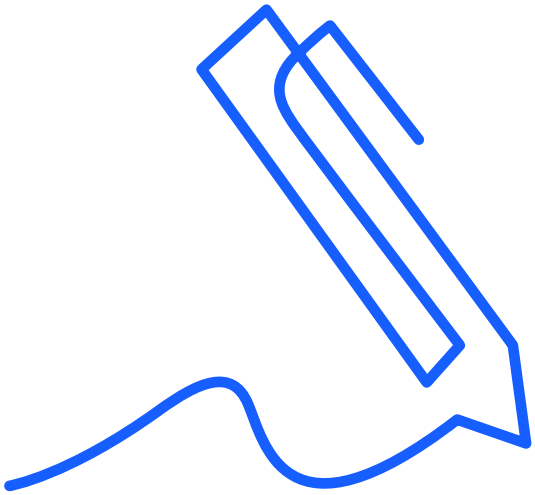

Privacy Policy

1. Introduction

Anytime is the direct sales channel for the insurance products offered by the Greek company (Société Anonyme) «INTERAMERICAN HELLENIC INSURANCE COMPANY S.A.» (hereinafter "INTERAMERICAN" or "we", "us" or "our") which is responsible for the processing of your personal data in the context of the services provided to you. The Company:

- Has been established in Greece and its Registration Number 000914001000 in the General Commercial Registry (GCR).
- Its Tax Registration Number is 094328889 and belongs to the TAX OFFICE: COMMERCIAL COMPANIES' ATHENS OFFICE and TRADE REGISTER.
- Its registered office is located at 124-136, Syngrou Avenue, 117 82, Athens - Greece.
- Is a member of the Athens Chamber of Commerce and Industry, with the number 110043.
- It is registered at the Registrar of Companies of the Republic of Cyprus as a foreign company with registration no. SA 3036 and operates a branch of insurance operations in Cyprus, located at Griva Digeni 42-44, 1080, Nicosia.
- It is supervised by the BANK OF GREECE and the MINISTRY OF DEVELOPMENT, COMPETITIVENESS, INFRASTRUCTURE, TRANSPORT AND NETWORKS in respect of its activities in Greece and by the Superintendent of Insurance in respect of its activities in the Republic of Cyprus.

Please read this privacy notice carefully as it contains important information on who we are and how and why we collect, store, use and share your personal data. It also explains your rights in relation to your personal data and how to contact us or supervisory authorities in the event you have a complaint.

For INTERAMERICAN and its employees, the respect for privacy and the protection of the confidentiality and security of the personal data of its insured persons, its associates and all natural persons who in any way transact with the Company are a key priority. We would like to assure you that our Company collects, processes and stores your personal data in accordance with the General Data Protection Regulation (EU) 679/2016 and the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data Law of 2018 (Law 125(I)/2018), as well as with any other applicable legislation and decisions of the competent supervisory authorities for the protection of personal data and takes all necessary measures to prevent incidents of theft, loss and leaks of personal data.

With regards to your visit on the website www.anytimeonline.com.cy, the Company is the data controller.

2. What categories of personal data do we collect and process?

We process your personal data in various ways, depending on the insurance risk we have undertaken. This data may be:

✓ Identification Data, such as name, surname, date of birth, ID / passport number, tax ID number, social security number.

✓ Contact Data that we collect when you enter into an insurance policy but also at any other stage of our cooperation, such as email / correspondence address, phone numbers / fax.

✓ Payment Data, such as bank accounts, debit / credit and other bank cards.

✓ Insurance Data necessary for the assessment, control, conclusion and management of the insurance policy, data relating to road behaviour in the case of motor insurance.

✓ Special Categories of Personal Data, such as health data (physical condition, any disabilities, medical history, administration of medication, etc.).

✓ Settlement Data, such as information necessary for the handling of insurance claims contained in the request form for the payment of compensation/purchase/payment of premium or in accompanying documents/supporting documents or documents related to such request form.

✓ Browsing Data, in case you visit our website, information related to your visit may be recorded (e.g. IP address). Additionally, when using our website, cookies may be stored on the device you are using.

✓ Data we collect when using and submitting a complaint form such as full name, telephone number, correspondence or email address.

✓ Data we collect when you call our call center, in which case your call is recorded, as well as the number you are calling us from.

✓ Finally, we collect information when you enter the offices of our Company where we record your name. A closed-circuit television (CCTV), the operation of which you will be informed of in good time when you enter our buildings, will record your image, in full compliance with all the provisions of the applicable legislation.

✓ When the law requires us to collect personal data, or when this is necessary for us to be able to offer you our products or services but you do not provide us with such data when requested, this may prevent or delay us from offering our products or services to you. In such a case, we may need to cancel a product or service you have with us, but we will notify you about this at the time this happens.

3. Where do we collect your personal data from?

We collect data:

- from the submission of the insurance proposal, the application for amendment / conversion / cancellation / purchase, the request for the provision of insurance benefit, notification of damage,
- through authorized employees, our insurance intermediaries that belong to the various sales network channels of our Company as well as our third-party partners (e.g. technical consultants, experts, damage assessors),
- directly from you personally, by phone, through our website, by text message or email and through any of our digital applications that you may be using, such as the "my anytime" application,
- from publicly accessible sources,
- in relation to special categories of data, which mainly consist of health data, the Company may, in addition to such data you provide with your explicit consent, collect data from health care providers it has contracted with (e.g. hospitals, private clinics, diagnostic centers, doctors),
- from visitors / users of our website, only when they themselves voluntarily provide data in order to submit their requests electronically,
- through the security systems on our premises, such as the closed-circuit television (CCTV) cameras,
- from marketing activities for promoting our products, from the collection of contact information for sales purposes (leads) and when organising lotteries and contests whereby we collect personal data, provided you give your express consent for the further processing of such data.

4. The purposes for which we process your personal data

According to the law, we can only use your personal data if we have good reason to do so, e.g.:

- to comply with our legal and regulatory obligations;
- to execute our contract with you or to take measures following a request from you before entering into the contract;
- for our legitimate interests or those of third parties, where your interests and fundamental rights do not override our own interests or the interests of those third parties; or
- where you have given your consent.

A legitimate interest is when we have a business or commercial reason to use your data, so long as your rights and interests do not override our interest.

By submitting the insurance proposal to our Company in order to become insured, you declare to us that you want to obtain insurance from our Company for the risk that you have chosen.

On the basis of the information / data you provide to us in the insurance proposal, we must include you in a homogeneous risk category and calculate, on the basis of your statements, the appropriate and proportional premium for you, calculating and estimating, among other things, the frequency and the severity of the damage that may arise.

To do this, it is necessary that you provide us with the personal data specifically mentioned in the relevant fields of the insurance proposal. These data are relevant for the assessment of the insurance risk and the fulfilment of the purpose and the operation of the insurance policy.

On the basis of the above, we process the Personal Data of our insured persons but also of all the natural persons who transact with us, for more than one purpose and in particular:

Purpose / Activity	Legal Basis
To assess the risk for the purpose of undertaking it, determine the terms of the insurance, the premium and ultimately the conclusion of the requested insurance policy, its management during the insurance period, the control and settlement of indemnity in case the risk occurs and the payment of the amount provided by the insurance terms.	a. Processing is necessary to execute the contract. b. With your consent, after being provided with specific information.
For motor accidents involving bodily injury, we collect and process special categories of personal data (health).	a. With your express consent, after being provided with specific information. b. For founding, exercising or supporting legal claims.

In the event of notification of damage to the motor department and settlement of compensation, we collect and process personal data that come to our knowledge following an accident which involves a third party in any way. It is necessary for the Company to have knowledge of such data in order for us to be able to process the claim for compensation. For this exact reason, if you, as a third party, do not consent to the processing or object to it before your claim is settled, it will not be possible to continue the compensation process.	a. With your express consent, after being provided with specific information. b. Processing is necessary to execute the contract. c. For founding, exercising or supporting legal claims.
For the Company's compliance with legal obligations such as pursuant to tax legislation, the UN and EU sanctions lists.	Processing is necessary for the Company to comply with its legal obligations.
To manage a request and / or complaint.	Processing is necessary for the Company to comply with its obligations under the applicable legal and regulatory framework.
To improve the Company's website, products and services, to conduct marketing and for market research which the Company may carry out to examine the level of customer satisfaction regarding the quality of the Company's services as well as the promotion of new products and services.	a. Processing is necessary for the Company's legitimate interests to (a) improve its business and services and (b) be kept informed as to the level of customer satisfaction regarding the quality of its services. b. With your consent, after being provided with specific information.
To manage our relationship with you, including the following: (a) Notify you of changes in the way our business operates or in the way we transact with you; (b) Update the data we have in relation to you.	a. Processing is necessary to execute the contract. b. Compliance with the Company's legal obligations. c. Necessary for the Company's legitimate interests to communicate with the persons it transacts with and to manage its relationship with them.

To operate, manage and protect our business, including: (a) to ensure compliance with business policies; (b) business reasons, such as performance improvement, quality education and control; (c) the prevention and detection of fraud, such as by conducting investigations into other, past or future, insurance claims or claims in the context of combating and restricting insurance fraud; (d) the prevention of unauthorized access and modifications to systems; (e) statistical analysis to help us manage our business, e.g. in relation to our financial performance, our customer base, our product range or other performance improvement measures; (f) ensuring safe work practices, personnel administration and evaluations.	a. Processing is necessary for the Company's improvement and for its legitimate interests (i) to properly and efficiently operate and manage its business, (ii) to protect its business and (iii) to restrict instances of fraud. b. Necessary for the Company's compliance with its legal and regulatory obligations. c. With your consent, after being provided with specific information.
External checks and quality checks, collection and provision of information and filing of documents required by law or related to checks, questions or inquiries by regulators or authorities.	a. Processing is necessary for the Company's improvement and for its legitimate interests to properly control and monitor its operations and affairs. b. Necessary for the Company to comply with its legal and regulatory obligations.

It is clarified that, where the above table lists more than one legal ground for one purpose or activity, such grounds may also apply alternatively and the Company may, depending on the case, rely on only some of them (and not necessarily on all of them).

We will use your personal data only for the purposes for which we have collected it, unless we reasonably believe that we should use it for some other reason and that reason is compatible with the original purpose.

If we need to use your personal data for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in accordance with the above rules, where this is required or permitted by law.

5. Where do we transfer your Personal Data?

Your data will be transferred to departments of our Company which are responsible for underwriting, for the proper and uninterrupted operation of your insurance policy, as well as for your compensation. Namely, the underwriting department, the publishing department, the compensation department, the accounting department, the legal department, the Regulatory Compliance department.

We may also share or disclose personal data to:

- our parent company «Achmea B.V.», based in the Netherlands, as well as other affiliated companies of the Achmea Group;
- professional advisors, including lawyers, business consultants and auditors, who provide legal, consulting and audit services;
- insurance funds and international insurance agencies, public services, police and judicial, public, supervisory, regulatory, tax and independent authorities, such as the Bank of Greece and the Superintendent of Insurance of Cyprus, the Cyprus Information Center, the Department of Road Transport and the Motor Insurer's Fund;
- specifically with respect to motor insurance, accident investigators, technical automotive service companies, residual motor waste management companies as well as other insurance companies, in order to settle damages in a road traffic accident;
- to the companies providing roadside assistance service to our insured personly, currently G.N. Auto Odyky Express Road Service Limited;
- insurance intermediaries, experts, investigators and compensation management companies;
- other insurance companies and organizations;
- doctors, medical institutions and health professionals;
- third parties with whom we maintain, from time to time, contracts of collaboration in order to provide the proper indemnity to our insured in accordance with the insurance policy terms, as well as for proper assessment of the damage; such as for example the company Lambros Papasavvas & Co Ltd;
- to companies that provide services to us, such as file storage and management companies, file destruction companies, I.T. companies and telephone service providers.

In all of the above cases, we only transfer your personal data when there is a legal basis to do so. We allow third parties to handle your personal data only if we are satisfied that they are taking appropriate measures to protect your personal data. We also impose contractual obligations on service providers to ensure that they may only use your personal data for providing services to us and to you.

6. Automated data processing

Automated personal data processing and relevant (automated) decision-making occurs only in private and other vehicles insurance, mainly through the direct sales channel of insurance products offered by INTERAMERICAN under the trade name «Anytime». Through these automated means, in which the risk-taking rules implemented by our Company have been largely incorporated, decisions are made faster, with greater accuracy, transparency and consistency.

Specifically, for cases where automated data processing takes place as described above, the following apply:

(a) Automated processing is necessary to assess the insurance risk, i.e. so that the Company can offer the most suitable and appropriate insurance product as well as the strictly proportional price for insuring it (premium). Specifically, the rationale behind automated processing rests on mathematical or statistical analyses of those significant, in terms of insurance, technical parameters that have been adopted by the Company and that make possible the following: i) objective risk assessment, ii) integration into a homogeneous risk group based especially on the frequency and iii) the severity of the damage that this risk may cause, as well as its proper pricing;

(b) following this automated processing, a higher premium may arise. However, in these cases, checks are regularly carried out by our employees;

(c) we take all necessary measures required by the General Data Protection Regulation (EU) 2016/679 when making a decision on the basis of automated processing, including the creation of profiles, and these measures are especially concerned with ensuring human intervention, the use of appropriate statistics or mathematical procedures and the application of technical and organizational measures in order to correct factors that lead to inaccuracies as well as minimizing the risk of errors during the processing;

(d) the Company may use automated procedures during the insurance period to carry out checks in order to avoid insurance fraud and to comply with its obligations arising from the international sanctions lists of the European Union, the United Nations, the USA, the USA and the Netherlands, to the extent permitted by law.

(e) you have the right to express your opinion on a decision made on the basis of the abovementioned automated procedure, to challenge it and to request a review by a competent employee. In order to exercise your rights, you should contact our Company or the Data Protection Officer (see below «How to submit requests, queries or complaints»).

7. How long will your personal data be kept?

We will keep your data for as long as you maintain a contractual relationship with us, in both paper and electronic form. In the event that, for any reason, this relationship is interrupted, we will keep them for as long as required until the limitation period of any relevant claims expires and up to twenty (20) years unless the legislation provides for a different retention period.

However, if the application for insurance of the insurance policy that you submitted to us has not been accepted, we will keep it for a period of up to five (5) years from submission for the purposes of assessing the insurance risk and combating insurance fraud.

In the event of a legal dispute is pending beyond the above processing times we will keep data until its conclusion by an irrevocable court decision.

Recorded calls are kept in our file for up to 5 years and then deleted, while CCTV data is kept for 15 days. In the event of an incident to the detriment of the Company, its employees or third party visitors, the images in which the specific event has been recorded, may be kept in a separate file for a longer period of time, in accordance with applicable law.

8. Use of cookies

Our company uses cookies for the smooth operation of its website. For more information, you can read our Cookie Policy.

9. Your rights

You have the following rights with respect to your personal data:

1) Right of Access - the right to know which data of yours we are processing, the purpose for which they are processed and their recipients, as well as to receive copies of the data kept at our Company.

2) Right to Rectification - the right to request that any deficiencies or inaccuracies in your data be rectified, although we may need to verify the accuracy of the new information you have provided.

3) Right to Erasure - the right to request the erasure of your personal data, if you no longer wish this data to be processed, and if there is no legal basis for our Company to own and process it.

When can we deny requests to erase? You should know that the right to erasure is not an absolute right, and there are cases where it cannot be fulfilled, such as when your information is processed based on certain legal grounds such as those described above, including forwarding or defending legal claims on behalf of or against the Company.

Do we need to inform other recipients of your personal data about your request to erase? In case your right to erase is fulfilled, if we have provided the personal data that you want erased to third parties, we will take measures to inform them of your request to erase, so that, in turn, they erase that personal data but this may not always be feasible or may require a disproportionate effort on the part of our Company.

4) Right to Restriction of Processing - the right to restrict the processing of your personal data when you disagree with the accuracy of the information and until the accuracy of the information is verified or if the processing is no longer necessary for the Company but you need it, in order to file, exercise or defend a legal claim or where the use of the data is unlawful but you do not want us to erase it.

Should we inform other recipients of your personal data about the restriction? In the event that we have shared your personal data with third parties, we will take action, if possible, to inform them about the restriction on the processing of your information, so that they do not continue to process it.

When can we refuse requests to restrict processing? You should be aware that this right is not an absolute right, and there are cases where it cannot be fulfilled, such as when your information is processed based on certain legal grounds, such as those described above, including the filing or defending legal claims on behalf of or against the Company.

5) Right to Data Portability - the right to receive your data in a structured and commonly used format.

6) Right to Object - the right to object to the processing of your personal data where we are relying on a legitimate interest (or the interests of a third party) and there is something about your particular situation that makes you want to object to the processing on this ground as you feel that this has an impact on your fundamental rights and freedoms. You also have the right to object when we process your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your data, which override your rights and freedoms.

7) The right not to be subject to automated individual decision-making - The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning or similarly significantly affects you to a significant degree.

8) Withdrawal of consent - The right to withdraw your consent at any time, in cases where we rely on your consent for the processing of your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise if this is the case at the moment you withdraw your consent.

For more information on each of these rights, including circumstances in which they apply, please contact us or visit the website of the Office of the Commissioner for Personal Data Protection (www. dataprotection.gov.cy).

If you wish to exercise any of these rights, please:

- send an email to us at dpo1@interamerican.com.cy or submit a contact form on our website or by mail - see below: «How to submit requests, queries or complaints»;
- clearly define the right you wish to exercise in relation to the personal data you request and provide us with the information relating to your request;
- provide enough information to recognize you;
- provide proof of your identity.

If your request is not clear, we may request further personal data for clarification.

You will not have to pay any fees to access your personal data or to exercise any of the other rights. However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in such cases.

If you exercise any of these rights, we will take every possible measure to satisfy your request within thirty (30) days of receiving the relevant request, after informing you either of its satisfaction or of the objective reasons that prevent its satisfaction.

10. How we ensure the security of your data

We are absolutely committed to ensuring the security of your data. To achieve this, we apply all modern and suitable technical and organizational measures for the purposes of processing, the responsiveness of which we check at regular intervals in order to:

- protect your personal data from unauthorized access and improper use;
- secure our I.T. systems and protect information.

Examples of measures that support both the physical and electronic security of the data that are processed by our Company are the physical presence of security staff in our buildings, the installation of a closed-circuit monitoring system of areas we consider critical, the implementation of a Proper Use of Resources Policy, a Security Policy and support processes, installation of a firewall, antivirus and antimalware software, installation of a data leakage prevention system (dlp), the use of 2 Factor Authentication, encryption for certain cases and more.

11. Marketing and processing of personal data for promotional purposes

Provided you have given us your express consent, we also process your non-sensitive data (but not the specific categories of personal data) for the purposes of promoting other or supplementary (to your needs) insurance products or services either of our Company or of other companies of the INTERAMERICAN Group or for the performance of targeted marketing activities or market research. In this context, our Company will send you updates for the promotion of services or new products, special offers using the ways of communication that you have stated at the start of our cooperation. Relevant actions may also be taken through companies which we have contracted with (such as MailChimp, Facebook and Eloqua), in which case data will be transferred to our associated research and promotional companies. If you want us to stop sending you such updates, every time you receive an immediate service promotion update, we will also notify you of how you may withdraw your consent.

You may at any time object to this processing of your data (for marketing or research purposes) by sending a request to the Data Protection Officer. In this case, your data will no longer be processed for marketing or research purposes.

12. Personal data of minors

The Company does not seek nor does it intentionally collect personal data from persons under the age of fourteen (14) years (or any age limit set by law), nor is the content of the website addressed to persons of these ages. For minors under the age of 14 who participate or have an interest in insurance as insured persons and/or the beneficiary or victim of the covered act, consent-based processing is lawful only if the consent is granted or approved by the person responsible for the minor's parental care. The minor must give their consent personally when they reach the age of 14 or the age provided by law.

13. Transferring your personal data outside the EEA

To deliver our products and services to you, it is sometimes necessary for us to share your personal data outside the European Economic Area (EEA), such as with our service providers outside the EEA.

These transfers are subject to special rules under European and Cypriot data protection law.

Whenever we transfer your personal data outside the EEA, we ensure that a degree of protection equal to or similar to that provided in the EEA countries is provided, by ensuring that at least one of the following safeguards is implemented:

- We will transfer your personal information to countries that have been deemed to provide an adequate level of protection for personal information by the European Commission.
- Where we transfer your personal information to countries that have not been deemed to provide an adequate level of protection for personal information by the European Commission, we may use specific contracts approved by the European Commission which give personal information the same protection it has in Europe.
- Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal information shared between the Europe and the US.

If you would like more information on this topic, please contact us.

14. How to submit requests, queries or complaints

For any queries or complaints, you can contact our Company by sending a letter to the address Griva Digeni Avenue 42 - 44, 1080, Nicosia or by calling 800 88 800 or by sending an email to helpdesk@anytimeonline.com.cy or by filling in the contact form on our website.

If you have any queries regarding the processing of your personal data, if you wish to exercise any of your rights or to file a complaint regarding your personal data, you can contact our Company's Data Protection Officer by sending a letter to the address Griva Digeni Avenue 42 - 44, 1080, Nicosia or by email at: dpo1@interamerican.com.cy
Additionally, if you are not satisfied with our response to your request, you always reserve the right to contact (1) the Office of the Commissioner for Personal Data Protection in Cyprus, address Iasonos 1, 1082 Nicosia, PO Box 23378, 1682 Nicosia, Telephone No: +357 22818456 Fax No: +357 22304565 or by sending an email to: commissioner@dataprotection.gov.cy and also (2) the Hellenic Data Protection Authority (HDPA), which is based in Athens and may accept the submission of relevant complaints, either by calling the Call Center: + 30-210 6475600 or by submitting your written request in person at the Protocol's office: 1-3 Kifissias Ave., Postal Code 115 23, Athens) or by email to contact@dpa.gr
The law also gives you the right to submit a complaint to a competent supervisory authority in the European Union (or European Economic Area) state in which you work, have your habitual residence or in which the alleged breach of the data protection laws took place (if it is different from the above).

* This Privacy Notice was updated on 01/05/2020. We reserve the right to amend or update this Privacy Notice at any time. We will notify you of any changes, by posting the new Privacy Notice, by posting it on our Company's website and informing you by any appropriate means, including emails. We also encourage you to read this Privacy Notice regularly for any changes.

SmartDrive
Privacy Policy

Our Company's main priority is the protection of your personal data that it processes. Our Company constantly complies with the applicable legislation on Personal Data Protection.
We urge you to read this information notice carefully in order to be adequately informed on the type of data we process when you obtain insurance through our Company's Cyprus branch under the Smart Drive Program. The data subject for the purposes of this notice is either the person in whose name the insurance policy under the Smart Drive program is issued or the main driver of the insured motor vehicle, in case these are different persons. References to «you», «yours» etc. will be interpreted accordingly.
It is clarified that this information notice is supplementary to the Company's general privacy policy above concerning personal data protection in the context of the business of its Cyprus branch. In case you are insured under the Smart Drive Program, both notices apply to you.
Please, read both carefully.

1. General information and processor

«INTERAMERICAN HELLENIC INSURANCE COMPANY S.A.» (hereinafter the "Company", "INTERAMERICAN", "we", "us" or "our"), is a Greek company based in Athens at 124-126 Syggrou Ave., with the Registration Number 000914001000, in the General Commercial Registry (GCR), contact no. 210-9462200 and email: custserv@interamerican.gr.
The Company is registered with the Registrar of Companies of the Republic of Cyprus as a foreign company with registration number AE 3036 and has a branch engaged in insurance activities in Cyprus (hereinafter the "Branch") at 42-44 Griva Digeni Avenue, Nicosia 1080), contact no. 800 88 800 and email: helpdesk@anytimeonline.com.cy.
The company is the data controller, responsible for the collection, storage and generally the processing of personal data of the Smart Drive applications (the "Application") users who are insured through the Branch.

2. What personal data we collect and how

In addition to what is included in the Company's general privacy policy above, additional data is collected and processed for the purposes of the Smart Drive program.

a. The Collection and Processing of the data of the insured / User

When registering for the test period of the Application, no personal data is requested.

Initially, when you connect to the Application, in case you have a Smart Drive insurance policy with INTERAMERICAN, you electronically fill in the username and password. This information does not identify you and is the only information required to use the Application and will be not reused for a purpose incompatible with the scope of the service. It is reminded that you are exclusively responsible for maintaining the confidentiality of the Application's password (if required) and fully responsible for all activity that takes place on the Application. In case of a Trial Use of the Application, no data is required when you register and no password is required.

b. Collection of the User's Primary Data

The application may collect and process "Primary Data" (including location data) for the operation of the automated route recording function even when the application is closed or is not in use, which data is stored only on the user's device (without being transferred to the processor). Only Primary Data recorded during a route is transferred to the data processor (our technical service provider), OSeven ("OSeven"), for processing on our behalf. The following constitutes Primary Data:

- Time data: The time of recording of the following parameters.
- Location data: Longitude, latitude and altitude of the vehicle, horizontal and altitude accuracy of the location, speed of the vehicle, direction of movement of the vehicle.
- The angles formed by the local axes of the mobile phone in relation to the North and to the horizontal level (ground).
- Rate of change in the angles formed by the local axes of the mobile phone to the North and to the horizontal level (ground) in terms of time.
- Accelerometer data: Acceleration values on the three local axes (the three dimensions) of the mobile phone, including and excluding the acceleration of gravity.
- Gyroscope data: Angular velocity values around the three local axes of the mobile phone.
- WiFi: Record of WiFi operation on a mobile phone. It is used to improve driving record accuracy given it was pre-used by Apple and Google in conjunction with GPS. At the same time, it is used to send data from the device of the Application's user (the «User») to and from the platform of the Provider at the choice of the User.
- Activity Recognition / Motion and Fitness data: Data of the User's activity (indicatively walking, stopping, driving).
- Screen Status (Android only): Data on screen activation (active or inactive) as an additional criterion for determining mobile usage while driving.

- Mobile device data. These are provided by Google and Apple and include the manufacturer's name, device model, operating system name and version, and the type of device sensors (e.g. accelerometer, gyroscope, compass, etc.) used to record data. These data are used for (i) providing support / service to you and for (ii) targeted troubleshooting.
- Push Notification Token Data: A unique alphanumeric code generated by Apple and Google which is sent to the mobile phone. The specific code relates to a single installation of the Application only. In case of uninstalling and reinstalling the Application, a new code is generated stating the date and time it was generated. The specific code with the date and time is registered (i) for sending Notifications (ii) for providing service / protection / security to the User and (iii) for identifying any uninstallation and reinstallation of the User's Application, for the purpose of detecting non-recorded Routes.
- Data for the time and date of your entry / exit (Sign in / Sign out) from the Application. They are used for your support / service and for calculating the duration and/or frequency you are in Signed out mode in order to detect non-recorded Routes. In case you are in Sign out mode, the Application's recording is blocked.
- Data for the time and date of activation / deactivation of Location Services (GPS). Used for support / service.
- Data for the time and date of activation / deactivation of Location Services (GPS). They are used for your support / service and for calculating the duration and/or frequency that you keep the GPS inactive in order to detect non-recorded Routes. In case it is inactive, the Application's recording is blocked.
- Data for the time and date of activation / deactivation of Activity Recognition / Motion and Fitness data. They are used for providing support / service to you and to calculate the duration and/or frequency that you keep this setting inactive in order to detect non-recorded Routes. In case it is inactive, the Application's recording is blocked.
- Data for the time and date of activation / deactivation of Compass Calibration (only for iOS). They are used for providing support / service to you and for the calculation of the duration and/or frequency that you keep this setting inactive in order to detect non-recorded Routes. In case they are inactive, the accelerometer and gyroscope data collection is blocked and so is the Application's recording.
- Data for the time and date of activation / deactivation of the Application's recording through its settings. They are used for providing support / service to you and for calculating the duration and/or frequency with which you keep the recording capability inactive, in order to detect non-recorded Routes. In case the recording of th Application is inactive, the Application's recording is restricted.
- Data for the time and date of activation / deactivation of automatic background services (Background App Refresh, iOS only). They are used for your support / service and to calculate the duration and/or frequency that you keep this setting inactive in order to detect non-recorded Routes. In case it is inactive, the Application's recording is blocked.
- Data for the time and date of WiFi activation / deactivation. They are used for your support / service and for calculating the hours and/or frequency that you keep this setting inactive in order to detect non-recorded Routes. If WiFi is inactive, it has been noticed that there may be a delay in the Application's recording or it may be unable to operate.
- Data regarding the paired Bluetooth devices.

3. The purposes for which the above «Primary Data» are recorded are the following:

- For technology providers to determine, if available, the duration of speeding.
- To determine the use of the mobile phone (how many times the User has made use of the mobile phone) and the duration of the use of the mobile phone, during a Route. It is clarified that only the use of the device during driving is examined (for speaking or recording a message or any other use of the mobile phone). The use of specific applications or their content, which concern the User's personal data to which the Company cannot have any access, is not detected.
- To determine «Incidents of Abrupt Driving Behaviour» (abrupt accelerations, decelerations) and the deceleration and acceleration profiles.
- To determine the distance travelled in hours of increased risk (10pm - 4am).
- To determine the distance travelled per Route and the total per time period (day, week, month, year) and until the end of the Insurance Policy or the Trial Period.
- To erase records that do not correspond to the actual driving behaviour of the User.
- In particular, with regard to the data relating to longitud and latitude from the GPS records, these are stored and maintained on OSeven's platform for:
    - The development, evaluation and optimization of the «Map Matching» algorithms, calculation of speed and direction and distance travelled.
    - Mapping the risk of the different sections of the road network both in aggregate and for different types of risk.
    - The representation of each Route, as well as aggressive driving events on a map, at the request of the User.
    - Displaying on a map the areas of high concentration of high-risk behaviour for each User.
    - The evaluation of the type of vehicle and the status of the User (driver or passenger of the car) per Route.

By evaluating all of the above, the "Driving Behaviour and Vehicle Use Data" which correspond to the actual driving behaviour of each User are calculated, and the score is then extracted, which is sent, amongst other data, to you and to INTERAMERICAN for the purposes of the Test Period or the insurance policy of the Smart Drive program under which you are covered.

Extracting Driving Behaviour and Vehicle Use Data

From the above processing of the «Primary Data» through the technologies developed by OSeven, the «Driving Behaviour and Vehicle Use Data» are extracted. Indicatively, these concern the following:

- Number of Routes (per time period - day, week, month, year).
- Time and date of driving per Route.
- Distance travelled (per Route and in total per time period - day, week, month, year).
- Duration of driving (per Route and in total per time period - day, week, month, year).
- Number of steep brakes and degree of deceleration (per Route and in total per time period - day, week, month, year).
- Number of sharp accelerations and degree of acceleration (per Route and in total per time period - day, week, month, year).
- Average / maximum speed during a Route.
- Distance or duration of speeding in the driving area, for as long as the speeding lasts, if available from a technology provider (per Route and in total per period of time - day, week, month, year).
- Average speed of the User when they exceed the speed limit, if available from a technology provider.
- Road type (urban road network, provincial road network, highway), within which the User moves, if available from a technology provider (per Route and in total per time period - day, week, month, year).
- Duration of mobile phone use, while driving, per Route. The user's device (mobile phone) is detected and recorded in car activity, while driving (indicatively recording a message, speech or any other movement made by the User with his mobile phone) (per Route and in total per time period - day, week, month, year).
- Distance travelled in hours of increased risk (10pm - 4pm) (per Route and in total per time period - day, week, month, year).

- The classification of the User of the Application per Route (if they were a driver or passenger of the vehicle).
- The classification of the User of the Application per Route, with respect to the type of vehicle in which they are travelling (car, train or bus, motorcycle, plane, ship, bicycle).

The driving behaviour evaluation model per route takes into account the following parameters:

- Duration of speeding in the driving area and average speed over the speed limit, if available from a technology provider.
- Duration of mobile phone use while driving.
- Sharp decelerations (number and intensity) and deceleration profile.
- Sharp accelerations (number and intensity) and acceleration profile.
- Distance travelled in hours of increased risk (10pm - 4am).

The total score of the User and the vehicle respectively is calculated according to the weighted average of your scores for Routes you have driven (with distance being a weighing factor).

When covered by Smart Drive insurance, OSEven will send to INTERAMERICAN a total score regarding your driving behaviour, up until when the payment notice for the renewal is issued. Additionally, at the end of each month, it will send to INTERAMERICAN the monthly distance travelled recorded by the application, with you as driver, in order to determine the completion of the minimum requirement of recorded kilometres (250) each month. The final decision on whether or not there will be a reduced premium will be made by human intervention, by an authorized employee of INTERAMERICAN.

The above data will not be disclosed to third parties, subject to the contents of this information notice, except following a court summons, a public authority request or other legal procedure or any other event where national, European or international legislation imposes the above obligation.

The legal ground which INTERAMERICAN relies on for the above processing (collection of insurance policy data, the primary data of the users of the application as well as the driving behaviour data) is the execution of our contract while the legal ground for the processing that takes place if we are ever required to transfer data to public authorities, is for compliance with our legal obligations.

4. Data retention period

The personal data of the Users are kept exclusively and only for the period of time required for the fulfilment of the respective purpose for which they were collected, in full compliance with applicable legislation. When the purpose of processing your personal data is completed, then these are erased. The specific retention periods for each of the relevant processing purposes are listed below.

Regarding the data collected through the Application:

In the case of Trial Use, we do not process or store any personal data of the User. Therefore, Primary Data and Driving Behaviour and Vehicle Use Data cannot be linked to any personal data of the User.

When you enter into an insurance policy under the Smart Drive program, the only data we transmit to OSeven are the user's and the transaction's unique codes which cannot on their own be linked to a natural person. This data is stored on the OSeven platform within the European Union. Therefore, it is not possible for OSeven to identify the insured motor vehicle or the User, even if an insurance policy is entered into, since the data in its system are pseudonymized (the pseudonymization has been carried out by INTERAMERICAN).

When using the Application once an insurance policy is entered into, the retention period of the data collected by OSeven is seven (7) days after the termination of the insurance policy, if not renewed. After 7 days, the Primary Data and the Driving Behaviour and Vehicle Use Data collected through the Application are disconnected from the unique user codes, resulting in complete anonymity of the already pseudonymous data collected by OSeven as the processor. This process is irreversible.

5. Automated data processing

Automated processing of personal data and the relevant (automated) decision-making takes place in the «Pay how you drive» program. Automated data processing is performed as described above in sections 2 and 3.

(a) Automated processing is necessary to rate the insured's driving behaviour and its ultimate goal is to provide an incentive (lower premium) to improve the driving behaviour of the insured.

(b) This automated treatment may result in a lower premium. In any case, there will be human intervention between the driving behaviour score formed based on the application and the decision to offer the lower premium.

(c) The Company shall take all measures required under the General Data Protection Regulation and the Code of Conduct for Personal Data of the HAIC when making a decision on the basis of automated processing, including profiling, with these measures being in particular concerned with ensuring human intervention, the use of suitable statistical or mathematical procedures and the application of technical and organizational measures in order to correct factors that lead to inaccuracies and to minimize the risk of errors during processing.

(d) Lastly, the Company may use automated procedures during the insurance period in order to carry out checks to avoid insurance fraud and to comply with obligations arising from the international sanctions lists of the European Union, the United Nations, the USA, the USA and the Netherlands, to the extent permitted by law.

(e) You have the right to express your opinion on a decision taken on the basis of the above automated procedure, to challenge it and to request a review by a competent employee. To exercise your rights, you should contact the Data Protection Officer (contact details: dpo1@interamerican.com.cy).

6. Your rights

Under the General Data Protection Regulation of the European Union and national law, you have various rights regarding your personal data. More information on these and how you can exercise them is included in the Company's general privacy policy above.

In relation to the right of access to the personal data in connection with the Application specifically, please note the following.

You have the possibility to be informed through the Application for Driving Behaviour and Vehicle Use Data, such as the following (per Route and per period of time, where calculation per period is possible): Route date, Route start time, Route end time, Route duration, distance travelled, distance or duration when speed limit is exceeded in the driving area for as long as the speeding lasts, average speeding speed, rating by category (categories are: acceleration, deceleration, speed limit, duration of mobile phone use while driving), number of Routes, driving duration, number of steep brakes, number of steep accelerations, region / city in which you are moving when driving, your categorisation for each Route (if you are a driver or passenger), as well as and the final categorisation you choose, the categorisation for the type of vehicle you are in per Route (car, train or bus, motorcycle, plane, ship, bicycle), as well as the final classification you choose.

Moreover, you have the possibility, if you enable this in the Application's settings, to display each Route on a map and to display driving behaviour data (speed limit, mobile phone use while driving, steep brakes, steep accelerations) on the map.

Through the request of access, you can be informed of the personal data concerning you exclusively, their source, the purpose of their processing, the recipients or the categories of recipients, the evolution of the processing for the period of time since your latest update, the rationale behind the automated processing and of the notification to third parties to whom the data has been disclosed. It is emphasized that INTERAMERICAN, as the data controller, has chosen not to have access to the Primary Data collected through the application with the aim to protect your personal data.

In any case, it is noted that access to and information on the logic behind the automated processing will not be able to reach such an extent so as to reveal the source code of the application used and the algorithm on which it operates.

7. How and with whom we share your personal data (recipients of personal data)

Information on how and with whom we generally share your personal data is included in the Company's general privacy policy above.

The following apply especially in relation to the Primary Data and the Driving Behaviour and Vehicle Use Data collected through the Application.

We have chosen not to have access to this data. We only take the score of the User's driving behaviour to determine whether he is entitled to a discount and the total distance travelled per month to check whether the relevant term in your insurance policy is observed for a minimum monthly distance.

OSeven processes the Primary Data and the Driving Behaviour and Vehicle Use Data on our behalf, as the data processor. In its system, OSeven maintains Primary Data and Driving Behaviour and Vehicle Use Data, which are pseudonymized (not linked to a natural person, but to an id user - only INTERAMERICAN has access to the link between the insured and the id user). We note that, in any case, OSEven undertakes, both itself and its associates, to use your data exclusively for the performance of lawful activities or any kind of activities they perform on our behalf and not for their own benefit. In cases where OSeven transfers your data to third-party processors, it signs a special agreement with the processors to ensure that the processing is carried out in accordance with the applicable legal framework, that suitable measures are taken for protecting the confidentiality and security of personal data and that each User will be able to exercise their rights freely and unhinderedly.

OSeven may transmit the User's Primary Data and Driving Behaviour and Vehicle Use Data across the borders within the European Union, always in a non-personalized form, to its parent company, or other subsidiaries, joint ventures or other companies that are under the same control. (collectively, «Collaborating Companies»).

It is also possible to transfer the User's Primary Data and Driving Behaviour and Vehicle Use Data to a company that merges with OSEven, or acquires it or buys its assets.

OSeven may transfer your personal data outside the European Union only during use of the functions of the Firebase service of Google.

The Application utilises the functions of the Firebase service of Google for achieving the optimal operation and technical support of the Application. Without these functions, then the Application or parts of it may not function properly or even at all. These functions are: Firebase Cloud Messaging, Firebase Crashlytics, Firebase Remote Config and FirebaseDynamic Links.

Additionally, the Application utilises the GoogleAnalytics for Firebase function for the purpose of analysing user behaviour and improving the Application based on their preferences. The GoogleAnalytics for Firebase is not under any circumstances used for marketing and promotional purposes.

You may find information regarding the collection and processing of your personal data by the aforementioned Google services here. Such data may be transferred outside the European Union at Google's systems. Such transfer is made by using Standard Contractual Clauses, as approved by the European Commission.

8. Data security

The Company assures users that it takes all suitable technical and organizational measures for the security of their personal data, to ensure the confidentiality of their processing and protection from accidental or unfair destruction / loss / alteration, prohibited dissemination or access and any other form of illicit processing.

Although our company has chosen not to have access to the primary data collected through the Application, it has ensured that its data processor and provider of the application (OSeven) collaborates with the most reliable cloud computing providers and uses commercially widespread security practices and techniques, following the recommendations of European regulations and national legislation, such as pseudonymization, encryption and firewalls.

Your Primary Data and Driving Behaviour and Vehicle Use Data are stored securely in OSeven's database, while your personal data collected on entering into the insurance policy as well as the data transmitted by OSeven to INTERAMERICAN (scores for driving behaviour and total distance travelled each month), are stored securely in INTERAMERICAN's database.

However, no matter how effective the technology is, no security system is or remains impenetrable.

Therefore, even though we have taken care to adopt all the technically modern practices and to fully align with the strictest standards of the current legislation, these cannot fully guarantee the security of the database of their systems, nor that the information that they provide will not be stolen, as they are transmitted over the internet.

9. Amendments

This Information Notice on the processing of personal data for the Smart Drive Program has been drafted in accordance with the provisions of the General Data Protection Regulation No. 2016/679/EU and was last updated on 1/5/2020. In case of updates, any amendments will be posted on the Company's mobile application and website, and will note the date of the update.

10. Personal Data Protection Officer / How to submit requests, queries or complaints

The relevant information is included in the Company's general privacy policy, found above.

Notification concerning the processing of personal data through video surveillance

1) Data Controller:
The company INTERAMERICAN HELLENIC INSURANCE COMPANY S.A.will process your personal data collected from the use of a video surveillance system as the data data controller. You can find our contact details in section 7 below.

2) Purpose and legal basis of processing
We operate a surveillance system for security purposes, to protect individuals and property. For this reason, the processing is necessary for the legitimate interests pursued by the company INTERAMERICAN as data controller (article 6, paragraph 1(f) of the General Data Protection Regulation 2016/679).

3) Our legitimate interests
Our legitimate interest arises from the need to protect our premises, facilities and the property located there, from illegal acts. The same applies with regards to the safety of life, the physical integrity and health as well as the property of our staff and third parties legally present in the supervised area. We wish to inform you that the installed cameras focus on the property which they are intended to protect, ie the safety of our property and people, therefore we have restricted the scope of the image to the absolutely necessary spaces in front of the entry points and exit points, in the cash register/ reception area, in the corridors, but also in critical areas in our facilities (such as electromechanical installations, warehouses, computer rooms, car parks, etc., where visitors are not allowed access) without however recording images of persons or sound from indoor or outdoor adjacent areas. The way our cameras are installed, they do not in any case record the movement of persons in adjacent outdoor areas and roads, nor internally in work spaces, recreational spaces or in the bathrooms. Additionally, our company applies privacy masks to all installed cameras when taking pictures, ie any faces and any adjacent traffic areas (roads, passers-by, etc.) are sketched over. Our company implements all modern and appropriate technical and organizational measures for the processing of video surveillance data, the responsiveness of which is checked regularly. In addition to all the above, before a person enters in the scope of the video surveillance system, we ensure that he is informed, in an appropriate, obvious and understandable way, that he is about to enter an area where a closed circuit television is operating and that he is given all the necessary information regarding the processing, the nature of the system used and who the Data Controller is. We have displayed information signs visible to the public and our employees in internal areas where cameras have been fitted.

4) Recipients
Only authorised personnel, employed by us and the security company which we work with, has access to stored material. Such material is not transferred to third parties, except in the following situations: a) to competent judicial, governmental and police authorities as part of an investigation of a criminal offence, which relates to people or the property of the Data Controller, b) to competent judicial, governmental and police authorities who legally request to receive data in the exercise of their authority, and c) to the victim or offender of a criminal offence, if the data may be used as a evidence for the offence.

5) How long personal data is kept
Our recording system processes and keeps sketched the images it receives from the video surveillance system. The data from the CCTV system is kept for 15 days, in accordance with the law, and is erased after this period expires. In case we discover an incident during this time, we will isolate the relevant part of the video and keep it for up to an additional month, in order to investigate the incident and initiate legal proceedings to protect our legitimate interests. If the incident concerns a third party, we will keep the video for up to an additional 3 months.

6) Data subjects' rights

The data subjects have the following rights:

- Right to access: you have the right to know whether we are processing your image and, if this is the case, to receive a copy thereof.
- Right to restriction of processing: you have the right to require us to restrict processing of your personal data, for example by not deleting data which you consider necessary for establishing, exercising or supporting legal claims.
- Right to object: you have the right to object to the processing of your personal data.
- Right to erasure: you have the right to require us to delete your personal data.

You may exercise your right by using our contact details below ("How to submit a request, question or complaint"). In order to examine a request concerning your image, you must specify to us when (approximately) you were within the range of the cameras and to hand over a picture of yourself to us, to help us locate your personal data and hide the data of third parties. Alternatively, we may give you the opportunity to come to our premises in order to show you the images in which you appear. We also note that, exercising the right to object or erasure does not immediately lead to the your data being deleted or to any changes in the processing. In any case, we will reply to you in detail as soon as possible, within the time frames provided by the GDPR.

7) How to submit a request, question or complaint

If you have any questions concerning the processing of your personal data, if you want to exercise any of your rights or submit any complaint with respect to your personal data, you may contact the Data Protection Officer of our Company by sending a letter at Griva Digeni Avenue 42 – 44, 1080 Nicosia or by e-mail at helpdesk@anytimeonlince.com.cy or by calling at 800 88 800.

Furthermore, if are not satisfied with our reply to your request, you always have the right to address your request to the Office of the Commissioner for Personal Data Protection in Cyprus, at Iasonos 1, 1082 Nicosia P.O. Box 22378, 1682, Tel: +357 22818456 Fax: +357 22304565 or by sending an email at: commissioner@dataprotection.gov.cy and the Data Protection Authority in Greece, which is based in Athens and accepts the submission of complaints, either by calling at +30-210 6475600 or by submitting your request in writing at Kifisias Avenue 1-3, P.O. Box 115 23, Athens or by email at contact@dpa.gr.