VERSION: 2026.01

PRIVACY NOTICE

THIS PRIVACY NOTICE EXPLAINS HOW MYZONE PROCESSES YOUR PERSONAL DATA WHEN YOU USE THE MYZONE APP.

IT ALSO EXPLAINS HOW WE WILL PROCESS YOUR APP ACCOUNT DATA WHERE YOU USE YOUR APP ACCOUNT LOGIN DETAILS TO ACCESS A FACILITY ACCOUNT. FACILITY ACCOUNTS ARE ONLY ACCESSIBLE BY INDIVIDUALS WHO ARE EMPLOYEES OR OWNERS OF FACILITIES.

PLEASE READ IT CAREFULLY.

Effective for existing customers: January 2026

Introduction

Your privacy is very important to Myzone. Please read our Privacy Notice carefully and contact us if you have any questions.

Where you are based in the following jurisdictions, you should read the additional provisions contained in Schedule 1, which supplement the information in this Privacy Notice. In case of a conflict between the main body of this Privacy Notice and the supplement, the supplement will take precedence:

Australia

Canada

European Union

Kingdom of Saudi Arabia

Mexico

New Zealand

United Arab Emirates

United States (California, Virginia, Connecticut, Utah and Colorado (as well as other U.S. states that implement similar rights in the future).

The United Kingdom, the Isle of Man, and the above countries are approved countries.

Additional Global Compliance Notice

If you are located in a country that is not approved, it is your sole responsibility to ensure that your use of our App and Myzone Services complies with the applicable laws and regulations of that country. While we aim to align our services with recognised international privacy and consumer protection standards, we do not warrant or represent or guarantee that the App, the Myzone Service, its features (including premium and social functionalities), or related data processing activities meet the specific legal or regulatory requirements of jurisdictions not listed above.

- You are solely responsible for understanding and complying with any laws that apply in that country which are relevant to your use of the App and/or the Myzone Service, including age of digital consent, data protection laws, and health or fitness technology regulations;
- Myzone shall not be liable for any legal consequences, penalties, or losses or damages arising from your use of the App and/or the Myzone Service in a manner not permitted under your local laws;
- If you are unsure of your legal standing to use Myzone in your country, you should obtain independent legal advice before proceeding.

Where required by law or lawful authority, Myzone will cooperate with regulatory bodies or respond to valid legal requests, even in jurisdictions not otherwise listed above.

App	means the Myzone mobile software applications (and/or any part thereof) designed for downloading to mobile devices.
Facility	means a facility at which Myzone products can be used (i.e., any organised body or establishment, whether governmental, educational, commercial, or community-based).
Facility Account	means an account, accessible via a weblink, which the staff and owners of a Facility may access to manage the Facility's Myzone account.
Myzone Services	means all and/or any services that are provided by Myzone (or on behalf of Myzone) in relation to the App or Facility Account.

In this Policy "**Myzone**", **"we"**, **"us"** and **"our"** mean Myzone Holdings Limited. Myzone is the controller of your data and provides the Myzone Services. **"you"** or **"your"** means the individual who is accessing or using the Myzone Services.

Who are we and how can you contact us?

Myzone has its registered office and business address at Level 3, Gordon House, 10a Prospect Hill, Douglas, Isle of Man IM1 1EJ, British Isles. Myzone has registered with the Isle of Man Information Commissioner with the following details: R000702.

Questions or comments about this Privacy Notice may be submitted by mail to the address above, via support@myzone.org, or by telephone at +44 (0)115 7788 311.

Myzone has appointed a Data Protection Officer, who can be contacted at dpo@myzone.org.

Our representative in the UK is:

Myzone Group Limited, incorporated in England and Wales, number 9634208. Registered Office: Uwm House, 6 Fusion Court, Leeds, West Yorkshire, LS25 2GH, UK

Their contact details are: Myzone Group Limited, Suite 305, Third Floor, Merchants Court, 21-23 Castle Gate, Nottingham, NG1 7AQ.

or support@myzone.org

Our representative in the EU is:

Myzone Iberia S.L. Registered Office: C/ Roc Boronat, 147, Pl.1008018 Barcelona, Spain. Registration no: NIF B56597214

Their contact details are: Myzone Iberia, C/Menorca 19 PLANTA 7 46023 Valencia

Or support@myzone.org

What information do we collect?

Myzone collects the categories of personal information set out below. We receive this information from you, your devices, your use of the services and from third parties (see **Do we get personal data from third parties?** for further details). We use and disclose these categories of information for the purposes described in this Privacy Notice. The categories are:

- **Biometric and health data**, such as details of your exercises, activities or health data.
- **Contact data**, such as your email address, mailing address and phone number.
- **Demographic data**, such as your sex, age, and physical characteristics or description.
- **Geolocational data**, certain features and functionalities of the App are based on your

location. To provide these features and functionalities while you are using your mobile device, we may, with your prior consent, automatically collect geolocational information from your mobile device or wireless carrier and/or certain third-party service providers (collectively, "Geolocational Data"). Collection of such Geolocational Data occurs only when the App is running on your device. You may decline to allow us to collect such Geolocational Data, in which case we will not be able to provide certain features or functionalities to you.

- **Identity data**, like your name or username, profile photo, or other photos, Myzone status, and other similar identifiers.

- **Content data**, includes information stored on your device, including friends' lists, photos, videos or other digital content.

- **Usage data**, such as the usage data we receive when you access or use the App or a Facility Account. This includes information about your interactions with the services (such as times and periods of usage and non-usage).

- **Enquiry information**, means information you share with us when you make an enquiry or support call, including information collected via chatbots.

- **Profile data**, means information you add to your account, including your biography or country, password and your preferences.

- **Inferences** drawn from any of the above, including the number of calories you burned, distance and personalised exercise and activity goals.

- **Marketing and communications data**, includes your preferences in receiving marketing from us and our third parties.

- **Authentication data**, being information provided to us by an approved third-party authentication service where you choose to register or log in using that service.

International data transfers

Myzone is based in the Isle of Man; as such, when you use the Myzone Services, we receive your data and then, where you are based outside the Isle of Man, send it back to your country for use by you and your Facilities.

Where a Facility you wish to connect with is based in a country which has been deemed adequate for the purposes of the Isle of Man legislation (which means it provides 'essentially equivalent' protection to the protections applied to your data in the Isle of Man), we will transfer it on this basis.

Where a Facility is in a country which has not been deemed 'adequate', we rely on your consent to the transfer of the data.

IMPORTANT: Where you provide your consent, because the country the data is being transferred to is not deemed adequate, it is important that you note:

a. We will be transferring the information set out in the 'Facilities' section of 'Do we disclose any information to third parties?' to the Facility;

b. We will be transferring the data to enable the Facility to provide services to you in accordance with your arrangement with the Facility;

c. You can withdraw your consent at any time by removing their facility code in your App account;

d. The country in which the Facility we are sharing data with is not deemed adequate by the Isle of Man (which follows the approach of the EU), and we have not put in place any additional safeguards in respect of this sharing. This means that your data will not be subject to the same level of protection it receives in the Isle of Man (which reflects that provided in the EU), which includes the risk that:

i. Your data may not be subject to the same level of security;
ii. You may not be able to exercise the same rights in respect of your data;
iii. There may not be a supervisory authority with whom you can raise issues and who is responsible for enforcing data protection rules; and
iv. There may not be the same key principles which govern the processing of personal data, as apply in the Isle of Man. This may mean data can be held for longer than it would be in the Isle of Man, or may be inaccurate, for example.

Myzone also sends data (or it is sent on our behalf) to a range of organisations based in the following countries/regions, for the processing set out in this Privacy Notice:

- Australia
- Germany
- Singapore
- Spain
- United Kingdom
- United States of America

Where we do so, we will only share the data with those organisations where:

a. The receiving organisation is based in a country which has been deemed adequate by the UK, EU and Isle of Man (which means it provides 'essentially equivalent' protection to the protections applied to your data in the Isle of Man, UK or EU). Adequate countries, at the date of this Privacy Notice, are all European Union member states plus Norway, Iceland, Liechtenstein, Andorra, Argentina, Faroe Islands, Guernsey, Israel, Jersey, New Zealand, Republic of Korea, Switzerland, Uruguay, Canada (where the data is covered by Canada's Personal Information Protection and Electronic Documents Act), Japan (for certain transfers), the United States of America (where entities have satisfied certain requirements) and the United Kingdom; or

b. We (or the organisation sending the data on our behalf) have implemented standard contractual clauses with the receiving organisation, approved under EU, Isle of Man and UK law, which impose obligations on the receiving organisation and give you rights in respect of your data. We (or the organisation sending the data on our behalf) will also undertake a risk assessment to ensure that these clauses enable 'essentially equivalent' protection to the protections applied to your data in the Isle of Man, UK or EU.

Where a country has been deemed adequate by only some jurisdictions (the EU, UK, or Isle of Man), but not by others, we may decide to use only the standard contractual clauses approved by the jurisdictions that do not deem the country adequate.

You can contact us at any time using the contact details set out in this Privacy Notice if you would like a copy of the standard contractual clauses or the adequacy decision relied upon for our transfers.

Do we disclose any information to third parties?

We do not share your personal data with any other party except in the following situations:

Group companies

We may share your information with group companies **(Myzone Group Companies)** to provide you with support in relation to the App or Facility Account:

Myzone Inc, incorporated in Illinois, USA, number 70161893. Registered Office: 1755 Park St. Suite 200, Naperville, IL 60563, United States;

Myzone Group Ltd, incorporated in England and Wales, number 9634208. Registered Office: Uwm House, 6 Fusion Court, Leeds, West Yorkshire, LS25 2GH UK;

Myzone (APAC) Pty Ltd, ACN 606 655 887. Registered Office: 18 Sangiorgio Court, Osborne Park, WA 6017, Australia;

Myzone (Europe) GmbH, De-Saint-Exupéry-Straße 10, 60549 Frankfurt am Main, Registered office: Frankfurt am Main, Germany, Court of Registration: AG Frankfurt am Main, HRB 115303;

Myzone Tech (Asia) Pte. Ltd, incorporated in Singapore, number 202011967G. Registered office: 6 Eu Tong Sen Street #11-20 The Central, Singapore 059817;

Myzone Iberia S.L. Registered Office: C/ Roc Boronat, 147, Pl.1008018 Barcelona, Spain. Incorporated in Spain. Registration no: NIF B56597214

Subcontractors and Partners

We may share information with subcontractors or advisers that provide us with services, and partners with whom we work, so we can provide you with Myzone Services.

Our subcontractors, advisers and partners are required to keep the personal data that they receive confidential. These subcontractors, advisers and partners include the following:

- Hosting providers;
- Software providers and software support providers;
- Providers of support for the App;
- Credit checking and fraud prevention providers;
- Our professional advisers, including lawyers, bankers, accountants, auditors and insurers who provide legal, banking, accounting and insurance services;
- Marketing platforms to assist with marketing and customer services;
- Providers of automated features such as chatbots;
- Support platforms to help us track, prioritise and solve customer support issues; and
- Project management software providers;
- Analytics providers to help us gain insights into how our services are used and to help us improve:

Website analytics and conversion measurement:

When you interact with our website, we use analytics tools to understand how visitors use our site and how effective our marketing activities are. If you submit an enquiry or become a customer, we may link certain website analytics identifiers to your customer record so we can measure whether our website and marketing activity result in genuine enquiries or sales.

Where applicable, we may share limited conversion information with our analytics and advertising partners to support reporting, attribution, and optimisation of our marketing campaigns. These partners may act as data processors or, for certain advertising activities, joint controllers. We do not share direct identifiers such as your

name or email address for these purposes.

You can withdraw your consent for marketing and analytics-based processing at any time, and this will prevent further use of your data for conversion tracking and attribution.

Your Facilities

You can register to use your Myzone device/App at a Facility by selecting their facility identifier (facility ID, code or name) in your App account.

When you register a Facility, we will send them:

- your contact data;
- your demographic; and
- your identity data.

Where the Facility is not in a country deemed adequate under Isle of Man law, you provide your consent to such a transfer.

Additionally, the Facility can access data, as follows, when you have participated in any class or individual activity;

- the start time and duration of such activity;
- the number of calories burnt;
- the number of Myzone Effort Points (MEPs) earned;
- Heart rate data and heart rate zones;
- the names of your social connections linked with their Facility;
- the average effort percentage;
- your Myzone level status;
- the number of "likes" and the number of comments you have made on activities of other Myzone users and those relating to your activities.

If you do not want Facilities to have access to your information, you should not register a facility in your account.

We will also share the data contained in your App account, including your Biometric and health data, email address, Myzone device ID (if applicable), phone number, gender, reference ID, membership card number, target HR Zone, monthly target, resting heart rate, and maximum heart rate. We will permit the Facility to make changes to your nickname, Myzone device ID (if applicable), phone number, date of birth, gender, reference ID, membership card number, target HR Zone, monthly target, resting heart rate, maximum heart rate, your name and your email address, on your behalf, to ensure your data stays accurate.

If you do not want Facilities to have access or to make changes to your information, you should not register a facility in your account. If you have registered a facility to your account and wish to remove it, you should contact support via the App.

Individuals connected with Facilities are not our employees or agents, and you should satisfy yourself that the Facility has procedures in place to protect your privacy (and, if applicable, the privacy of any child).

A Facility may remove its facility identifier from your App account. It may also change the facility identifier to another facility identifier within its group to improve your experience.

Sharing your information with law enforcement

We may report to law enforcement agencies any activities that we reasonably believe to be potentially unlawful, or that we reasonably believe may aid a law enforcement investigation into potentially unlawful activity. In addition, we reserve the right to release your information to law enforcement agencies if we determine, in our sole judgment, that the release of your

information may protect the safety or property of any person or entity. Your data will only be shared with law enforcement agencies in the country in which you are located, unless it is reasonable for us to share it with authorities in other jurisdictions, but we will only do so where we are able to do so in accordance with our legal obligations.

Sharing your information as required by law or to bring or defend legal claims

We may share your information with others as required by law or as we believe is necessary to exercise our legal rights, to defend against legal claims that have been brought against us, or to defend against possible legal claims that we determine in our sole discretion might be brought against us. This may include sharing your information with governmental entities, or third parties in connection with subpoenas, court orders, other legal processes.

You may permit other Myzone users to access your information

You may choose to permit other Myzone users to access your activities, Biometric and health data and (provided you are aged 18 or over) images. If any user (including coaches/trainers) connected with a Facility wish to access this information (and your phone number) through their account, you will be advised by email, and you must provide your consent to their access.

Do we get personal data from third parties?

We will only receive personal data from organisations you give us permission to pull data from or to which you provide us with access (for example, you may link your Myzone account with your Apple Health account). We will tell you, at the time you provide the necessary instructions, what information we will be receiving.

Third-party authentication services

We allow you to create and access your Myzone account using an authentication service provided by an approved third-party platform. Approved platforms may include Meta, Google, Apple, and Microsoft. Use of a third-party authentication service is optional. You decide whether to connect your Myzone account to a third-party authentication service, and you can choose an alternative registration or login method where available. Where you choose to use a third-party authentication service, we receive certain personal data from that provider to enable account creation, authentication, and ongoing account access. The personal data we receive from a third-party authentication service may include:

- a unique user identifier provided by the authentication service
- your name
- your email address
- confirmation that the authentication has been successful

The exact data shared depends on the third-party platform you choose and the settings you have configured with that platform. We do not receive your password for the third-party authentication service.

We use this information solely to:

- create and authenticate your Myzone account
- link your Myzone account to the relevant authentication service
- help prevent unauthorised access and fraud

The third-party authentication provider processes your personal data independently under its own privacy notice and terms. We recommend that you review the relevant provider's privacy information before connecting your account.

You can disconnect a third-party authentication service from your Myzone account at any time through your third-party platform settings. If you do so, you may need to set an alternative login method to continue accessing your account.

How long do we keep your personal data?

We keep the information held on your account (which consists of all of your data except your Usage

data, Enquiry data and Marketing and communications data) until you use your account settings to, or otherwise ask us to, delete the data or your account in its entirety.

We will periodically review your account, and if you have not used your account in two years, we will notify you of our intention to delete your account at that point, and if you do not respond within one month, the information will be deleted within 6 months.

If you choose to close your Myzone account, your personal data will generally stop being visible to others on our Myzone services within 24 hours. We delete closed account information within 28 days of account closure, except as noted below.

When your account is deleted or closed, we delete any health data we hold about you, and we remove any identifiers from the rest of the data, so that it cannot be linked back to you in any way. This anonymised data will be used as set out in the section entitled **Anonymisation**, below.

Information you have shared with other users may remain visible after you close your account or delete information, or after we delete your account or after you revise your privacy options (see **Managing your privacy options**), as we do not control data that you have made available to third parties that they copy or extract from our systems. Your profile may continue to be displayed in the services of others until they refresh their account settings.

We keep other data we hold about you for the following periods:

Enquiry information: Where you make an enquiry while logged into the App or a Facility Account, we will keep that enquiry and details of who made the enquiry until your account or the Facility Account is deleted.

Marketing and communications data: Until you opt-out.

We may retain your personal data for longer than set out above if we are required to do so by law or regulatory requirements, to resolve any disputes or enforce our rights, or to prevent fraud or investigate security concerns. We will only keep the data for the time required in order to fulfil the purpose for which we retain the data and in no event shall we keep it longer than 7 years, unless we notify you otherwise.

Managing your privacy options

We have provided you with a means of managing your privacy settings. You can update your default settings in the App and control what and with whom you share your personal information.

The default settings are as follows (unless you are under age 18 and using a sub account of your parent or guardian, see the section on children's accounts for more details on this below):

Allow my connections to see "My Moves" data = ON (visible)

Allow my connections to see "My Photos" = ON (visible)

Allow my connections to see "My Connections" = ON (visible)

"Allow me to be viewed as a connection of a connection" = ON (visible)

You may at any time change your account settings so as to turn any of the settings above to "OFF".

Security

We store data on servers that are either owned or leased by us. We rent space for our servers from a dedicated hosting service provider that is compliant with ISO 27001 standards of security. We store our data at Domicilium, based in the Isle of Man, British Isles. The Quality and Information Security Management Systems of Domicilium have been approved by Lloyd's Register Quality Assurance (LRQA) to the following Quality and Information Security Management Standards: ISO 9001:2022; ISO/IEC 27001:2022.

We work hard to keep your data safe. We use a combination of technical, administrative, and physical controls to maintain the security of your data. No method of transmitting or storing data is completely secure, however. If you have a security-related concern, please contact us at the

Myzone contact details provided: support@myzone.org.

Children's accounts and Myzone's collection of information from children

The App is not directed to children under the age of 13. We adhere to the Children's Online Privacy Protection Act (COPPA) and will not knowingly collect personal information from any child under the age of 13. We ask that minors (under the age of 13) not use the App. If a child under the age of 13 has provided us with personal information, a parent or guardian of that child may contact us and request that such information be deleted from our records.

Once a child has attained the age of digital consent they give their own explicit consent to the processing of their personal data via their Myzone account, as they will have attained the age for valid consent.

Use limits

Users under 18 years of age are not permitted to upload photos. Users cannot search and locate other users unless the other party is at least 18 years old. Parties that are connected to a child's Myzone account can comment on a child's "moves" activity. Other chat functions and geolocation services are disabled.

Persons under the age of 13, or any higher minimum age in the jurisdiction where that person resides, are not permitted to create accounts. If we learn that we have collected the personal information of a child under the relevant minimum age, we will take steps to delete the information as soon as possible. Parents who believe that their child has submitted personal information to us and would like to have it deleted may contact us at; support@myzone.org.

Change in control or sale of Myzone and any Myzone Group Companies

Myzone may share your personal data and information as part of a sale, merger or change in control of all and/or any part of Myzone and/or any Myzone Group Companies, or in preparation for any of these events, where it is necessary, and we have a legitimate interest in running our business to do so.

Purposes for which we use your personal data

We have set out below the purposes (in addition to the change of control or sale purpose, set out above) for which we will use your data, the type of personal data we will use and the lawful basis for our use of the data.

Purpose or Activity	Type of Personal Data	Legal Basis for processing
To register you as a user	Identity data Contact data Demographic data Biometric and health data Profile data Marketing and communications data	Performance of a contract
To provide the Myzone Services (other than in relation to the Facility Account) to you (including sharing your data in accordance with the applicable settings).	Identity data Contact data Demographic data Images Geolocation data Content data Inferences Profile data Biometric and health data	Performance of a contract We will also obtain your consent where we are processing health data and geolocation data
To supply you with customer support	Identity data Contact data Profile data	Performance of a contract with you

Purpose or Activity	Type of Personal Data	Legal Basis for processing
	Usage data Enquiry information Geolocation data	
To provide you with access to a Facility Account and associated functionality, where applicable	Identity data Contact data Profile data	Our legitimate interest in providing the Facility Account functionality
To provide you with support when you are using a Facility Account	Identity data Contact data Profile data Usage data Enquiry information	Our legitimate interest in providing support for a Facility Account
For security purposes or to prevent or investigate possible fraud and/or other breaches of our terms and conditions of use of the Myzone Services and/or any attempts to harm the Myzone Services and/or any users of the Myzone Services and/or any third parties (including suppliers and Facilities) that may be in any way connected or associated with the Myzone Services	Identity data Contact data Usage data Profile data	Our legitimate interest in securing our services and enforcing our terms and conditions
To notify you in relation to Myzone legal obligations and documents, including changes to our terms and conditions or privacy notice, and to provide security messages, service announcements and administrative messages	Identity Information Contact Information	Our legitimate interest in keeping our users updated on important information To comply with legal obligations (to inform you of any changes to our terms and conditions or privacy notice or any other information we are legally required to provide)
To deal with queries and complaints from users	Identity data Contact data Enquiry information	Our legitimate interest in dealing with enquiries and complaints from users to operate our business and improve our services Performance of contract where we use the information to assist with performing our contract with you
To improve our offering to users	Identity data Contact data Demographic data Usage data Enquiry information Profile data	Our legitimate Interests in improving our products and services
To run prize draws or competitions	Identity data Contact data	Performance of contract (where terms and conditions are agreed) Our legitimate interests in engaging users
To administer, maintain, protect and update Myzone's systems (including security or technical related issues)	Identity data Contact data Profile data Usage data	Our legitimate interest in maintaining, updating and securing our systems

Purpose or Activity	Type of Personal Data	Legal Basis for processing
To anonymise your data for research or statistical purposes (see below for further information on anonymisation)	All data	Our legitimate interest in using the anonymised information for analytics and research
To share information with law enforcement	All data	Society's legitimate interests in assisting law enforcement If we share personal data, we shall do so on the basis processing is necessary for reasons of substantial public interest
To prepare for and enable a sale of some or all of the Myzone group	All data	Our legitimate interest in arranging the sale of all or part of the Myzone group
To determine what marketing to send you and to send you marketing emails	Identity information Contact information Profile information Usage data Marketing and communications data	Consent (where required by law) Our legitimate interest in promoting our business
To use your data for invitations and communications promoting membership and network growth, engagement and our Myzone Services, such as by showing your connections that you have used a feature on our Services	Identity information Profile information	Our legitimate interest in promoting our products and services
To help others find your profile, suggest connections for you and others and enable you to invite others to become a connection of yours	Identity information Profile information	Your legitimate interest in connecting with other people, improving your experience of our services. Our legitimate interest in offering enhanced functionality
To defend and bring insurance claims	All	Our legitimate interest in defending or making insurance claims Where we need to process your health data, we will only do so where we have a suitable legal right to do so

Where we share your health data (to the extent not covered in the table above), we will only do so with your consent or, where you are not able to give consent in your country, with the consent of a parent or guardian.

We will also rely on your consent to transfer your data to Facilities in countries not deemed adequate (see "**International data transfers**") and to transfer the additional personal data to Facilities (see the "Your Facilities" section of "**Do we disclose any information to third parties?**").

In addition to the purposes set out above, we may be required to:

a. process personal data we hold about you to comply with legal obligations we are subject to from time to time. Where possible, we will notify you of these obligations

and they will include responding to government bodies, where required, and responding to subject access requests; and

b. process your personal data to defend or pursue legal claims. In this case we will rely on our legitimate interests in pursuing a claim or defending ourselves. Whenever we use your data in these instances we shall ensure we have assessed whether your interests outweigh those being pursued in the specific case.

You must, at a minimum, provide your name, nickname, email address and secondary email address, phone number, date of birth, age, sex, weight, height, location, facility ID and belt ID to register as a user.

Regarding the above legal bases:

Legitimate Interests means that it is necessary to process your personal data for the purposes of our legitimate interests or for the legitimate interests of third parties (e.g., Facilities and/or Myzone Group Companies), provided that such processing shall not outweigh your rights and freedoms.

Performance of a Contract means we need to process your personal data for the purposes of our performing a contract with you (or entering into a contract with you).

Marketing

Myzone may use your Identity data, Contact data, Profile data, Usage data, and your Marketing and Communications data to decide upon what we think you may or may not want or need, or what may or may not be of interest to you. This is how we decide which products, services and offers may be relevant for you.

We will only send electronic marketing to you where you have consented to us doing so. You can ask us to stop sending you electronic marketing messages at any time by logging into your account and adjusting your marketing preferences or by contacting us on the contact details set out in this Privacy Notice.

Anonymisation

We will anonymise the data held on your App account when your account is closed. The information held on your App account is all of your data except your Usage data, Enquiry data and Marketing and Communications data. We will however never anonymise your health data.

We anonymise the data by removing key identifiers such as your name, email address and phone number, so that the information can no longer be linked to you.

We regularly review our anonymisation process to ensure that you cannot be re-identified from the information we have anonymised. As we do not anonymise health data and we remove any identifiers from the rest of your data, the risks of anonymising your data is low.

Once anonymised, anonymised information is not personal data and so you no longer have any rights in respect of this information, as it cannot be linked back to you.

We use anonymised information for analytics and statistical purposes. We will never make it public.

Your rights

We do not conduct any automated decision-making. You have the right, in respect of the personal data we process in respect of you, 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 for erasure where there is a reason, set out under law, which means we do not have to. If this is the case this will be notified to you, if applicable, at the time of your request.

When we delete your account completely we remove all identifiers from your information (other than health information which is deleted in its entirety).

Once an account has been deleted, we will not be able to recreate it.

Please note that the deletion of your account will render the Myzone Services unusable.

In some cases, we may hold identifiable information on our back-up systems. Where this is the case, it is put beyond use, and will be deleted within 90 days.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) to process your personal data 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, which overrides your right to object. This will never be the case in respect of direct marketing.

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 to us and which we rely on consent to use or we use the information to perform a contract with you. Users have a right to move their data from one Facility to another. However, if the other facility is not a Myzone customer, we will only be able to assist in transferring data if this is technically feasible. If you wish to transfer your account or receive a copy of your data, contact support@myzone.org.

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 services to you. We will advise you if this is the case at the time you withdraw your consent.

Exercising your rights Many of your rights above can be exercised via your account settings and tools to control our use of your personal data. For example, through your account settings, you can limit how your information is visible to other users of the services. If you need further assistance regarding your rights, please contact our Data Protection Officer at: dpo@myzone.org and we will consider your request in accordance with applicable laws.

Language

This policy was written in English. To the extent a translated version conflicts with the English version, the English version prevails.

Complaints

Should you wish to raise a concern about our use of your information (and without prejudice to any other rights you may have), you have the right to do so with your local supervisory authority, where you are based in the UK or EEA:

- If you are based in the UK, your supervisory authority is the ICO who can be contacted on the details set out here: https://ico.org.uk/make-a-complaint/data-protection-complaints/data-protection-complaints/
- If you are based in the EEA, your supervisory authority can be found here: https://edpb.europa.eu/about-edpb/about-edpb/members_en

You will also be able to raise a complaint with the Isle of Man supervisory authority, whose contact details can be found at Isle of Man Government - Isle of Man Information Commissioner

We would, however, appreciate the chance to deal with your concerns before you approach the relevant supervisory authority, so please contact us in the first instance at: dpo@myzone.org.

Changes to our Privacy Notice

Myzone will use your personal data for the purposes for which Myzone collected it, unless Myzone consider that Myzone needs to use it for another reason and Myzone believes that the relevant reason is compatible with the original purpose. If Myzone need to use your personal data for an unrelated purpose, Myzone will notify you, and we will explain the relevant legal basis of processing.

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.

If we decide to change our Privacy Notice, we will post those changes on this page, send an email notifying you of any changes or display a message on the App, and/or update the Privacy Notice modification date below. If the change relates to the use of children's accounts, an email will be sent to the relevant responsible adult, being the parent or guardian of the child, as well as the child.

Accessibility Statement

We are committed to making sure that our Site is accessible to everyone. To access this Privacy Notice in an alternative form, please contact us by:

- **Phone:** If you use assistive technology and run into any difficulties while using our site, please give us a call at +1 877 506 2878 and we will do everything we can to make it right.
- **Email:** If you prefer email, write us at dpo@myzone.org.

For more information, please see our Accessibility Statement.

Schedule 1- Additional jurisdiction-specific provisions

Australia

In addition to our general Privacy Notice set out above, this section sets out some specific details regarding how our Privacy Notice specifically applies to Australian users.

In collecting, holding, using, disclosing and otherwise managing the personal information of Australian users, we will comply with the *Privacy Act 1988* (Cth) ("**Australian Privacy Act**") and the Australian Privacy Principles contained in the Australian Privacy Act.

Under the Australian Privacy Act, "personal information" includes information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and regardless of whether the information or opinion is recorded in a material form or not. "Sensitive information" includes information about your health, racial or ethnic origin, genetic or biometric information.

Collection: Our Privacy Notice sets out the kinds of information we will collect from you. We will only collect your personal information from you, unless it is unreasonable or impracticable to do so or you have consented, in which case we may collect it from other sources. If we do not collect certain personal information from you, we may be limited in the products or services we can provide to you.

By providing or disclosing "sensitive information" to us, including through use of the Myzone Services, you consent to us collecting, holding, using and disclosing that "sensitive information" in accordance with this Privacy Notice. Details regarding the types of "sensitive information" that we may collect are set out in this Privacy Notice and include biometric and health information.

Disclosure: Our Privacy Notice sets out details regarding the third parties to whom we may disclose your personal information. Some of these third parties may be located outside Australia, including in the USA, EEA, Singapore and UK.

Access and Correction: As set out in our general Privacy Notice, you have the right to seek access and correction of your personal information. We take reasonable steps in the circumstances to ensure personal information we hold, use or disclose is accurate, up-to-date, complete, relevant and not misleading.

You may update information via your account. Additionally, upon request, we will grant access to the extent required or authorised by the Australian Privacy Act or other law and take steps reasonable in the circumstances to correct personal information where necessary and appropriate.

We will endeavour to respond to your request to access or correct your personal information within a reasonable period after your request. If we refuse your request to access or correct your personal information, we will provide you with written reasons for the refusal and details of complaint mechanisms. If you are dissatisfied with our refusal to grant access to, or correct, your personal information, you may make a complaint to the Office of the Australian Information Commissioner.

Privacy Complaints: In addition to the complaints section of our general Privacy Notice, please direct all privacy complaints to our privacy team via support@myzone.org. At all times, privacy complaints will be treated seriously, will be dealt with promptly, will be dealt with in a confidential manner, and will not affect your existing obligations or affect the commercial arrangements between us.

Our privacy team will commence an investigation into your complaint. You will be informed of the outcome of your complaint following completion of the investigation. In the event that you are dissatisfied with the outcome of your complaint, or the time in which we take to action or resolve it, you may refer the complaint to the Office of the Australian Information Commissioner.

The Office of the Australian Information Commissioner contact details are below:

Phone	1300 363 992
Online enquiry	https://www.oaic.gov.au/about-the-OAIC/contact-us
Website	www.oaic.gov.au

Address	Office of the Australian Information Commissioner
GPO Box 5288 Sydney NSW 2001	

Canada

In addition to our general Privacy Notice set out above, this section sets out some specific details regarding how our Privacy Notice specifically applies to users located in Canada.

In collecting, using, and disclosing the personal information of Canadian users, we will comply with the *Personal Information Protection and Electronic Documents Act* (Canada) and any applicable substantially similar provincial legislation.

Under Canadian law, "personal information" includes any information about an identifiable individual.

Collection and Use: Our Privacy Notice sets out the kinds of information we will collect from you, how we use and disclose that information. We will only collect your personal information from you, unless it is unreasonable or impracticable to do so or you have consented, in which case we may collect it from other sources. If we do not collect certain personal information from you, we may be limited in the products or services we can provide to you.

Marketing and Promotions. We will only send commercial electronic messages to you where you have consented to us doing so. You can ask us to stop sending you electronic marketing messages at any time by logging into your account and adjusting your marketing preferences, by clicking the "unsubscribe" mechanism contained in the message or by contacting us on the contact details set out in this Privacy Notice.

Consent. We will only collect, use, and disclose your personal information when we have your consent, which may be express or implied, depending on the circumstances, or as otherwise required or permitted by law. You have the right to withdraw your consent at any time, subject to contractual or legal obligations.

If you submit a request to withdraw your consent to use, communicate and store your personal information, how we handle that request will depend on the situation and reasons. Depending on the situation:

- You may withdraw your consent, but we will no longer be able to provide you a service or product that requires such consent;
- You may not withdraw your consent because processing your personal information is necessary or mandatory.

In either case, we may be legally required to retain certain personal information.

Disclosure and International Transfers: Myzone Limited collects your personal information and the data collected is transferred outside of Canada/Quebec to the Isle of Man. Our Privacy Notice sets out details regarding the Myzone group companies and third parties that we may disclose your personal information to. These third parties are also be located outside Canada/Quebec, including in the USA, EEA, Singapore and UK. We have contractual safeguards in place with all service providers to ensure you information will be protected in accordance with this Privacy Notice and applicable law.

If you have any questions about our use of third-party service providers, you may contact our Data Protection Officer.

We may also disclose your personal information under the following circumstances:

- You have authorized us to disclose the information to a third party for a specific purpose;

- If a person is acting as your representative or if we reasonably believe that the person has appropriate authorization to act (for example, a legal guardian), or is a person who owns a service or product jointly with you;

- To satisfy legal requirements;

- If we are required to provide personal information in response to a legitimate court order, subpoena to submit documents or investigation by authorities or as otherwise required by applicable law;

- If Myzone sells its business or assets, in whole or in part, or is involved in a merger, as required by such a transaction, or as part of due diligence pertaining to the transaction;

- As otherwise required or permitted by applicable law.

Who has access to your information. Your personal information is disclosed only to our authorized employees who have a business need to access it, for example: our customer service centre, billing department and personnel responsible for providing products and services to our customers. These employees can only access the personal information they require to perform their job functions.

Access and Correction. As set out in our general Privacy Notice, you have the right to seek access to and correction of your personal information.

You may update information via your account. Additionally, upon request, we will grant access to the extent required or authorised by Canadian law and take steps reasonable in the circumstances to correct personal information where necessary and appropriate.

We will endeavour to respond to your request to access or correct your personal information within a reasonable period after your request.

Request Deletion. You have the right to request deletion of your personal information if it is incorrect or not justified for the purposes for which it was collected.

Privacy Complaints: In addition to the complaints section of our general Privacy Notice, please direct all privacy complaints to our Data Protection Officer (contact details above in the main body of this Privacy Notice).

In the event that you are dissatisfied with the outcome of your complaint, you are entitled to contact the Office of the Privacy Commissioner of Canada toll-free: 1-800-282-1376. You may also contact the Office of the Information and Privacy Commissioner if you are located in Alberta or British Columbia or la Commission d'accès à l'information du Québec, if you are located in Quebec.

EU

In addition to our general Privacy Notice set out above, this section sets out some specific details regarding how our Privacy Notice specifically applies to users located in the European Union ("EU").

When processing personal data of European users, we will comply with the EU Regulation 2016/679 (General Data Protection Regulation, "**GDPR**") and applicable local data protection laws based on the user's residency.

1. Lawful Basis for Processing:

As explained above (c.f. "Purposes for which we use your personal data"), we process your personal data in accordance with applicable data protection law. This means that we only process your data if we have a legal basis for doing so. The legal bases listed above also exist under the European GDPR, although there are some local deviations.

We process personal data on several legal bases:

- **Consent** (Articles 6(1) and 9(2)(a) GDPR)

means that we explicitly ask you for your permission to process your personal data. This is particularly necessary when processing special categories of data, such as health data.

Your consent is voluntary and can be withdrawn at any time.

- **Special provision for children**

Country	Legal basis	Age of digital consent	Requirement for children below age
France	Articles 6(1)(a), 8(1) GDPR and Article 45 of Law no. 78-17 of 6 January 1978, as amended	15	Parental or guardian authorisation is required for children under 15
Germany	Articles 6(1)(a), 8(1) GDPR	16	Parental or guardian authorisation is required for children under 16
Portugal	Articles 6(1)(a), 8(1) GDPR and Article 16 of Law no. 58/2019 (LPDP)	13	Parental or guardian authorisation is required for children under 13
Republic of Ireland	Articles 6(1)(a), 8(1) GDPR and Section 31 of the Data Protection Act 2018	16	Parental or guardian authorisation is required for children under 16
Spain	Article 6(1)(a) GDPR and Article 7 of Organic Law 3/2018 (LOPDGDD)	14	Parental or guardian authorisation is required for children under 14
The Netherlands	Articles 6(1)(a), 8(1) GDPR and Article 5 of the GDPR Implementation Act (UAVG)	16	Parental or guardian authorisation is required for children under 16

- **Performance of a contract** (Article 6(1)(b) GDPR):

Means that we require your personal data for the preparation or performance of a contract with you, for example, when providing you with the Myzone Services or replying to your support tickets.

- **Legal Obligations** (Article 6(1)(c) GDPR):

Mean any processing activity, which is necessary for us to comply with legal obligations, recognizing differences across jurisdictions such as retention requirements under local tax and trade laws.

- **Legitimate Interests** (Article 6(1)(f) GDPR):

Means that the processing of your personal data is necessary for the purposes our legitimate interests, which override your interests or fundamental rights or freedoms which require protection of personal data. You can find our interests listed in the "Purpose of Activity" section listed under "Purposes for which we use your personal data".

2. Rights of the Data Subject

As stated under 'Your rights' above, you have various rights in relation to us, including under the GDPR:

- **Right of Access (Article 15 GDPR):**

You have the right to obtain confirmation from us as to whether or not personal data concerning you is being processed, and, where that is the case, access to the personal data and the information listed in Article 15(1)(2) GDPR.

- **Right to Rectification (Article 16 GDPR):**

You have the right to have inaccurate personal data concerning you corrected without undue delay.

- **Right to Erasure ('Right to be Forgotten', Article 17 GDPR):**

Subject to the requirements of Article 17 GDPR, you have the right to have your personal data deleted, for example when it is no longer necessary for the purposes for which it was collected.

- **Right to Restriction of Processing (Article 18 GDPR):**

Subject to the requirements of Article 17 GDPR, you have the right to restrict processing of personal data, for example, if the accuracy of the personal data is contested, or the processing is unlawful.

- **Right to Data Portability (Article 20 GDPR):**

Subject to the requirements of Article 20 GDPR, you have the right to receive personal data in a structured, commonly used format and transmit that data to another controller.

- **Right to Object (Article 21 GDPR):**

You have the right to object to processing based on legitimate interests or direct marketing on grounds relating to your particular situation.

- **Rights related to Automated Decision Making and Profiling (Article 22 GDPR):**

You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you.

3. Data Protection Officer (DPO):

You may contact our DPO at dpo@myzone.org for any concerns or inquiries, with responses tailored to meet local data protection standards.

4. Transfer of Data to Third Countries:

In order to provide the Myzone Services, your personal data may be transferred and stored outside your country. This includes countries and regions outside of the European Economic Area (EEA) and countries or regions that do not have laws that provide the same level of data protection.

Where we collect your personal data from within the EEA, a transfer outside the EEA will take place only:

- to a recipient in a jurisdiction approved by the European Commission as offering an adequate level of protection of personal data (so called adequacy decision). A list of approved countries can be found here: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, or

- to a recipient with whom we have concluded an agreement approved by the European Commission which covers the EU requirements for transfer of personal data to data processors or data controllers outside the EAA, like standard contractual clauses and considering additional safeguards required by local regulations.

5. Data Retention:

Data is retained as long as necessary for the purposes specified, within the constraints of the GDPR and specific local laws that may mandate different retention periods.

6. Security Measures:

We have implemented robust security measures to protect your personal data against unauthorized access, in compliance with GDPR and any specific requirements of local legislation (c.f. section “Security”).

7. Notification of Data Breaches:

Our data breach notification protocols adhere to GDPR standards and account for local law requirements, ensuring effective communication to affected individuals and authorities.

8. Automated Decision-Making and Profiling:

We do not use your personal data for automated decision-making processes, including profiling, that produce legal effects concerning or significantly affecting you. This practice aligns with Article 22 GDPR and is observed strictly across all jurisdictions.

9. Right to lodge a complaint

If you believe that we are not processing your personal data in accordance with applicable data protection law, you are encouraged to contact our Data Protection Officer (DPO). In any case and if you are not satisfied with our response, you can lodge a complaint with your local supervisory authority, for example:

Country	**Supervisory authority**	**Contact details**
France	French Data Protection Authority (Commission Nationale de l’Informatique et des Libertés – CNIL)	Address: 3 Place de Fontenoy, TSA 80715, 75334 Paris Cedex 07, France. Website: https://www.cnil.fr. Complaints may be submitted online.
Germany	German Data Protection Authorities (DPAs)	A list of all German supervisory authorities is available at: https://www.bfdi.bund.de/DE/Service/Anschriften/anschriften_node.html. You may lodge a complaint with any German Data Protection Authority.
Portugal	Portuguese Data Protection Authority (Comissão Nacional de Proteção de Dados – CNPD)	Address: Av. D. Carlos I, 134, 1.º, 1200-651 Lisbon, Portugal. Website: https://www.cnpd.pt. Telephone: +351 213 928 400.
Republic of Ireland	Irish Data Protection Commission (DPC)	Address: 21 Fitzwilliam Square South, Dublin 2, D02 RD28, Ireland. Website: https://www.dataprotection.ie. Telephone: +353 (0)761 104 800.
Spain	Spanish Data Protection Agency (Agencia Española de Protección de Datos – AEPD)	Address: C/ Jorge Juan, 6, 28001 Madrid, Spain. Website: https://www.aepd.es/es. Telephone: +34 901 100 099 or +34 91 266 35 17.
The Netherlands	Dutch Data Protection Authority (Autoriteit Persoonsgegevens)	Website: https://autoriteitpersoonsgegevens.nl. Complaints can be submitted via the authority’s online portal.

You also have the right to lodge a complaint with the supervisory authority in the Member State of your habitual residence, place of work, or place of the alleged infringement, in accordance with Article 77 of the GDPR.

You can find the contact details for your local data protection authority on the European Data Protection Board's website for EEA residents

(https://www.edpb.europa.eu/about-edpb/about-edpb/members_en), or through government websites for those residing outside the EEA.

10. Interaction with Local Laws:

We recognize that local data protection laws may impose additional obligations or grant further rights. Our policies are adapted accordingly to ensure comprehensive compliance tailored to the legal landscape relevant to each user's residency.

Under French law, you have the right to define instructions regarding the retention, erasure, or communication of your personal data after your death. These instructions may be general or specific and must be respected by the data controller.

Kingdom of Saudi Arabia

This section of the Privacy Notice only applies if you reside in Saudi Arabia. This section uses certain terms that are defined in the Saudi Arabia Personal Data Protection Law ("**Saudi PDPL**").

In collecting, holding, using, disclosing and otherwise managing the personal data of Saudi users, we will comply with the Saudi PDPL and its Regulations – namely the Implementing Regulation of the Saudi PDPL and Regulation on the Personal Data Transfer outside Saudi Arabia.

For the purpose of the Saudi PDPL, Myzone Holdings Limited is the controller and is responsible for the processing of your personal data as set out in this Privacy Notice. You can contact us at dpo@myzone.org.

Data retention

We will retain your personal data in an identifiable form only for the period necessary to fulfil (i) the purposes outlined in this Privacy Notice, (ii) our business and operational purposes and in line with our legal and regulatory obligations.

We will only retain your personal data after the purposes for which we collected it no longer exist, in the following cases:

- if there is a legal or regulatory requirement for retaining your personal data for a specific period, in which case the personal data shall be destroyed upon the lapse of that period or when the purpose of the collection is satisfied, whichever is longer.
- if your personal data is closely related to a case under consideration before a judicial authority and the retention of the data is required for that purpose, in which case the personal data shall be destroyed once the judicial procedures are concluded.

International transfer requirements

Please note that we transfer your personal data to countries or organisations outside of Saudi Arabia. We may also share your personal data with our affiliates or subcontract the processing of your data to, or otherwise share your data with, service providers located inside or outside Saudi Arabia. Such third parties may be engaged in, among other things, the provision of services to you, the processing of transactions, payments and/or the provision of support services. We will fulfil any requirements in relation to the international transfers of personal data under applicable laws.

Data security

We ensure your personal data is appropriately protected by utilizing the necessary physical, technical, administrative, and procedural security measures to prevent unauthorized access, collection, use, disclosure, copying, modification, or disposal. We safeguard and protect your data in a manner that complies with the applicable data protection regulation of Saudi Arabia.

In order to protect your personal data, we have put in place a number of technical and organizational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data, or unauthorized access, such measures include [please include the relevant security measures] taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organizational measures include restricting access to personal data solely to authorized persons with a legitimate need to know for the purposes of the processing operations.

Direct marketing

We will not send you any communications for the purpose of direct marketing without obtaining your prior explicit consent. If you consent to receive such direct marketing communications, you have at any time a right to opt out by contacting us via the email dpo@myzone.org or follow the instructions provided in the direct marketing communication.

Additional individual rights

In addition to the rights set out above in the Privacy Notice, you also have the following rights:

- right to be informed about the legal basis and the purpose of the collection of your personal data.
- right to request access to your personal data that we hold about you.
- right to request your personal data from us in a readable and clear format.

- right to request corrections to your personal data if incorrect, and/or modifications to your personal data if incomplete or updates where your personal data held by us is out of date. In this instance you may request us to restrict processing of your personal data that is incorrect.
- right to request destruction of your personal data.
- right to withdraw your consent you previously gave us to the extent any of your personal data is collected based on consent.
- right to lodge a complaint with the data protection authority in respect of our processing activities regarding your personal data.
- right to claim compensation for material or moral damage if you are harmed as a result of any violation stipulated under the applicable laws.

If you'd like to exercise your rights under the Saudi PDPL, please contact us via the email dpo@myzone.org.

Complaint or Objection Filing Method

If you have any concerns, or if we do not comply with the Saudi PDPL, you can file a complaint at dpo@myzone.org. If you are not satisfied with how we process your complaint, or if we fail to respond within 30, you can file a complaint to Saudi Data and Artificial Intelligence Authority as provided below:

SDAIA Address

Kingdom of Saudi Arabia

Riyadh

Website: sdaia.gov.sa.

National Data Governance Platform (DGP) (dgp.sdaia.gov.sa)

Mexico

This section of the Privacy Notice applies if you reside in Mexico.

In collecting, using, storing, and disclosing personal data of users located in Mexico, we comply with the Federal Law on the Protection of Personal Data Held by Private Parties (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) and its Regulations.

Controller
For the purposes of Mexican data protection law, Myzone Holdings Limited is the data controller responsible for the processing of your personal data.

Consent
We process your personal data with your consent where required under Mexican law. Consent may be express or implied depending on the category of personal data. Explicit consent is required for the processing of sensitive personal data, including health and biometric data.

Sensitive personal data
Sensitive personal data includes information relating to health and biometric identifiers. We will obtain your express consent before processing such data, except where an exception applies under Mexican law.

International transfers
Your personal data may be transferred to Myzone group companies and service providers located outside Mexico, including in the Isle of Man, the United Kingdom, the European Union, the United States, Singapore, and Australia.

We ensure that international transfers are carried out in accordance with Mexican law and that recipients assume obligations consistent with this Privacy Notice.

Your rights (ARCO rights)
Under Mexican law, you have the right to:

- access your personal data
- rectify inaccurate or incomplete personal data
- cancel personal data where permitted by law
- object to the processing of your personal data for certain purposes

You may exercise your ARCO rights by contacting our Data Protection Officer using the contact details set out in the main body of this Privacy Notice.

Right to lodge a complaint
If you believe that your data protection rights have been infringed, you may lodge a complaint with the National Institute for Transparency, Access to Information and Personal Data Protection (INAI).

National Institute for Transparency, Access to Information and Personal Data Protection (INAI)
Website: https://www.inai.org.mx

New Zealand

This section of the Privacy Notice applies if you reside in New Zealand.

In collecting, holding, using, and disclosing personal information of users located in New Zealand, we comply with the Privacy Act 2020 and the Information Privacy Principles contained within it.

Collection and use

We collect personal information only for lawful purposes connected with the provision of the Myzone Services. Where practicable, we collect personal information directly from you.

Consent

Where required by New Zealand law, including for the processing of health information, we will obtain your consent. You may withdraw your consent at any time, subject to legal or contractual restrictions.

Disclosure and overseas transfers

Your personal information may be disclosed to Myzone group companies and service providers located outside New Zealand, including in the Isle of Man, the United Kingdom, the European Union, the United States, Singapore, and Australia.

Where we transfer personal information outside New Zealand, we take reasonable steps to ensure that the recipient protects the information in a way that is comparable to the protections under the New Zealand Privacy Act 2020, including through contractual safeguards.

Access and correction

You have the right to request access to, and correction of, personal information we hold about you. We will respond to such requests within the timeframes required by New Zealand law.

Right to lodge a complaint

If you are not satisfied with our response to a privacy concern, you have the right to lodge a complaint with the Office of the Privacy Commissioner.

Office of the Privacy Commissioner

Website: https://www.privacy.org.nz

Telephone: +64 4 474 7590

United Arab Emirates

In addition to our general Privacy Notice set out above, this section provides specific details on how our Privacy Notice applies to users located in the United Arab Emirates (UAE).

In collecting, using, and disclosing the personal information of UAE users, we will comply with the relevant privacy laws and regulations in the UAE, including the UAE Federal Law No. 45 of 2021 on the Protection of Personal Data (the "Data Protection Law") and any other applicable regulations.

Under UAE law, "personal data" refers to any information that relates to an identified or identifiable individual, including but not limited to contact information, identification numbers, or any other details that can be used to directly or indirectly identify a person.

International data transfers:

We transfer your personal data to countries or organisations outside of the UAE. We will fulfil any requirements in relation to the international transfers of personal data under applicable UAE laws, ensuring that the data is protected in accordance with the Data Protection Law.

Data subject rights:

In addition to the rights set out above in the Privacy Notice, you also have the following rights under UAE law:

- Right to be informed about the legal basis and the purpose of the collection of your personal data.
- Right to request access to your personal data that we hold about you.
- Right to request your personal data from us in a readable and clear format.
- Right to request corrections to your personal data if incorrect, and/or modifications to your personal data if incomplete or updates where your personal data held by us is out of date. In this instance, you may request us to restrict processing of your personal data that is incorrect.
- Right to request destruction of your personal data.
- Right to withdraw your consent you previously gave us to the extent any of your personal data is collected based on consent.
- Right to lodge a complaint with the data protection authority in respect of our processing activities regarding your personal data.
- Right to claim compensation for material or moral damage if you are harmed as a result of any violation stipulated under the applicable laws.

Complaint or Objection Filing Method:

If you have any concerns, or if we do not comply with the UAE Data Protection Law, you can file a complaint the UAE Data Office.

United States (California, Virginia, Connecticut, Utah and Colorado (as well as other U.S. states that implement similar rights in the future).

Data Protection Laws means those data protection laws, regulations, guidelines, government issued rules and directives in the jurisdictions listed above applicable to processing personal data, including without (i) (the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020,(ii) the Colorado Privacy Act,(iii) the Virginia Consumer Data Protection Act, (iv) the Utah Consumer Privacy Act, (v) the Connecticut Data Privacy Act and (vi) the data protection laws of the United States and any other state or country, all as enacted or amended from time to time and any associated regulations or instruments and any other data protection and/or data security laws, regulations, regulatory requirements or codes of practice.

Privacy Rights

Your Rights. As a resident in a U.S. jurisdiction listed above, you have the right under the applicable Data Protection Laws to exercise free of charge:

(a) ***Disclosure of Personal Information We Collect About You.*** You have the right to know:

- The categories of personal information we have collected about you;
- The categories of sources from which the personal information is collected;
- Our business or commercial purpose for collecting or selling personal information;
- The categories of third parties with whom we share personal information, if any; and
- The specific pieces of personal information we have collected about you.

Please note that we are not required to:

- Retain any personal information about you that was collected for a single one-time transaction if, in the ordinary course of business, that information about you is not retained;
- Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information; or
- Provide the personal information to you more than twice in a 12-month period.

(b) ***Disclosure of Personal Information Sold or Used for a Business Purpose.*** In connection with any personal information we may sell or disclose to a third party for a business purpose, you have the right to know:

- The categories of personal information about you that we sold and the categories of third parties to whom the personal information was sold; and
- The categories of personal information that we disclosed about you for a business purpose.

(c) ***Right to Deletion.*** Subject to certain exceptions set out below, on receipt of a verifiable request from you, we will:

- Delete your personal information from our records; and
- Direct any service providers to delete your personal information from their records.

Please note that we may not delete your personal information if it is necessary to:

- Complete the transaction for which the personal information was collected, provide a good or service requested by you, or reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform a contract between you and us;
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity;
- Debug to identify and repair errors that impair existing intended functionality;

- Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law;
- Comply with the California Electronic Communications Privacy Act or any comparable law in Colorado, Connecticut, Utah or Virginia;
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when our deletion of the information is likely to render impossible or seriously impair the achievement of such research, provided we have obtained your informed consent;
- Enable solely internal uses that are reasonably aligned with your expectations based on your relationship with us;
- Comply with an existing legal obligation; or
- Otherwise use your personal information, internally, in a lawful manner that is compatible with the context in which you provided the information.

(d) ***Protection Against Discrimination.*** You have the right to not be discriminated against by us because you exercised any of your rights under the Data Protection Laws applicable to you. This means we cannot, among other things:

- Deny goods or services to you;
- Charge different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;
- Provide a different level or quality of goods or services to you; or
- Suggest that you will receive a different price or rate for goods or services or a different level or quality of goods or services.

  Please note that we may charge a different price or rate, or provide a different level or quality of services to you, if that difference is reasonably related to the value provided to us by your personal information

(e) ***How to Exercise Your Rights*****.** If you would like to exercise any of your rights as described in this Privacy Policy, please:

- Call us, toll-free, at +1 877 506 2878 ; or
- Email us at dpo@myzone.org.
- Please note that you may only make a related data access or data portability disclosure request twice within a 12-month period.
- If you choose to contact directly, you will need to provide us with:
- Enough information to identify you (e.g., your full name, address and customer or matter reference number);
- Proof of your identity and address (e.g., a copy of your driving license or passport and a recent utility or credit card bill); and
- A description of what right you want to exercise and the information to which your request relates.

We are not obligated to make a data access or data portability disclosure if we cannot verify that the person making the request is the person about whom we collected information, or is someone authorized to act on such person's behalf.

Any personal information we collect from you to verify your identity in connection with you request will be used solely for the purposes of verification.

If you have an established business relationship with us, you may choose to opt out of our sharing their contact information with third parties for direct marketing purposes. If you wish to opt out, please send an e-mail to our Data Protection Officer at: dpo@myzone.org.

Do Not Track

We do not monitor, recognize, or honor any opt-out or do not track mechanisms, including general web browser “Do Not Track” settings and/or signals.

Sale or Share of Personal Information of Consumers under 16 Years of Age

Myzone does not knowingly sell or share (for cross-context behavioral advertising) the personal information of consumers under 16 years of age. For more information about treatment of children’s personal information, see our **Privacy Notice**.

Personal Information Sales and/or Sharing Opt-Out and Opt-In Rights and Your Choices related to Cross-Context Behavioral Advertising and Profiling

You have the right to opt-out of the sale and/or sharing of their Personal Information.

Additionally, residents have the right to opt-out of profiling. In general, “profiling” is the automated processing of Personal Information to evaluate, analyze and/or predict personal aspects such as economic status, personal preferences, interests, behavior, etc. However, such profiling may not involve any further action. In other words, profiling effectively means gathering information about an individual (or group of individuals) and evaluating their characteristics or behavior patterns in order to place them into a certain category or group, in particular to analyze and/or make predictions about, for example, their interests and/or likely behavior. We may use your Personal Information to for such purposes at it relates to our marketing and advertising campaigns. To opt-out of such profiling, a consumer or their representative may submit a request to opt out of sharing, or selling or profiling by sending an email to support@myzone.org.