

Privacy Policy

Last Updated: May 25, 2025

We take the protection of your privacy as a high level of responsibility. Please read this document (the “Privacy Policy” or the “Policy”) carefully and with attention.

Who we are

Use of the terms “Company”, “we” and ”us” in this Privacy Policy means **TRAFFIC SQUAD LTD**, a company duly incorporated and existing under the laws of Cyprus, registration number HE 458761, with principal address at: 81, Griva Digeni, Marinos Court, 3 rd Floor, Office 301, 6043 Larnaca, Cyprus. We are a software development company that is focused on providing various services in a digital advertising market.

This Privacy Policy

This Privacy Policy explains how information, including personal information, may be collected, used, and disclosed by Company with respect to the use of this website located at <https://tipacrm.com/> (the “Website”, the “website”, the “Site”, the “site”).

Our Services and Compliance with Law

Providing our services, we typically do not directly interact with the owners of personal information unless the owner of information is our client. Rather we process information (including personal information, if any), provided by our clients using various software and services, and not always our software in this regard. Therefore, we obligate our clients to comply with all applicable laws in all applicable jurisdictions, while obtaining information and to indemnify us of any claims arising from such non-compliance. If you are our client, we collect, process and use information in accordance with applicable agreement between you and us and this Policy.

In relation to personal data collected on this Website, Company acts as a data controller.

Changes to this Privacy Policy

We reserve the right to revise this Privacy Policy from time to time. The most current version of the Privacy Policy will determine the order and procedure of your information usage and will always be reflected on our Privacy Policy page. You agree that you are solely responsible for tracking changes on the Website. We do our best to publish any new information about changes in the Privacy Policy, but the user must independently check the Privacy Policy for updates when accessing the Website. Your continued use of the Website constitutes your acceptance of the new Privacy Policy and any changes made.

Contact Us

If you have questions, want to find out more about our privacy practices, or if you would like to make a complaint, submit a request or to exercise any of these rights, please contact us and our Data Protection Officer (DPO) by email: contact@tipacrm.com.

II. THIS WEBSITE AND PERSONAL INFORMATION COLLECTED THEREIN

By using the Website, you are accepting the terms of this Privacy Policy. IF YOU DO NOT AGREE TO TERMS OF THIS PRIVACY POLICY IN THEIR ENTIRETY, YOU MAY NOT ACCESS THIS WEBSITE OR OTHERWISE USE THE WEBSITE.

When you access and browse our Website, we may collect certain personal information either automatically or voluntarily. We categorise collected data as follows:

- Cookie Data
- Subscription Data
- Contact Forms Data

Cookie Data

We collect a variety of data using cookies and various other standard (typical for the industry) technology, including:

Cookies. Cookies are a technology that is based on small-size data files containing a string of alphanumeric characters that usually include a unique identifier and are placed on a user's device or computer. Cookies are usually stored at the user's computer permanently (persistent cookies) or temporarily. We use cookies to maintain security, operate the Website, show relevant advertisements, and optimize user experience.

Tags and Pixels. Tags and Pixels are blocks of code that we may use to track your browsing on the Internet: from resources to any particular websites or applications to track your browsing behavior. Sometimes web beacons are used for these purposes as well. They are usually transparent or invisible graphic images, no larger than 1x1 pixel, they are placed on a page or otherwise. It is often used in combination with cookies.

Cookie Data is categorized as follows:

- Essential cookies
- Advertising cookies
- Analytics cookies
- Entertainment cookies
- Functional cookies

Essential cookies
We use these cookies so that our website may function properly (e.g. so that you may adjust your screen size). These cookies may not be disabled. We will utilize this information should we identify any vulnerability, bug, or crash on the website to diagnose and address the issue effectively. Without it, distinguishing the cause of such malfunctions would be challenging. Also, this information helps us to keep the functionality of the website smooth and provide you with all available features. The names and storage periods of the cookies are specified in cookie settings on the Website.
Advertising cookies

We and/or third parties use these cookies or identifiers to track information about your activity to provide more relevant advertising to you. The use is only with your consent. You can opt in/opt out of these cookies by actively selecting the corresponding checkbox on the Website or adjusting your cookie settings. Be aware that these cookies might be associated with our advertising and marketing efforts, serving to offer you potentially appealing deals, or control the frequency of ads you encounter. Choosing not to accept these cookies could impact the content you encounter on the websites you browse. The names and storage periods of the cookies are specified in cookie settings on the Website.

Analytics cookies

We and/or third parties use these cookies or identifiers to analyze how visitors use this website; we use them to improve our Website. The use is only with your consent. You can opt in/opt out of these cookies by actively selecting the corresponding checkbox on the Website or adjusting your cookie settings. The names and storage periods of the cookies are specified in cookie settings on the Website.

Entertainment cookies

We and/or third parties use these cookies to display or play digital content online and analyze your interaction with that content. The use is only with your consent. You can opt in/opt out of these cookies by actively selecting the corresponding checkbox on the Website or adjusting your cookie settings. The names and storage periods of the cookies are specified in cookie settings on the Website.

Functional cookies

We and/or third parties use these cookies to remember your choices and preferences while you are using our Website, or when you revisit it. The use is only with your consent. You can opt in/opt out of these cookies by actively selecting the corresponding checkbox on the Website or adjusting your cookie settings. The names and storage periods of the cookies are specified in cookie settings on the Website.

Subscription Data

By entering your email address in the designated field on our Website, you authorize us to send you emails containing news and updates about the website, as well as information about our services.

Data	Why?	What is the legal basis for processing?	How long is it stored?
Email address	To provide you with the information about our latest news and updates	Your consent	For 1 year or unless you chose to unsubscribe
<p>You have the option to stop receiving marketing emails by either (a) reaching out to us directly or (b) clicking the unsubscribe link provided in every marketing email you receive from us. Upon unsubscribing, your subscription data will be removed from the relevant database.</p>			

Contact Forms Data

When you reach out to us through the Website forms or the contact information provided on our Website, you might furnish us with the following information:

Data	Why?	What is the legal basis for processing?	How long is it stored?
Your Name	To be able to address you properly	Legitimate interest in assisting you with your inquiry	For 1 year
Email address	To be able to contact you back	Legitimate interest in assisting you with your inquiry	For 1 year
Company name	To be able to address you properly and provide you with relevant information	Legitimate interest in assisting you with your inquiry related to particular company	For 1 year

How did you hear about us	To be able to understand what relevant information about us you might already know	Legitimate interest to assign a proper team to assist you	For 1 year
Message	To be able to analyze your issue precisely	Your consent	For 1 year
Without this information, we won't be able to resolve your issue, respond to your request, get in touch with you, or address you appropriately.			

We only store information in case of necessity. Typically, we delete all the information quarterly based on the terms above. Some information such as cookies may expire in accordance with your device settings. We do not need such information and we usually delete it unless it is necessary for performing our services to the user.

Please be aware that certain laws and regulations may subject us to store user information for a particular period: money laundering laws, financial reporting regulations, tax laws etc. Furthermore, we may have to comply with the decision of the court of appropriate jurisdiction and maintain information for the longer period.

To determine the corresponding retention period for personal data, in addition to processing objectives, we also consider the volume, nature, and category of data, the potential risk of harm from unauthorised use or disclosure of data, as well as the relevant requirements of the applicable legislation.

Eventually, we can minimise your data that we process or even make your data anonymous (for research or statistical purposes) so that it is no longer connected with you personally. If the data is anonymised, we can use this information essentially indefinitely since it no longer contains any data.

III. EEA USERS

Your Rights and Applicability of the EU Laws

Our Data Protection Officer can be reached via e-mail: contact@tipacrm.com.

Data Subject Rights of The Residents of The European Economic Area

If you are a resident of the EEA, you have certain data protection rights. Company endeavours to take reasonable steps to allow you to correct, amend, delete, or limit the use of your personal information, thus to enforce all rights provided to you under the General Data Protection Regulation (the “GDPR”).

The GDPR gives certain rights to individuals in relation to their personal data. Accordingly, Company is happy to offer transparency and access controls to help users take advantage of those rights.

Company applies substantially similar standards of data protection to all its users, considering any limitations, exemptions, or privileges imposed by your national laws, if applicable.

You (as a ‘data subject’) may send requests to us regarding your personal data via email to the following address: contact@tipacrm.com.

Please note that when you contact us, you must go through the identification process and describe your specific requirements so that we can process your lawful request and give a lawful response. If we cannot identify you via messages or requests, or if we have reasonable suspicions about your identity, we may ask you to provide proof of identity. This is the only way we can avoid disclosing your personal data to someone who may impersonate you, i.e. the identification process is carried out in your best interests. Any additional information collected for verification purposes will only be used to verify identity.

While we process requests as quickly as possible, we ask you to keep in mind that providing a complete and lawful response regarding personal data is a complex process that can take up to a month. If we need more time to prepare a complete response, we will let you know. If Company needs something from you to be able to deal with your request (eg. ID documents), the time limit will begin once we have received this.

You have the right to:		How?
Access	you have the right to request access to personal data we possess about you, or data we hold that requires updating or correction	you may request a copy of your data via contact@tipacrm.com
Be informed	you have the right to be informed of personal data we process and how we process it	you will be informed through: this Privacy Policy the information provided to you when you use our services or we will answer your questions when you contact us
Rectification	you have the right to request correction of inaccurate data or complete information that is incomplete	you may edit your personal data within the dashboard account or by contacting us at contact@tipacrm.com

Erasure	<p>you have the right to request erasure of certain personal data.</p> <p>For example, we will delete your personal data when:</p> <ul style="list-style-type: none"> your personal data is no longer necessary for its originally intended purpose, or you withdraw consent, and Company no longer has a legal basis for processing your personal data, or you object to the processing, and the Company lacks an overriding legitimate interest in processing that personal data. <p>Please note that sometimes, the Company will be unable to delete your personal data. For example, when:</p> <ul style="list-style-type: none"> we have a legal obligation to keep the data, or we need this data to establish, exercise or defend a legal claim, or our legitimate interest in using the data overrides your interest in having it deleted. For example we may need this data to protect our systems from fraud 	<p>you may delete your data the following ways:</p> <ul style="list-style-type: none"> by erasing it from your dashboard account, or by requesting the erasure of your data. To make such request please contact our DPO at contact@tipacrm.com
Restriction of processing	<p>you have the right to request us to stop processing your personal data. This right is applicable if:</p> <ul style="list-style-type: none"> your data is inaccurate; the processing of data is unlawful; you object to the processing of your data; we do not need your information for the originally intended purpose 	<p>you may send request to restrict processing of your data by contacting our DPO at contact@tipacrm.com</p>

Object to processing	<p>you have the right to object to processing of your personal data.</p> <p>The right to object may be exercised in the following situations:</p> <p>Company processes your personal data for direct marketing purposes, or</p> <p>we process your data based on our legitimate interest</p>	<p>you may send your objection request to our DPO at contact@tipacrm.com</p>
Data portability	<p>you have the right to request a copy of your data in electronic format and also the right to transmit your data to a third-party IT environment. You may exercise the right to data portability when certain conditions apply:</p> <p>the processing is based on your consent or needed for the performance of a contract with you;</p> <p>the processing is made only electronically, without any paper-based files included.</p>	<p>you may request a copy of your data via contact@tipacrm.com</p>
Not to be subject to Automated decision making	<p>you have the right not to be subjected to a decision solely based on automated processing, including profiling, that has legal effects or significantly impacts them in a similar manner.</p>	<p>Company does not carry out this type of processing</p>
Lodge a complaint	<p>you have the right to file a complaint with the data protection authority in the country where you reside, permanently live, work, or where a violation of data protection occurs.</p>	<p>please visit website of the Data Protection Authority in the country where you reside, permanently live, work, or where a violation of data protection occurs</p>

If you would like to exercise any of these rights, please contact us via: contact@tipacrm.com.

IV. UK DATA SUBJECT RIGHTS

After Brexit, the UK is no longer regulated domestically by the EU's General Data Protection Regulation (GDPR), which governs processing of personal data from individuals inside the EU. Instead, the UK now has its own version known as the UK-GDPR (United Kingdom General Data Protection Regulation). The new UK-GDPR took effect on January 31, 2020.

Under the UK-GDPR, individuals can exercise: the right to be informed; the right of access; the right to rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object to processing; the rights in relation to automated decision making and profiling and the right to lodge complaints. Please see the description of these rights above.

If you would like to exercise any of these rights, please contact us via: contact@tipacrm.com.

V. DATA PROTECTION RIGHTS OF THE RESIDENTS OF BRAZIL

Company strives to maintain compliance with the principles and requirements of data processing under the Lei Geral de Proteção de Dados Pessoais (“LGPD”), including, but not limited to, age-gating requirements.

We hereby inform You about the following rights you have under the LGPD:

- Confirmation: confirmation of the existence of processing;
- Access: access to the data;
- Rectification: correction of incomplete, inaccurate or outdated data; anonymization, blocking or elimination of unnecessary or excessive data or of data processed in noncompliance with the provisions of LGPD;
- Data portability: portability of the data to other service providers or suppliers of product, at the express request;
- Anonymization: anonymization, blocking or elimination of the personal data processed with the consent of the data subjects, except in the events set forth in article 16 of LGPD;
- Deletion: You have the right to have your personal data deleted if the processing of that data was based on consent;
- Information: You have the right to be informed about sub-processors and other third parties that access or process your personal data. You also have the right to be informed about Your consent choices and the consequences of refusing consent;
- Revocation: revocation of the consent, pursuant to the provisions of paragraph 5 of article 8 of LGPD;
- Bring complaint: lodging a complaint with the Data Protection Authority;
- Opposing the processing of personal data where there is non-compliance with the provisions of LGPD;
- Request review: You have the right to request the review of decisions made solely on the basis of automated processing of personal data which affect Your interests. This includes decisions used to define Your personal, professional, consumer and credit profile, or the aspects of Your personality.

If you would like to exercise any of these rights, please contact us via: contact@tipacrm.com.

VI. DATA PROTECTION RIGHTS OF THE RESIDENTS OF CHINA

Company complies with all the principles and requirements of data processing under the Personal Information Protection Law (the “PIPL”). The aforementioned principles include among others: accuracy, accountability and security, purpose limitation, collection limitation, openness and transparency, lawfulness and necessity.

We hereby inform You about the rights You have under the PIPL:

- You have the right to know, decide, refuse, and limit the handling of their personal information by others unless laws or regulations stipulate otherwise;
- You have the right to access and copy Your personal information in a timely manner, except when the laws and regulations require confidentiality;
- You have the right to correct or complete inaccurate personal information in a timely manner;
- You have the right to request Us to explain Our personal information handling rules;
- You have the right to deletion of Your personal information if (i) the agreed retention period has expired, or the handling purpose has been achieved; (ii) We as a personal information handler cease the provision of Our services; (iii) You rescind consent where the processing of personal information was based on Your consent; (iv) the information is handled in violation of laws, regulations or agreements;
- You have the right to request Us to transfer Your personal information to another personal information handler.

If you would like to exercise any of these rights, please contact us via: contact@tipacrm.com.

VII. US PRIVACY

The Company complies with all the principles and requirements of data processing under Virginia Consumer Data Protection (CPDA), Colorado Privacy Act (CPA), Connecticut's Act Concerning Personal Data Privacy and Online Monitoring, also known as the Connecticut Data Privacy Act (CTDPA), Utah Consumer Privacy Act (UCPA), Delaware Personal Data Privacy Act (DPDPA), Iowa Consumer Data Protection Act (ICDPA), Montana Consumer Data Privacy Act (MCDPA), Nebraska Data Privacy Act (NDPA), New Hampshire Senate Bill 255, New Jersey Senate Bill 332, Oregon Consumer Privacy Act (OCPA), Tennessee Information Protection Act (TIPA), Texas Data Privacy and Security Act (TDPSA).

- You can request access to the personal information we hold about you, or ask for it to be updated or corrected. Depending on the applicable laws, you may have additional rights related to your personal information.
- You have the right to obtain your personal information in a usable format and transfer it to another party, known as the right to data portability.
- You can request the deletion of the personal information we hold about you.
- You can opt out of certain types of personal information processing, such as targeted advertising and the sale of your personal information.

We do not sell personal data as commonly defined by this law. A sale includes disclosing personal data to a third party for monetary or other valuable consideration.

To exercise any of your data rights, submit a data rights request as outlined in this Privacy Policy.

If the processing of your personal information falls under this law and your request is declined, you have the right to appeal the decision. You can appeal by replying directly to the email you received regarding your request. Additionally, you may have the right to file a complaint with the Attorney General regarding the outcome of your appeal.

If you have any questions regarding your rights, please contact us via: contact@tipacrm.com.

California residents only

The California Consumer Privacy Act (hereinafter the "CCPA") that was later amended/alterd by The California Privacy Rights Act (hereinafter the "CPRA") provides consumers (California residents) with specific

rights regarding their personal information. This Provision describes your CCPA rights and explains how to exercise those rights.

This Provision does not apply to employment-related personal information collected from California-based employees, job applicants, contractors, or similar individuals.

This language is added to our existing Privacy Policy and our Terms of Use in compliance with CCPA that became effective January 1, 2020. This Provision is subject to amendments we may implement as a result of recommendations and directions issued by the Attorney General's Office in the State of California. We encourage you to visit the website of the State of California Department of Justice Office of the Attorney General.

Access to Specific Information

You have the right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive and confirm your verifiable consumer request, we will disclose to you:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- Our business or commercial purpose for collecting or selling that personal information.
- The categories of third parties with whom we share that personal information.
- The specific pieces of personal information we collected about you.

If we sold or disclosed your personal information for a business purpose, two separate lists disclosing:

- sales, identifying the personal information categories that each category of recipient purchased; and
- disclosures for a business purpose, identifying the personal information categories that each category of recipient obtained.

Deletion Request Rights

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we will delete (and direct our service providers to delete) your personal information from our records, unless an exception applies.

We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

- Complete the transaction for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you.
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
- Debug products to identify and repair errors that impair existing intended functionality.
- Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
- Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 et. seq.).
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent.

- Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
- Comply with a legal obligation.
- Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

Exercising Access and Deletion Rights

Exercise

To exercise the access and deletion rights described above, please submit a verifiable consumer request to us by contacting us via e-mail at: contact@tipacrm.com.

You may only make a verifiable consumer request for access or deletion once within a 12-month period.

Please read the Provision "Verifiable Consumer Requests" carefully and submit your request in accordance with the rules of the Provision.

Response Timing and Format

We endeavor to respond to a verifiable consumer request within thirty (30) calendar days of its receipt. If we require more time, we will inform you of the reason and extension period in writing.

We will deliver our written response by the same means of communication you provided in writing for the purposes of verifiable consumer request.

Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal information that is readily usable and should allow you to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

You do not need to create an account with us to exercise your opt-out rights. We will only use personal information provided in an opt-out request to review and comply with the request.

Non-Discrimination

We will not discriminate against you for exercising any of your CCPA rights. Unless permitted by the CCPA, we will not:

- Deny you goods or services.
- Charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties.
- Provide you a different level or quality of goods or services.
- Suggest that you may receive a different price or rate for goods or services or a different level or quality of goods or services.

However, we or our counter-agents may offer you certain financial incentives permitted by the CCPA that can result in different prices, rates, or quality levels. Any CCPA-permitted financial incentive we offer will reasonably relate to your personal information's value and contain written terms that describe the program's

material aspects. Participation in a financial incentive program requires your prior opt-in consent, which you may revoke at any time.

Other California Privacy Rights

California Civil Code Section § 1798.83 permits users of our Website that are California residents to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes. To make such a request, please write to us at: contact@tipacrm.com.

Categories of Personal Information We Collect, Sell, and Disclose

The list of the categories of personal information we collected about consumers during the previous 12 months (please, note, that pursuant to CCPA, "collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior) consists of the following categories of information, defined by CCPA:

- Identifiers, such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, e-mail address, account name, social security number, driver's license number, passport number, or other similar identifiers.
- Characteristics of protected classifications under California or federal law. Such information may include age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth, and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.
- Geolocation data.

We do not sell and do not disclose the categories of personal information set forth in the list above (i.e., identifiers, Section 1798.80 categories, protected classifications, commercial information, Internet or other electronic network activity information, and geolocation data).

Verifiable Consumer Requests

Only you, or a person registered with the California Secretary of State that you authorize to act on your behalf, may make a verifiable consumer request related to your personal information.

- The verifiable consumer request must:
- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.
- We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you.
- We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

- In any request in connection with your rights stated heretofore, please specify which right you are seeking to exercise and the scope of the request. At a minimum, we will request the following information to constitute your request as a verifiable consumer request:
- your full name;
- a reasonable proof of address indicating that you are a resident of the State of California;
- the region in which you are located at the time you are making your request;
- device validation information/device identifiers, if applicable;
- the CCPA right(s) you desire to exercise in your request.

Please be advised that in some instances, based on the categories of identifiable information we collect or will collect, your identifiers, as defined by CCPA, will not be available to us or our contractors. Simply put, your name or social security number may be irrelevant to the information about you that we or our contractors could have collected or sold. On the other hand, the subject information may collect relevant data about your device and about your browsing habits, such as cookies. Therefore, we may additionally request supporting evidence that unambiguously demonstrates that the device and the information in connection therewith are yours, such as screenshots of cookies or screenshots of the relevant settings of the certain mobile device. We may provide you with additional instructions as to what we need or ask you to respond to a few questions to appropriately verify your identity and the ownership of the subject device. Although the process may take time, it is necessary for the protection of your personal information and making sure that an unrelated third party cannot "guess" your device's credentials in order to get access to the relevant information.

Please note that at all times we may require information from you to help us to verify your identity and to process your requests. If we are unable to verify your identity, we may deny your requests.

VIII.STORAGE AND SHARING OF USER INFORMATION

We do not sell or lease your personal data. Nonetheless, we might disclose your personal data if it's reasonably necessary to fulfil our commitments to you and/or for our legitimate interest in maintaining and improving the website. Specifically, your personal information may be shared with the following recipient categories:

- our affiliates, who may act as data controllers processing your personal data, including their names and contact details, can be accessed in the footer;
- our subcontractors and team members, such as the support team, or technical team;
- third-party solutions that provide us with data storage facilities;
- government institutions that may request access to your personal data; we may share user information with law enforcement, regulatory authorities, courts with competent jurisdictions, emergency services or other necessary third parties for legal, protection, security, and safety purposes, including but not limited to the purpose of compliance with laws or regulatory requirements and to responses to lawful requests including requests of governmental entities, enforcement of our own policies and agreements, protection of our clients, agents, employees, directors, officers and alike;
- marketing and customer relationship management services, that attract visitors to our website, manage leads, and improve the overall customer experience;
- in connection with mergers, acquisitions, events of change of control, including but not limited to sale or transfer of all or a part of our business or assets; in this case, your informed consent, if applicable, will be granted to a new entity in accordance with the event of a change of control.

Please be aware that we and the mentioned recipients are located in regions that might not offer the same level of data protection as your home country. We will strive to safeguard your personal data during processing, storage, or transfer.

Standard Contractual Clauses:

- If we are governed by the General Data Protection Regulation (GDPR) and transfer personal data to a country with different data protection standards than your own, we will implement additional safeguards, such as Standard Contractual Clauses (SCC). These clauses are considered suitable data protection measures under the GDPR and aim to provide a comparable level of data protection by data recipients. This involves, for instance, robust encryption before transmission, stringent encryption key requirements, and encryption of data-at-rest.

Transfer Impact Assessment:

- Beyond the SCC, we conduct regular assessments of the recipient country's laws and practices. This ensures that the security measures and protections implemented by that country and the data recipients are verified.
- Security Measures (Technical and Organizational Measures):
- We may use various measures such as data pseudonymization, encryption, anti-virus software, and strict access/transfer controls. This is not an exhaustive list but provides an overview of some of the technical and organizational measures we might employ.

IX. YOUR CHOICES TO AVOID TARGETED ADVERTISING

Notice on OBA and opt-outs

Please be aware that although we believe that targeted advertisement is beneficial for all parties involved, we do not circumvent any devices, and there are many ways and technologies to stop receiving targeted advertising that our clients may apply using our technology. Note that different platforms and devices use different identifiers and different technologies, and also that each browser and each device has its own applicable settings. Please be advised that should you delete your cookies the information of your withdrawal from a targeted advertisement may also be deleted. Same may be applicable to cookie-blocks. Please note that you will continue to receive advertising after you opt-out, but it may not be tailored to your interests. Please also note that our opt-out mechanism is browser or device specific. Therefore, if you use multiple browsers/devices you will need to perform the opt-out operation for each browser or device. Certain devices and device configurations may prevent our opt-out from operating correctly. Persons located in the European Economic Area have the right to object to our processing of their personal data and/or revoke their consent as described below. We do not respond to or honor "do not track" (a/k/a DNT) signals or similar mechanisms transmitted by web browsers, except as required by applicable law.

In-ad opt-out

You may opt-out of OBA advertisements within a mobile website by clicking on the enhanced notice included within that advertisement, and then selecting "opt-out" within the page to which you are redirected through the following link when advertisement materials and/or inventory are shown from Company. To "Opt-out" [click this link](#).

In-app opt-out

If your consent to the targeted advertisement was granted through the application, please withdraw your consent directly from that application. In addition, your device setting likely allows you to generally withdraw or block personalized advertising: for instance, For Apple Devices: Go to Settings, Select Privacy, Select Advertising, and enable the "Limit Ad Tracking" setting. For Android Devices: Open the Google Settings App, Select Ads, and enable the "Opt out of interest based advertising" setting. Note: The actual opt-out instructions for each device may differ slightly depending on the operating system and updates. Also, after choosing to opt-out via any of the mechanisms described, if you use a different device or a different browser, or if you delete browser

cookies, you may need to repeat the opt-out steps for that particular device or browser. Please be advised that this Provision is not intended to serve as your user manual for your device, and you should always contact the manufacturer to obtain all relevant information on how to withdraw your consent.

X. POLICY TOWARDS CHILDREN

Our services are not intended for the use of children (those under the age of 18 or older if the country of your residence determines higher age restrictions). We do not knowingly collect or use personal data from children.

If you become aware that your child has provided us with personal information without your consent, please contact us.

If we discover that we have gathered the personal information of a child, we will promptly take appropriate measures to remove such personal data.

XI. IMPORTANT INFORMATION REGARDING SOCIAL MEDIA WEBSITES, TESTIMONIALS, AND BLOG COMMENTS MANAGEMENT

Please pay attention, due to the fact that our blog is maintained with the help of a third-party service, you might need to register before leaving a comment. Please also note that we are not eligible to manage your personal information or data placed in the comment section of our blog by users. In case you need to delete information containing your personal information from the comments on our blog, you'll have to login into a third-party application or address them directly with your data deletion request.

Be aware, such tools like social media widgets, buttons, social media scripts, hyperlinks to FB, LinkedIn, or Instagram, along with Twitter, and Telegram messenger services, belong to the third-party app providers. These third-party app providers may utilize above-mentioned tools for: information collection about your on-site behavior (pages visited), viewing your IP address, and cookies collection in order to optimize and streamline your browsing experience.

All of your actions and the way you interact with these social media tools, features or the social media, gets subjected solely to their privacy policies.

Submitting your data directly through social media, as well as via comments, and forum sections on websites, remember that your personal ID information can be accessed (in case you haven't restricted your social media privacy settings), and used by the third parties without your consent or pre-agreement.

XII. SECURITY

To prevent unauthorised access and disclosure, to maintain data accuracy, and to ensure the appropriate use of your information, we utilise industry standard physical, technical, and administrative procedures to safeguard any personal information we collect. Please note that no transmission or storage of information, however, can ever be guaranteed to be completely secure, though we take all reasonable precautions to protect against security incidents.

Company is very serious about the security of personal data. To ensure the secure storage of your data, we have implemented a variety of technical and administrative tools that protect data from any unauthorised or illegal processing and any loss, destruction or damage. We regularly test our security measures to ensure they remain operational and effective.

The data you provide will be safely stored on servers, which are inaccessible to the public.

Company adheres to the principle of data minimisation. We process information that is really necessary for us to perform certain functions and for the specific goals defined in this Policy. Your data is available only for a limited number of employees who need access to the relevant data to fulfil their functional duties.