

General Privacy Policy (since: 06/06/2024)

Who we are

If you are reading this privacy policy (“**Policy**”), it is because you have somehow got in touch with Virgin Active Limited (“**Virgin**”, “**we**”, “**our**”, “**us**”) registered in England and Wales (company number 03448441 and VAT GB 777976151) with registered office at 26 Little Trinity Lane, Mansion House, London, EC4V 2AR.

We provide this Policy as **Controller** of your **Personal Data** to help you better understand how we handle your data, for what purposes and how you can control your information.

At the end of this document, you will find **Definitions**, referring to more detailed explanations of the capitalized terms.

What data we collect and process

The types of **Personal Data** we collect depends on how you interact with us. The categories below may be provided directly by you or by third parties:

- **Identification data:** any data that identifies you such as your name, surname, national and tax IDs details, and account details (e.g., nickname).
- **Contact details:** any information allowing us to contact you through any means such as e-mail and postal addresses, mobile number, push notifications, social media accounts. This category also includes IDs shared by social media (e.g., Meta) that allow us to show our ads to you. Social media act as **Joint Controllers** with us when we use their business targeting services.
- **Filled data:** any information inserted by you in our **Forms**, including in your Virgin membership contract.
- **Images:** pictures or videos relating to you when visiting our **Clubs** and **Events** or when you sign up for your membership.
- **Access data:** your presence in a specific **Club** at a certain time based on the check-in of your Virgin membership ID, the compilation of our **Forms**, or via **Images**.
- **Location data:** determined by inserting an address, city, or zip code or **Club** or when you consent to share your location via your **IP Address** or via the **Device**’s GPS. We make every possible effort to ensure this Information is not used to infer your Sensitive data.
- **Device data:** your **IP Address**, the date, time and the requested URL, **Unique Identifiers** and other information such as the type of your **Browser** or **Device**, the website you have arrived from (site of origin), the information you look at and any other actions carried out on our **Pages** or **App**. This information is collected using **Cookies**, **SDK** and **Other Tracking Technologies** that are on your **Browser** or **Device**. You can find the complete list of **Cookies** and **SDK** in the footer and privacy settings of our **Pages** and **App**. You can limit our collection of your location by changing your **Browser** or **Device** settings, as set out in the “How to control your Data and manage your choices” section below.
- **Payment data:** some payment data (e.g., bank ID codes) provided to pay your Virgin membership fees for yourself or for a third party. Please note that credit card details are processed only by payment gateways/credit institutions as autonomous **Controllers**. We only see the completion of the payment operation when payment is made by credit card.
- **Sensitive data:** mostly data relating to your health (e.g., your health statement, height, weight, “moves” which are a way of measuring and recording physical activity etc.). This information is provided by you directly as a membership requirement or via your use of our **Services** (e.g., to record your training).
- **Data inferred by your activity:** information based on your online and offline interactions with our **Forms** and **Services** (e.g., if you are interested in specific group classes, training days or hourly slots; when you contact us by e-mail, telephone regarding our products or request other information, we will collect and maintain a record of your contact details, communications and our responses) that allow us to create inferred data thanks to the **Combination and/or Crossing**. We do not infer information based on your Sensitive data.
- **Third party data:** any Identification data, Contact details, Filled data relating to a person other than you such as doctors, friends, spouses, guests, members, children etc, that we may process for the provision of our **Services**. If you provide us with the data of third parties (e.g., guests, Payment data for a gift), you will be held responsible for having shared such information with us. You must be legally authorized to share it (i.e., authorized by the third party to share their information or for any other legitimate reason). You must fully indemnify us against any complaints, claims or demands for compensation of damages which may arise from the processing of third-party **Personal Data** in violation of applicable data protection law.
- **Joint data:** any Contact details shared by **Business partners** (e.g., social media, co-branding companies, etc.) to whom we ask to send or display our ads to their users based on certain criteria/interests. These so-called micro-targeting and/or retargeting activities typically do not lead to the direct collection of **Personal Data** by us. Instead, they usually allow us to obtain **Aggregated data** on the effectiveness of those ads or lead to the registration of new members via our **Forms**. In

accordance with UK legislation, in carrying out these activities both we and our business partners make every reasonable effort to verify the lawfulness of the data (including joint controllership agreements) before they are used. You can request more information on our list of active business partners and the obligations of the respective parties by writing to [dpo\[at\]virginactive.co.uk](mailto:dpo[at]virginactive.co.uk)











How you engage with us determines the types of data we collect and the purposes we process such data for, as shown in our grids. You are not obliged to provide any information to us, but if you do not provide information when requested, this will impact some or all our purposes.

Digital user

If you are a digital user visiting our [Pages](#) and [App](#), we process your data as below.










 Purpose	 Data	 Legal Basis	 Fully automated means	 Retention Period	 Recipients
Responding to your requests (e.g. via e-mail, chat, call)	Identification data, Contact details, Filled data	 Your request	No	Fulfilment of your request	Personnel, Service providers, Authorities.
Providing our Services (e.g., e-commerce, Events) and related support	Identification data, Contact details, Filled data, Location data, Device data, Payment data	 Contract / terms and conditions	No	Fulfilment of the contract	Personnel, Service providers, Authorities.
Sending out marketing communications /surveys (via e-mail, phone, text, instant messengers, push notifications etc.) <ul style="list-style-type: none"> Classification of marketing communications based on objective, non-inferred criteria (e.g., gender, location, purchases) 	Identification data, Contact details, Joint data, Aggregated data	 Consent	No	Up to 2 years or until marketing consent is withdrawn	Personnel, Service providers, Business partners
	Identification data, Location data, Aggregated data	 Our legitimate interest in sharing relevant content that does not annoy you	No		Personnel, Service providers, Business partners
Customizing our Services including providing to you any Content that may be useful to you	Identification data, Location data, Filled data, Aggregated data, Data inferred by your activity, Device data, Access data.	 Consent	No	1 year or until consent is withdrawn	Personnel, Service providers.
Retargeting you on social media (e.g. Meta) and other display platforms	Contact details, Device Data, Data inferred by your activity.		Yes		Personnel, Service providers, Business partners
Analysing and improving our Services and creating new services and features	Location data, Filled data, Aggregated data, Data inferred by your activity	 Our legitimate interest in creating and maintaining Services that are truly useful to you	No	1 year for Personal Data 5 years for Aggregated data	Personnel, Service providers.



If you visit our **Clubs** (e.g., as a guest or a potential member), we process your data the same as above for a Digital user and for the additional purposes described below.

 Purpose	 Data	 Legal Basis	 Fully automated means	 Retention	 Recipients
Monitoring and protecting our Clubs, Personnel , guests and members	Images (CCTV), Access data	 Our legitimate interest in securing our and our guests' property and physical integrity	No	7 days	Personnel, Service providers, Authorities.
Registering your presence via our Forms at the entrance for safety and compliance reasons (e.g., evacuations)	Identification data, Contact details, Filled data, Access data	  Your request to access and our compliance with health and safety laws	No	3 months	Personnel, Service providers, Authorities.
Protecting you and us in case of injuries	Identification data, Contact details, Filled data, Sensitive data	 Protecting your vital interest and ourselves in the case of legal claims	No	As long as necessary	Personnel, Service providers, Authorities.

Member

If you become a member, we process your data the same as above for a Digital user, Visitor and for the additional purposes described below.

 Purpose	 Data	 Legal Basis	 Fully automated means	 Retention	 Recipients
Providing our main Services (e.g., access to Clubs , classes) and related support	Identification data, Contact details, Filled data, Payment data, Third party data	 Contract / terms and conditions	No	Fulfilment of the contract	Personnel, Service providers, Authorities.
<ul style="list-style-type: none"> Registering and recognising you in a Club as a member 	Images (or Identification data)	 Contract / terms and conditions	No	Fulfilment of the contract	Personnel, Service providers, Authorities.
Providing our ancillary Services (e.g., App , personal training services, Club access bracelet/wristband, syncing and sharing your training data with your Device , body composition checker , booking health checks)	Identification data, Contact details, Filled data, Payment data, Third party data, Sensitive Data	 Your request	No	Fulfilment of your request	Personnel, Service providers (e.g., Technogym S.p.A), Business Partners (e.g., doctors, Device's manufacturer etc.)

Protecting you and us in case of injuries	Sensitive data, including Third party data (health statement) upon your request	 Consent (via our Forms or your Device) / conduct or defence of legal claims	No	As long as you are a member	Personnel, Service providers, Authorities
Providing loyalty programmes as per our terms and conditions (e.g., vouchers, PT discounts or free sessions, VIP experiences, access and events, free upgrades)	Identification data, Contact details, Filled data, Access data (no Sensitive data is used)	 Your request	No	As long as you are a member	Personnel, Service providers, Business Partners (e.g., Endurance Zone Ltd and the rewards providers), Authorities

Regardless of whether you are a Digital user, Visitor or a Member, we process the data that you provide as required by the applicable law and regulations. Moreover, we process your data to prevent fraudulent and illegal behaviour or activities which could compromise you, our security, **Services** and Members. These processing operations are based on legal obligations upon us and our legitimate interest. Except for the retention periods / criteria described in the grids above or mandatory periods defined by the law, we may process your data for these purposes for no longer than 5 years.


Where your data are

Your data may be stored, accessed, used, processed, and disclosed outside your jurisdiction, including within the European Union, the United States of America, or any other country where our **Service providers** and sub-processors are located, or where their servers or cloud computing infrastructures may be hosted. We take steps to ensure that the processing of your data by our Recipients (as defined in the grids above) is compliant with the applicable data protection laws, including the UK laws to which we are subject. Where required by UK and/or EU data protection law, transfers of your data to recipients outside of the UK and/or EU will be subject to adequate safeguards (such as the EU or UK standard contractual clauses for data transfers between EU or the UK and non-EU countries), and/or other legal basis according to the UK and the EU legislation. For more information on the adequate safeguards, we have implemented with regard to data that is transferred to third countries, please write to: dpo[at]virginactive.co.uk

How you can control your data and choices

Based on how you got in touch with us, you can ask at any time to:

- **Access your Personal Data:** we will provide the data we have about you, such as Identification data, Contact details, preferences expressed etc., together with the version of this Policy you received when you provided them, and the source of the data (if, for example, they were provided to us by third parties);
- **Exercise your right to the portability of your Personal Data:** we will provide you with an interoperable file containing your data (csv, json, html files);
- **Correct your Personal Data:** for example, you can ask us to modify your e-mail address or telephone number if they are incorrect;
- **Limit the processing of your Personal Data:** for example, when you think that the processing of your data is unlawful or that processing based on our legitimate interest is not appropriate;
- **Delete your Personal Data:** for example, when you do not want to use our **Services** or do not want us to retain your data any longer;
- **Update your preferences for processing based on your consent:** you may request us to not send you promotional communications and/or to not personalize our **Services** including any **Content that may be useful to you**. More specifically:

-  Revoke your consent for the purposes for which we have collected it through the account settings of our **Pages** and **App**;
- Stop the sending of promotional communications by clicking on the link at the bottom of each e-mail and/or clicking on the "STOP" link to any text or other message you receive notification;
- Set up your preferences regarding data collected by the **Browser** and the **Device**;
- If you want to opt out from the push notification, you can withdraw your consent at any time, depending on the **Browser** or **Device** you are using according to its instructions.


- Block the sharing of some of your data within the **Programmatic Advertising** platforms that allow us to send you **Content that may be useful to you**, by using the [AdChoices](#) tool; the ones provided by the [Digital Advertising Alliance](#) or the [European Interactive Digital Advertising Alliance](#) in Europe.
- Block the sharing of some of **Unique Identifiers** via your **Device**. For iOS Devices: you can turn on the “Limit Ad Tracking” setting by going to Settings>Privacy>Advertising and select/toggle on “Limit Ad Tracking”. On the same page, you can also reset your advertising ID (so-called IDFA). For Android Devices: turn on the “Opt out of Ads Personalization” setting by going to Settings > Privacy > Advanced > Ads and select/toggle on Opt out of Ads Personalization.
- Limit the processing of Location data from your **Device** by choosing to enable the tracking of your location only for a short period of time or by providing us only with your address or zip code;
- Block the processing of **Other Tracking Technologies** (e.g., pixels) in our e-mail communications via your e-mail application. For example, on Outlook, the blocking of such tracking is turned off by design unless you press "Download images".



Contact the competent supervisory authority whose contact details are available [here](#).

In accordance with the applicable data protection laws, we will reply to your request within one month of its receipt (extendable for two further months in case of particular complexity). Please mind that some of your rights may not be available (e.g., correcting your data in CCTV footage) or be subject to restrictions if the applicable law allows.

You can exercise any of the rights listed above:

- by using a user-friendly web-form [here](#);
-  by writing to our Data Protection Officer (personaldata@virginactive.co.uk) or via letter to Virgin Active Limited with registered offices at 26 Little Trinity Lane, Mansion House, London, EC4V 2AR.
- By writing to the third parties who shared your data with us (e.g., **Business partners**, social media) via their e-mail address or your account settings on their platforms.

What is not cover by this Policy

This Policy explains and covers the processing operations that we carry out as **Controller**. The icons illustrated are under a [free license](#) or under [CC BY 4.0](#) by Maastricht University European Centre on Privacy and Cybersecurity (ECPC).

The Policy does not cover processing carried out by parties other than Virgin and in particular does not cover the processing carried out by our **Business partners** as autonomous **Controllers** including those carried out by social media platforms within **Our Pages** and **App**. With respect to such, we do not assume any responsibility for the processing of your data not covered by this Policy.

Changes to the Policy

This Policy is entered into force on the date indicated at the beginning of this document. We reserve the right to modify or update this Policy, in full or in part, at our discretion or as a consequence of changes in applicable regulations. We will inform you of substantial changes via your Contact details.

Definitions

Aggregated data: refers to statistical information about you that does not contain your Personal Data. We use this information for analysing and improving our Services and creating new services and features and to create statistical reports for Business partners.

App: refers to the mobile application “Virgin Active” available in the UK app stores (e.g. Apple Store and Google Play).

Authorities: refers to a government, being supranational, federal, state or governmental, prefectural or local government, statutory, administrative or regulatory body, court, agency, including a law enforcement agency, or any other authority in any part of the world (also outside of your jurisdiction) whose regulations, directives, notices, resolutions, orders, decrees, injunctions, warrants, subpoenas, or judgments are binding upon us and requires us to disclose your Personal Data. We will not share your data without your consent, unless we are under a legal obligation to comply with said regulations.

Browser: refers to programs used to access the internet (e.g., Safari, Chrome, Firefox, etc.).

Business partners: means third-party entities who communicate your Personal Data to us only after they have contractually assured us that they have obtained your consent or that they have another legal basis that legitimizes their communication/sharing of such data with us. This definition also includes the selected partners with whom we may share i) Aggregated data for business intelligence or partnership purposes or ii) if needed, a minimum set of your Personal Data based on your request (e.g. for providing you with rewards based on our loyalty programme). You may ask the disclosure of Business partners processing your Personal Data by using a user-friendly web-form [here](#).

Clubs: these include our fitness centres in the UK.

Combination and/or Crossing: this is the set of fully automated and non-automated operations which we used to create inferred data about you. We may also combine and/or cross information from different sources.

Content that may be useful to you: for example, if you search for a particular Service, we may display similar Services on our Pages or through Programmatic Advertising. Customization of the content may occur through the Combination and/or Crossing of data.

Controller or Joint Controller: refers to the legal person, public authority, service or other entity which, individually or jointly, determines the purposes and means for processing your Personal Data. In other cases, it may be preceded by the word "autonomous" (e.g., "autonomous Controller") to indicate that your Personal Data is processed by a subject other than us.

Cookie: A cookie is a small text file that is downloaded onto your device (e.g., smartphone, computer) when you access our Pages. It allows websites to recognize your Device and store information about your preferences or past actions (e.g., the fact that you visited our Pages, your language and other information). The information collected via cookies may be about you, your preferences or your Device and is mostly used to make our Pages work as you expect them to. Information collection via cookies does not usually directly identify you, but it can give you a more personalized experience on our Pages you are visiting, as they might be used to record your preferences regarding the use of Cookies (technical cookies), analyse and improve our Services and create new services and features or customizing our Services, including Content that may be useful to you.

Device: refers to the electronic device (e.g., iPhone) which you use to visit our Pages.

Events: refer to any event or webinar organised or managed by us as Controller.

Forms: any form through which we can directly collect your data (e.g., account sign-up, guest pass, visitors book etc.).

IP Address: is a unique number used by your Browser or your Device in order to connect to the internet. The internet service provider provides this number allowing identification of the provider and/or the approximate area where you are located. Without this data, you cannot connect to the internet and use our Services or use Content that may be useful to you.

Other Tracking Technologies: pixel tags (tracers used with Cookies and embedded in images on web pages to track certain activities, such as the viewing of Content that may be useful to you, or to see if an e-mail has been read) or Unique Identifiers embedded in links to promotional communications that send us information when clicked on.

Pages: includes our website (<https://www.virginactive.co.uk/>) and our social media pages.

Personal Data: means any information relating to an identified or identifiable natural person whether directly or indirectly, as well as any information that is linked or reasonably linkable to a particular individual or household. For example, an e-mail address (if it refers to one or more aspects of an individual), IP addresses, and Unique Identifiers are considered Personal data.

Personnel: our employees and collaborators who have undertaken an obligation of confidentiality and abide by specific rules concerning the processing of your Personal Data. This category also includes our or our Service providers' system administrators which assist us with the management of our IT systems and therefore can access, modify, suspend and limit the processing of your Personal data. These individuals have been previously selected, adequately trained and their activities tracked by systems they cannot modify.

Programmatic Advertising: these are platforms that share the information they collect about you, such as your IP Address and the data collected by Cookies, SDKs and Other tracking technologies, with entities who have an interest in showing you Content that may be useful to you. In our case, if you visualize a particular product on our Pages, we will ask participants in Programmatic Advertising to grant us an advertising space on one of the websites you visit in order to display Content that may be useful to you. On this point, we would like to reiterate that the communication of your Personal data to participants in Programmatic Advertising is based on your prior and specific consent provided on the banner when the first visiting our Pages. If you want to know how you can object to such communications, please follow the instructions in the "How you can control your Data and manage your choices" section above.

SDK: are software libraries that are installed together with a mobile application. They allow the collection of data in the same way as the Cookies do on the Browser. Depending on the settings of your Device, SDKs can collect Information about your location, Unique Identifiers, and Personal data inferred by your activity.

Sensitive Data: means Personal Data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and the processing of genetic data, biometric data aimed at uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Service providers: refers to an entities that we engage to process your Personal Data solely on behalf of and pursuant to the written instructions provided by us or external individuals (contractors) to whom we delegate some processing activities. For example, security systems providers, accounting, administrative, legal, tax, financial and debt collection consultants, data hosting platform providers, body measurement providers like Technogym S.p.A, etc. You may ask the disclosure of Service provides processing your Persona Data by using a user-friendly web-form [here](#).

Services: collectively, this means all the services/product available and accessible via our Pages, App and our Clubs.

Unique Identifiers: consist of information that can uniquely identify you through your Browser and Device. On the Browser, your IP Address and Cookies are considered Unique Identifiers. On your Device, advertising identifiers provided by manufacturers, such as Apple's IDFA and Android's AAG, which we use for analysing and improving our Services and creating new services and features including Content that may be useful to you, are considered Unique Identifiers. Please note that for these purposes and in line with the opinions of the relevant European and UK Supervisory Authority, we do not use other Unique Identifiers such as MAC Addresses and IMEIs as they are not resettable by you.