Política de Privacidad

supported and reviewed by:

§ 1 Information regarding the collection of personal data

(1) We take data protection and the safe handling of your data seriously. To meet constantly growing requirements, T-Systems Multimedia Solutions GmbH has been mandated as an external data protection officer. In all issues regarding data protection, we are supported by the many years of expertise from T-Systems MMS, allowing us to fulfill legal and technological requirements.

With this privacy policy, we fulfill our information obligations in accordance with Articles 13 and 14 of the EU General Data Protection Regulation (GDPR).

Below, we provide information on the collection of personal data when using this website. Personal data is all data that relates to you personally, e.g. your name, address, email address, user behavior.

(2) The data controller in accordance with Article 4 para. 7 GDPR is

simplesurance GmbH
Am Karlsbad 16
10785 Berlin

Tel.: 34 900 802389
Email: support.es@simplesurance.com

You can contact our data protection coordinator at dataprotection@simplesurance.de.

(3) When you contact us by email or using a contact form, the data you provide (mandatory information is: your email address, the content of your message) will be stored by us in order to answer your questions. We may also process the data you provide in order to inform you of other interesting and similar offers from our own portfolio or to send you emails containing technical information (Article 6 para. 1 lit. f GDPR). You may object to this processing at any time by emailing dataprotection@simplesurance.de without incurring any costs other than the transmission costs according to the basic tariffs. We will delete the data collected within this context as soon as processing is no longer necessary, or alternatively, if any obligation of statutory retention exists, processing will be limited.

(4) In case we employ contracted service providers for individual functions of our offer or would like to use your data for advertising purposes, we will inform you in detail about the respective processes. We will also specify the defined criteria for the storage period.

§ 2 Your rights

According to the GDPR, you have the following rights:

- To request information on the categories of the processed data, processing purposes, any data recipients, the planned storage period (Article 15 GDPR);
- to request the correction or completion of incorrect or incomplete data (Article 16 GDPR);
- to revoke provided consent at any time with effect for the future (Article 7 para. 3 GDPR);
- to request the deletion of data in certain cases within the framework of Article 17 GDPR – in particular, if the data is no longer required for the intended purpose or is processed unlawfully, or you revoke your consent in accordance with Article 7 para. 3 GDPR or object in accordance with Article 21 GDPR;
- to request the restriction of data under certain conditions if deletion is not possible or the obligation to delete is in dispute (Article 18 GDPR);
- to data portability, i.e. you can receive the data you have provided to us in a common machine-readable format such as CSV and, if necessary, transmission to other parties (Article 20 GDPR);
- to complain to the responsible supervisory authority about data processing

Please send all information, deletion and correction requests, requests for information, inquiries about data portability or objections to data processing by email or post to

simplesurance GmbH persönlich/vertraulich
Am Karlsbad 16
10785 Berlin

Email: dataprotection@simplesurance.de

Tel.: 0900-800378 (toll free | Mon. - Fri 9:00 a.m. -6:00 p.m.)

We would also like to draw your attention to the fact that you can object to the future processing of your personal data in accordance with the legal requirements pursuant to Article 21 GDPR at any time. The objection may be lodged in particular against processing for direct advertising purposes.

§ 3 Collection of your personal data when you visit our website

(1) If you use the website for information purposes only, i.e. if you do not register or otherwise provide us with information, we only collect the personal data that your browser transmits to our server. If you wish to view our website, we collect the following data which is technically necessary for us to display our website to you and to guarantee stability and security (Legal basis is Art. 6 para. 1 sentence 1 lit. f GDPR):

- IP address
- Date and time of request

- Time zone difference from Greenwich Mean Time (GMT)
- Content of the request (specific page)
- Request status/HTTP status code
- The amount of data transferred in each case
- The website making the request
- Browser
- Operating system and its interface
- Language and version of the browser software.

(2) Cookies
Cookies are small files stored on users' computers. A variety of data can be stored within cookies. A cookie serves primarily to save the data of a user (or the device on which the cookie is stored) during or after their visit to an online offering. Temporary cookies, as well as "session cookies" or "transient cookies", are cookies that are deleted after a user leaves an online offering and closes their browser. For example, the content of a shopping cart in an online shop or a login status can be stored in a cookie of this kind. Cookies are referred to as "permanent" or "persistent" if they remain stored even after the browser has been closed. For example, this allows the login status to be saved if users visit the site again after several days. Likewise, users' interests may be stored in a cookie of this nature and used for measuring reach or marketing purposes. "Third-party cookies" are cookies that are offered by providers other than the data controller who operates the website (if it's only the data controller's cookies, they are referred to as "first-party cookies").
We may use temporary and permanent cookies and clarify this within the framework of our Privacy Policy and cookie banner.

We use technically necessary cookies.
The legal basis for the use of cookies is the existence of a legitimate interest in the stability and security of our IT systems within the meaning of Article 6 para. 1 lit. f GDPR.
We will obtain your consent for the use of further cookies (legal basis Article 6 para 1 a GDPR) via our cookie banner: https://www.simplesurance.co.uk/.

§ 4 Transfer of data

Your personal data will not be transferred to third parties for purposes other than those listed below.

We will only disclose your personal data to third parties if

- you have given your express consent pursuant to Art. 6 para. 1 sentence 1 lit. a GDPR,
- the disclosure pursuant to Art. 6 para. 1 sentence 1 (f) GDPR is necessary to safeguard our legitimate interests or to safeguard the legitimate interests of third parties and there is no reason to assume that you have an overriding legitimate interest in not disclosing your data,

- in the event that there is a legal obligation for disclosure in accordance with Article 6 para. 1 sentence 1 lit. c, and
- this is legally permissible and required in accordance with Article 6 para. 1 sentence 1 lit. b GDPR for the processing of contractual relationships with you.

§ 5 Use of our online shop

(1) If you would like to order in our webshop, it is necessary for the conclusion of the contract that you provide your personal data, which we need to process your order and to fulfil the contract. The information required for processing the contract is marked separately; any further information is voluntary. We use the data you provide to process your order. For settlement of payment we forward your payment data to our bank. The legal basis for this is Article 6 para. 1 Sentence 1 lit. b GDPR.

(2) We may also process the data you provide in order to inform you of other interesting and similar offers from our own portfolio or to send you emails containing technical information (Article 6 para. 1 lit. f GDPR). You can object to this processing at any time by emailing

dataprotection@simplesurance.de without incurring any costs other than the transmission costs according to the basic tariffs.

(3) There is no risk involved in paying for your insurance policies. Simplesurance transfers your contact details as well as the ordered insurance to the partners Saferpay (www.saferpay.com, SIX Payment Services AG, Hardturmstrasse 201, CH-8005 Zurich), Stripe (www.stripe.com, Stripe, Inc., 510 Townsend Street, San Francisco, CA 94103, USA), Klarna (www.Klarna.com, Klarna Bank AB, Sveavägen 46, 11134 Stockholm, Sweden) or PayPal (www.paypal.com, PayPal (Europe) S.à.r.l. et Cie, S.C.A., 22-24 Boulevard Royal, L-2449 Luxembourg) in separate, specially encrypted forms. You will then be automatically forwarded to the partner's secure server, where you can enter the required payment information. Payment-relevant data is only entered with certified external payment providers. Simplesurance does not save any payment-related data, such as credit card or account information.

(4) We are obligated by commercial and tax law to store your address, payment, and order data for a period of ten years. However, after two years we limit the processing of your data, that is, your data will only be used to comply with legal obligations.

(5) To prevent unauthorised access to your personal data by third parties, especially financial data, the order process is encrypted using TLS technology.

§ 6 Online social media presence

Fan pages on Xing and LinkedIn

simplesurance GmbH operates fan pages on Xing and LinkedIn. These pages are operated on the basis of our legitimate interests in providing up-to-date and supportive information and interaction options for and with our users and visitors in accordance with Article 6 para. 1 lit. f GDPR.
Every time the simplesurance GmbH pages are accessed in social networks, various data is generated, such as the amount of data transferred, the IP address used or the time of access. The respective network operators use cookies, i.e. small text files that are stored on the various end devices of the users, to store and further process this information. If the user has a corresponding profile of the network and is logged in to it, the storage and analysis also occur across devices.
The technical access as well as the further use of this data, which arise in the context of fan-page access, generally lie with the operator of the social network.
simplesurance GmbH has neither access to the usage data collected, nor can we determine how this data is used by the network operator.
Furthermore, we would like to point out that the data processing by social networks may occur outside the EU or the European Economic Area. For further details on the handling of data collected by social networks, please contact the respective operator of the social network itself.
The respective Privacy Policies can be found at:
XING: https://privacy.xing.com/en
LinkedIn: https://www.linkedin.com/legal/privacy-policy?_l=en The data transfer to the USA is based on EU standard contractual clauses.

§ 7 Privacy Policy for our Facebook fan page

At https://www.facebook.com/Simplesurance/ we operate an official company page, a "fan page", on the social network Facebook.
The protection of your personal data is of particular concern to us. We, therefore, process your data exclusively on the basis of the statutory provisions and in compliance with the relevant data protection regulations.

In this Privacy Policy, we inform you about data processing on our company page on the social network Facebook. We also explain the rights that users of this fan page have with regard to the storage and use of their personal data.

1. The joint controllers responsible for operating this Facebook page are:

Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland ("Facebook")
and
Simplesurance GmbH, Am Karlsbad 16, 10785 Berlin, Germany
You can view the agreement on joint responsibility under this link: https://www.facebook.com/legal/terms/page_controller_addendum.
According to this agreement, Facebook Ireland assumes primary responsibility for the processing of the Insights data and undertakes to fulfil all obligations under the General Data Protection Regulation with regard to the processing of the Insights data.

2. Data protection officer:

The data protection officer of Facebook Ireland Ltd. can be reached under the following link:
https://www.facebook.com/help/contact/540977946302970
You can reach our data protection officer by post at our postal address with the addition “persönlich/vertraulich an die Datenschutzbeauftragte" (personal/confidential to the data protection officer) or by emailing: dataprotection@simplesurance.de

3. Purposes of processing

We use the summarized data available on Facebook to make posts and activities on our Facebook page more attractive for users. We use, for example, the distribution by age and gender for adapting our manner of address, and the preferred visiting times of the users for time-optimised planning of our contributions. Information about the type of end devices used by visitors helps us to adapt the posts to them in terms of visual design. According to the Facebook terms of use, which each user has agreed to in the context of creating a Facebook profile, we can identify the subscribers and fans of the site and view their profiles and other shared information.
According to its own information, Facebook uses the information to provide and support the Facebook products and associated services described in the Facebook Terms of Use and Instagram Terms of Use. Further information is available at https://www.facebook.com/privacy/explanation

4. Processing of data

4.1 Cookies

The moment you access our fan page, you will be informed about the use of cookies via a cookie banner from Facebook and you will be asked for your consent.

4.2 Facebook Insights

The fan page operator can access statistical data of various categories via the so-called "Insights" of the Facebook page. Facebook generates statistics and makes them available to us. This function cannot be switched off nor can the generation and processing of the data be prevented. Further information is available at the following link:
https://www.facebook.com/business/help/144825579583746?helpref=search&sr=15&query=insights
For a selectable period as well as for each of the categories fans, subscribers, people reached and interacting individuals the following data is provided by Facebook:
Total number of page views, "Like" - information, page activities, post interactions, range, video views, post range, comments, shared content, answers, proportion of men and women, country and city of origin, language, views and klicks in the shop, clicks on route planners, clicks on telephone numbers. In addition, data is thereby provided about the Facebook groups that are linked with our Facebook page.
The constant development of Facebook changes the availability and processing of the data so that you can refer to Facebook's Privacy Policy for more information: https://www.facebook.com/about/privacy/

5. Legal basis

These pages are operated on the basis of our legitimate interests in providing up-to-date and supportive information and interaction options for and with our users and visitors in accordance with Article 6 para. 1 lit. f GDPR.

6. Transfer of data abroad

According to its own statements, Facebook shares information received both internally between the Facebook companies and with external partners. For this purpose, the information provided is transferred by Facebook Ireland to the USA and

other third countries. Transfers to so-called third countries are made, according to Facebook's own information, on the basis of the standard contractual clauses approved by the European Commission and, if applicable, on the adequacy decisions issued by the European Commission.

§ 8 Integration of Vimeo videos

(1) We use Vimeo to integrate videos from the provider, which are stored on http://www.vimeo.com and can be played directly from our website. These are all integrated and embedded in the "Extended Privacy Mode", i.e. no data about you as a user are transferred to Vimeo if you do not play the videos. Only when you play the videos will the data referred to in para. 2 be transmitted. We have no influence on this data transfer.

(2) When you visit this website, Vimeo is notified that you have accessed the corresponding sub-page of our website. Furthermore, the data mentioned under § 3 of this declaration will be transmitted. This takes place, regardless of whether Vimeo makes a user account available, via which you are logged in, or whether no user account exists. Vimeo stores your data as usage profiles and uses it for the purposes of advertising, market research and/or requirements-oriented design of its website. Such evaluation also takes place (even for users who are not logged in) for the purposes of providing customised advertising and to inform us about activities on our website. You have the right to object to the creation of these user profiles, whereby you must contact Vimeo to exercise this right.

(3) For more information on the purpose and scope of data collection and processing by Vimeo, please refer to the Privacy Policy. There you will also find further information on your corresponding rights and settings options for protecting your privacy: https://vimeo.com/privacy. The data transfer to the USA takes place on the basis of EU standard contractual clauses. Vimeo is operated by Vimeo, Inc., headquartered at 555 West 18th Street, New York, New York 10011.

§ 9 Use of Plausible Analytics

(1) Since data protection is important to us, we refrain from using invasive web tracking tools such as Google Analytics. Plausible Analytics takes a particularly privacy-friendly approach to analyzing your visit.
(2) We use Plausible Analytics to continuously optimize our offer both technically and in terms of content, in particular to understand and improve the use of our website by users.

Plausible Analytics does not set any cookies and does not store any information in the browser.
(3) Below you will find more information about Plausible Analytics and the privacy policy of this tool. Service provider: OÜ Plausible Insights, Västriku tn 2, Tartu 50403, Estonia; website: https://plausible.io/, privacy policy: https://plausible.io/data-policy.
(4) You are not tracked across devices and websites with this, unlike many other analytics tools. Also, all data collected per day is isolated and accumulated. Plausible Analytics collects the following information, among others, for this purpose:

- Date and time of your visit
- title and URL of the pages visited
- incoming links
- the country you are in
- the user agent of your browser software

Plausible does not use or store cookies on your terminal device. All data is stored completely anonymized in the form of a so-called hash. A hash is an encryption of data that is not reversible, i.e. cannot be decrypted. In this way, we can analyze your visit without storing personal data that would be readable by us, Plausible Analytics or third parties.

§ 10 Use of Google Fonts

(1) On our website we use Google Fonts. These are the "Google Fonts" of the company Google Inc. For the European area, the company Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Ireland) is responsible for all Google services.
(2) No cookies are stored in your browser. The files are requested via Google domains fonts.googleapis.com and fonts.gstatic.com. According to Google, the requests for CSS and fonts are completely separate from all other Google services. If you have a Google account, you do not need to worry that your Google account data, while using Google Fonts will be transmitted to Google. The data is only stored locally on our servers, so that a data transfer to third countries is excluded.
(3) Google Fonts is an important component to ensure the quality of our website. All Google Fonts are automatically optimized for the web. This saves data volume and is a great advantage especially for use on mobile devices. When you visit our site, the low file size ensures a fast loading time. Furthermore, Google Fonts are secure web fonts. Different image

synthesis systems (rendering) in different browsers, operating systems and mobile devices can lead to errors. Such errors can sometimes visually distort texts or entire web pages. Thanks to the fast Content Delivery Network (CDN), there are no cross-platform problems with Google Fonts.
Google Fonts supports all major browsers (Google Chrome, Mozilla Firefox, Apple Safari, Opera) and works reliably on most modern mobile operating systems, including Android 2.2+ and iOS 4.2+ (iPhone, iPad, iPod). We therefore use Google Fonts so that we can present our entire online service as uniformly as possible.
(4) Your data is not transmitted to external Google servers. If you have consented to Google Fonts being used, the legal basis for the corresponding data processing is this consent. According to Art. 6 Para. 1 lit. a DSGVO (consent), this consent constitutes the legal basis for the processing of personal data as it may occur during the collection by Google Fonts.

§ 11 Use of Friendly Captcha

(1) Our website uses the "Friendly Captcha" service (www.friendlycaptcha.com). This service is an offer from Friendly Captcha GmbH, Am Anger 3-5, 82237 Wörthsee, Germany. Friendly Captcha takes a particularly privacy-friendly approach to protecting websites and online services from spam and bots.

(2) Friendly Captcha generates a unique crypto puzzle (puzzle request) for each user. As soon as the user starts filling out a form, it is performed fully automatically. This task is solved in the background and once it is solved, a confirmation is sent by Friendly Captcha to the server that this is a natural person.

(3) Friendly Captcha processes and stores in the aforementioned process (puzzle request) the following personal data:

- Browser, operating system, domain name and the trail name of the website in question.

- The puzzle itself, which contains information about the account and the website key to which the puzzle refers to.

- A timestamp.

In addition, Friendly Captcha processes and stores anonymized via one-way hashing IP addresses that cannot be personally identified.

(4) The personal data mentioned in point 3 will be deleted after 30 days.

(5) For more information on data processing by Friendly Captcha, please refer to the Privacy Policy of Friendly Captcha at https://friendlycaptcha.com/de/legal/privacy-end-users/

(6) The legal basis for processing the data are our legitimate interests (Art. 6 para. 1. lit. f DSGVO) in the protection of our website against fraudulent access by bots, i.e. spam-protection and protection against attacks such as bulk requests

§ 12 Use of Hotjar

We use Hotjar to better understand the needs of our users and to optimise the offerings and experience on this website. Using Hotjar's technology, we get a better understanding of our users' experiences (e.g. how much time users spend on which pages, which links they click, what they like and what they do not, etc.) and that helps us to align our offer to our users' feedback. Hotjar uses cookies and other technologies to collect data about the behaviour of our users and their devices, in particular, the IP address of the device (recorded and stored in an anonymous form only during your use of the website), screen size, unique device identifiers, information about the device used browser, country, preferred language for displaying our website. Hotjar stores this information on our behalf in a pseudonymous user profile. Hotjar is contractually prohibited from selling the data collected on our behalf.

The legal basis for the use of Google Analytics is your consent in accordance with Article 6 para. 1 sentence 1 lit. a GDPR, which you can provide via our cookie banner. We have concluded an order processing agreement with Hotjar in accordance with Article 28 GDPR.

§ 13 Customer inquiries via Zendesk

We use the Zendesk Support Widget, a customer service platform from Zendesk Inc., 989 Market Street #300, San Francisco, CA 94102, USA, to process customer inquiries. For this purpose, necessary data such as last name, first name, postal address, telephone number, email address are recorded via our website in order to be able to answer your questions.

You can find more information on data processing by Zendesk in Zendesk's Privacy Policy at http://www.zendesk.com/company/privacy.

If you contact us by email or using a form, we will only use the personal data you provide to process the specific request. All details will be treated confidentially. The data provided and the message history with our service desk will be saved for follow-up questions and subsequent contact. We have concluded an order processing agreement with Zendesk in accordance with Article 28 GDPR. The data transfer to the USA takes place on the basis of EU standard contractual clauses.

§ 14 Use of review portals eKomi, Trustpilot and opineo.pl

After you have reported a claim to us and this has been processed, we may ask you to evaluate our services. This is done entirely voluntarily and only after you click on the link sent. With Trustpilot (Trustpilot A/S, Pilestraede 58, 5. Floor, 1112 Copenhagen K, Denmark) and opineo.pl - only for claims reported in Poland - (Ringier Axel Springer Polska sp. z.o.o., ul. Domaniewskiej 49, 02-627 Warszawa, you will be asked to give your name (alias without personal reference possible) and email address to provide a general assessment of our company. We cannot assign your rating to the claim you reported and we cannot identify you if you do not use any personal data that we already know.

After you have concluded an insurance contract with us or after processing your claim report, you will automatically be asked to rate our services. This is done entirely voluntarily and only after you click on the link sent. Your data (email address and order ID or name) will only then be forwarded to the independent service provider eKomi (www.ekomi.de, eKomi Ltd., Zimmerstrasse 11, 10969 Berlin). eKomi then only receives your data to obtain ratings via Simplesurance. The processing of your data by eKomi is automated. We can assign the evaluation submitted to eKomi to the

concluded contract or to the claim you reported. Obtaining ratings through our service provider is carried out at our behest and in accordance with an order processing contract (Article 28 GDPR).

These contacts are based on Article 6 para. 1 lit. f GDPR in conjunction with Recital 47 GDPR (direct advertising as a legitimate interest of simplesurance GmbH). You may object to the processing of your data for advertising purposes at any time by email to dataprotection@simplesurance.de without incurring any costs other than the transmission costs according to the basic tariffs.

You can find the privacy policies of our service providers at:

eKomi	https://www.ekomi.de/de/datenschutz/
Trustpilot	https://de.legal.trustpilot.com/for-reviewers/end-user-privacy-terms
Opineo.pl	https://polityka-prywatnosci.onet.pl/index.html

§ 15 Data protection for applications and the application process

You can apply exclusively via our online portal https://www.simplesurance.com/de/karriere. To be able to view our vacancies there, you will reach the website of our service provider Greenhouse. The transmission of your applicant data to us is encrypted.

We process your data in our IT systems as part of the application process. The legal basis for this is Article 6 para. 1 lit. b GDPR.

If you provide us with your application documents (for example as an unsolicited application) and your personal data by unencrypted email or by post, you consent to this transmission method. You also consent to us communicating with you in the application process by unencrypted email, for example, to confirm receipt of your application by unencrypted email. The legal basis for the communication channel is Article 6 para. 1 lit. a and f GDPR.

You may revoke your consent to unencrypted email communication at any time by sending an email to dataprotection@simplesurance.de with effect for the future.

We collect and process the personal data of applicants for the purpose of facilitating the application process. Processing may also be carried out electronically. This is particularly the case if an applicant sends us corresponding application documents, for example by email or via a web form on the website. If we conclude an employment contract with an applicant, the data transmitted will be stored for the purpose of processing the employment relationship in compliance with the statutory provisions and transferred to HR. If we do not conclude an

employment contract with the applicant, the application documents will be automatically deleted six months after notification of the rejection decision or the completion of the application process for this position, provided that the deletion does not conflict with any other legitimate interests on our part (e.g. statutory retention periods). The legal basis for this is Article 6 para. 1 lit. b GDPR. Another legitimate interest in this sense is, for example, a duty to provide evidence in proceedings under the General Equal Treatment Act (AGG). If you have consented to your data being stored in the Talent Pool for a longer period of time, your data will be stored for a further 2 years.

The further application process is handled by our service provider Greenhouse, i.e. all your communicated data will be transmitted to Greenhouse.

Management of application data and procedures by Greenhouse

We use the services of Greenhouse (www.greenhouse.io, Greenhouse Software Inc., 455 Broadway, New York NY, 10013 USA) for our application management and the associated processes.

Personal data that is made available to us as part of the online application process is stored and processed on Greenhouse's servers in the USA. The storage and processing take place on the basis of EU model contractual clauses, which also guarantee an adequate level of data protection. If necessary, we will process your data in order to process your application. We will not pass on your application data to other companies or third parties for any other use of the data, except for processing your application.

Rights of the data subject

In accordance with the GDPR and the BDSG (Federal Data Protection Act), you have the right to information, correction, deletion, restriction of processing and data transfer. If you want to assert your rights, you may contact our HR department directly at dataprotection@simplesurance.de.

§ 16 Data security

We use the most common TLS protocol (Transport Layer Security)/SSL (Secure Socket Layer) protocol together with the highest level of encryption supported by your browser. Usually, this is a 256-bit encryption. If your browser does not support 256-bit encryption, we use 128-bit v3 technology instead.

The transmission of a single page of our website in encrypted form is indicated on our website by the display of a closed key or lock icon in the bottom status bar of your browser.

We also use suitable technical and organizational security measures to protect your data against accidental or intentional manipulation, partial or complete loss, destruction or unauthorized access by third parties. Our security measures are continuously improved corresponding to technological developments.

§ 17 Deletion periods

Your personal data will be deleted, provided that statutory retention obligations do not preclude this, if you have made use of your right to have the data deleted, if the data is no longer required for the purpose for which it was saved, or if its storage is inadmissible for other legal reasons.

§ 18 Validity and changes to this Privacy Policy

This Privacy Policy is currently valid and is dated December 2023.

As a result of the development of our website and offers thereof or due to changed legal or regulatory requirements, it may be necessary to change this Privacy Policy. You can access and print out the current Privacy Policy at any time on our website.