



PASSPORTCARD'S PRIVACY NOTICE, DECLARATION OF CONSENT AND RELEASE OF CONFIDENTIALITY

Please read this statement carefully. This Privacy Notice and declaration of consent and release of secrecy (“**Privacy Notice**”) is about the processing of personal data. It explains to you which personal data is processed for which purposes. "Personal data" is any information relating to an identified or identifiable natural person.

The controller of the personal data is

PassportCard Deutschland GmbH (hereinafter: "**PassportCard**" or "**We**")

Address: Caffamacherreihe 8-10, 20355 Hamburg, Germany

Phone number: +49 (0)40 46 00 20 333

Email: kundenbetreuung@passportcard.de

Managing Director: Eithan Wolf

You can contact our data protection officer at:

PassportCard Deutschland GmbH

Data Protection Officer

Address: Caffamacherreihe 8-10, 20355 Hamburg, Germany

Email: datenschutz@passportcard.de

This Privacy Notice applies for the collection of personal data via our website under <http://www.passportcard.de/>, via our mobile app (“**APP**”) as well as for any other collecting of your personal data including inbound or outbound calls via telephone.

This Privacy Notice applies for our customers, our business partners, our contractors as well as for applicants for a position in our company.

If necessary and where legally required, we will also inform you separately about the processing of your personal data in other contexts if this has not yet been done by this Privacy Notice.



Declaration of consent for the processing of health data, transfer of personal data to outside EU and release from confidentiality of medical providers and professionals, insurance companies and brokers

PassportCard expressly informs and points out that you are free to confirm this declaration of consent and to object it for the future. We have to point out, however, that it will generally not be possible to conclude or implement an insurance contract with PassportCard without your consent in the processing of your health data.

If reference is made to this Privacy Notice and the confirmation of this declaration of consent is requested, this confirmation also includes the following statements with regard to the processing of your health-related personal data, also in countries outside the EU and the release of the general obligation to confidentiality for insurance companies and medical professions:

By confirming this Privacy Notice, I agree that PassportCard collects, stores and processes the information I provide to PassportCard when applying for an insurance offer and in the future (including health-related data) to the extent necessary to review the application and to establish, to perform and to finish an insurance agreement. I also agree that PassportCard stores my health-related data – even if a contract with PassportCard is not concluded – for a period of 3 years from the end of the calendar year of my request.

By confirming this Privacy Notice, I agree that PassportCard transfers my personal data including health-related data if necessary, for the purpose of my insurance agreement to

- service providers,
- (re-)insurance companies,
- if necessary, also to my employer if my employer has concluded the insurance contract with PassportCard, which also covers my person, and
- in particular medical providers and medical experts as listed under paragraph 7 of this Privacy Notice

I agree that this personal data including health-related data is processed there for the same purposes as stated in this Privacy Notice and that personal data including health-related data is returned to PassportCard.

Insofar as necessary I release PassportCard and its employees as well as medical providers by confirming this declaration from its obligation to confidentiality with regard to personal data including health-related data protected by Section 203 of the German Penal Code.

By confirming this Privacy Notice, I agree that PassportCard collects my health data from doctors and other medical providers, nurses, hospital staff, personal insurers, statutory health insurance funds and authorities and uses them for these purposes, insofar as this is necessary for risk assessment or for the performance of contractual obligations of PassportCard.

This confirmation also expressly refers to service providers, especially to medical service providers, in countries outside the EU, in particular if I use services in these countries.



We will not use or disclose your personal data for purposes other than those purposes specified in this Privacy Notice. We will do our best to protect the privacy of your personal data. If you have any concerns about the way we process your personal data, you are welcome to contact our Data Protection Officer and our data protection team at: datenschutz@passportcard.de or write to us to: PassportCard Deutschland GmbH, Hamburg, Data Protection Officer, Caffamacherreihe 8-10, 20355 Hamburg, Germany. We will look into your enquiry and make good-faith efforts to resolve any existing or potential dispute with you. If you remain unhappy with the response you received, you can also refer the matter to the relevant supervisory authority. You will find the contact details of the supervisory authority in paragraph 15 of this Privacy Notice.

1. Processing of personal data of children under the age of 18

We are legally obliged to only provide our services to people who are at least 18 years. By concluding a contract with PassportCard, you confirm that you are over 18 years of age.

2. How and why we need your personal data – provision of services

Your personal data is collected from the personal digital spaces we provide you (APP, webpage and self-service webpage), by our sales department, or by our services representatives, and also, of you agree, via telephone.

We use the personal data we collect and receive to provide our service and, where appropriate, and if the legal requirements are met, to study and analyze the functionality of our services, website and APP and to analyze users' activities, to provide support, to measure service activity, to conduct surveys and send questionnaires, to maintain our service, to make it better and to continue developing the service and to communicate with natural persons working for our business partners.

We may use your email address to contact you when necessary, to send you reminders and to provide you information and notices about our service, provided that other necessary prerequisites are also fulfilled.

We obey the law and expect you to do the same. If necessary, we may use your personal data to enforce our terms, policies and legal agreements, to comply with court orders and warrants, and assist law enforcement agencies, to collect debts, prevent fraud, misappropriation, infringements, identity thefts and any other misuse of our service, and to take any action in any legal dispute and proceeding.

Though you are not required by law to provide us your personal data, failing to provide us with any necessary personal data might jeopardize our ability to provide you with essential services including providing you with health insurance coverage and/or managing pending claims you may have filed with us.

3. The personal data you provide in order to apply for an insurance policy

As a potential insured member, we may ask you to provide us with your personal data. We may ask you for your name, your contact details, your gender, your birthday, your passport number (or other forms of state issued identification number), your email address, profession, medical history and/or current status and financial information. If you wish to enroll any of your family member to our insurance policy, we may ask you the same information about them as well. If you are enrolled to our insurance policy as part of a corporate group, we may also ask for your workplace and job title. Subject to your consent, we will also store our phone conversation with you.

As an insured member we may ask you to provide additional personal details, such as medical documents and legal documents and your premium debt status. When you file an insurance claim with us, we may collect and process your medical bills, your written correspondences with us and any written notes taken about you by our customer representatives.

If you, as a potential insured member or as an insured member, correspond with us by telephone, recording our phone conversation with you is subject to your consent and we will make sure to ask for it before we record you.

If you purchased an insurance cover with us via a credit/debit card, please note that we comply with the Payment Card Industry Data Security Standard (PCI DSS). Accordingly, we have implemented data security and organizational measures that protect your payment information such as credit/debit card number and keep them in confidence.

If you provided us with your bank account information for future insurance payments, we will keep those in confidence in accordance with the data protection standard described in this statement.

When you contact us, or when we contact you, we process the personal data. We may participate in correspondences you



have with treating and/or advising physicians for rendering you further services and/or examining eligibility for insurance.

We advise you to be cautious when uploading insurance related content through our APP and/or our self-service website and/or through emails. Please also avoid any involuntary disclosure of your personal data or disclosure of others' personal data without their consent.

On the basis of Art. 22 subsection 2b in connection with § 37 German Federal Data Protection Act, we might also make use of automated individual decision making, weighing up your personal health status with our experiences to provide you with optimal insurance cover. In exceptional cases, we may also decide that no insurance cover can be granted as the (cost) risk for other insured members of PassportCard is too high.

Processing of personal data of a person other than the applicant:

By providing us with personal data of other persons (e.g. family members), you guarantee that you have informed these persons of the contents of this Privacy Policy and that you have obtained all necessary declarations of consent from the respective persons to receive their personal data, including their health data, in accordance with this Privacy Policy.

4. The personal data that we collect when you access our website or APP

When you access our website or mobile app, our servers may log certain "traffic/session" information from your device, such as the country from which you use the service, the browser type, operating system, geolocation and the Internet Protocol (IP) address. We also collect information about your activity, for example your log-in and log-out time, the duration of sessions, viewed webpages or specific content on webpages, etc. Log-files store this information with your full IP-address in case of a corresponding declaration of consent.

5. Is there an obligation to provide personal data?

We are required to collect your personal data as set out in paragraph 3. Without this data, we will generally not be able to provide you with health insurance coverage and/or manage pending claims you may have filed with us. In some cases, we are under a legal obligation to process personal data. Examples are to detect, prevent and investigate fraud or to facilitate the exercise of your consumer rights. Further we may need to process your personal data to detect, prevent and investigate any other actual or suspected violations of law or misuse of our service.

6. On what legal basis do we process your personal data?

We process personal data under the following lawful grounds: (i) the processing of special categories of personal data such as the data concerning health is based on your explicit consent; (ii) the processing of your personal data is necessary for us to perform the agreement with you and to take steps at your requests prior to entering into the agreement between us; (iii) the processing of your personal data is necessary for us to comply with legal obligations to which we are subject; (iv) the processing of your personal data is necessary for legitimate interests, such as cyber security and data protection, fraud detection, service maintenance and control, support, back-up, data disaster recovery.

7. Who receives your personal data?

Except as set out in this Privacy Notice, we do not sell, trade or otherwise transfer your personal data to outside parties. Your personal data may be transferred to the following categories of recipients:

Affiliates

- Parent companies, subsidiaries, and other affiliated company (the DavidShield group)

Within PassportCard your personal data is provided to the respective departments that need such data for the execution of the insurance policy you have chosen.

Please find a list of the affiliated companies here <http://www.davidshieldgroup.com/>.

Service providers

- Administrative services providers
- Third party information technologies providers (such as cloud providers)

Third-party service providers engaged by us and working on our order to support data processing (so-called "processors") may also receive data for these purposes. Service providers can also be commissioned to provide server capacity (so-called cloud service providers).



Third parties

Your personal data will be disclosed by us to third parties only if this is necessary for the fulfillment of our legal and/or contractual obligations, if we or the third party have a legitimate interest in the disclosure without affecting your legitimate interests, or if you have given your consent in relevant cases. In addition, data may be transferred to third parties to the extent we are required to do so by law or by enforceable regulatory or judicial order. Third parties to whom we may transfer your personal data, irrespective of the services we provide, include:

- Medical providers, especially doctors and medical experts
- Legal representatives
- Insurance consultants
- Corporate contact personnel (applicable to groups/business insurance policies)
- Insurance brokers and agents
- Law enforcement departments (after providing us with a valid legal request for disclosure)
- Insurance companies that ultimately will be responsible to pay your insurance claim (if applicable)
- Experts for the purpose of assessing inter alia injuries, diseases and their causes
- Relevant financial institutions such as: banks, credit cards processors, clearing houses, Payment Service Providers (gateway companies), and card issuers

8. Where do we process your personal data?

Your personal data is generally processed in Germany. Not all of the parties listed in paragraph 7 above are located in the European Economic Area. If we need to transfer personal data to a party which is located outside the EEA, we ensure that the transfer shall take place in accordance with the general principles of transfer as laid down in the GDPR. To the extent necessary under EU privacy laws and regulations, we have implemented data onward transfer instruments, such as the Controller to Processor Standard Contractual Clauses (SCCs), the Controller to Controller SCCs. The transfer may be subject to appropriate safeguards included in the EU-US Privacy Shield Framework.

In certain cases, we may need to transfer your personal information to countries outside Europe. This transfer is either necessary for the fulfillment of our insurance contract (see Art. 49 subsection 1 sentence 1b GDPR) or covered by your consent declaration (see above).

9. Handling of your publicly available personal data

Prior to our first communication with you, we may have received your personal data from social media and other public online platforms on which you publicly published your personal data. This personal information may include, but is not limited to, your personal and contact information, geographical location and other types of data that appears, publicly, in your social media and other public accounts.

10. How long will we store your personal data?

We need your personal data to adjudicate any claims you may file with us under your health insurance policy and or with the insurance company (for example to receive insurance reimbursements). We will store your personal data for at least the minimum amount of time required by the regulations of your jurisdiction.

In Germany, we are subject to various retention and documentation requirements pursuant to, inter alia, the German Commercial Code (Handelsgesetzbuch - "HGB") and the Tax Code (Abgabenordnung - "AO"). The retention and documentation periods specified therein last up to ten years. Finally, the storage period is also governed by statute of limitations periods, which can be up to thirty years, for example, pursuant to secs. 195 et seq. of the German Civil Code (Bürgerliches Gesetzbuch - "BGB"), whereby the general limitations period is three years. As claims for damages based on injury to life, limb, health or freedom become statute barred 30 years after the respective act, breach of duty or other event causing the damage was committed, customers' personal data must in principle be kept by us for this time.

If after a request for an offer for an insurance agreement, a contract with PassportCard is not concluded, health-related data is stored for a period of 3 years from the end of the calendar year of the request. Other, not health related personal data is, in such a case, stored for a period of 6 years after the end of the year of the respective application based on HGB and AO (obligation to store business letter for at least 6 years).

11. Data protection related information for applicants for a job at our company

We use, process and store personal data that you provide to us in connection with an application for a job at our company



based on Article 6 subsection 1a GDPR, and your respective consent declaration which is expressed in the transmission of these documents.

Application documents are processed by employees of our Human Resources department and as the case may be by superiors of the respective department. Beyond that, applicants' personal data can, for organizational reasons, be exchanged within our corporate group (see above under paragraph 7 and under <http://www.davidshieldgroup.com/>), for example for the purpose of the better organization of trainings.

Applicants' personal data will be deleted not later than 6 months after the rejection of the respective application unless there is a consent to a longer storage provided by the respective applicant.

12. Personal data security

We will use our best efforts to protect the confidentiality of your personal data. We use reasonable data security measures in line with the high industry standards. We also adopted strict rules that include technical and physical administrative measures for protecting your personal data, including protecting against personal data misuse and against unauthorized hacking.

All correspondence between you and PassportCard is secured and, where necessary, encrypted.

13. Web services disclaimer

Our websites might include links to external third-party websites. If you follow a link to any of these websites, please note that they have their own privacy notices which should be reviewed. Please note that we are not responsible for the privacy protection, policies, and use of any software offered in these external websites. We will not be responsible for any direct or indirect damages caused from the use of third-party websites.

14. Cookies

We use standard analytics tools of Google Analytics and IBM. The privacy practices of these tools are subject to Google's own privacy policy at: <http://www.google.com/analytics/learn/privacy.html> and IBM's privacy policy at: <https://www.ibm.com/watson/data-privacy/>. Google Analytics and IBM use cookies to provide its service.

The website uses so-called "cookies". These are small files that are stored on the user's computer when he or she visits the website. How we use Cookies is outlined below.

The 3 main types of cookies we use on our site are:

Strictly necessary cookies

These cookies are essential. Without them you might not be able to get the information or service you have asked for. They are needed for things like logging whether you see error messages – so we can make improvements and fix bugs – as well as allowing you to apply online for an insurance solution on our online form.

Analytics and measurement cookies

We use several technologies to understand how visitors use our website or app. These help us to identify areas for improvement, and to collect and report on commercial data (like sales volumes). We may, for example, analyse website usage and identify a page where people struggle to know what to do next; we'd then use session capture to observe some individual site visitors and find out what the issue is.

Tools we use for analytics and measurement include:

Google Analytics (Google Inc.)

Our website uses Google Analytics, a web analysis service from Google Inc. ("Google"). Google Analytics employs so-called "cookies", text files that are stored to your computer in order to facilitate an analysis of your use of the site. The information generated by these cookies about your visits to our site is transmitted to Google's servers in the US and stored there. However, using the IP anonymization ("anonymizeIP") activated for this website, Google will shorten your IP address (IP masking) within the member states of the European Union, or other countries within the European Economic Area (so-called IP masking). Only in exceptional cases will the full IP address be transferred to a Google server in the USA, and will be shortened there for further processing. On behalf of the website provider,



Google will use this information to evaluate your use of the website, to compile reports on the website activities, and to provide other services related to website use to the provider. The IP addresses transferred in the context of Google Analytics from the App will not be put together with other Google data. You can prevent cookies from being installed by adjusting the settings on your browser software accordingly. You should be aware, however, that by doing so you may not be able to make full use of all the functions of our website. You can prevent the transfer of data created by the cookie and related to your use of the website (including your IP address) to Google and the processing of this data by Google, by downloading and installing the browser plugin available under the following link (<https://tools.google.com/dlpage/gaoptout?hl=en>).

You can prevent the identification by Google Analytics on this website, by clicking on the following link. An opt-out cookie will be placed which prevents the future collection of your data when visiting this website:
<https://tools.google.com/dlpage/gaoptout?hl=en>

You can find further information about terms of use and data protection at
<http://www.google.com/analytics/terms/gb.html> or at

<http://www.google.com/intl/gb/policies/privacy/partners/>

We would like to point out that on this website Google Analytics uses the “anonymizeIP” function in order to ensure anonymous detection of IP addresses (so-called IP masking). This ensures that one cannot create a personal reference using IP addresses.

Smartlook

In the context of our legitimate interest in a technically flawless online offer and its economically efficient design and optimization, we use the analysis software Smartlook from Smartsupp.com s.r.o., Milady Horakove 13, 602 00 Brno, Czech Republic according to Art.6 paragraph 1 letter f GDPR.

This tool captures movements on the observed web pages in so-called heat maps. This enables us to identify anonymously where visitors click and how far they scroll. This enables us to make our website better and more customer friendly. The protection of your personal data is very important to us when using this tool. All data is collected without us being able to assign it to specific users. We can only track how the mouse is moved, where clicks are made and how far it was scrolled. We also record the screen size of the device, the type of device, browser information, the country from which access was made and the preferred language. If personal information about you or third parties is displayed on a website, Smartlook automatically hides it. These data are therefore not comprehensible for us.

You can use a "do not track header" to prevent the Smartlook tool from being used. Then no data will be collected about your visit to our website. For this purpose you must set your browser accordingly. You can find instructions on how to do this at: <http://www.akademie.de/wissen/do-not-track-datenschutz>.

You can also disable the Smartlook tool by using the opt-out button under: Smartlook Opt-Out.

The privacy policy of Smartlook can be found here: <https://help.smartlook.com/en/articles/3244452-privacy>
There you will also find information on how to undo the Smartlook use from our website.

CleverReach

This website uses CleverReach for sending newsletters. The provider is CleverReach GmbH & Co. KG, Mühlenstr. 43, 26180 Rastede, Germany. CleverReach is a service to organize and analyze the dispatch of newsletters. The data entered by you for the purpose of receiving the newsletter (e.g. e-mail address) is stored on the CleverReach servers in Germany or Ireland.

Sending out our newsletters with CleverReach allow us to analyze the behavior of the newsletter recipients. Among other things, we can analyze how many recipients opened the newsletter message and how often which link in the newsletter was clicked on. With the help of the so-called conversion tracking, we can also analyze whether a predefined action (e.g. purchase of a product on our website) has taken place after clicking on the link in the newsletter. For further information on data analysis by CleverReach newsletters, please see <https://www.cleverreach.com/en/features/reporting-tracking/>. Data processing is carried out on the basis of your consent (Art. 6 para. 1 letter a GDPR). You can revoke this consent at



any time by unsubscribing from the newsletter. The legality of the data processing operations already carried out remains unaffected by the revocation.

If you do not wish that CleverReach carries out the analysis, you need to unsubscribe from the newsletter. For this purpose, we provide a corresponding link in every newsletter message. You can also unsubscribe from the newsletter directly on the website.

The data that you provide us with for the purpose of subscribing to the newsletter will be stored by us until you unsubscribe from the newsletter and will be deleted from our servers as well as from the servers of CleverReach after the newsletter has been cancelled. Data that has been stored for other purposes (e.g. email addresses for the member area) remains unaffected.

You can find more details in the CleverReach privacy policy at: <https://www.cleverreach.com/en/privacy-policy/>.

Conclusion of a contract for commissioned data processing

We have concluded a contract with CleverReach for commissioned data processing and fully implement the strict requirements of the German data protection authorities when using CleverReach.

Geolocation

If you have agreed to so-called geolocation in your browser or operating system or other settings of your respective end device, we use this function to offer you individual services related to your current location (e.g. the location of the nearest branch). We process your location data processed in this way exclusively for this function. If you terminate the use, the data will be deleted.

Google Tag Manager

Google Tag Manager is used on this website. Google Tag Manager is a solution from Google Inc. that allows companies to manage website tags through an interface. Google Tag Manager is a cookie-less domain which does not collect any personal information. Google Tag Manager triggers other tags that may collect data, which we herewith specifically point out. Google Tag Manager does not access this data. If deactivated by the user at domain or cookie level, it is also in place for all tracking tags implemented with Google Tag Manager.

You may prevent the storage of cookies by adjusting your browser software accordingly; however, we point out that in this case you may not be able to use all functions of this website to their full extent.

You can also prevent the collection of data generated by the cookie and related to your use of the website (including your IP address) to Google and the processing of this data by Google by downloading and installing the browser plugin available at the following link: <https://tools.google.com/dlpage/gaoptout?hl=en>

Google Web Fonts

Google Web Fonts (<http://www.google.com/webfonts/>) are used to improve the visual presentation of various information on this website. The web fonts are transferred to the cache of the browser when the page is opened, so that they can be displayed. If the browser does not support Google Web Fonts or prevents access, the text will be displayed in a standard font. When the page is opened, no cookies are stored for the website visitor. Data transmitted in connection with the page view is sent to resource-specific domains such as fonts.googleapis.com or fonts.gstatic.com. They are not associated with data that may be collected or used in connection with the parallel use of authenticated Google services such as Gmail. If the browser does not support Google Web Fonts or prevents access, the text will be displayed in a standard font.

For information about Google Web Fonts' privacy policy, please visit: <https://developers.google.com/fonts/faq#Privacy>
General information on data protection is available in the Google Privacy Center at: <http://www.google.com/intl/en/privacy/>

Google Marketing Services

We use the marketing and remarketing services ("Google Marketing Services") of Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA, ("Google"). Google's marketing services are disabled by default on our websites and will only be enabled once you have given us your consent to set tracking cookies. The data processing is carried out in accordance with Art. 6 Para. 1 lit. a) GDPR on the basis of your consent.

Google's marketing services allow us to better target ads for and on our website to show users only ads that potentially match their interests. If e.g. the user is shown ads for products that he or she has been interested in on other websites, this is called "remarketing". For these purposes, when you access our and other websites on which Google marketing services are active, a code is executed directly by Google and so-called (re)marketing tags (invisible graphics or code,



also known as "web beacons") are incorporated into the website. With their help, an individual cookie, i.e. a small file, is stored on the user's device (instead of cookies, comparable technologies can also be used). The cookies can be set by various domains, including google.com, doubleclick.net, invitemediamedia.com, admeld.com, googlesyndication.com or googleadservices.com. This file records which websites the user has visited, what content he is interested in and which offers he has clicked on, as well as technical information on the browser and operating system, referring websites, visiting time and other information on the use of the online offer. The IP address of the user is also recorded, however, we inform within the framework of Google Analytics that the IP address is shortened within member states of the European Union or in other countries which are contracting parties to the Agreement on the European Economic Area and is only in exceptional cases transferred in full to a Google server in the USA and shortened there. The IP address is not combined with user data within other Google offers. This aforementioned information may also be combined with such information from other sources. If the user subsequently visits other websites, the ads tailored to his interests may be displayed. User data is processed pseudonymously within the scope of Google marketing services. This means that Google does not store and process e.g. the name or e-mail address of the users, but processes the relevant data cookie-related within pseudonymous user profiles. I.e. from Google's point of view, the ads are not managed and displayed for a specifically identified person, but for the cookie holder, regardless of who that cookie holder is. This does not apply if a user has expressly permitted Google to process the data without this pseudonymisation. The user information collected by "DoubleClick" is transmitted to Google and stored on Google's servers in the USA.

The Google marketing services we use include the online advertising program "Google Ads". In the case of Google Ads, each Ads customer receives a different "conversion cookie". Cookies can therefore not be tracked on the websites of Ads customers. The information collected through the cookie is used to compile conversion statistics for those Ads customers who have opted in to conversion tracking. The Ads customers are provided with the total number of users who clicked on their ad and were redirected to a page with a conversion tracking tag. However, they do not receive information that personally identifies users.

Another Google marketing service used by us is the "Google Tag Manager", with the help of which further Google analysis and marketing services can be integrated into our website (e.g. "Ads", "DoubleClick" or "Google Analytics").

For more information about Google's use of data for marketing purposes, please visit the website: <https://www.google.com/policies/technologies/ads>, Google's privacy policy is available at <https://www.google.com/policies/privacy>.

If you wish to opt-out of collection by Google marketing services, you can use the preferences and opt-out options provided by Google at <http://www.google.com/ads/preferences>

Facebook Pixel

The so-called "Facebook Pixel" of the social network Facebook is used as part of our online offer, which is operated by Facebook Inc. or, if you are resident in the EU, by Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland ("Facebook"). Facebook Pixel is deactivated by default on our websites and is only activated once you have given us your consent to set tracking cookies. The data processing is carried out in accordance with Art. 6 para. 1 lit. a) GDPR on the basis of your consent.

With the help of the Facebook Pixel, Facebook is able to determine the visitors of our offer as a target group for the presentation of ads, so-called "Facebook Ads". Accordingly, we use Facebook Pixel in order to display the Facebook ads placed by us only to those Facebook users who have also shown an interest in our Internet offer. This means that with the help of the Facebook Pixel we want to ensure that our Facebook ads correspond to the potential interest of the users and do not appear annoying. With the help of Facebook Pixel, we can also track the effectiveness of Facebook ads for statistical and market research purposes by seeing whether users are redirected to our website after clicking on a Facebook ad.

Facebook Pixel is integrated directly by Facebook when our websites are opened and can store a so-called cookie, i.e. a small file, on your device. If you then log in to Facebook or visit Facebook when logged in, the visit to our website will be noted in your profile. The data collected about you is anonymous to us, so we cannot draw conclusions about the identity of the user. However, the data is stored and processed by Facebook so that a connection to the respective user profile is possible. The data processing by Facebook is carried out within the framework of Facebook's data usage policy. Accordingly, you can find more information on how the remarketing Pixel works and generally on the display of Facebook ads in the Facebook data usage policy: <https://www.facebook.com/policy.php>.

You can object to tracking by Facebook Pixel and use of your information to display Facebook ads. To do so, go to the page set up by Facebook and follow the instructions on the settings for usage-based advertising:

<https://www.facebook.com/settings?tab=ads> or declare your objection via the US website <http://www.aboutads.info/choices/> or the EU website <http://www.youronlinechoices.com/>. The settings are platform independent, i.e. they are applied to all devices, such as desktop computers or mobile devices



Facebook Retargeting (Custom Audience)

A Facebook Ireland Limited pixel is integrated into this website (website custom audience pixel). This pixel is used by Facebook Ireland Limited to collect information about the use of this website (e.g. information about items viewed). This information can be associated with your person with the help of other information that Facebook Ireland Limited has stored about you, for example, due to your ownership of an account on the social network "Facebook". Based on the information collected via the pixel, interest-related advertisements about our offers can be displayed in your Facebook account (retargeting). The information collected through the pixel may also be aggregated by Facebook Ireland Limited and the aggregated information may be used by Facebook Ireland Limited for its own promotional purposes and for promotional purposes of third parties. For example, Facebook Ireland Limited may infer certain interests from your surfing behavior on this website and may also use this information to promote offers from third parties. Facebook Ireland Limited may also combine the information collected via the pixel with other information that Facebook Ireland Limited has collected about you via other websites and/or in connection with the use of the social network "Facebook", so that a profile about you can be stored at Facebook Ireland Limited. This profile may be used for advertising purposes. For more information on data protection at Facebook Ireland Limited, please click here: <https://www.facebook.com/policy.php>

The legal basis for data processing is Article 6(1)(a) GDPR and (f) GDPR

Your consent to cookies

Strictly necessary cookies do not require your consent.

For analytical and measurement cookies as well as for targeting or advertising cookies we request your consent before placing them on your device. You can give your consent by continuing to use our website or by clicking on the appropriate button on the banner displayed to you when visiting our website.

What about links to other websites and their Cookies?

We often link to other sites to give you extra information or services. Where these are provided by a third party, you may leave our website by clicking through to theirs. In this case, the Cookies policy set out on the third party's website will also apply. As this won't be controlled by us, you should read their policy to find out what information is being collected and how it's used.

How to control Cookies

You can restrict, remove or block Cookies through your browser settings at any time.

In addition to what is specified in this document, the user can manage preferences for Cookies directly from within their own browser and prevent – for example – third parties from installing them. Through the browser preferences, it is also possible to delete Cookies installed in the past, including the Cookies that might possibly have saved the consent for the installation of Cookies by this website. It is important to note that by disabling all Cookies, the functioning of this site may be compromised. Users can find information about how to manage Cookies in their browser at the following addresses: Google Chrome, Mozilla Firefox, Apple Safari and Microsoft Windows Explorer.

In the case of services provided by third parties, users can exercise their right to withdraw from the tracking activity by utilizing the information provided in the third party's privacy policy, by clicking the opt-out link – if provided – or by contacting the third party.

15. What rights do I have?

As the data subject, you are entitled to the following data protection rights:

Access: You have the right to request access to personal data related to you and stored at PassportCard and about the scope of data processing and data transfer performed by PassportCard and to obtain a copy of your stored personal data. See Art. 15 GDPR.

Rectification: With respect to your personal data stored at PassportCard, you have the right to demand the immediate rectification of incorrect personal data and you have the right to have incomplete personal data completed



Erasure: You have the right to demand the immediate deletion or erasure of your personal data stored by PassportCard, if the legal requirements are satisfied.

This is the case, in particular, if

- your personal data is no longer needed for the purposes for which it was collected;
- the sole legal basis for processing such data was your consent, and you have withdrawn such consent;
- you have objected to processing on the legal grounds relating to your particular situation, and we cannot prove that there are overriding legitimate grounds for processing;
- your personal data were processed unlawfully; or
- your personal data must be erased in order to comply with legal requirements.

If we have transmitted your data to third parties, we will inform them about the erasure to the extent required by law. Please note that your right to erasure is subject to certain limitations. For example, we may not and/or must not erase data that we are still required to retain due to statutory retention obligations. In addition, your right of erasure does not extend to data that we need in order to assert, exercise or defend against legal claims.

Restriction to the Processing:

Under certain conditions, you have the right to request that processing be limited (i.e., the marking of stored personal data with the aim of limiting its processing in the future). The requirements are:

- The accuracy of your personal data is contested by you and PassportCard must verify the accuracy of the personal data;
- the processing is unlawful, but you oppose the erasure of the personal data and request the restriction of their use instead;
- PassportCard no longer needs the personal data for the purposes of processing, but you require the data to establish, exercise or defend your legal claims.
- you have objected to processing pending the verification of whether the legitimate grounds of PassportCard override your legitimate grounds.

Where processing has been restricted, such data will be marked accordingly and, with the exception of storage, will be processed only with your consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the EU or an EU Member State.

Data Portability: To the extent that we automatically process your personal data that you have provided to us based on your consent or any contract with you, you have the right to receive such data in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from PassportCard. You also have the right to have the personal data transmitted directly from PassportCard to another controller where technically feasible, provided that such transmission does not adversely affect the rights and freedoms of others. See also Art. 20 GDPR.

Right to Object: If we process your personal data on grounds of legitimate interests or in the public interest, then you have the right to object to the processing of your personal data on grounds relating to your particular situation. In addition, you have an unrestricted right to object if we process your data for our direct marketing purposes. Please see our separate note in the section titled “Information about your right to object”.

Withdrawal of Consent: If you have given consent to the processing of your personal data, then you can withdraw such consent at any time. Please note that the withdrawal applies prospectively only. Processing that occurred before the withdrawal of consent remains valid.

Complaint: Furthermore, you have a right to file a complaint with a data protection authority (Datenschutzaufsichtsbehörde), if you believe that the processing of your personal data is unlawful. The right to file a complaint does not affect any other administrative or judicial remedies.



The address of the data protection supervisory authority responsible for PassportCard is:
Hamburger Beauftragte für Datenschutz und Informationssicherheit
Ludwig-Erhard-Str. 22
20459 Hamburg

<https://datenschutz-hamburg.de/>

Information about Your Right to Object

Right to object for personal reasons

You have the right to object to the processing of your personal data on grounds relating to your particular situation. The prerequisite for this is that the data processing takes place in the public interest or on the basis of a legitimate interest, balanced against your legitimate interests. This applies also to profiling.

Insofar as we base the processing of your personal data on a legitimate interest, we generally assume that we can demonstrate compelling legitimate grounds but will, of course, examine each individual case.

In the event of an objection, we will no longer process your personal data, unless

- we can demonstrate compelling legitimate grounds (“zwingende schutzwürdige Gründe”) for the processing of these data that override your interests, rights and freedoms, or
- your personal data serves the establishment, exercise or defence of legal claims.

Right to object to the processing for direct marketing purposes

You have the unrestricted right to object to the processing of your personal data for direct marketing purposes, which include profiling to the extent that it is related to such direct marketing without providing any reason.

In the event of an objection, we will no longer process your personal data.

Exercise of the right of objection

The objection can be made without form and should preferably be made to the contact data listed in this data protection notice.

16. Disclosure of personal data in case of emergency

In cases of an emergency, we may choose to disclose your personal data to a third party if all of the following apply:

1. We are approached by a third party, who is your close relative or is otherwise connected to you, asking us to disclose your personal data (we will verify by reasonable means the third party’s connection to you).
2. We are unable to contact you after reasonable efforts, depending on the nature and scope of the emergency.
3. We conclude after reasonable evaluation that the requested disclosure is necessary in order to protect your vital interests.

17. Notification of changes

We may change the terms of this Privacy Notice occasionally. We will notify you via our website or mobile app. Please read all occasional changes to this Privacy Notice as they may affect your privacy rights.

18. Less secured communication during emergencies

You might need our services during unfortunate circumstances such as emergency medical care, hospitalization, during various types of check-ups with your doctors and more. During these times, and within the scope of our services, you will need to share with us personal data relating to your specific problem. While we prefer using secured communication channels through which you may provide us, and we may send you, personal data, we also understand that these channels will not always be available to you during times of need. Thus, if you are interested in sending us, and receiving from us, respectively if you send us personal data about you via unsecured communication channels (such as WhatsApp, S.M.S and any other IM or unsecured channel) you accept the above mentioned risks. Please note that we will not be liable for any system failure or personal data hacking while using these channels and to use these channels you retain the sole and full responsibility for using these unsecured methods of communications. However, we will also inform you separately in this regard.



19. Use of WhatsApp

WhatsApp is a service provided by WhatsApp Inc., which in turn is part of Facebook Inc.

PassportCard uses this external application exclusively as a service channel. PassportCard is in no way responsible for the content and data shared, uploaded and processed via WhatsApp outside of PassportCard's own network. The data protection guidelines of WhatsApp apply to this.

Please read the data protection policy of WhatsApp carefully before using WhatsApp. By using WhatsApp, you automatically agree to these policies.

When you send us a message via WhatsApp, you are sending us your telephone number. We only use this number for WhatsApp communication with you. We only use the contents of the chat to process your request.

Please note the WhatsApp terms of use, on which we have no influence: If you install and use WhatsApp on your mobile phone, you agree to the terms of use of WhatsApp terms of use. These include, but are not limited to, granting WhatsApp Inc. access to your phone number and contacts stored on your phone.

We do not answer personal or confidential questions (i.e. with content that concerns personal data) via WhatsApp. Therefore, please provide an e-mail address or telephone number for this purpose.

Important: PassportCard will never ask you to share sensitive data with us via WhatsApp. If we need your data, a member of staff will inform you of a way to share it, e.g. a phone call or email.

20. Direct Marketing

If you purchased an insurance cover with us and are therefore an existing customer, we have included you in our marketing distribution list. We will send you in the future information on our company and its offers. You can opt out from our marketing distribution list by sending us a request to kundenbetreuung@passportcard.de or by clicking the remove option in our notices. Opting out from the marketing distribution list will have no effect on your contractual rights. We will inform you on this right and possibility in the course of every single marketing information.

If you do not have an insurance cover with us and are interested in receiving information about the products we offer, you can contact us at kundenbetreuung@passportcard.de and request to be listed on our marketing distribution list. The provisions of this Privacy Notice then apply.



LEGAL INFORMATION DOCUMENT

Dear Customer,

We would like to present you with the following general legal information regarding your insurance cover under the PassportCard Deutschland GmbH ("PassportCard") international private medical insurance policy ("Policy").

Based on the information that you have provided to us, we would like to recommend you the coverage under the PassportCard Policy as it will provide you with medical insurance cover whilst you are in your country of destination.

Please note that it is critical that you provide us with accurate information at all times. Any information which is not accurate may affect the quality and appropriateness of the service that PassportCard is able to provide to you and may put your insurance cover at risk. For any queries or to provide us with updates regarding your personal or medical information, please contact our customer service representatives at: kundenbetreuung@passportcard.de.

We have set-out below a select review of certain legal information which are detailed in greater depth in the PassportCard Policy terms and conditions provided to you at the time of purchasing your insurance cover and which is also available on our website: www.passportcard.de

1. Identity of the insurer

Name: VYV International Benefits ("VYV" or "Insurer")

Address: 7 Square Max Hymans, 75748 Paris Cedex 15, France

Jurisdiction: France

Commercial Register: ORIAS - Paris Trade and Companies register

acting in the name and on behalf of

MGEN International Benefits SAS, 3 square Max-Hymans, 75 748 Paris Cedex 15, France; and MFPrévoyance, 4 place Raoul Dautry, 75015 Paris, France.

2. Identity of broker

Name: PassportCard Deutschland GmbH

Address: Caffamacherreihe 8-10, 20355 Hamburg, Germany

Jurisdiction: Germany

3. Main business activity of the broker

Currently, the primary line of business for PassportCard is the distribution of the PassportCard Policy. PassportCard distributes the Policy underwritten by the insurer in this line of its business. PassportCard receives a sales commission in this respect.

4. Target market

The PassportCard insurance plan is targeted to the European internationally mobile community market. When the PassportCard literature refers to 'Europe' it is referring to the states that are included in the Schengen Area.



5. The Association for Insurance Coverage

The Association was set-up by PassportCard for the purpose of holding the group health insurance policy that it has entered into with the Insurer. The Association is the legal owner of the PassportCard insurance policy to which each individual member is subscribed and then provided with individual insurance cover.

6. The existence of a guarantee fund or other compensation schemes

A guarantee fund does not exist.

7. Essential features of the insurance cover

For details on the insurance benefits covered by the Policy, please refer to the documents provided to you at the time of purchasing your insurance cover and, in particular, the Table of Benefits and the underwriting document (if applicable).

8. Premium Rates

The premium rate that you will be required to pay in order to receive insurance cover under the Policy is annually determined according to the age of each person to be included in your insurance cover and, according to the location of your country of destination. In addition, an underwriting premium may be added to the premium rate based on the health declaration or questionnaire that you provided during the application process to receive the insurance cover.

The total premium amount will be stated on your Membership Certificate which was provided to you at the time of purchasing your insurance cover and which will periodically be updated in accordance with changes to the details contained in such document.

Any future change to the premium will be notified to you at least two months prior to such change coming into effect. During the two months' notice period, you will have the right to request the termination of the insurance cover before such rate comes into effect.

9. Premium Payments

The initial/first premium instalment is payable prior to the start date of your policy and not earlier than 14 days of the mentioned date. Subsequent premiums are due on the first day of the chosen payment period - quarterly/ monthly / annually according to the payment plan you selected at the time of purchasing your insurance cover.

10. Non-payment of Premium

In the event that you fail to pay the premium that is due, in full, within 1 (one) month following its due date, the Insurer's obligation to pay benefits may be waived. In addition, the insurance cover may be terminated 30 (thirty) days after you have been sent notification of the Insurer's intention to terminate your insurance cover ("30 day notice period"). Such notice shall then be cancelled if the due premium is paid within the 30 day notice period.

11. Recouping of Payments

In case of charges that are not respected by the member or withdrawn without commercial legal justification, we will charge damages at the amount of 10 EUR per charge from the member that may be charged also via direct debit if this is the payment method chosen and the customer provides their non-disputable permission to withdraw that also in direct debit (SEPA).

12. Duration of the insurance cover

The effective start date of your insurance cover is stated on your Membership Certificate. Your insurance cover may also be terminated upon the initiation of PassportCard or the Insurer



in accordance with the Policy terms and conditions which were provided to you at the time of purchasing your insurance cover and which are also available on our website. Upon termination, the insurance policy shall also be terminated for other persons included under your insurance cover.

Termination results in the immediate cancellation of entitlement to benefits for all services provided after the termination date.

13. Applicable law

The law of the Federal Republic of Germany shall apply to the pre-contractual relations.

14. Applicable language

Your insurance cover, together with the corresponding documents will be kept in the English or German language.

15. Complaint Management

If you have a question or complaint regarding your insurance cover, please send it to the following address:

PassportCard Deutschland GmbH
Caffamacherreihe 8-10
20355 Hamburg
Germany

or by e-mail: kundenbetreuung@passportcard.de

16. Complaint to the competent supervisory authority

In the event of complaints against us, you may contact PassportCard's customer service center at the following email address: kundenbetreuung@passportcard.de

If the response you are given does not meet your satisfaction, you have the option of contacting the German insurance supervisory authority. Their address is:

Handelskammer Hamburg
Adolphsplatz 1
20457 Hamburg

This does not affect the policyholder's right to take legal action.

17. Protection of Personal Data

Please refer to the data privacy notice that was provided to you together with other documents at the time you purchased your insurance cover. The data privacy notice is also available on the PassportCard website.



18. Revocation Instruction

Section 1

Right of revocation, consequences of revocation and special notes

Right of revocation

You may revoke your request for insurance cover in text format (e.g., letter, email) within 14 days without indicating any reasons.

The revocation period commences from the time you received

- the insurance certificate
 - the contract terms, including the terms and conditions of the insurance plan, which in turn include the tariff provisions,
 - this instruction,
 - product information sheet, and
- the further information listed below in section 2

in writing.

The timely dispatch of the revocation is sufficient to comply with the revocation period.

The revocation notice is to be addressed to:

PassportCard Deutschland GmbH
Caffamacherreihe 8-10
20355 Hamburg
Germany

Email: kundenbetreuung@passportcard.de

Consequences of Revocation

In the event of an effective revocation, the insurance cover will terminate and we will refund to you the portion of the premiums attributable to the period after receipt of the revocation if you have agreed that the insurance cover will commence before the end of the revocation period. In this case, we may retain the part of the premium that is attributable to the time until receipt of the revocation; this is an amount equal to 1/30 of the monthly premium for each day that insurance cover has existed. Reimbursement of the premium will occur without undue delay, at the latest thirty (30) days following receipt of the revocation.

If the insurance cover does not begin before the end of the revocation period, the effective revocation results in the return of benefits received and the surrender of benefits derived (e.g. interest).

Special Note

Your right of revocation expires if the insurance cover is completely fulfilled by you and us at your express request before you have exercised your right of revocation.



Section 2

List of further information required for the start of the time limit

With regard to the further information referred to in section 1 sentence 2, the information requirements are detailed below.

The insurer has to provide you with the following information:

- 1) the identity of the insurer and of the branch, if any, through which the contract is to be concluded; the commercial register with which the legal entity is registered, and the corresponding register number;
- 2) the identity of a representative of the insurer in the member state of the European Union in which you are resident, if there is such a representative, or the identity of a person acting in a professional capacity other than the insurer, if you are dealing with that person, and the capacity in which such person is acting with respect to you;
- 3)
 - (a) the insurer's address for service and any other address that is relevant to the business relationship between the insurer and you, in the case of legal persons, associations of persons or groups of persons also the name of a authorized representative; insofar as the notification is made by transmission of the contractual provisions including the General Conditions of Insurance, the information must be in a prominent and clear form; if the notification is made by transmission of the form;
 - (b) any other address relevant to the business relationship between an agent or representative of the insurer or any other person acting in a commercial capacity pursuant to number 2 and you, in the case of legal persons, associations of persons or groups of persons, also the name of a person authorized to represent them; insofar as the communication is by transmission of the terms and conditions of the contract, including the General terms and conditions of insurance, the information must be provided in a prominent and clearly designed form;
- 4) the main business activity of the insurer;
- 5) the essential features of the insurance benefit, in particular information on the type, scope and due date of the insurer's benefit;
- 6) the total price of the insurance including all taxes and other price components, whereby the premiums are to be shown individually if the insurance relationship is to comprise several independent insurance contracts, or, if an exact price cannot be stated, details of the basis for its calculation, which enable you to check the price;
- 7)
 - (a) if applicable, any additional costs incurred, stating the total amount to be paid, as well as any other taxes, fees or costs that have not been paid through or charged by the insurer;
 - (b) any costs incurred by you for the use of any means of distance communication, if such additional costs are charged;



- 8) details relating to payment and performance, in particular on the method of payment of the premiums;
- 9) the period of validity of the information provided, for example, the period of validity of limited offers, in particular with regard to the price;
- 10) information on how the contract is concluded, in particular on the commencement of the insurance and the insurance coverage as well as the duration of the period during which the applicant shall be bound by the application;
- 11) the existence or non-existence of a right of cancellation and the conditions, details of the exercise thereof, in particular the name and address of the person to whom the revocation is to be declared, and the legal consequences of the revocation, including information on the amount you may have to pay in the event of revocation; if the notification is sent by transmitting the terms of the contract, including the general Conditions of Insurance, the information must be provided in a prominent and clearly highlighted and clearly designed form;
- 12)
 - (a) Information on the duration of the contract;
 - (b) Information on the minimum term of the contract;
- 13) details of the termination of the contract, in particular the contractual termination conditions; insofar as the notification is made by the contractual provisions, including the general terms and conditions of insurance, the information shall be provided in a prominent and clearly designed form;
- 14) the member states of the European Union whose law the insurer is subject to establishing relations with you prior to the conclusion of the insurance contract;
- 15) the law applicable to the contract;
- 16) the languages in which the terms of the contract and the preliminary information referred to in this subsection are communicated, as well as the languages in which the insurer agrees, with your consent, to communicate during the term of this contract; and of this contract;
- 17) possible access for you to an out-of-court complaint and redress procedure and, if applicable, the conditions for such access; in this context, it must be expressly state that the possibility for you to take legal action, remains unaffected;
- 18) name and address of the competent supervisory authority and the possibility of a complaint to this supervisory authority.

End of the instruction on the right of revocation.

HEALTH INSURANCE PLAN

Insurance Product Information Document

Insurer: VYV International Benefits, acting in the name and on behalf of MGEN International Benefits SAS and MFPrévoyance

Distributing Agent: PassportCard Deutschland GmbH ("PassportCard")

Product: International Private Health Insurance - PassportCard Premium

PassportCard



This document is a high level summary of the contract's benefits and exclusions. It does not display the full list of benefits and/or exclusions. You can find the complete information on this product in the contractual and pre-contractual documentation. Benefits indicated with a green tick are systematically in the policy. Some of the benefits which are listed as insured are limited according to PassportCard's Terms and Conditions of Insurance. An overall annual limit applies to this product, as stipulated in the table of benefits. The contract shall be governed by and construed in accordance with German law. All claims arising from and in connection with the insurance contract shall be governed by German law.

Who is covered by the insurance?

The insurance product is a health insurance for individuals. The policyholder is the "Association for Insurance Coverage", 15 rue Bernoulli, 75008 Paris, France. Persons that wish to be insured as "Primary Members" or "other Covered Persons" can become members of the association. Each Insured Person has direct claims against the insurer.



What is insured?

The benefit amounts are subject to the PassportCard Terms and Conditions of insurance and the table of benefits.

- ✓ **Extensive inpatient and outpatient coverage**
- ✓ **Hospital accommodation and board in private room**
- ✓ **Cancer treatments**
- ✓ **Bone marrow and organ transplants**
- ✓ **Surgery**
- ✓ **Ongoing care for chronic conditions**
- ✓ **Office visits and check-ups**
- ✓ **Maternity and newborn care**
- ✓ **Medical imaging**
- ✓ **Inpatient and outpatient prescription medications**
- ✓ **Comprehensive therapy and psychotherapy services**
- ✓ **Extensive wellness services**
- ✓ **Rehabilitation and nursal services**
- ✓ **Emergency medical evacuation**
- ✓ **24/7 assistance services**
- ✓ **Medical emergency travel coverage worldwide up to 60 consecutive days**

Optional benefits - can be chosen to add to your plan:

- **Dental coverage**

Deductible:

Available with or without a deductible on hospitalization/inpatient treatment as mentioned on the Membership Certificate.



What is not insured?

The specific exclusions are set out in the PassportCard Terms and Conditions of insurance.

- ✗ **Experimental or unproven treatment or drug therapy**
- ✗ **Cosmetic surgery**
- ✗ **Health conditions arising from participation in war or criminal acts**



Are there any restrictions on cover?

- ! **Cover is restricted to the selected geographical area (zone)**
- ! **There are waiting periods for certain benefits**
- ! **Some benefits are limited in amount and/or number of treatments**
- ! **Cover is subject to the PassportCard Terms and Conditions of insurance**



Where am I covered?

In the zone/s of cover you selected as stated on your Membership Certificate.



What are my obligations?

- Continue to meet all the obligations under the PassportCard Terms and Conditions of insurance, in particular answering all questions of the insurer on insurability correctly and completely before joining the insurance.
- Provide receipts and other supporting documentation as requested.



How to pay the insurance premium?

The insurance premium is payable monthly, quarterly, semi-annually or annually. The method and frequency of payment will be as selected by you and will be stated on your Membership Certificate.

Collection of the insurance premium will start up to 14 days prior to the date the policy becomes active.



When does the cover start and end?

Your Membership Certificate shows the date your insurance cover comes into effect. Insurance cover remains in effect until the date the Primary Member is no longer eligible for coverage under the policy, or the date the master policy ends, or until otherwise terminated (whichever is the earliest). For dependants, cover will cease on the date the Primary Member ceases to be eligible for cover under the policy or if the dependant is no longer a dependant as defined in the PassportCard Policy Terms and Conditions. See PassportCard's Policy Terms and Conditions of insurance for further details.



How do I cancel the contract?

Policies may be cancelled by a written notice any time upon giving 30 days' notice.