

## PRIVACY POLICY/NOTICE

THIS PRIVACY POLICY AND NOTICE (“NOTICE”) DESCRIBE HOW INFORMATION ABOUT YOU, MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEWIT CAREFULLY. THIS POLICY DESCRIBES OUR POLICIES WITH REGARD TO “PERSONAL INFORMATION” AND WITH REGARD TO “PROTECTED HEALTH INFORMATION.

### **Privacy policy**

This Notice governs the Privacy Policy that applies to HomeFit+ application (the “App”) owned and operated by Dynamic Health & Fitness LLC (“DHF”) and its private partners that have licensed GoMotive platform. The App is located on the Apple and Gōogle stores.

This Notice does not apply to the privacy policy that your health care or fitness provider may use in their office. By using our App you represent that you are 18 years old or older and you consent to the information collection and use practices described herein.

### **CHANGES TO THIS NOTICE**

We reserve the right to change the terms of this Notice and our Privacy Policy. In case we change this Notice and our Privacy Policy we will post and communicate any changes.

### **WHAT PERSONAL INFORMATION WE COLLECT**

When you register for the App, we collect your name and email address.

### **WHAT STEPS DO WE TAKE TO PROTECT YOUR INFORMATION ONLINE**

DHF and its partners endeavor to secure your personal information from unauthorized access, use or disclosure by putting into place physical, electronic and managerial procedures to safeguard the information we collect through this App. Additionally, your account information is accessible online only through the use of a password. Please be aware, however, that despite our efforts, no security measures are perfect or impenetrable. To protect the confidentiality of your personal information, you must keep your password confidential and not disclose it to any other person. You are responsible for all uses of the App by any person using your password. Please advise us immediately by emailing us at [jmorgan@grayinstitute.com](mailto:jmorgan@grayinstitute.com) if you believe your password has been misused. You should also note that email is not secure, and you should not send any confidential or sensitive information to us via an unsecured email.

DHF and its partners utilize state of the art General Data Protection Regulation (the “GDPR”) and personally identifiable information (PII) controls. Your data will be encrypted. The creation, modification, and viewing of your data are tracked by DHF and its partners within its structured database.

The processing of personal data, such as name, address, e-mail address, or telephone number of a user shall always be pursuant to the GDPR, and in accordance with further country-specific data protection and privacy regulations applicable to the App. By means of this Notice we wish to inform the general public about the nature, scope, and purpose of the personal data we collect, use, and process. In addition, our App users are informed through this Notice of the rights to which they are entitled.

We as a “controller,” have implemented numerous technical and organizational measures to ensure the most complete protection of personal data processed through our App. However, Internet-based data transmissions can, in principle, entail security gaps, so that absolute protection may not be always guaranteed.

### **1. Definitions**

In accordance with the GDPR, our data protection Notice should be readable and understandable for the general public as well as for our customers and business partners. To this effect, we would first like to explain the terminology used.

In this data protection Notice, we use, amongst others, the following terms:

#### **(a) Personal data**

Personal data means any information relating to an identified or identifiable natural person (“data subject”). An identifiable natural person is subject who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social profile of that natural person.

**(b) Subject matter of the data**

The data subject is an identified or identifiable natural person whose personal data are processed by the controller for the purpose of processing.

**(c) Processing**

Processing is any operation or set of operations which is performed upon personal data or sets of personal data, including by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise divulcation, alignment or combination, restriction, erasure or destruction.

**(d) Limitation of processing**

Restriction of processing is the marking of stored personal data with the aim of limiting their processing in the future.

**(e) Profiling**

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, primarily to analyse or predict aspects of the individual's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

**(f) Pseudonymisation**

Pseudonymisation is the processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is stored separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

**(g) Controller**

The controller is the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data.

**(h) Processor**

Processor is a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.

**(i) Recipient**

The recipient is a natural or legal person, public authority, agency or other body, to whom personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular investigation are not considered recipients; the processing of such data by such public authorities must occur in accordance with the applicable data protection rules according to the purposes of the processing.

**(j) Third party**

A third party is a natural or legal person, public authority, agency or entity other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

**(k) Consent**

The data subject's consent is a freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or clear affirmative action, signifies consent to the processing of personal data concerning him or her.

**2. Name and address of the data controller**

The data controller for the purposes of the GDPR is:

Dynamic Health & Fitness, LLC Attn: Jay Morgan

8509 Van Wie Dr W Baldwinsville, NY 13027

[jmorgan@grayinstitute.com](mailto:jmorgan@grayinstitute.com)

Any interested person may, at any time, contact the data controller directly with all questions and suggestions relating to data protection.

**3. Data collection and general information**

DHF collects a series of general data and information when a data subject or automated system calls up the App. This general data and information are stored in the server's log files. The following information can be collected: (1) the operating system used by the access system, (2) the date and time of access to the website, and (3) any other similar data and information that can be used in the event of hacks on our computer systems.

When using this data and general information, DHF does not draw any conclusions on the subject.

#### **4. Routine deletion and blocking of personal data**

The controller processes and stores the personal data of the data subject only for the period necessary to achieve the purpose of storage, or insofar as this is permitted by the European or other legislative authorities in laws or regulations to which the controller is subject.

If the purpose of archiving is not applicable or if a retention period prescribed by the European legislative authority or another competent legislative authority expires, personal data are regularly blocked or deleted in accordance with legal requirements.

#### **5. Rights of the data subject**

##### **(a) Right of confirmation**

Every data subject has the right to obtain from the data controller confirmation as to whether or not personal data concerning him or her exist. If a data subject wishes to make use of this right of confirmation, he or she may, at any time, contact any employee of the controller.

##### **(b) Right of access**

Every data subject has the right to obtain from the data controller free information about his personal data stored at any time and a copy of this information. In addition, European directives and regulations grant the data subject access to the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;
- where possible, the expected period for which the personal data will be kept or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller the rectification or erasure of personal data, or the restriction of the processing of personal data relating to the data subject, or to object to such processing;
- the existence of a right to lodge a complaint with the supervisory authority;
- if the personal data are not collected from the data subject, any available information on their origin;
- the existence of automated decision-making processes, including profiling, as referred to in Article 22(1) and (4) of the GDPR and, at least in such cases, meaningful information about the logic involved, as well as the significance and expected consequences of such processing for the data subject.

In addition, the data subject has the right to obtain information on the transfer of personal data to a third country or an international organization. In such a case, the data subject has the right to be informed of the appropriate safeguards relating to the transfer.

If a data subject wishes to make use of this right of access, he or she may, at any time, contact any employee of the controller.

##### **(c) Right of rectification**

Every data subject has the right to obtain from the data controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject has the right to complete incomplete personal data, including by submitting a supplementary declaration.

If a data subject wishes to exercise this right of rectification, he or she may, at any time, contact any employee of the controller.

##### **(d) Right to erasure (right to be forgotten)**

Every data subject has the right to obtain from the data controller the erasure of personal data concerning him or her without undue delay, and the controller shall therefore erase personal data without undue delay if one of the following grounds applies, provided that the processing is not necessary:

- Personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.
- The data subject withdraws the consent on which the processing is based in accordance with Article 6(1)(a) of the GDPR, or Article 9(2)(a) of the GDPR, and where there is no other lawful basis for the processing.
- The data subject objects to the processing pursuant to Article 21(1) of the GDPR and there is no legitimate reason for the processing, or the data subject objects to the processing pursuant to Article 21(2) of the GDPR.
- Personal data have been unlawfully processed.
- Personal data must be erased in order to comply with a legal obligation to which the data controller is subject.
- Personal data has been collected in connection with the provision of information society services as referred to in Article 8(1) of the GDPR.

If one of the aforementioned scenarios applies, and a data subject wishes to request the erasure of personal data stored by DHF, he or she may, at any time, contact any employee of the controller. An employee of DHF shall immediately comply with the erasure request.

Where the controller has made personal data public and is required pursuant to Article 17(1) to erase those personal data, the controller shall, in view of the available technology and the costs of implementation, take reasonable steps, including technical measures, to inform other controllers of the personal data that the data subject has requested to delete and to destroy any links, copies or replicas of such personal data, insofar as their processing is not required. An employee of DHF shall arrange the necessary measures in individual cases.

**(e) Right to restriction of processing**

Every data subject has the right to obtain from the data controller the restriction of processing if one of the following conditions applies:

- The accuracy of personal data is contested by the data subject, for a period allowing the controller to verify the accuracy of those personal data.
- The processing is unlawful and the data subject objects to the deletion of personal data and instead requests the restriction of their use.
- The controller no longer needs the personal data for processing purposes, but is required by the data subject to restrict the use thereof for the establishment, exercise or defense of legal claims.
- The data subject objected to the processing pursuant to Article 21(1) of the GDPR pending verification that the legitimate grounds of the controller override those of the data subject.
- If one of the aforementioned conditions is met, and a data subject wishes to request the restriction of the processing of personal data stored by DHF he or she may, at any time, contact any employee of the controller, who shall therefore arrange the restriction of the processing.

**(f) Right to data portability**

Every data subject has the right to receive personal data concerning him or her that have been provided to the data controller in a structured, commonly used and machine-readable format. He or she has the right to transmit such data to another controller without hindrance to the controller to whom the personal data have been provided, to the extent that the processing is based on the consent referred to in Article 6(1)(a) of the GDPR or point (a) of Article 9(2) of the GDPR, or a contract within the meaning of Article 6(1)(b) of the GDPR, and the processing is carried out by automated means, provided that the processing is not necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Furthermore, in exercising his or her right to data portability pursuant to Article 20(1) of the GDPR, the data subject has the right to transmit personal data directly from one controller to another where technically feasible, on the condition that he or she does not adversely affect the rights and freedoms of other parties.

In order to assert the right to data portability, the data subject may at any time contact any employee of DHF.

**(g) Right to object**

Every data subject shall have the right to object at any time on grounds relating to his or her particular situation, to the processing of personal data concerning him or her, which is based on point (e) or (f) of Article 6(1) of the GDPR. This also applies to profiling based on these provisions.

DHF shall no longer process personal data in the event of an objection, unless we can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defense of claims.

If the DHF processes personal data for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing. This shall apply to profiling insofar as it is related to such direct marketing.

In addition, the data subject shall have the right, on grounds relating to his or her particular situation, to object to processing of personal data concerning him or her by DHF for scientific or historical research purposes, or for statistical purposes pursuant to Article 89(1) of the GDPR, unless the processing is necessary for the performance of an activity carried out for reasons of public interest.

In order to exercise the right to object, the data subject may contact any employee of DHF. In addition, the data subject shall be free, in the context of the use of Information Society services and notwithstanding Directive 2002/58/EC, to exercise his or her right to object by automated means using specific techniques.

**(h) Automated individual decision-making, including profiling**

Every data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects on him or her, or significantly affects him or her, provided that the decision (1) is not necessary for entering into or performing a contract between the data subject and a controller or (2) is not authorized by Union or Member State law to which the controller is subject and which also lays down appropriate measures to safeguard the data subject's rights and freedoms and legitimate interests, or (3) is not based on the data subject's explicit consent.

If the decision (1) is necessary for entering into, or performing, a contract between the data subject and a data controller, or (2) is based on the data subject's explicit consent, DHF shall implement suitable measures to safeguard the rights and freedoms of the data subject and his/her legitimate interests, or at least the right to obtain human intervention by the controller in expressing

his or her point of view and contesting the decision.

If the data subject wishes to exercise the rights concerning automated individual decision-making, he or she may, at any time, contact any employee of DHF.

**(i) Right to withdraw data protection consent**

Every data subject has the right to withdraw their consent to the processing of their personal data at any time.

If the data subject wishes to exercise the right to withdraw consent, he or she may, at any time, contact any employee of DHF.

**7. Legal basis for processing**

If the processing of personal data is necessary for the performance of a contract to which the data subject is party, such as when the processing operations are necessary for the supply of goods or the provision of any other service, the processing is based on Article 6(1)(b) GDPR. The same applies to processing operations that are necessary for the performance of pre-contractual measures, for example in the case of requests relating to our products or services. Our company is subject to the legal obligation to process personal data, e.g. for the fulfillment of tax obligations, the processing being also based on Article 6(1) GDPR.

In rare cases, the processing of personal data may be necessary to protect the vital interests of the data subject or of another natural person. This would be the case, for example, if a visitor was injured on our premises and their name, age, health insurance data or other vital information had to be transmitted to a doctor, hospital or other third party. Then the processing would be based on Art. 6(1)(d) GDPR.

Finally, processing operations could be based on Article 6(1)(f) GDPR. This legal basis is used for processing operations that are not covered by any of the above-mentioned legal grounds, if the processing is necessary for the purposes of the legitimate interests pursued by our company or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require the protection of personal data.

**8. Duration of data storage**

The criteria used to determine the retention period for personal data are the respective statutory retention periods. After the expiry of this period, the corresponding data are routinely deleted, provided that they are no longer required for the fulfillment of the contract or the initiation of a contract.

**9. Provision of personal data as a legal or contractual requirement; Requirement necessary to enter into a contract; Obligation of the data subject to provide personal data; Possible consequences of not providing such data**

We underline that the provision of personal data is in part required by law (e.g. tax regulations) or may also result from contractual provisions (e.g. information about the contractual partner).

Sometimes, in order to enter into a contract, a data subject may be required to provide his/her personal data, which must subsequently be processed by us. The data subject shall, for example, provide us with personal data when our company enters into a contract with him or her. Failure to provide personal data would result in the suspension or non-conclusion of said contract.

Before personal data are provided by the data subject, the data subject shall contact any employee. The employee shall clarify to the data subject whether the provision of the personal data is required by law or contract or is necessary for the conclusion of the contract, whether there is an obligation to provide the personal data and the consequences of not providing the personal data.

**10. Data Transfers**

While the EU-U.S. Privacy Shield framework for the transfer of data from EU to the U.S. has been invalidated, DHF is committed to comply with all the relevant and applicable law to transfer controlled data from the country in which such data was originally collected to Canada and the United States. This means that data transfer from the EU to Canada and to the United States will occur affording a level of protection essentially equivalent to that guaranteed within the EU.

**11. Existence of automated decision-making processes**

As a responsible company, we do not use automated decision-making or profiling.

Last updated: November 2022.