

Privacy Policy

PERSONAL DATA PRIVACY POLICY APPLICABLE TO USERS

TotalBodyUp, ("TotalBodyUp," "we," and "us") respects the privacy of its users ("you") and has developed this Privacy Policy to demonstrate its commitment to protecting your privacy. This Privacy Policy describes the information we collect, how that information may be used, with whom it may be shared, and your choices about such uses and disclosures. We encourage you to read this Privacy Policy carefully when using our application or services. By using our website or application (our "Service"), you are accepting the practices described in this Privacy Policy.

This Privacy Policy statement of Noatel Europe LTD, based in Chester House, 81-83 Fulham High Street, London, SW6 3JA, UK (hereinafter the "Data Controller" or "Company") sets out the procedures followed by us to collect, store and use the personal data concerning you (the "Data Subject" or "User"), and acquired through the use of our TotalBodyUp Application (or App), in accordance with Regulation (EU) 2016/679 (the "GDPR") and any other applicable privacy provisions laid down by the European Union, or the member States. The personal data concerning you shall be processed by us lawfully, fairly and in a transparent manner.

If you have any questions about our privacy practices, please refer to the below for information on how to contact us.

I. Personal Data Controller and Protection Officer

The Personal Data Controller responsible for your personal information is Noatel Europe LTD, based in Chester House, 81-83 Fulham High Street, London, SW6 3JA, UK. Please email any requests relating to the processing of any personal data concerning you to info.totalbodyup@noateleurope.co.uk, specifying your country of residence.

II. Categories of processed data, processing purposes and legal basis

With your consent, we may collect information that can identify you such as your name and date of birth ("personal information") and other information that does not identify you. We may collect this information through our website or our mobile application. By using the Service, you are authorizing us to gather, parse and retain data related to the provision of the Service. When you provide personal information through our Service, the information may be sent to servers located in Italy and countries around the world.

The Company, in compliance with art. 13 (1)(c), shall process the categories of personal data shown below, for the following purposes:

Purpose	Legal basis	Categories of processed data
a) To enable you to use the App the Company needs certain personal data (e.g. to create or modify your user account, allow you to use the application, send technical information about how the app works, process and reply to any requests, contact our support staff).	Processing is necessary for the performance of a contract to which you are party or in order to take steps at your request prior to entering into a contract (art. 6(1)(b) of the GDPR).	Common data: name, Apple and Google Play ID, date of birth, gender.
b) To let the User fully enjoy the Application's services and allow the Data Controller to access User's physical and health data.	The legal basis for the processing is consent of the Data Subject (art. 6(1)(a) of GDPR).	Health data, which fall under the special categories of personal data pursuant to art. 9 GDPR. These also include information on User's weight and physical activity (fitness level).
c) To carry out activities aimed at improving App user experience (e.g. market researches, statistical analysis, or other researches and analysis aimed at improving products and services, as well as for assess customers satisfaction in relation to App's services).	The legal basis for the processing is legitimate interest of the Data Controller (art. 6(1)(f) of GDPR) The legitimate interest of the Data Controller is reach improvements in relation to its products and services.	Common aggregated data (such as gender, date of birth or level of activity) and navigation information (such as cookie data, IP address, browser used, time of the visit, access time)
d) To discharge the Company's legal obligations and any other obligations arising out of the instructions received from the authorities (request for cooperation from a law enforcement or other government agency; to establish or exercise our legal rights; to defend against legal claims)	Compliance with a legal obligation to which the Data Controller is subject (art. 6(1)(c) and (e) of the GDPR)	Identification and common data such as: name, date of birth, Apple ID, Google Play ID.
e) To process any request for information and/or clarification raised by the Data Subject (also by allowing them to contact our support staff)	The legal basis for the processing is the legitimate interest of the Data Controller (art. 6(1)(f) of GDPR). Legitimate interest of the Data Controller is to process and give a proper feedback to any request raised by the Data Subject.	Identification information (such as name and date of birth) and eventual further information inserted within the contents of Data Subject's request.

III. Anonymous data collected automatically.

When you access our website or App, some information, such as IP address, is transferred. You are also providing information about the end device used (computer, smartphone, tablet etc.), the browser used (Internet Explorer, Safari, Firefox etc.), time of visit to the website, language, the operating system used by your device, access times and the referring website address.

We automatically collect this information from your browser or device by using various technologies but we cannot use this data to identify an individual user. We only use this information to determine how attractive our offers are and to track and improve their performance or content, if necessary, and make their design even more appealing to you.

We also may share aggregated, non-personal information, or personal information in hashed, non-human readable form, with third parties, including advisors, advertisers and investors, for the purpose of conducting general business analysis or other business purposes.

For example, we may engage a data provider who may collect web log data from you (including IP address and information about your browser or operating system), or place or recognize a unique cookie on your browser to enable you to receive customized ads or content. To opt-out of cookies that may be set by third party data or advertising partners, please go to:

<http://www.aboutads.info/choices/>.

These could be the technologies implemented to collect data:

- **Cookies and Use of Cookie Data.**

When you visit our website or App, we may assign your device one or more cookies to facilitate access to our Service and to personalize your experience. Through the use of a cookie, we also may automatically collect information about your activity on our website, the time and date of your visits and the links you click. If we advertise, we (or third parties) may use certain data collected on our Service to show you TotalBodyUp advertisements on other sites or applications.

- **Tracking Pixel tags.**

We embed pixel tags (also called web beacons or clear GIFs) on web pages, ads, and emails. These tiny, invisible graphics are used to access cookies and track user activities (such as how many times a page is viewed). We use pixel tags to measure the popularity of our features and services. Ad companies also use pixel tags to measure the number of ads displayed and their performance (such as how many people clicked on an ad).

- **Mobile Device IDs.**

If you're using our app, we use mobile device IDs (the unique identifier assigned to a device by the manufacturer), or Advertising IDs (for iOS 6 and later), instead of cookies. We do this to store your preferences and track your use of our app. Unlike cookies, device IDs cannot be deleted, but Advertising IDs can be reset in "Settings" on your iPhone. Ad companies also use device IDs or Advertising IDs to track your use of the app, track the number of ads displayed, measure ad performance and display ads that are more relevant to you. Analytics companies use device IDs to track information about app usage.

- **AppsFlyer**

Our apps and website are analyzed with technologies from AppsFlyer Inc. (111 New Montgomery St, San Francisco, CA 94105, United States). Various session and interaction data are collected from you and stored for this purpose. We need this information to improve the content and usability of our apps and website and to optimize the user experience for you. The session and interaction data are at no time processed in personalized form, but under a pseudonym. For more information on data processing by AppsFlyer, please refer to the Privacy Policy of the provider: <https://www.appsflyer.com/privacy-policy/>.

The legal basis for use is Art. 6 (1)(f) GDPR. AppsFlyer is certified under the Privacy Shield Agreement and thus guarantees compliance with European data protection legislation.

IV. Push notifications as part of the user experience and for marketing purpose

We may make use of push notification for marketing purposes on your mobile iOS and/or Android device even if the app is not open. In this case we'll require your consent if you wish to receive our push notifications. Our app only uses push notifications for marketing purposes if you have given your explicit consent to these. You can disable push notifications in settings at any time. If you use an Android device, push notifications are permitted automatically unless you disable this in your settings. You can disable these notifications by going into "Settings" on the app or by changing the app settings on your mobile device.

V. Data retention of User's Personal Data

We take security measures to help safeguard your personal information from unauthorized access and disclosure and will keep hold of your data for no longer than necessary. The length of the time we'll retain it will depend on any legal obligations we have, the existence of your consent, the nature of the contracts we have in place with you or our legitimate interest as a business. The Data Controller adopts all technical and organizational measures for preventing the loss, improper use and alteration of Data Subjects' Personal Data, and, in some cases, may adopt data encryption measures, too. Personal Data processed to fulfill legal obligations and obligations related to the use of the Application, (points II.a) and II.b)) will be kept for a period not exceeding the one necessary for the said purposes and, in each case, for no more than 10 (ten) years from the termination of the agreement (i.e., after the cancellation of the Application's account) except for any legal obligation that set a longer data retention period. At the end of this period, the processed data will be deleted or anonymized. Users' Personal Data processed for the purposes referred to in point II.c) will be kept until the User withdraws his/her consent (through functions and settings made available within iOS environment) or until termination of the agreement. Then, they shall be immediately deleted or anonymized. User's Personal Data processed for the purposes referred to in points II.d), II.e) and II.f) will be kept for no more than two years from the termination of the agreement (i.e., after the deletion of the Application's account). At the end of this period, the processed data will be deleted or anonymized.

VI. Rights of the Data Subjects

The Users, at any time and free of charge, can have and/or exercise the following rights, as specified in the GDPR:

a) the right to be informed on the purposes and methods of the processing;

- b) the right of access (in accordance with Article 15 GDPR);
- c) the right to obtain a copy of the data held overseas and obtain information concerning the place in which such data are kept;
- d) the right to ask for updating, rectification or integration of the data (in accordance with Article 16 GDPR);
- e) the right to request the cancellation, anonymization or blocking of the data (in accordance with Article 17 GDPR);
- f) the right to restrict the processing (in accordance with Article 18 GDPR);
- g) the right to object to the processing, wholly or partly, also where it is carried out through automated individual decision-making, including profiling (in accordance with Article 21 GDPR);
- h) the right to withdraw the consent to the processing of the data freely and at any time – in such a case, the processing carried out before withdrawal of consent shall remain valid;
- i) the right to data portability (in accordance with Article 20 GDPR) (i.e. to receive an electronic copy of User's personal data, if the User would like to port his/her personal data to himself or a different provider);
- j) the right to limitation of the processing (in accordance with Article 34 GDPR).

Data Subjects also have the right to lodge a complaint before the competent national data protection or judicial authority about our processing. For the exercise of their rights, Users may contact the Data Controller, in writing by sending a letter with proof of receipt to the Company's headquarters, or by sending an email to info.totalbodyup@noateleurope.co.uk. If Data Subject is under the age of 18 in California, in certain circumstances, he/she may request and obtain removal of Personal Data or content shared by him/her and posted on the App. Please This would not ensure complete or comprehensive removal of the content or information posted on the App by the User.

VII. How you can access your information

If you have a TotalBodyUp app, you have the ability to review and update your personal information. More information about how to contact us is provided above. You also may remove the app at any time by visiting the "Settings" page for your device. If you remove the app, we will retain certain information associated with your account to fulfill legal obligations and obligations related to the use of the Application, (points II.a) and II.b)) will be kept for a period not exceeding the one necessary for the said purposes and, in each case, for no more than 10 (ten) years from the termination of the agreement (i.e., after the cancellation of the Application's account) except for any legal obligation that set a longer data retention period. At the end of this period, the processed data will be deleted or anonymized.

VIII. Mandatory or optional nature of the supply of personal data and consequences of the refusal to answer

You can choose not to provide us with certain information, but that may result in you being unable to use certain features of our Service because such information may be required in order for you to register as user; purchase products or services. The provision of User's Personal Data for the purposes referred to in points II.a) and II.b) above is mandatory. Any refusal to provide the requested data could make it impossible to create an account and to enjoy the App's services. The processing of Personal Data for the purposes referred to in points II.c) above is optional. Any refusal to provide such data will not result in any detrimental consequences within the use of the App. The processing of User's Personal Data for the purposes referred to in points II.d) and II.e) above occurs on the basis of the legitimate interest of the Data Controller, pursuant to art. 6(1)(f) of the GDPR. In any case, Data Subjects can at any time exercise the rights referred to in point no. VII to have such processing ceased.

IX. Recipients of Personal Data and third-parties

Personal Data we collect may be shared with other Noatel Europe companies and third parties to develop, match profiling data and deliver targeted advertising on our Service and on websites or applications of third parties, and to analyze and report on advertising you see. We may combine non-personal information we collect with additional non-personal information collected from other sources. To be able to provide our service to you, to discharge the Company's legal obligations and any other obligations arising out of the instructions received from the authorities and to run our business, we may share data with third parties from the following categories of recipient:

- Public, judicial or police authorities, within the limits established by applicable laws and regulations (in this case users' data will not be disclosed, unless such disclosure is deemed necessary for the fulfillment of legal obligations and/or regulations);
- service providers, advertising partners, marketing agencies and ad networks. These companies provide professional service to us and may use tracking technologies, such as cookies or web beacons, to collect information about users who view or interact with their advertisements.
- Noatel Europe Company partners whom TotalBodyUp is part of. We may merge your information to improve your experience in our websites and apps. We may obtain both personal and non-personal information about you from other Noatel Europe businesses, business partners and other third parties.

We do not provide any non-anonymized personal information to third parties. These third-party websites may independently solicit and collect information, including personal information, from you and, in some instances, provide us with information about your activities on those websites. We recommend that you consult the privacy statements of all third-party websites you visit by clicking on the "privacy" link typically located at the bottom of the webpage you are visiting.

X. Transferring Personal Data to a third country outside the EEA

We will implement appropriate measures to ensure that your personal data remains protected and secure when it is transferred outside of your home country, in accordance with applicable data protection and privacy laws.

The Company may also transfer personal data of the Data Subjects to countries located outside the European Economic Area (EEA). In such cases, the Company will make sure that such transfer is based on appropriate safeguards listed in the GDPR, including (a) the standard contractual clauses developed by the European Commission; (b) the decisions of adequacy of the European Commission concerning the States in which the addressees are based; (c) binding corporate rules adopted by the Company and approved by the competent authorities or that are parties of agreements with the Company in this regard.

XI. Children's privacy

Although our Service is a general audience Service, we restrict the use of our service to individuals age 13 and above. We do not knowingly collect, maintain, or use personal information from children under the age of 13. If you believe we have received personal data from children under the age of 13, please email us at info.totalbodyup@noateleurope.co.uk

Please be reminded that, if the processing requires your consent for one or more processing purposes, you may give your consent only if aged at least 13 years (see art. 8 of the GDPR). If you are aged below 16, the consent must be given by a parent or other holder of parental responsibility (in the latter case, the Data Controller shall make every reasonable effort to verify that consent is given or authorised by the holder of parental responsibility).

Should we become aware that we have collected the personal data of a child aged below 13 years without the consent of a parent or holder of parental responsibility, we shall delete the data and close the relevant account forthwith.

XII. Changes and updates to this Privacy Policy

We may occasionally modify, update and/or integrate this Privacy Policy, also in view of future changes that may involve the Applicable Privacy Laws. It is understood that any modification, integration or update will be communicated to the Data Subjects promptly and on time via email or at the time of the start of the Application. In this regard, it could be required to the User to read the new version of the Notice and to accept it before continuing to use the Application.

Date of last amendment: 2019.03.26