

MOVE Score Data Privacy Statement

June 1st, 2024

Welcome to MOVE Score, a service of Dolphin Technologies GmbH, Stella-Klein-Löw-Weg 11, A-1020 Vienna, Austria (hereinafter "**Dolphin**", "**we**", "**us**" or "**our**").

The MOVE Score app informs you ("**User**" or "**you**") about both your MOVE Score and your MOVE IQ. The MOVE Score represents your overall risk while driving on the road and considers how much you drive and your driving behavior (MOVE IQ), such as obeying speed limits, cornering speed, braking and acceleration behavior as well as not using your smartphone while driving.

Your additional benefit is that the MOVE Score App allows you to share the MOVE Score with any insurance company you authorize. In such a case the insurance company will request the score associated to the hash of your email address. We will forward this request to you and only share the MOVE Score after your confirmation.

Further information can also be found on our product website at www.movescore.app. Information about us can be found at www.dolphin.io. Please read the documents carefully as they govern your use of the Service.

This Data Privacy Statement applies to the processing of personal data when you are using our Service (as defined below). It explains which personal data we collect, process and store.

If you have any questions about the collecting, storage and processing of personal data, please contact us at privacy@movescore.app.

1. Name and address of the Data Controller

Dolphin Technologies GmbH
Stella-Klein-Löw-Weg 11
1020 Vienna / Austria
email: privacy@movescore.app

2. Scope of Application, General Principles

- 1.1. This Data Privacy Statement applies to the processing of personal data when using our "**Service**", meaning Dolphin's
 - MOVE Score App ("**App**");
 - Website www.movescore.app ("**Website**");
 - all of our Content (as defined in Section 4) and
 - all modifications and new features.
- 2.1. By using our Service and/or signing up for an Account ("**Account**"), you agree to be bound by this Data Privacy Statement including any policies or other terms referred to in or incorporated by this Data Privacy Statement (such as our Terms of Use). If you do not agree with this Data Privacy Statement or our Terms of Use, you must not use our Service.
- 2.2. We are committed to the sensitive handling and active protection of personal data as well as transparent information for users, especially regarding data collection and use. **However, please keep in mind that the main purpose of our Service is to collect and analyze user data. Therefore, it is in the nature of the contract between you and Dolphin that personal data (particularly data on location, mobility, etc.) will be processed.**
- 2.3. To technically cover data protection as good as possible, we encrypt the data collected and rely on encrypted transmission to our high available and secure server infrastructure.

2.4. **“Personal Data”** refers to any information that relates to an identified or identifiable individual. This includes not only obvious identifiers like a person's name, address, email address or social security number but also less obvious data such as online identifiers, location data and more. Essentially, if a piece of information can be used to identify an individual directly or indirectly, it qualifies as personal data. If data are anonymized in such a way that it can no longer be linked to a person (**“Anonymized Data”**), they are no longer “personal data” and therefore not included in the scope of data protection law.

2.5. **„Processing“** in accordance with the GDPR means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.2. In general, personal data will be deleted as soon as they are no longer required to achieve the purpose for which they were collected or to comply with contractual or legal obligations. This is the case when the data is no longer required for the performance of the contract. Even after the contract has been concluded, it may be necessary to store personal data of the contractual partner to comply with contractual or legal obligations.

3. **Registration, Creating an Account**

3.1. When you register for our Services and create an Account, the following data and information are collected, stored and processed:

- hash of your email address

to provide the highest level of privacy, the email address you are entering during registration is hashed on your smartphone. We only receive this hash value and thus are practically not able to personally identify you.

3.2. You may delete your Account at any time by informing us via email at privacy@movescore.app. When doing so, please make sure to send from the same email address as you used for registration, as otherwise we will not be able to identify your Account. Please note that in such a case all collected data will be deleted from our systems. This does not apply to anonymized processing results and information we need to comply with contractual or legal obligations (like billing information).

4. **Using our Service**

4.1. Our Service is designed to collect, evaluate and analyze driving behavior. When you are using the App, we therefore collect process and store the following data:

- location data,
- sensor data (gyroscope, acceleration sensor, magnetometer),
- activity data provided by the smartphone operating system which we receive from your smartphone,
- smartphone brand,
- smartphone model,

- smartphone operating system.

4.2. The legal basis for the processing of the data is your consent pursuant to Art 6 (1) lit a GDPR, which you give us in the course of registration. Since the processing of the data is the main purpose of our Service, the additional legal basis for the processing of the data is also in any case Art 6 (1) lit b GDPR.

5. **Automated individual decision-making, including profiling (Art. 22 GDPR)**

5.1. Based on the collected data as shown in chapter 4, the Service automatically calculates your personal MOVE Score which represents your overall risk while driving. MOVE Score considers the number and duration of your trips as well as the type of roads you travel on, with highways being the safest and rural roads posing higher risks. In addition, the MOVE IQ, which consists of the elements (a) compliance with speed limits, (b) general driving behavior (cornering, acceleration, braking) and (c) distraction (usage of smartphone while driving), is considered.

If you share your MOVE Score with an insurance company of your choice, your MOVE Score can be considered in premium calculations and allow discounts and other benefits for safe drivers.

5.2. The legal basis for the processing of the data is your consent pursuant to Art 22 (2) lit c GDPR, which you give us during registration. When you are sharing your MOVE Score with a Third Party like an insurance company, the additional legal basis for the processing of the data is also in any case Art 22 (2) lit a GDPR.

6. **Communication, User Journey**

6.1. We may contact you via push messages within our App. For this purpose, we collect, process and store the following data:

- location data,
- smartphone sensor data,
- activity data provided by your smartphone (operating system),
- App-ID,
- function calls in the app.

6.2. To send messages, we make use of external service providers:

- Google Firebase Cloud Messaging – Google LLC, Ireland
Gordon House, Barrow Street, Dublin 4, Ireland,
- For automated messaging workflows: Peaberry Software Inc. – “Customer.io”, USA,
921 SW Washington Street, Suite 820, Portland, Oregon 97205

Data Storage in European Union

You can find more information on how Peaberry Inc. handles user data in their privacy policy:

<https://customer.io/legal/privacy-policy/>

6.3. The legal basis for the processing of the data in order to communicate directly with you is the fulfillment of the contract or pre-contractual measures between you and Dolphin pursuant to Art 6 (1) lit b GDPR.

7. **Mandatory Third-Party components – Software Development Kits (SDK)**

The following SDKs are essential for the App to function and cannot be deactivated. These SDKs ensure the functionality of our App and are technical interfaces that transmit various user or technical data to third-party providers or receive data from them. The SDKs are active as long as the app is installed and used.

The legal basis for the processing of the data is your consent pursuant to Art 6 (1) lit a GDPR, which you give us during registration. Since the SDKs are technically mandatory for our Service, the additional legal basis for the processing of the data is also in any case Art 6 (1) lit b GDPR.

7.1. Google Firebase Cloud Messaging – Google LLC, Gordon House, Barrow Street, Dublin 4, Ireland

We use Firebase Cloud Messaging to send you push messages. These are messages that are displayed on your device without opening the App. When you install the App, your device is assigned a pseudonymized reference ID (Firebase installation ID), which serves as the destination for the push messages. When you uninstall the App, this ID is processed for a certain period before it is permanently deleted. Upon reinstallation, a new ID is assigned to your device. This ID can be (de)activated at any time in the settings of your device. If you deactivate it, you will only receive our messages when the App is open.

For more information on Firebase Cloud Messaging, in particular on the processing duration, please refer to the Google Firebase data protection information: <https://firebase.google.com/>.

7.2. Google Firebase Remote Config - Google LLC, Gordon House, Barrow Street, Dublin 4, Ireland

We use Firebase Remote Config to manage the configuration of the MOVE Score App on your smartphone. When you install the App, your device is assigned a pseudonymized reference ID (Firebase installation ID), which is used to select configuration values and send them to your device. When you uninstall the App, this ID is processed for a certain period before it is permanently deleted. Upon reinstallation, a new ID is assigned to your device.

For more information on Firebase Remote Config, in particular on the processing duration, please refer to the Google Firebase data protection information: <https://firebase.google.com/>.

7.3. Sentry.io - Functional Software, Inc., 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA

We use Sentry to ensure that our Service runs smoothly and to be able to respond as quickly as possible when errors occur. Sentry will automatically record and report errors that occur on the server or client side. We ensure that personal information is removed as much as possible.

For more information on Sentry, in particular on the processing duration, please refer to the Sentry data protection information: <https://sentry.io>.

8. **Optional Third-Party components – Software Development Kits (SDK)**

The following SDKs are optional and may be set according to individual preferences. These SDKs ensure the functionality of our App and are technical interfaces that transmit various user or technical data to third-party providers or receive data from them. The SDKs are active as long as the app is installed and used.

The legal basis for the processing of the data by all of the following SDKs is your consent pursuant to Art 6 (1) lit a GDPR, which you may give and revoke in the respective settings section.

- 8.1. Google Analytics – Google LLC, Ireland (if you are located in EU)
– Google LLC, Mountain View, CA94043, USA (if you are located outside EU)

We use Google Analytics in order to increase the performance and usability of the App and to measure the efficiency of our advertising measures. For this purpose, we transmit data to Google that is required to enable our evaluations. Google Analytics collects the following data:

- Installation UUID,
- Firebase Instance ID,
- Mobile Advertising ID,
- Android ID / IDFV,
- Pseudo ID / Contract ID,
- Crash Trace (tracking of app crashes),
- Smartphone info (brand, model, operating system, smartphone settings, etc.),
- IP address (to display the region),
- Function calls in the app,
- App events,
- the frequency with which the app is used.

The data collected is stored for up to 14 months. You can find more information on the terms of use and data protection at Google here: <https://policies.google.com/privacy>.

- 8.2. Google Ads – Google LLC, Ireland (if you are located in EU)
– Google LLC, Mountain View, CA94043, USA (if you are located outside EU)

We use Google Ads to inform you about products and offers that may be of interest to you by means of advertisements such as banner ads on external websites. These advertisements are provided by Google via servers that can set cookies (to record which advertisements are displayed and clicked on). If you click on the banner, further cookies are set which contain the unique cookie ID, the number of ad impressions per placement (frequency), the last impression and opt-out information. This allows your browser or device to be recognized. We only receive statistical evaluations from Google, based on which we can recognize which advertisements are particularly effective.

We also use Google's Campaign Manager tool. For this purpose, Google sets cookies to prevent displaying the same ads more than once. Furthermore, these cookies make it possible to understand whether you perform certain actions, such as clicking on advertisements. We can also use the remarketing function to present advertisements on other Google websites (e.g. YouTube). Google stores cookies for this purpose, which are used to analyze which offers you are interested in.

In all these cases, it is not possible for us to identify the individual User, whereas Google may identify you, e.g. by assigning you to an existing Google account or recording your IP address.

Data collected is stored for up to 2 years. You can find more information on the terms of use and data protection at Google here: <https://policies.google.com/privacy>.

8.3. Meta Ads - Meta Platforms, Inc., 1601 Willow Road, Menlo Park, CA 94025, USA

We use Meta Ads with the Meta Pixel and the Conversions API to tailor and optimize our ads to your interests and to measure the effectiveness of our advertising efforts by analyzing the actions people take on our websites and apps. We also use the Meta Pixel (a JavaScript code that is implemented on websites and in apps and can process data) and the Conversions API for remarketing purposes to contact you again within 180 days. The Conversions API connects the data collected by the Meta pixel directly to Meta's systems. This enables us to show you interest-based advertisements ("Facebook ads") when you visit the Facebook social network or other sites, applications or services that also use the tool. Our goal is to ensure that you see ads that are relevant to you in order to make the application, our website, or offers more interesting to you. The aforementioned direct connection to Meta's systems is established only after you have given your consent. If you are registered with a Meta service, Meta may also associate your actions with your account.

Meta is considered a joint controller within the meaning of Art. 26 GDPR with regard to the following processing operations

- Use of Event Data (i.e., information we share with Meta about individuals and the actions they take on our websites and in applications, such as visits to our websites, installations of our applications) for the purpose of targeting our advertising,
- Use of Event Data to deliver commercial and transactional messages,
- Use of Event Data to improve the delivery of ads, personalize features and content, and improve and secure Facebook products.

A more detailed description of these processing operations can be found at https://de-de.facebook.com/legal/technology_terms in sections 2.a.iii through 2.a.v.1.

However, Meta is solely responsible for the processing that occurs after collection and transfer. In this context, we have entered into an agreement with Meta, which can be found here: https://www.facebook.com/legal/controller_addendum. This agreement defines the respective responsibilities for fulfilling the obligation of joint responsibility. Further information can also be found at https://www.facebook.com/legal/terms/business_tools_joint_processing and https://de-de.facebook.com/legal/technology_terms. We have agreed with Meta that Meta can be used as a contact point for the exercise of data subject rights. This does not limit the responsibility for data subject rights.

The information required by Art. 13 (1) a) and b) GDPR in Meta's data policy at <https://www.facebook.com/about/privacy>. There you will also find further information on how Meta processes personal data (including the legal basis on which Meta relies) and how to exercise data subjects' rights vis-à-vis Meta.

Data collected is stored for up to 180 days.

9. **Accessing our Website**

9.1. When you access our Website, the following data and information are automatically collected from the accessing system:

- information about the browser type and the version used,
- operating system,
- IP address,
- date and time of access.

9.2. This data is also stored in the log files of our system. This data is not stored together with your other personal data. The legal basis for the temporary storage of the data and the log files is the protection of our legitimate interests (Art 6 (1) lit f of the EU General Data Protection Regulation – GDPR).

9.3. The temporary storage of your IP address by the system is necessary to enable provision of the retrieved data to your electronic device. For this purpose, your IP address must remain stored for the duration of the session. The storage of other data in log files is done to ensure the functionality of the Website. In addition, your data serves us to optimize the Website and helps us to prevent malfunctions and misuse of our systems. These purposes are also our legitimate interest in data processing according to Art 6 (1) lit f GDPR.

9.4. The data is deleted as soon as it is no longer required to achieve the purpose for which it was collected. In the case of the collection of data for the provision of the Website, this is the case when the respective session has ended. In the case of storage of data in log files, this is the case after a few days at the latest, unless a longer storage period is necessary to comply with contractual or legal obligations. Beyond this, storage is only possible for statistical purposes or to optimize our Website and the content offered. In this case, your IP address is deleted or alienated so that an assignment of the calling client is no longer possible.

10. **Cookies**

10.1. Our Website uses cookies. Cookies are text files that are stored in the internet browser or by the internet browser on your computer system. When accessing our Website, a cookie may be stored in the cache of your internet browser, provided that you have not deactivated this function in your internet browser. This cookie contains a characteristic string of characters that enables the browser to be uniquely identified when the Website is accessed again. We use cookies in order to be able to adapt our Website to the preferences of the user and to be able to recognize the user when the Website is accessed again. Cookies are particularly necessary for functions that are only available after the registered user has logged in.

10.2. The following data is stored in the cookies (depending on the use of the Website):

- log-in information,
- data that the user has entered in an input field of the Website,
- characteristic string,
- IP address, date and time of access.

10.3. When accessing our Website, you will be notified by means of an information banner about the use of (analyzation) cookies and you will be asked to give your consent to the processing of the personal data used in this context. In this context, a reference to this Privacy Policy is also made. The legal basis for

the processing of personal data using cookies for analyzation purposes is Art 6 (1) lit a GDPR if you have given us your consent.

10.4. Technically necessary cookies are required to simplify the use of the Websites for you. Some functions of our Website cannot be offered without the use of cookies (e.g. recognition of the browser after a page change). Analysis cookies are used to improve the quality of our Website and its content. Through the analysis cookies, we learn how the Website is used and can thus constantly optimize our offer.

10.5. *Google Analytics*

On our Website we use Google Analytics. The provider of this service is Google LLC, 1600 Amphitheatre Parkway Mountain View, CA 94043, USA. Google Analytics uses cookies for analysis. You can find more information on how Google Analytics handles user data in Google's privacy policy: <https://policies.google.com/privacy?hl=en-US>.

Please note that by using Google Analytics personal data may be transferred to a Google server in the USA. On behalf of Dolphin, Google will use this information for the purpose of evaluating your use of the Website, compiling reports on Website activity and providing other services relating to Website activity and internet usage to us. The IP address transmitted by your browser as part of Google Analytics will not be merged with other Google data.

Google Analytics is used for the purpose of improving the quality of our Website and its content. By evaluating anonymized data, we learn how the Website is used and can thus continuously optimize our offer.

10.6. Cookies are stored on your computer and transmitted to our Website by you. Therefore, you as a user have full control over the use of cookies. By changing the settings in your internet browser, you can deactivate or restrict the transmission of cookies. Cookies that have already been saved can be deleted at any time using the corresponding browser function. This can also be done automatically. If cookies are deactivated for our Website, however, it may no longer be possible to use all the functions of the Website to their full extent.

10.7. You may delete cookies that are already on your client at any time. Most modern browsers also offer the option of deactivating cookies in general. To do this, check the settings or the help menu in your browser.

11. **Your rights as a Data Subject under the GDPR**

11.1. *Right of Access*

In accordance with Art 15 GDPR, you can request confirmation from us as to whether personal data relating to you is being processed by us. If such processing is taking place, you can request information about the following: the purposes for which the personal data is processed; the categories of personal data which are processed; the recipients or categories of recipients to whom your personal data has been or will be disclosed; the planned duration of the storage of your personal data, if specific information on this is not possible, criteria for determining the storage period; the existence of a right to rectification or erasure of your personal data, a right to restriction of processing by us or a right to object to such processing; the existence of a right of appeal to a supervisory authority; any available information about the origin of the data if the personal data is not collected from the data subject; the existence or non-existence of automated decision-making, including profiling, pursuant to Art 22(1) and (4) GDPR and, where applicable, meaningful information about the logic involved and the scope and effects of such processing for the data subject. You have the right to request information as to whether the personal data concerning you is transferred to a third country or to an international organization. In this context, you may request to be informed about the appropriate safeguards pursuant to Art 46 GDPR in connection with the transfer.

11.2. *Right of Rectification*

Pursuant to Art 16 GDPR, you have the right to rectification and/or completion if your personal data is incorrect or incomplete. We must carry out the correction without delay.

11.3. Right to Restriction of Data Processing

Under the conditions of Art 18 (1) GDPR, you may request the processing of your personal data may be restricted.

11.4. Right to Deletion

Pursuant to Art 17 GDPR, you may request that we delete your personal data without delay. In such case, we are obliged to delete this data without delay if one of the reasons listed in Art 17 GDPR applies. The right to deletion does not apply if the processing is required pursuant to Art 17 (3) GDPR.

11.5. Right to Notification

If you have asserted to right to rectification, deletion or restriction of data processing, we are obliged to inform all recipients to whom your personal data has been disclosed of this rectification or deletion or restriction of data processing, unless this proves impossible or involves a disproportionate effort. You have the right to be informed about the recipients.

11.6. Right to Data Portability

In accordance with Art 20 GDPR, you have the right to receive your personal data that you have provided to us in a structured, common and machine-readable format.

11.7. Right to Object, Right to Revoke

Pursuant to Art 21 GDPR, you have the right to object at any time to the processing of your personal data that is carried out on the basis of Art 6 (1) lit e or lit f GDPR for reasons arising from your particular situation. We will then no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing which predominate your interests, rights and freedoms, or the data processing serves to assert, exercise or defend legal claims. If the personal data is processed for the purpose of direct marketing, you have the right to object at any time to the processing of personal data for the purpose of such marketing. If you object to the processing for direct marketing purposes, the personal data will no longer be processed for these purposes. Pursuant to Art 22 GDPR you have the right to obtain human intervention in case of profiling and automated decision taking. Pursuant to Art 7 (3) GDPR, you have the right to revoke a declaration of consent under data protection law at any time. The revocation of consent does not affect the lawfulness of the data processing carried out on the basis of the consent until the revocation.

11.8. Right of Complaint to a Supervisory Authority

Regardless of any other administrative or judicial remedy, you have the right to file a complaint with a supervisory authority, in particular in the Member State of your residence, your place of work or the place of the alleged breach, pursuant to Art 77 GDPR, if you think that the processing of your personal data infringes the GDPR. The supervisory authority with which the complaint has been filed shall inform the complainant about the status and the results of the complaint, including the possibility of a judicial remedy pursuant to Art 78 GDPR. The competent supervisory authority for Austria is the Austrian Data Protection Authority.