PRIVACY POLICY
Effective 1 October 2025

INTRODUCTION

At **MY CYBER GUARD**, we value your privacy and are committed to protecting your personal information. This Privacy Policy explains how we collect, use, store and disclose your information when you use our products and services.

Because some services are delivered by our technology partners, including **Digimune**, this document includes two parts:

1. **MY CYBER GUARD** Privacy Policy – which covers the collection and handling of personal information by **MY CYBER GUARD** in accordance with the Australian Privacy Principles (APPs) and the General Data Protection Regulation (GDPR).
2. Digimune Privacy Policy – which applies when you use services powered by Digimune. Digimune's policy sets out how your information is managed in compliance with GDPR, CCPA, POPIA and other international privacy laws.

Together, these policies explain your rights, how your information is protected, and who to contact if you have any questions or concerns.

PRIVACY POLICY
Effective 1 October 2025

MY CYBER GUARD PRIVACY POLICY

About This Policy

This Privacy Policy explains how **MY CYBER GUARD** ("we", "our", "us") collects, uses, discloses and protects your personal information when you:

- Buy our products or services
- Visit our website
- Communicate with us

We comply with the Australian Privacy Principles (APPs) in the *Privacy Act 1988 (Cth)* and, where applicable, the General Data Protection Regulation (GDPR).

Some of our services are provided by third parties — including **Digimune**, **AWN Insurance**, **Norton** and **AdGuard**. When you use those services, their privacy policies also apply.

2. The Personal Information We Collect

We may collect:

- Name, contact details (email, phone, address)
- Account login details
- Payment details (processed securely via payment providers — we don't store full card numbers)
- Device and technical information (IP address, browser type, operating system)
- Service usage data (e.g., identity scan results, security alerts)
- Support and communication history
- Other data that you supply voluntarily

We only collect sensitive information (eg. identity documents) with your consent and where necessary to deliver the service.

3. How We Collect Your Information

We collect information when you:

- Purchase or activate a product
- Set up an account
- Contact us for support
- Visit our website (cookies and analytics)
- Respond to surveys or promotions

We may also receive information about you from our partners (Digimune, AWN Insurance, Norton, AdGuard) if needed to provide your service.

4. How We Use Your Information

We use your personal information to:

- Provide, activate and support your products and services
- Process payments and send invoices
- Send security alerts, updates and important notices
- Respond to your questions or complaints
- Improve our website, services and customer experience
- Comply with legal obligations

We do **not** sell your personal information.

5. Sharing Your Information

We may share your information with:

- Our service providers and partners (eg. Digimune, AWN Insurance, Norton, AdGuard) so they can deliver their products to you
- Payment processors for secure transactions
- IT and cloud service providers who help us operate
- Government agencies or regulators when required by law

Where your data is transferred overseas (eg. to Digimune's servers), we take steps to ensure it is protected in line with the APPs and GDPR.

6. Your Privacy Rights

Under the APPs and GDPR (if applicable), you have the right to:

- Access the personal information we hold about you
- Request corrections if it's inaccurate
- Request deletion, in certain circumstances
- Restrict or object to certain processing
- Request a copy of your data in a portable format (GDPR)

You can exercise these rights by contacting us (details below).
We may need to verify your identity before actioning your request.

7. Data Security

We use appropriate technical, administrative and physical safeguards to protect your information. However, no system is 100% secure – we encourage you to use strong passwords and enable security features where available.

8. Data Retention

We keep your personal information only for as long as needed to provide the service, meet legal obligations, or resolve disputes. When it's no longer required, we securely delete or anonymise it.

9. Cookies and Tracking

Our website uses cookies and similar technologies to improve functionality, analyse usage and personalise your experience. You can adjust your browser settings to block cookies, but this may affect site functionality.

10. Contact Us

If you have questions, concerns, or complaints about your privacy or this policy, contact:

MY CYBER GUARD Privacy Officer
Email: anthony@mycyberguard.au
Telephone: 0427 866 761
Address: 9/91 Mulga Rd, Oatley NSW Australia 2223

If you are not satisfied with our response, you can contact the **Office of the Australian Information Commissioner (OAIC)** at www.oaic.gov.au.
If you are in the EU, you may also contact your local data protection authority.

11. Changes to This Policy

We may update this policy from time to time. The latest version will always be published on our website with the "Effective Date" at the top.

DIGIMUNE PRIVACY POLICY

Effective October 1, 2020. This privacy policy ("Policy") explains how information is collected, used and disclosed by DIGIMUNE and applies to information collected when you access or use our public websites, including at www.digimune.com (collectively, "Sites"), when you use our cloud-hosted social media and digital protection products and services, including those at cloud.digimune.com (collectively, "Services"), or when you attend a DIGIMUNE event or otherwise interact with us.

Who "we" are

When we say "DIGIMUNE," "we," "us" or "our" in this Policy, we are referring to we are referring to DIGIMUNE© and all our affiliated companies.

Who "you" are

When we say "you," we are referring to a customer, to a visitor to our Sites or to a participant at a DIGIMUNE event or activity, such as conference attendee. A "customer" is an entity or organization that has acquired a subscription to DIGIMUNE for Business Services ("business customer"), or an individual that has acquired a subscription to DIGIMUNE for Everyone Services.

Scope of Policy

In addition to describing our practices for collecting, using and disclosing personal information, this Policy describes the rights individuals have to control the use of their personal information. When we say "personal information" in this Policy we are referring to any information relating to an identified or identifiable natural person, which may include the individual's name, identification number, location data, email address, social media handle or other online identifier. If you use the Services through a business customer (like your employer), the terms of the customer's contract for the Services may restrict our collection or use of your personal information more than what is described in this Policy.

Changes to Policy

We may change this Policy from time to time. The most recent version of the Policy is reflected by the date at the top of this Policy. All updates and amendments are effective immediately upon notice, which we may give by any means, including by posting a revised version of this Policy or other notice on the Site. We encourage you to review this Policy often to stay informed of changes that may affect you. Your continued use of the Sites or Services signifies your ongoing acknowledgment of this Policy.

Contacting us

Please contact us with any questions or comments about this Policy, including questions around how we process your personal information. You can reach us by email at info@digimune.com. INFORMATION COLLECTED The following paragraphs 6 through 10 describe the personal information we collect.

Information you provide to us

When you register for or use the Services, modify your Services account, consult with our customer support or success teams, send us an email, participate in any interactive features of the Sites or Services, participate in a survey, participate in a contest, participate in a DIGIMUNE activity or event, apply for a job, integrate the Services with another website or service, or communicate with us in any way, you are voluntarily giving us information that we collect. The types of personal information we may collect directly from you include your first name, last name, picture, employer name, job title, industry, username, email address, phone number, physical address, social media handle and IP address. In cases where we ask you for certain information, for example when completing a form requesting a whitepaper, we will tell you what information is required. If you are a customer, we also store the information that you provide to the Services, which in the case of a business customer includes the information types listed above with respect to the business customer's personnel.

Information collected for and by our customers

If you are a customer using the Services, you may process personal information that you have collected from your own personnel (if a business customer) or other individuals. You are responsible for making sure that you have appropriate permission for us to collect and process information about those individuals. If you are an employee or contractor of one of our business customers, please contact that business customer directly to update or delete your information. If you contact us, we will provide notice to our business customer of your request. If you are an EU resident, please refer to paragraph 23 for additional detail.

Information we collect from your use of Services

We receive information about how and when you use the Services, store it in log files or other types of files associated with your account, and link it to other information we collect about you. This information includes, for example, your IP address, time, date, browser used, and actions you have taken within the application. This type of information helps us to improve our Services for both you and for all of our users.

Information we collect automatically

When you access the Services or browse our Sites, we collect information about your visit, your usage of the Services and your web browsing. That information may include your IP address, your operating system, your browser ID, your browsing activity and other information about how you interacted with the Sites or other websites. We may collect this information as a part of log files as well as through the use of cookies or other tracking technologies. Our use of cookies and other similar technologies, such as Google Analytics, is discussed more detail in our Cookie Statement.

Information from other sources

From time to time we may obtain personal information about you (or in the case of business customers, your personnel) from third party sources, such as public databases, social media platforms, third party data providers and our joint marketing partners. We take steps to ensure that such third parties are legally permitted or required to disclose such information to us. We use this information, alone or in combination with other information (including personal information) we collect, to enhance our ability to provide relevant marketing and content to you and to develop and provide you with more relevant products features, and services.

How we use information

We may use and disclose personal information described in this Policy only to:

- provide, operate, maintain and support the Services;
- send system alert messages, for example, we may inform you of temporary or permanent changes to our Services, such as planned outages, new features, version updates, releases, abuse warnings and changes to this Policy;
- communicate with customers (and business customers' personnel) about their accounts and provide customer support, training and other requested services;
- bill and collect money owed to us by customers, including sending emails, invoices, receipts, notices of delinquency and alerting customers if a different credit card number is needed (we use third parties for secure credit card transaction processing, and we send billing information to those third parties to process your orders and credit card payments);
- enforce compliance with our Acceptable Use Policy, our other agreements with a customer, and/or applicable law, which may include tools and algorithms that help us prevent violations;
- protect the rights and safety of our customers and third parties, as well as our own;
- respond to lawful requests by public authorities, including to meet national security or law enforcement requirements;
- meet legal requirements, including complying with court orders, valid discovery requests, valid subpoenas, and other appropriate legal mechanisms; prosecute and defend a court, arbitration, or similar legal proceeding;
- provide information to our professional advisors and representatives, such as attorneys and accountants, to help us comply with legal, accounting or security requirements;
- in the case of personal information of our employees, perform human resources activities such as onboarding, training and payroll;
- improve our products, technology and Services, including for example, aggregating information from your use of the Services or visits to our Sites and sharing this information with third parties to improve the Services and Sites;
- send you informational and promotional content in accordance with your marketing preferences (provided you have not unsubscribed from promotional emails);
- promote use of our Services to you and others, for example to suggest additional features of our Services that you might consider using (again, provided you have not unsubscribed from promotional emails);

- process and deliver contest or sweepstakes entries and awards;
- transfer your information in the case of a sale, merger, consolidation, liquidation, reorganization, or acquisition, provided that (1) any acquirer will be subject to our obligations under this Policy, including your rights to access and choice and (2) we will notify you of the change either by sending you an email or posting a notice on the Sites; and
- link or combine personal information with other information we collect or obtain about you (such as information we source from our third party partners), to serve you specifically, such as to deliver Services according to your preferences or restrictions, or for advertising or targeting purposes in accordance with this Policy. (Any combination of personal information with other information is treated as personal information under this Policy.)

Sharing information within our group and with our service providers

We share personal information described in this Policy with third-party vendors and service providers who are working on our behalf and require access to your information to carry out that work. These service providers are authorized to use your personal information only as necessary to provide services to DIGIMUNE and/or the Services and are bound to contractual obligations to maintain the confidentiality of your information. Many of these service providers, like us, are headquartered in the United States and operate internationally. Accordingly, you should be aware that your personal information may be processed in countries other than your country of residence, and that those countries may have different privacy and data protection laws than where you reside.

Safeguarding personal information

We take reasonable and appropriate measures to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the risks involved in the processing and the nature of the personal information. However, no means of processing of personal information is 100% secure and while we comply with our legal obligations, we cannot guarantee absolute security.

Information changes and retention

If you are a customer, you may update, correct or delete personal information about you (or your personnel, if a business customer) by logging into your online account and modifying your information or by emailing us. We will retain personal information that we process on behalf of our customers for as long as the customer's account is active and as may otherwise be appropriate to fulfil the purposes outlined in this Policy, for example to comply with legal obligations, resolve disputes, prevent abuse and enforce agreements.

Social media

(This paragraph applies to our public Sites, not the features or functionality of the Services.) Our Sites may include social media features. These features on our Sites may collect information about your IP address

and which page you are visiting on our Site, and they may set a cookie to make sure the features function properly. Additional information on cookies set by social media providers is provided in our Cookie Statement. Social media features and widgets are either hosted by a third party or hosted directly on our Site. We also maintain presences on social media platforms. Any information, communications, or materials you submit to us via a social media platform is done at your own risk without any expectation of privacy. We cannot control the actions of other users of these platforms or the actions of the platforms themselves. Your interactions with those features and platforms are governed by the privacy policies of the companies that provide them.

Community forums and blogs

We may have public blogs or other forums on our Sites from time to time. Any information you include in a comment on a public blog may be read, collected and used by anyone. To request removal of your personal information from our blogs or testimonials, contact us at the email address listed above. In some cases, we may not be able to remove your personal information, in which case we will let you know if we are unable to do so and why.

Links to third-party sites and services

Our Sites and Services include links to, or integrations with, other sites and services whose privacy practices may be different from ours. If you submit personal information to any of those sites or services, your information is governed by their privacy policies.

Individuals under the age of 18

Neither the Sites nor the Services are intended for use by individuals under 18 years of age. No one under age 18 may provide any information on or through the Sites or the Services. We do not knowingly collect personal information of individuals under 18. If a parent or guardian becomes aware that his or her child, who is under 18, has provided us with information, he or she should contact us.

Notice for California residents

California Civil Code section 1798.83 permits California residents to request certain information regarding our disclosure of personal information to third parties. To make such a request, please contacts us as provided in paragraph 5. Notices for European Union Residents

Transfers of personal information from the European Union to the United States

As noted above, we, and many of our service providers, are headquartered in the United States and operate internationally. In addition to ensuring those providers are bound by restrictions on use and disclosure of personal information, our agreements with them also reflect the legal mechanisms in place to ensure the transfer of personal information is in compliance with European data protection law, typically EU-U.S. Privacy Shield certification or standard contractual clauses (also known as model clauses).

EU Data Processing Addendum

We are committed to only processing personal information in compliance with applicable privacy and data protection law, which may include the General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR"). Our business customers processing the personal information of EU residents may request our personal data processing addendum which incorporates the standard contractual clauses, in addition to (or instead of, as applicable) relying on DIGIMUNE's EU-U.S. Privacy Shield certification (discussed in paragraph 27 below).

Controllers, processors and your GDPR rights

Under the GDPR, a "processor" is a person or entity that processes personal information on behalf of the controller, and the "controller" is the person or entity that determines how and why personal information is processed. This distinction recognizes that not all persons or entities involved in the processing of personal information have the same degree of responsibility. In that vein, controllers are typically primarily responsible for managing EU residents' exercises of their rights under GDPR ("data subject rights"). Data subject rights include, among others, an individual's right to access, correct, restrict processing of and/or delete his or her personal information.

Our role as a processor for business customers

In the case of our business customers, the Services are intended to be used and managed by the business customer. In general, we are collecting and processing personal information in connection with a business customer's use of the Services on behalf of that customer. In that case, the business customer is acting as the controller and DIGIMUNE is acting as a processor according to the business customer's instructions. If you are an EU resident and believe DIGIMUNE is processing your personal information on behalf of a business customer, and you would like to exercise your data subject rights, please start by contacting the business customer.

Our role as a processor for individual customers

If you are an individual EU customer using DIGIMUNE for Everyone Services, you are the controller of the personal information that you process through our Services. Individual customers may access, correct, restrict processing of and delete that personal information through the functionality of the Services. If you have additional questions, please contact us as provided in paragraph 5.

Our role as a controller

In other cases, such as personal information used by DIGIMUNE for management of a customer's account, invoicing and marketing, DIGIMUNE will be the controller with respect to personal information. If you are an EU resident, in situations where we are the controller of your personal information and you would like to exercise your data subject rights, please contact us as provided in paragraph 5.

Legal bases for processing

The GDPR requires that personal information be processed lawfully and outlines specific legal bases for processing. We describe in paragraphs 6 through 10 above the personal information we may collect, and in paragraph 11 how we may use it. The legal bases under the GDPR for those uses depends on the personal

information collected and the context of its collection. DIGIMUNE has determined a basis for each use, including:

- performing a contract, or taking steps linked to a contract, such as providing the Services to you if you are an individual customer;
- subject to our interests not being overridden by your interests and fundamental rights and freedoms, pursuing legitimate interests in the conduct of our business, such as processing the data of our EU employees;
- processing your personal information where you have provided consent, such as when you submit an online form with your contact information on our Site requesting that we get in touch with you with information on our Services; and
- complying with legal obligations, such as responding to lawful requests by public authorities.

Privacy Shield

As noted, ZEROFOX participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework.

We are committed to subjecting all personal information received from EU member countries and the United Kingdom, in reliance on the Privacy Shield, to Privacy Shield Principles. To learn more about the Privacy Shield, visit the U.S. Department of Commerce's Privacy Shield website, where the Department also maintains a list of all Privacy Shield participants.

DIGIMUNE is responsible for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. We comply with the Privacy Shield for all onward transfers of personal data from the EU, United Kingdom, including the onward transfer liability provisions.

With respect to personal data received or transferred pursuant to the Privacy Shield, we are subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, we may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

DIGIMUNE is aware of the judgment of the Court of Justice of the European Communities in relation to Privacy Shield. We are watching developments closely, and making standard contractual clauses available to our customers who need them and do not already have them in place. In the meantime, we will continue to look after EU personal data in accordance with GDPR and the Privacy Shield Principles.

HR Data

This Policy also reflects the principles under which DIGIMUNE manages the processing of personal information that it receives from its employees in the EU in support of its human resources operations. DIGIMUNE has committed to cooperate with EU data protection authorities with regard to unresolved EU-U.S. Privacy Shield complaints concerning human resources data transferred from the EU in the context of the employment relationship.

Inquiries and Complaints

In compliance with the EU-U.S. Privacy Shield, we are committed to resolving complaints about our collection or use of EU residents' personal information. For inquiries or complaints regarding this Policy, we request that EU residents first contact DIGIMUNE as provided in paragraph 5. You may also approach your local data protection authority (referred to under the GDPR as your supervisory authority) which can provide further information about your rights and our obligations in relation to your personal information. CCPA Data Processing Addendum PRIVACY STATEMENT-CALIFORNIA This PRIVACY NOTICE FOR CALIFORNIA RESIDENTS supplements the information contained in the Privacy Statement of DIGIMUNE ("DIGIMUNE") and its subsidiaries (collectively, "we," "us," or "our") and applies solely to visitors, users, and others who reside in the State of California ("consumers" or "you"). We adopt this notice to comply with the California Consumer Privacy Act of 2018 ("CCPA") and other California privacy laws. Any terms defined in the CCPA have the same meaning when used in this notice.

Information We Collect

We may collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device ("personal information"). In particular, we have collected the following categories of personal information from consumers within the last twelve (12) months:

Category	Examples	Collected
Identifiers	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, or other similar identifiers.	YES
Commercial information	Records of products or services purchased, obtained, or considered, or other purchasing or consuming histories	YES

Personal information does not include:

- Publicly available information from government records.
- De-identified or aggregated consumer information.
- Information excluded from the CCPA's scope, like:
- Health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data;
- Personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FRCA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994.

We obtain the categories of information listed above from the following categories of sources:

- Directly from our Customers or their agents. For example, from documents that our Customers provide to us related to the services we are providing to them.
- Indirectly from our Customers or their agents. For example, through information we collect from our Customers in the course of providing services to them.
- Directly and indirectly from activity on our website. For example, from submissions through our website portal or website usage details collected automatically.
- From third parties that interact with us in connection with the services we perform. For example, from our partners that engage DIGIMUNE to provide services to their customers.

Use of Personal Information

We may use or disclose the personal information we collect for one or more of the following business purposes:

- To fulfill or meet the reason for which the information is provided. For example, if you provide us with personal information in order for us to provide our services, we will use that information to maintain the service for you.
- To provide you with information, products or services that you request from us.
- To provide you with email alerts, event registrations and other notices concerning our products or services, or events or news, that may be of interest to you.
- To carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for billing and collections.
- To improve our website and present its contents to you.
- For testing, research, analysis and product development.
- As necessary or appropriate to protect the rights, property or safety of us, our customers or others.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
- As described to you when collecting your personal information or as otherwise set forth herein.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by us is among the assets transferred.

We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

Sharing Personal Information

We may disclose your personal information to a third party for a business purpose. When we disclose personal information for a business purpose, we enter a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except performing the contract. In the preceding twelve (12) months, we have disclosed the following categories of personal information to provide services:

- Category A: Identifiers. We disclose your personal information for a business purpose to the following categories of third parties:
    - Our affiliates.
    - Service providers.
    - Third parties to whom you or your agents authorize us to disclose your personal information in connection with products or services we provide to you.

Personal Information Sales In the preceding twelve (12) months, we have not sold, rented, or traded any personal information.

Your Rights and Choices

The CCPA provides consumers (California residents) with specific rights regarding their personal information. This section describes your CCPA rights and explains how to exercise those rights. Access to Specific Information and Data Portability Rights 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 (also called a data portability request).
- 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 providers 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 and 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 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, Data Portability, and Deletion Rights

To exercise the access, data portability, and deletion rights described above, please submit a verifiable consumer request to us by visiting www.digimune.com. 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. You may also make a verifiable consumer request on behalf of your minor child. You may only make a verifiable consumer request for access or data portability twice within a 12-month period. 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. Making a verifiable consumer request does not require you to create an account with us. We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

Response Timing and Format

We will respond to a verifiable consumer request within 45 days of its receipt. If we require more time (up to 90 days), we will inform you of the reason and extension period in writing. If you have an account with us, we will deliver our written response to that account. If you do not have an account with us, we will deliver our written response by mail or electronically, at your option. 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 useable 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.

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.

Changes to Our Privacy Notice

We reserve the right to amend this privacy notice at our discretion and at any time. When we make changes to this privacy notice, we will notify you by email or through a notice on our website homepage.

Contact Information

If you have any questions or comments about this notice, our Privacy Statement, the ways in which we collect and use your personal information, your choices and rights regarding such use, or wish to exercise your rights under California law, please do not hesitate to contact us at www.digimune.com.

Notices for Residents of the Republic of South Africa

POPIA Terms and Conditions

The Protection of Personal Information Act, 2013 ("POPIA") came into effect on 01 July 2020. For purposes of these Data Protection terms and conditions, the following words are assigned the meaning as set out below: Accordingly, entities who are processors of personal information are required to ensure that they are fully compliance with POPIA within 1 year from its effective date. DIGIMUNE is currently providing services to you / your company and are required to ensure the necessary provision relating to POPIA apply to the provision of these services. To this end, the following terms and conditions are incorporated by reference into the terms and conditions relating to the provision of these services upon acceptance by you as provided for below.

Definitions

Applicable Privacy Law means Applicable Law applicable to the Processing of Personal Data under the Business or Customer Agreement, including but not limited to POPIA.

Authority means those governments, agencies, professional, and regulatory authorities that supervise, regulate, investigate, or enforce Applicable Law.

Operator or Processor means the person that Processes data on behalf of the Responsible Party.

POPIA means the Protection of Personal Information Act No 4 of 2013.

Privacy Authority means the Authority that enforces the Applicable Privacy Law in the relevant jurisdiction.

Process/Processed/Processing means obtaining, recording, or holding information or data or carrying out any operation or set of operations on it.

Responsible Party or Controller means the person that determines the purposes and means of Processing the data.

Sub-Operator means a sub-contractor that carries out Processing activities in the provision of the Services or fulfils certain obligations of DIGIMUNE under a Business or Customer Agreement.

Data Protection – When Service Terms Identify DIGIMUNE is Responsible Party or Data Controller

- DIGIMUNE may Process User Personal Information or Personal Data for the following purposes: (a) account relationship management; (b) sending bills; (c) order fulfilment / delivery; and (d) customer service (e) provision of products and services.
- As a cloud based services provider, DIGIMUNE may Process User Personal Information or Personal Data for the following purposes: (a) delivering User communications; (b) calculating Charges for each User; (c) identifying and protecting against threats to the Services; and (d) internal use for development and improvement of Services.
- DIGIMUNE may disclose User Personal Data and Traffic Data: (a) to DIGIMUNE Group Companies or suppliers and/or (b) if required by Applicable Law, court order, Information Regulator or Privacy Authority, or any Authority.
- DIGIMUNE's privacy policy containing details of how we process personal information can be found on digimune.com.

Data Protection – When Service Terms Identify DIGIMUNE is the Operator or Data Processor

- Processing User Personal Data: DIGIMUNE may only Process User Personal Data for:
    a) provision and monitoring of the Service; or
    b) any other purpose agreed between the Parties.
- De-identified Data: DIGIMUNE may use User Personal Data to create statistical data and information about service usage that does not identify a User.
- Sub-Operator: DIGIMUNE may engage Sub-Operators. An indicative list of current Sub-Operators or Sub-Processors is available on request.
- Sub-Operator Obligations: DIGIMUNE enters into binding agreements with its Sub-Operator that imposes upon the Sub-Operator substantially the same legal obligations for processing activities as these terms.
- Data Retention: DIGIMUNE may retain the User Personal Data for as long is permitted by law or as required to deliver the Service and will delete such User Personal Data within a reasonable time after the termination of the Agreement, unless Applicable Law requires DIGIMUNE to retain it.
- Data Access: DIGIMUNE limits access to User Personal Data to those persons necessary to meet DIGIMUNE's obligations in relation to the Service and takes reasonable steps to ensure that they: (a) are under a statutory or contractual obligation of confidentiality; (b) are trained in DIGIMUNE's policies relating to handling User Personal Data.

- Security: As required by Applicable Privacy Law, DIGIMUNE shall: (a) provide appropriate technical and organisational measures for a level of security appropriate to the risks that are presented by Processing; (b) comply with the security requirements contained in the DIGIMUNE information security policies; (c) provide Customer with such information, assistance and co-operation as Customer may reasonably require to establish compliance with the security measures contained in Applicable Privacy Law; (d) notify Customer without undue delay of any unauthorised access to User Personal Data that DIGIMUNE becomes aware of and that results in loss, unauthorised disclosure, or alteration to the User Personal Data; (e) provide reasonable assistance to Customer in relation to any personal data breach notification that Customer is required to make under Applicable Privacy Law; and (f) provide Customer reasonable assistance, prior to any Processing: (A) with carrying out a privacy impact assessment of the Services; and (B) with a consultation of the relevant Privacy Authority regarding Processing activities related to the Services.
- Transfer of User Personal Data out of South Africa: DIGIMUNE may Process or transfer User Personal Data in countries outside South Africa provided that: the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that (i) effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for lawful processing of personal information relating to a data subject as detailed in POPIA or any relevant local law (ii) includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country; (b) the Customer consents to the transfer; (c) the transfer is necessary for the performance of a contract between the Customer and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request; (d) the transfer is necessary for the conclusion of performance of a contract concluded in the interest of the Customer between the responsible party and a third party; or (e) the transfer is for the benefit of the Customer, and (i) it is not reasonably practicable to obtain the consent of the Customer to that transfer, and (ii) if it were reasonably practicable to obtain such consent, the Customer would be likely to give it.
- Law Enforcement: DIGIMUNE: (a) may receive legally binding demands from a law enforcement Authority for the disclosure of, or other assistance in respect of, User Personal Data, or be required by Applicable Law to disclose User Personal Data to persons other than Customer (a "Demand"); (b) is not in breach of any obligation to Customer in complying with a Demand to the extent legally bound; and (c) will notify Customer as soon as reasonably possible of a Demand unless otherwise prohibited.
- User Enquiries: When Customer is required under Applicable Privacy Law to respond to enquiries or communications (including subject access requests) from Users, and taking into account the nature of the Processing, DIGIMUNE will: (a) pass on to Customer without undue delay any such enquiries or communications received from Users relating to their User Personal Data or its Processing; and (b) have reasonable technical and organisational measures to assist Customer in fulfilment of those obligations under Applicable Privacy Law.
- Liability: Exclusions: Neither Party is liable to the other Party (whether in contract, tort (including negligence), breach of statutory duty, indemnity, or otherwise) for: (a) any loss (whether direct or indirect) of profit, revenue, anticipated savings, or goodwill; (b) any loss to or corruption of data; (c) any fines prescribed by any Authorities; (d) any loss arising from business interruption or

reputational damage; or (e) any indirect or consequential loss, regardless of whether any of these types of loss were contemplated by either of the Parties at the time of contracting for the relevant Services. Notwithstanding the above exclusions, neither Party excludes or limits any liability: (i) that cannot be excluded or limited by Applicable Law; or (ii) for fines related to breach of Sanctions and Trade Laws.

AWN INSURANCE PRIVACY POLICY

AWN Insurance privacy policy can be found here: https://awninsurance.com.au/PrivacyPolicy.aspx