your information with third parties, such as by publishing a design on a third party's website. In that case we will not be able to delete the information, and you will need to contact that third party directly.

If we are unable to resolve your request, or if you are concerned about a potential violation, you may be entitled to report the issue or make a complaint to the data protection authority in your jurisdiction.

You may have specific rights in relation to your information depending on where you live.

CHILDREN'S PRIVACY

Whilst some of our products are aimed for child safety and supporting guardians and the holders of parental responsibility to monitor and protect their child's safety. We do not knowingly solicit personal information from children and the services are not offered to children.

PRIVACY – ENQUIRIES, REQUESTS, COMPLAINTS, BREACHES

Enquiries regarding this Privacy Policy or the personal data we may hold on you, should be made to our customer service team, whose contact details are below.

If you think your personal data, held by us, may have been compromised in any way or you have any other Privacy related complaints or issues, you should also raise the matter with a representative of our customer service team as soon as possible.

We will take all reasonable steps to ensure your claims are investigated and a formal response will be provided to you, within a reasonable time, considering the circumstances of your claims. If any corrective action is determined to be required, as a result of that investigation, we will take all

reasonable steps to rectify the situation and advise you of such, again within a reasonable time considering the circumstances.

If we do not resolve your enquiry, concern or complaint to your satisfaction or you require further information in relation to any privacy matters, please contact the relevant Supervisory Authority, whose contact details are below.

Office of the Australian information Commission (Aust)

Telephone 1300 363 992
Email enquiries@oaic.gov.au
Office Address Level 3, 175 Pitt Street, Sydney NSW 2000
Postal Address GPO Box 5218, Sydney NSW 2001
Website www.oaic.gov.au

Information Commissioner's Office (UK)

Telephone +44 (0) 303 123 1113
Email casework@ico.org.uk
Office Address Wycliffe House, Water Lane, Wilmslow SK9 5AF
Website www.ico.org.uk

CONTACTING Spacetalk Holdings Pty Ltd

Telephone +61 (0) 8 8104 9588
Email privacy@spacetalkwatch.com
support@spacetalkwatch.com
Office Address 154 Fullarton Road, Rose Park SA 5067, Australia
Postal Address As above
Website www.spacetalkwatch.com

CONTACTING SPACETALKWATCH UK LTD

for individuals in the United Kingdom

Telephone +44 (0) 208 0175868
Email privacy@spacetalkwatch.co.uk
support@spacetalkwatch.co.uk
Office Address Office 9, Business First
Burnbrae Road, Linwood Industrial Estate
Paisely PA3 3FP
Postal Address As above
Website www.spacetalkwatch.co.uk

CONTACTING SPACETALKWATCH UK LTD

for individuals in the European Union and European Economic Area

Email datarequest@datarep.com.au quoting 'SpacetalkWatch UK Ltd' in the subject line.
Online webform www.datarep.com/data-request

Postal Address Mail your inquiry to DataRep at the most convenient of the addresses.

Please note: when mailing inquiries, it is essential that you mark your letters for 'DataRep' not 'SpacetalkWatchUK Ltd' or your inquiry may not reach us.

Country	Address
Austria	DataRep, City Tower, Brückenkopfgasse 1/6. Stock, Graz, 8020, Austria
Belgium	DataRep, Place de L'Université 16, Louvain-La-Neuve, Waals Brabant, 1348, Belgium
Bulgaria	DataRep, 132 Mimi Balkanska Str., Sofia, 1540, Bulgaria
Croatia	DataRep, Ground & 9th Floor, Hoto Tower, Savska cesta 32, Zagreb, 10000, Croatia
Cyprus	DataRep, Victory House, 205 Archbishop Makarios Avenue, Limassol, 3030, Cyprus
Czech Republic	DataRep, IQ Ostrava Ground floor, 28. října 3346/91, Ostrava-mesto, Moravska, Ostrava, Czech Republic
Denmark	DataRep, Lautruphøj 1-3, Ballerup, 2750, Denmark
Estonia	DataRep, 2 nd Floor, Tornimäe 5, Tallinn, 10145, Estonia
Finland	DataRep, Luna House, 5.krs, Mannerheimintie 12 B, Helsinki, 00100, Finland
France	DataRep, 72 rue de Lessard, Rouen, 76100, France
Germany	DataRep, 3rd and 4th floor, Altmarkt 10 B/D, Dresden, 01067, Germany
Greece	DataRep, 24 Lagoumitzi str, Athens, 17671, Greece
Hungary	DataRep, President Centre, Kálmán Imre utca 1, Budapest, 1054, Hungary
Iceland	DataRep, Kalkofnsvegur 2, 101 Reykjavík, Iceland
Ireland	DataRep, The Cube, Monahan Road, Cork, T12 H1XY, Republic of Ireland
Italy	DataRep, Viale Gioerfio Ribotta 11, Piano 1, Rome, Lazio, 00144, Italy
Latvia	DataRep, 4th & 5th floors, 14 Terbatas Street, Riga, LV-1011, Latvia
Liechtenstein	DataRep, City Tower, Brückenkopfgasse 1/6. Stock, Graz, 8020, Austria
Lithuania	DataRep, 44A Gedimino Avenue, 01110 Vilnius, Lithuania
Luxembourg	DataRep, BPM 335368, Banzelt 4 A, 6921, Roodt-sur-Syre, Luxembourg
Malta	DataRep, Tower Business Centre, 2nd floor, Tower Street, Swatar, BKR4013, Malta
Netherlands	DataRep, Cuserstraat 93, Floor 2 and 3, Amsterdam, 1081 CN, Netherlands
Norway	DataRep, C.J. Hambros Plass 2c, Oslo, 0164, Norway
Poland	DataRep, Budynek Fronton ul Kamienna 21, Krakow, 31-403, Poland
Portugal	DataRep, Torre de Monsanto, Rua Afonso Praça 30, 7th floor, Algès, Lisbon, 1495-061, Portugal
Romania	DataRep, 15 Piața Charles de Gaulle, nr. 1-T, București, Sectorul 1, 011857, Romania
Slovakia	DataRep, Apollo Business Centre II, Block E / 9th floor, 4D Prievozska, Bratislava, 821 09, Slovakia
Slovenia	DataRep, Trg. Republike 3, Floor 3, Ljubljana, 1000, Slovenia
Spain	DataRep, Calle de Manzanares 4, Madrid, 28005, Spain
Sweden	DataRep, S:t Johannesgatan 2, 4th floor, Malmo, SE - 211 46, Sweden