

# Privacy Policy and Terms & Conditions

## 1. Introduction:

Effective date: April 01, 2024

Magicminds/MagicMind Technologies Ltd. (“us”, “we”, or “our”) operates the <https://magicminds.io/> website and the Magicminds Family of Products (the “Service”, “Product/s”).

This page informs you of our policies regarding the collection, use, and disclosure of personal data when you use our Service or Product/s and the choices you have associated with that data.

We use your data to provide and improve the Products. By using the Product/s, you agree to the collection and use of information in accordance with this policy. Unless otherwise defined in this Privacy Policy, terms used in this Privacy Policy have the same meanings as in our Terms and Conditions.

## 2. How We Use and Process Your Personal Data

We process your personal data:

**Where it is necessary to fulfill our contract** with you at your request, in order to:

- Create and manage your account;
- Provide you with information and Services that you request;
- Authenticate your identity prior to enrolling in our Services;
- Verify your identity and entitlement to Services, when you contact us or access our Services;
- Process your purchase transactions;
- Update you on the status of your orders;
- Allow you to register the Services you purchase;
- Confirm that you received necessary service and transactional emails;
- Manage your subscriptions; and
- Provide you with technical and customer support.

Where you have provided your consent, in order to:

- Subscribe you to newsletters and send you product updates or technical alerts;
- Send you marketing communications and information on new Services;
- Communicate with you about, and manage, your participation in contests, offers, or promotions;
- Solicit your opinion or feedback and/or provide opportunities for you to test Services;
- Enable you to refer a friend who may be interested in our offerings, as permitted by law;
- As applicable, to enable non-essential cookies or similar technologies; and
- As applicable, to provide you with interest-based ads about Magicminds on sites other than our own.

**For the purpose of fulfilling our legal obligations**, we may be obligated to, for instance, keep and process records for tax purposes, accounting, other obligations such as court or other legal orders, and other necessary disclosures.

**For the purpose of promoting and operating our business and advancing our or a third party's legitimate interests**, such as the effective delivery of our Services, and communications to you as well as to our other customers and partners, in order to:

- Enable participation in interactive features of our Services,
- Notify you about changes to our terms or this Privacy Statement;
- Communicate commercial promotions and provide quotes for our Services;
- Inform you about additional Services that provide solutions to issues detected as a result of your request;
- Promote and administer co-branded offers with trusted partners;
- Confirm sales conversions and conduct lead generation activities;
- Better administer and understand the usability, performance, and effectiveness of our Services websites, and communications to you, including troubleshooting, debugging, reviewing customer service interactions, data analytics, testing, research, and statistical analysis;
- Improve our Services (including developing new Services) and customize and present content in the most relevant and effective manner for you and

for your device, including suggestions and recommendations about things that may be of interest to you;

- \*Enhance the security of our own networks and information systems;
- \*Develop cyber-threat intelligence resources; and
- \*Otherwise keep our Services, business, and users safe and secure, and comply with applicable laws and regulations or judicial process or government agencies, and to protect or exercise our legal rights and defend against legal claims.

### **\*For Network and Information Security Purposes and Cyber-Threat Intelligence:**

Our legitimate interests include developing threat intelligence resources aimed at maintaining and improving the ability of our information networks and systems to resist unlawful or malicious actions and other harmful events, such as cybercriminal activities, and attempts at identity theft or fraud (“cyber and identity threats”).

We only rely on our or a third party’s legitimate interests to process personal data when these interests are not overridden by your rights and interests.

## **3. When and Why We Disclose Your Personal Data**

We are committed to maintaining your trust, and we want you to understand when and why we disclose personal data to third parties. We do not sell your personal data or use or disclose sensitive personal information for purposes other than those set forth in the California Consumer Privacy Act (“CCPA”). Data obtained through short code programs will not be shared with any third-parties for their marketing

reasons/purposes. We may disclose the categories of personal described above in “Categories of Personal Data We Collect” to the entities and for the purposes described below.

We may disclose personal data about you with your consent, or:

- **With our Partners**

We may provide your personal data to our partners for the purpose of allowing them to conduct Magicminds business. Our partners may use your personal data to communicate with you and others about Magicminds Services either alone or jointly with partner products and services. We may provide your personal data to partners to confirm your eligibility for joint or co-branded offers or to communicate and administer such offers (e.g., report sales conversions, verify eligibility, assess effectiveness of joint offer, etc.). Our partners are not allowed to use any data including personal data that they receive from us for any purpose except for communicating, evaluating, improving, and administering the offer in question (Magicminds branded, co-branded, or joint offer). This will not affect the partner’s ability to use personal data that it may already have obtained from you or other sources. If you do not wish to receive promotional emails from our partners, you can unsubscribe directly using the unsubscribe link or tool provided in the partner’s email or other communication to you.

In the past 12 months since this Statement was last updated, we disclosed the following categories of personal data to our partners: User data, Product data, Website data, Third-party data.

- **With our Distributors or Resellers**

We may provide your personal data to our distributors, resellers, or partners for the purpose of distribution, sale, or management of our products. Our distributors, resellers, or partners may communicate with you about Magicminds services. In addition, you may purchase our products directly from our distributor, a reseller, or an app store. Because your relationship in these cases is with that distributor, reseller, or app store, such third party will also process your personal data.

In the past 12 months since this Statement was last updated, we disclosed the following categories of personal data to our partners: User data, Product data.

- **With Our Advertising Partners**

We engage in personalized (or targeted) advertising in our Services or on other sites when we advertise our Services elsewhere. We may provide or share (as defined by the CCPA) your personal data, including the data about your interests in our Services, to third parties for the purposes of serving you more relevant ads about our Services. Where we provide you with interest-based ads on a site other than our own, we do not track your other activities on that site. If you click on our ads, we will know the domain you came from.

In the past 12 months since this Statement was last updated, we disclosed or shared the following categories of personal data to our advertising partners: User data, Device Data, Website data.

- **With Data Analytics Providers**

We may provide your personal data to third parties to use the personal data in aggregate form to help us understand how our Services are being used or to understand the effectiveness of our marketing campaigns.

In the past 12 months since this Statement was last updated, we disclosed the following categories of personal data to our data analytics partners: User data, Product data, Website data.

- **With Service Providers Processing Data on Our Behalf**

We may use contractors and service providers to process the personal data we collect for the purposes described in this Statement, the relevant Product and Service Privacy Statements, and for business purposes such as financial auditing, data storage and security, troubleshooting and debugging, improving the functionality and usability of our websites and Services, improving and operationalizing threat intelligence and counter-threat measures, and for marketing and promoting our Services.

We contractually require service providers to keep data confidential, and we do not allow our service providers to disclose our data or your personal data to others without our authorization, or to sell it or use it for purposes unrelated to the services they provide (e.g., their own marketing purposes). However, if you have a separate and/or independent relationship with these service providers, their privacy statements will apply to such relationships. Such service providers may include benefit brokers, your employer (for products and services offered as an employee benefit), contact centers, payment card processors, and marketing, survey, or analytics suppliers.

In the past 12 months since this Statement was last updated, we disclosed the following categories of personal data to our service providers: User data, Product data, Website data, Third-party data.

- **With Payment Processors** If you pay for use of our services, you may use a third-party payment processor to take payment from you. These third parties are properly regulated and authorized to handle your payment information. However, they are independent controllers of your data with their own responsibilities.

Your billing data is processed by the payment processor from whom you purchased the product. Your data is processed according to the relevant processor’s privacy policy.

payment Processor	Link to Privacy Policy
Google Play Store (for mobile apps)	<a href="https://policies.google.com/privacy">https://policies.google.com/privacy</a>
Apple Store (for mobile apps)	<a href="https://www.apple.com/legal/privacy/">https://www.apple.com/legal/privacy/</a>

- **With Public Authorities and Legal Proceedings**

In certain instances, it may be necessary for us to disclose any of the personal data we collect to comply with a legal obligation, at the request of public authorities, or as otherwise required by applicable law. No personal data will be disclosed except in response to:

- A subpoena, warrant, or other legal process issued by a court or other public authority of competent jurisdiction;
- Discovery requests or demands as part of a civil lawsuit or similar legal process;
- Where disclosure is required to comply with applicable laws, or necessary for us to enforce our legal rights pursuant to applicable law;
- A request with the purpose of identifying and/or preventing credit card fraud or identity theft; or
- Where disclosure of personal data is necessary to prevent or lessen a serious and imminent threat of bodily or other significant harm to the data subject or other individuals potentially concerned.

In the past 12 months since this Statement was last updated, we disclosed the following categories of personal data to public authorities: User data, Product data, Website data.

- **For Restoration Services**

We may disclose your user data, security data, diagnostic information, and third-party data to financial institutions, financial services companies, and other third parties at your direction to provide restoration services and other Services to you.

In the past 12 months since this Statement was last updated, we disclosed the following categories of personal data to financial institutions: User data, product data.

- **With Third-Party Service Providers**

If you access third-party services through our Services, these third parties may be able to collect user data, security data, diagnostic information, and third-party data about you in accordance with their own privacy policies. Some examples include:

## Third-Party Login Providers

To register with us or to be able to log into our products, we offer you, in addition to our own procedure, the option to do this via the services Google, and Apple ID. For this purpose, we will redirect you to a page of the corresponding provider. You will share your log in data exclusively with the provider, who in turn exchanges data with us accordingly. Please note that the service provider also receives information from us in this way.

Provider	Links
Apple	<a href="https://www.apple.com/legal/privacy/">https://www.apple.com/legal/privacy/</a>
Google	<a href="https://policies.google.com/privacy">https://policies.google.com/privacy</a>

## Social Media and Internet Platforms

Our social media monitoring service uses API services from the platforms listed below. Our website and services may also contain links to those platforms. If you use the platforms listed below, your use is subject to the platforms terms of service and privacy policies available through the provided links.

Provider	Links
YouTube	Terms of Service: <a href="https://www.youtube.com/t/terms">https://www.youtube.com/t/terms</a> Privacy: <a href="https://policies.google.com/privacy">https://policies.google.com/privacy</a> Manage Settings: <a href="https://myaccount.google.com/permissions">https://myaccount.google.com/permissions</a>
Facebook	<a href="https://www.facebook.com/legal/terms/update">https://www.facebook.com/legal/terms/update</a> <a href="https://www.facebook.com/privacy/policy/">https://www.facebook.com/privacy/policy/</a>
Instagram	<a href="https://help.instagram.com/581066165581870?helpref=page_content">https://help.instagram.com/581066165581870?helpref=page_content</a> <a href="https://privacycenter.instagram.com/policy">https://privacycenter.instagram.com/policy</a>
Twitter	<a href="https://twitter.com/en/privacy">https://twitter.com/en/privacy</a> <a href="https://twitter.com/en/tos#update-intlTerms">https://twitter.com/en/tos#update-intlTerms</a> <a href="https://twitter.com/en/tos#update">https://twitter.com/en/tos#update</a>
LinkedIn	<a href="https://www.linkedin.com/legal/user-agreement">https://www.linkedin.com/legal/user-agreement</a> <a href="https://privacy.linkedin.com/">https://privacy.linkedin.com/</a>
Snapchat	<a href="https://snap.com/en-US/terms">https://snap.com/en-US/terms</a> <a href="https://snap.com/en-US/terms#terms-row">https://snap.com/en-US/terms#terms-row</a> <a href="https://values.snap.com/privacy/privacy-center">https://values.snap.com/privacy/privacy-center</a>
TikTok	<a href="https://www.tiktok.com/legal/page/us/terms-of-service/en">https://www.tiktok.com/legal/page/us/terms-of-service/en</a> <a href="https://www.tiktok.com/legal/page/eea/terms-of-service/en">https://www.tiktok.com/legal/page/eea/terms-of-service/en</a>



	<a href="https://www.tiktok.com/legal/page/row/terms-of-service/en">https://www.tiktok.com/legal/page/row/terms-of-service/en</a>
--	---

- **With Our Corporate Affiliates**

We may share the information we collect with our corporate affiliates, subsidiaries, branch offices and other members of our corporate group.

In the past 12 months since this Statement was last updated, we disclosed the following categories of personal data third-party corporate affiliates: User data, Product data, Website data, Third-party data.

- **For Business Transfers**

We may share the personal data we collect in connection with a substantial corporate transaction, such as the sale of a website, a merger, acquisition, consolidation, asset sale, or initial public offering, or in the unlikely event of bankruptcy.

## **4. Retention and Deletion of Your Personal Data**

We will keep your personal data on our systems as long as necessary to provide you with our Services, or for as long as we have another legitimate business purpose to do so, but not longer than permitted or required by law. When determining the specific retention period, we take into account various criteria, such as the type of service provided to you, the nature and length of our relationship with you, and mandatory retention periods provided by law and the relevant statute of limitations. When we no longer have an ongoing legitimate business reason to keep your personal data, your personal data will either be securely disposed of, or de-identified through an appropriate anonymization means.

## 5. Cross-Border Transfers of Personal Data Among Magicminds and to Third-Party Vendors

We are a global company and process personal data in many countries. As part of our business, your personal data may be transferred to Magicminds and/or its subsidiaries and affiliates in the United States, and to subsidiaries and third-party vendors of Magicminds located worldwide, including Magicminds entities. All transfers will occur in compliance with the applicable data transfer requirements laws and regulations.

Magicminds has certified to the EU-U.S. Data Privacy Framework and Swiss-U.S. Data Privacy Framework as set forth by the U.S. Department of Commerce regarding the transfer of personal information from the European Economic Area (EEA), the United Kingdom, and Switzerland to the United States.

If your personal data originates from the European Economic Area and is transferred to Magicminds subsidiaries, affiliates, or third-party vendors engaged by Magicminds to process such personal data on our behalf who are located in countries that are not recognized by the European Commission as offering an adequate level of personal data protection, such transfers are covered by alternate appropriate safeguards, specifically [Standard Contractual Clauses adopted by the European Commission](#).

If we are involved in a reorganization, merger, acquisition, or sale of our assets, your personal data may be transferred as part of that transaction.

## 6. How We Protect Your Personal Data

Securing personal data is an important aspect of protecting privacy. We take reasonable and appropriate physical, technical, and organizational security measures in accordance with applicable laws to protect your personal data against the risk of accidental loss, compromise, or any form of unauthorized access, disclosure, or processing. The relevant security controls are communicated throughout Magicminds to support the secure development of Services and maintain a secure operating environment. Our security approach includes:

### Physical Safeguards

We lock doors and file cabinets, control access to our facilities, implement a clean desk policy, and apply secure destruction to media containing personal data.

### **Technical Safeguards**

We implement and use information security standards, protocols, and technologies, including encryption, intrusion detection, and data loss prevention, and we monitor our systems and data centers to comply with our security policies.

### **Organizational Safeguards**

We conduct regular company-wide as well as role-specific training and awareness programs on security and privacy. If you have any questions about the security of your personal data or the security of the site, or wish to report a potential security issue, please contact [connect@magicminds.io](mailto:connect@magicminds.io). When reporting a potential security issue, please describe the matter in as much detail as possible and include any information that might be helpful. If you are having problems accessing your account, please contact our Member Support Center.

## **7. Your Privacy Rights and Choices**

You can view and update your personal data through your Magicminds Account. There are a variety of data protection laws around the globe that provide privacy rights to you as our customer. Subject to applicable laws, you may have the following rights:

- **Delete:** Right to delete or erasure (“right to be forgotten”) of personal data we have collected from or about you;

- **Access:** Right to know and access the personal data we have collected about you, as well as other information about our data processing practices;
- **Rectify:** Right to rectify, correct, update, or complement inaccurate or incomplete personal data we have about you;
- **Restrict:** Right to restrict the way we process your personal data;
- **Withdraw Consent:** Right to withdraw your consent to process your personal data;
- **Object:** Right to object to our processing of your personal data based on legitimate interest;
- **Object to Automated Individual Decision-Making:** Right to object to our processing of your personal data in automated individual decision-making;
- **Equal Service:** Right not to receive discriminatory treatment for the exercise of your privacy rights, subject to certain limitations;
- **Opt-Out:** Right to Opt-Out of the sale of personal data, or the Right to Opt-Out of sharing of personal data for cross contextual advertising. U.S. residents can opt out of personalized advertising, U.S. residents can also turn on the Global Privacy Control (GPC) to opt out of the sharing of your personal information for cross contextual advertising. Learn more at the [Global Privacy Control](#) website. You may have the right to opt out of the processing of your personal data for certain types of profiling in furtherance of decisions that produce legal or similarly significant effects. However, please note that we do not engage in such profiling.
- **Portability of Personal Data:** Right to obtain a portable copy of your personal data; and
- **Lodge a Complaint:** Right to lodge a complaint with a supervisory authority if you are not satisfied with the way we have handled your personal data, or any privacy request, or other request that you have raised with us.

To exercise any of your rights, or to raise any other questions, concerns, or complaints about our privacy practices, or about our use of your personal data and its privacy, or if you are not a customer of ours and want to know what personal data we have about you, please contact us as explained below (“Contact Us”). To exercise your rights under applicable law you can submit a request [connect@magicminds.io](mailto:connect@magicminds.io). You may appeal any decision with regard to your privacy request by contacting us

[connect@magicminds.io](mailto:connect@magicminds.io) or using the details provided in the “Contact Us” section below.

Once we receive your request, we will verify your identity and your authorization to take the actions requested, authenticating your identity at a level appropriate to the requested action. We require you to re-authenticate before we will disclose or delete personal data. You may be entitled, in accordance with applicable law, to submit a request through an authorized agent. To designate an authorized agent to exercise your privacy rights and choices on your behalf, please contact Magicminds Support.

Please note that there are exceptions and limitations to each of these rights, and that while any changes will be reflected in active user databases instantly or within a reasonable period of time, we may retain personal data for backups, archiving, prevention of fraud and abuse, analytics, satisfaction of legal obligations, or where we otherwise reasonably believe that we have a legitimate reason to do so, to the extent permitted by applicable law.

We will not discriminate against you for exercising your rights and choices, although some of the functionality and features available on a Service may change or no longer be available to you where the processing of certain data is essential to the use of the Service or feature.

## **8. Your Marketing Choices**

You may receive marketing messages and materials from us or our affiliates.

You have choices on what communications you wish to receive from us. If you do not want to continue receiving any marketing materials from us,

## You can email us at

[connect@magicminds.io](mailto:connect@magicminds.io) and we will promptly remove you from ALL correspondence.

If you choose not to receive marketing communications from us, we will honor your request.

However, we will continue to communicate with you as needed to provide the Services you are entitled to, to respond to your inquiries, or to otherwise relay transactional product or service-related messages.

Please also be aware that you may still receive information about our Services through other parties using their own mailing lists. For instance, marketing materials for our Services may also be contained in messages you receive from third parties, such as your employer if they offer our Services as part of their employee benefits.

### **How to Opt-Out of Interest-Based Advertising**

We partner with third parties to display advertising on our website or to manage our advertising on other sites. You may Opt-Out of many third-party ad networks, including those operated by members of the Network Advertising Initiative (NAI) and the Digital Advertising Alliance (DAA). For more information and available choices for third-party ad networks participating in the NAI and DAA programs, please visit their respective websites: <https://optout.networkadvertising.org/> (NAI) and [www.aboutads.info/choices](http://www.aboutads.info/choices) (DAA). If you are in the European Union, you may also do so by visiting Your Online Choices (click [here](#)). Please note that if you Opt-Out, you will continue to receive generic ads not based on your interests. Opting out of these networks does not otherwise limit the collection of information described elsewhere in this Statement.

Note: If your browser is configured to reject cookies when you visit the opt-out page, or you subsequently erase your cookies, use a different computer, or change web browsers, your opt-out may no longer be effective.

## **9. Product and Services Privacy Notices**

The enrollment, billing, and support privacy statement provides our customers with a detailed look at how personal data is collected and processed when enrolling for an Magicminds service or accessing support.

### **Enrollment and Support**

The enrollment process applies to all customers who are purchasing their Magicminds products and standalone features through the Magicminds eStore or by calling into an Magicminds contact center. This information is only collected once and is used to set up your account. Additional information may be collected at the discretion of the customer to maintain the account during the subscription to the product.

Support related information is only collected if you contact us for assistance through support channels such as online chat, email, phone, text, and online forms. Additional information may be collected at the discretion of the individual contacting support to help assist in the support process.

	Categories of Data and Personal Data Collected	Purpose of Processing Your Personal Data
<b>Data You Provide:</b>	<p><u>Account Data may include:</u></p> <ul style="list-style-type: none"> <li>● Name (while active or 36 months)</li> <li>● Email (while active or 36 months)</li> <li>● Magicminds account password (while active or 36 months)</li> <li>● Phone number (if given) (while active or 36 months)</li> </ul> <p><u>Payment Data may include:</u></p> <ul style="list-style-type: none"> <li>● Billing address (while active or 36 months)</li> <li>● Payment information (depending on method</li> </ul>	<p><u>Account Data:</u> This data is processed to bill the account for products and features purchased.</p> <p><u>Payment Data:</u> This data is processed to bill the account for the products and features purchased.</p>

	<p>can include Credit/Debit Card Information or PayPal account) (while active or 36 months)</p> <ul style="list-style-type: none"> <li>• National ID (region specific, if outside the United States) (while active or 36 months)</li> <li>• VAT/Tax ID (region specific, if outside the United States) (while active or 36 months)</li> </ul>	
<p><b>Data We Collect/Access:</b></p>	<p><u>Location Data</u> may include:</p> <ul style="list-style-type: none"> <li>• IP address (while active or 36 months)</li> </ul> <p><u>Website Data</u> may include:</p> <ul style="list-style-type: none"> <li>• Cookies from website (1 year)</li> </ul> <p><u>Device Data</u> may include:</p> <ul style="list-style-type: none"> <li>• Internal identifiers (while active or 36 months)</li> <li>• Browser details (while active or 36 months)</li> </ul>	<p><u>Location Data:</u> This data is processed for the purposes of delivering the content in accordance with your device(s), determining appropriate language settings for communicating with you, troubleshooting issues, detecting fraud and generating appropriate diagnostics reports.</p> <p><u>Website Data:</u> This data is used to monitor and facilitate website activity related to cookies.</p> <p><u>Device Data:</u> This data is used and generated internally at Magicminds</p>



		<p>for the purpose of tracking account activity between internal company systems, applications, and architecture. This data is also processed for the purpose of delivering the product in accordance with your device(s) as well as for trade compliance and fraud detection and prevention.</p>
<p><b>Data We Collect/Access from Third Parties:</b></p>	<p><u>Payment Data may include:</u></p> <ul style="list-style-type: none"> <li>● <u>Payment information</u> (depending on method can include Credit/Debit Card Information or PayPal account) (while active or 6 months)</li> <li>● Billing address (while active or 6 months)</li> </ul> <p>Security Data may include:</p> <ul style="list-style-type: none"> <li>● Device fingerprint ID from third party (while active or 36 months)</li> </ul>	<p>Payment Data: This data is processed by third parties to bill the account for products and features purchased and to authenticate the payment information used.</p> <p>Security Data: This data is processed by third parties and Magicminds to validate that an authenticated payment transaction occurred, and the payment card and account are appropriate for billing.</p>

## 10. Dark Web Scan – Our dark web scan utilizes an API provided by a 3rd party (Haveibeenpwned).

### Please note:

1. Magicminds does not collect your scanned email address.
2. You may not use our dark web scanning service for any purpose that would require FCRA compliance.
3. The scan results displayed may not be 100% accurate, complete, or up to date, so do not use it as a substitute for your own due diligence, especially if you have concerns about your email and/or password safety.
4. Magicminds software innovations does not make any representation or warranty about the accuracy of the information available through the API nor about the integrity of the 3rd party involved, and we encourage you to read their terms and privacy policy accordingly (Haveibeenpwned privacy policy).

## 11. Virtual Private Network (VPN) –

Magicminds guarantees a strict no-logs policy for the VPN Service, meaning that the Magicminds VPN Service is provided by an automated process, and your activities while using it are not monitored, recorded, logged, stored or passed to any third party. We do not store connection timestamps, session information, used bandwidth, traffic logs, IP addresses or other data. However, to fight abuse and enforce proper license usage, an algorithm keeps their username and the timestamp of the last session status while the session is active. This data is deleted promptly after the session is terminated. Our VPN feature is a derivative work of a VPN service provided by Private Communications Corporation, which utilizes OpenVPN

as its underlying technology, an open source software that uses VPN techniques to create secure point-to-point or site-to site connections in routed or bridged configurations and remote access facilities. OpenVPN is licensed under both the terms of the OpenVPN license and GPLv2.

## 12. Payments

We may provide paid products and/or services within the Service. In that case, we use third-party services for payment processing (e.g. payment processors).

We will not store or collect your payment card details. That information is provided directly to our third-party payment processors whose use of your personal information is governed by their Privacy Policy. These payment processors adhere to the standards set by PCI-DSS as managed by the PCI Security Standards Council, which is a joint effort of brands like Visa, Mastercard, American Express and Discover. PCI-DSS requirements help ensure the secure handling of payment information.

The payment processors we work with are:

Google Play In-App Payments – Their Privacy Policy can be viewed at <https://www.google.com/policies/privacy/>

PayPal or Braintree – Their Privacy Policy can be viewed at <https://www.paypal.com/webapps/mpp/ua/privacy-full>

RevenueWire Inc – Their Privacy Policy can be viewed at <https://support.safecart.com/privacy?popup=true>

PayPro Global, Inc – Their Privacy Policy can be viewed at <https://docs.payproglobal.com/documents/legal/privacypolicy.pdf>

Shopify Inc. – Their Privacy Policy can be viewed at

<https://www.shopify.com/legal/privacy> Links To Other Sites

Our Service may contain links to other sites that are not operated by us. If you click on a third party link, you will be directed to that third party's site. We strongly advise you to review the Privacy Policy of every site you visit.

We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

### 13. Children's Privacy

Our Service does not address anyone under the age of 13 ("Children").

We do not knowingly collect personally identifiable information from anyone under the age of 13. If you are a parent or guardian and you are aware that your Children have provided us with Personal Data, please contact us. If we become aware that we have collected Personal Data from children without verification of parental consent, we take steps to remove that information from our servers.

#### Quick Summary:

At Magicminds, we prioritize adherence to all pertinent regulations governing privacy and cookie usage. Our commitment to compliance extends to various regulatory frameworks, including the General Data Protection Regulation (GDPR), Canadian Anti-Spam Legislation (CASL), directives established by the European Union (EU), Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act, and the Children's Online Privacy Protection Act (COPPA).

Under the GDPR, we ensure that our data processing activities are conducted lawfully, transparently, and with the explicit consent of individuals when required. We implement robust data protection measures, including encryption and access controls, to safeguard personal data in accordance with GDPR requirements.

Compliance with CASL is central to our operations, as we prioritize obtaining consent before sending commercial electronic messages, ensuring clarity and accessibility in our communications, and providing mechanisms for recipients to unsubscribe easily.

Our operations align with EU directives concerning data protection and privacy, including the handling of personal data and adherence to privacy principles outlined in EU legislation.

In accordance with the CAN-SPAM Act, we maintain strict compliance by ensuring that our marketing emails include accurate sender information, provide recipients with a clear opt-out mechanism, and honor opt-out requests promptly.

Furthermore, we are committed to upholding the COPPA regulations by implementing measures to protect the privacy of children online, including obtaining verifiable parental consent before collecting personal information from children under the age of 13.

At Magicminds, our dedication to compliance with these regulations underscores our commitment to safeguarding user privacy and promoting responsible data practices.