Data and Security Statement

Our Philosophy

HYP3R Inc. (HYP3R or "we") believes that consumer trust is very important and that consumers' data privacy is essential. We believe that data privacy is not one-size-fits-all and must be tailored to the needs of the consumer. We believe that the experience enhancement craved by today's consumers and data privacy goals can be achieved hand-in-hand and don't work against each other. For this reason, we believe our products can be built to foster data privacy while enhancing consumer experience. We also believe that transparency is the key to ensuring consumer trust and a continuing positive relationship with our data subjects. Therefore, we are summarizing the many aspects of our data privacy program below.

Our Commitment

HYP3R is committed to protecting the privacy of Personal Identifying Information (PII or "data") we have. The data we use and store is for lawful purposes and based on a legal basis (including pursuing our legitimate business interests, opted-in consent when appropriate, contractual performance, and other legal bases). In addition to our philosophy around the importance of data privacy, we are committed to compliance with data privacy regulations governing us, including GDPR. We understand that data privacy compliance takes effort and is a continuous process. Therefore, we commit to periodic review and improvement of our related processes and practices.

At HYP3R, we are committed to doing the right things and continually improving them. This is true for our Products, and equally true to our approach to Data Privacy and Security, and readiness for all applicable laws such as General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) and ePrivacy Directive (ePD).

Our Understanding

HYP3R makes it a point to understand exactly what data we have, and from whom. We understand why we have it, how we use it, and on what legal basis we use it. We understand our responsibilities around protection of consumer's data as both a controller and a processor.

Our Principles

HYP3R subscribes to the following principles of data protection:

> **Fairness:** We believe that data should only be used fairly by companies based upon appropriate legal bases, including "legitimate interest" and "informed consent". We believe consumers should be able to understand what their data is being used, and for what purposes. Whenever we can and as is reasonable and appropriate, especially when

we collect data directly from consumers, we inform them about our usage purposes and we request opt-in permission.

For this purpose, we make our privacy policy publicly available through our website. In it, we clearly state the rights of our data subjects, how we process data, what data we process, the legal basis of such processing and how can a data subject exercise their rights under GDPR.

Furthermore, we allow any individual or institution to submit any privacy-related questions or comments related to our privacy practices, through email or mail, as stated in the "Contact Us" section in our Privacy Policy.

Access and Deletion: We ensure that our data subjects can both request access to their data and request deletion. We publish the methods for such requests on our website, and we will act on them in a timely fashion. We promote understanding of our employees on how to handle requests in an appropriate and timely fashion.

For this purpose, we enable any data subject to exercise their rights under GDPR by submitting a request through email or mail, as stated in the "Contact Us" section in our Privacy Policy. Furthermore, we guarantee a prompt turnaround for any GDPR request received by our customers from any data subject in our service-level agreement (SLA).

Accuracy: Accuracy of data is of high importance to HYP3R and to our customers. We use internal algorithms and checks to help ensure accuracy. In addition, we have mechanisms for data subjects to request updates to their data, and we will act on those requests in a timely fashion.

Minimization: HYP3R does not acquire, store or use data above and beyond what is needed for our business purposes and our customer's business purposes.

Storage: HYP3R periodically reviews our data for continued legal bases for using and storing it, and we actively purge data that is no longer needed.

Confidentiality: At HYP3R, we believe that maintaining the confidentiality of data is tantamount to good business and strong social responsibility. We make Data Security our priority, and subscribe to a strong Data Security Policy. We retain data privacy expertise in house and, when prudent, augment with external expertise, products, methodologies, and services. We also keep abreast of new threats and counter-measures.

Accountability and Reporting: HYP3R has designated a Data Privacy Officer (DPO) to ensure we place the right emphasis on Data Privacy. The DPO will be tasked with periodically reviewing and improving this statement and our GDPR policies and programs. If a data breaches happens, the DPO will also be the key point of contact for our investigations and for timely disclosure of data breaches to appropriate Data Privacy Authorities and/or data subjects.

Our Data Sources

HYP3R provides a variety of Products that enable our customers to effectively engage and acquire their own customers. Depending on which Products a customer elects to use, personal information or data about their customers (all of which we call "Customer Data") may be collected in one or more of the following ways:

- We may obtain publicly accessible Customer Data from social media networks and public websites based on certain search queries (e.g. location), as defined by the customer. All of the social data that HYP3R acquires and accumulates is publicly available by choice of the social network user within the rules and/or terms of services set forth by those social networks.
- We may obtain Customer Data from social media networks when a customer connect a social media account to our Products, which includes profile information, profile picture, user name, user ID associated with your social media accounts, public and private messages to customers, content published and any other information you permit the social network to share with third parties.
- We may obtain Customer Data from other sources, such as third-party information providers, or through mergers and acquisitions, and combine this with information previously collected.
- We may obtain Customer Data from 1st-party data uploaded by our customers to our Product.

In the case of Customer Data, we understand ourselves to be the Processor of data and our customers the Controller of data. While we maintain our own legal bases for processing and storing data, we believe that our corporate customers are independently responsible for Data Privacy as Controller of data. Our customers should maintain their own legal basis for processing and storing data (including informed consent, legitimate interests, contractual performance, etc.), as well as have their own compliance programs to cover their own data privacy responsibilities. While we cannot be responsible for other parties' privacy practices, we periodically request and review details from our customers on their Data Privacy programs and support our customers in their balancing of interests and their documentation of the legal basis for processing.

Your Personal Data

HYP3R collects information that you provide to us (all of which we call "Personal Data") when you visit our corporate website (hyp3r.com), visit our social media channels, when you purchase our Products, set up an account in our Products, connect a social account to our Products, use our Products, or communicate with us. We use this information to operate, maintain, improve and provide the features and functionality of the Products, as well as to personalize marketing communications and website content, such as digital advertising, email messages about products and service-related emails or messages (e.g. account verification notices).

Personal Data typically contains information on users that might include names, email addresses, phone numbers, URLs, social handles, online identifiers, organizational affiliations, job titles, key dates, location, and other information from social media networks when a customer connect a social media account to our Products, which includes profile information, profile picture, user name, user ID associated with your social media accounts, public and private messages to customers, content published and any other information you permit the social network to share with third parties.

In the case of Personal Data, we understand ourselves to be the Controller of data, based on the following legal bases: when you have given consent (ii) when data processing is necessary to perform a contract with a customer, and our legitimate business interests, such as improving and personalizing our Products, marketing new features or products that may be of interest to our customers.

Data Retention

HYP3R retains information for only as long as necessary for our legitimate business purposes. data obtained directly from the consumer may be retained for a commercially reasonable time after deactivation or termination for recordkeeping, audit, fraud detection / prevention, safety or other purposes. data obtained from other sources, such as vendors, are tracked separately and may be retained for as long as necessary for our legitimate business purposes. Data from our Corporate Customers shall be retained, stored and deleted according to our agreements with our corporate customers.

Data Storage and Transfer

HYP3R takes security of all our information, including PII, very seriously. We use commercially reasonable physical, technical and organizational measures designed to preserve the integrity and security of all information we collect. However, we recognize that no security system is impenetrable. So, we maintain processes to investigate breaches, prevent future breaches and notify affected persons and/or appropriate data privacy authorities in a timely fashion.

HYP3R is headquartered in San Francisco, California. Our Products are hosted and operated in the United States through Amazon Web Services (AWS) and its service providers. Our data reside in the US West Region. When at rest, data that we control remain in servers at AWS. AWS ensures that they will not move our data from the US West Region without our consent. Before we make any changes to the location of our data at rest, we will evaluate data privacy risks and mitigate those risks as appropriate. In addition, we periodically request Service Organization Control reports from AWS and review them to ensure AWS's information security policies and procedures are more than adequate for our purposes.

We may transfer data within the U.S., to any HYP3R affiliate worldwide or to third parties acting on our behalf for the purposes of processing or storage, as appropriate per our legal bases. We take measures to ensure information security for our data transfers.

Data Sharing

As HYP3R is the processor of data for our corporate customers, we are careful about how we handle PII. HYP3R is a multi-tenant Software-as-a-Service (SaaS) solution which is hosted in a private virtual cloud (PVC) that isolates data supplied by different corporate customers. This means that customer data shares the physical environment with other HYP3R customers but is logically isolated to ensure security. This hosting environment creates a high availability redundant enterprise grade installation with strong security. We have procedures in place to ensure that we do not share data between customers, and we only store their data as long as needed to deliver on our contract with them.

End-User Security and Access Management

The HYP3R System enables Role Based Access Control, which allows the customer to define authentication policies for increased security and specific access control. Sensitive data held by HYP3R is logically segregated by tenant and account-based access rules. HYP3R users accounts require unique usernames and passwords which must be provided for each session.
The HYP3R system issues a session cookie only to record encrypted authentication information for the duration of a specific session. Sessions are capped at a maximum of 2 hours with no activity. User application passwords have minimum complexity requirements. Passwords are individually salted and hashed. 2FA and Single Sign On (SSO) are supported options.

Threat detection

HYP3R continuously monitors the platform and supporting infrastructure for threats, system level vulnerabilities, configuration vulnerabilities, malware, viruses, and other potential risks.

Securing your data

The HYP3R platform and infrastructure is hosted by a secure and reliable cloud service provider with SOC 2 and ISO 27001/2 certifications. The platform and infrastructure are continuously monitored to provide high availability and security.

Operational Security

Employees

All employees receive regular information security and privacy training. Employees with access to production data receive additional training specific to their roles.

Security Assessments

We regularly conduct both internal vulnerability assessments (including architecture reviews by security researchers) and external assessments (including vulnerability assessments and penetration tests by certified security services providers).

IT Security Policies

Internal policies describe how HYP3R handles security and privacy incidents, detection, response, forensics, and notification to all stakeholders. We build security into our software development processes at all stages. From initial design considerations with a Vulnerability and Misuse Assessment (VAMA) to post-release, security is built into all aspects of our architecture and software development.

Incident response

HYP3R maintains a detailed incident response program with well-documented incident response, escalation, and notification plans with trained personnel available on a 24/7 basis to monitor and respond to any events or security incidents.
HYP3R response and escalation plans are tested on an annual basis and detailed customer post-mortems are made available within 2 business days of a major incident.

Secure Development - Coding, Infrastructure and Operations

Design

Security best practices (OWASP Top 10 reviews and CERT Secure Coding Standards) and security training help ensure that HYP3R technical employees make the best security decisions possible. Vulnerability and Misuse Assessments (VAMAs) on high-risk features identify potential security issues early in the development lifecycle.

Code vulnerability testing

To prevent code-level vulnerabilities, HYP3R utilizes secure coding approaches and static code analysis tools to avoid and identify security flaws.
Penetration Testing
Internal penetration tests are conducted regularly by an internal security team and external tests are provided by a qualified independent security organization. Any high risk vulnerabilities found are documented and immediately remediated. Post-mortem analysis is performed to identify the root cause and to update processes.

Release management

Prior to release, HYP3R validates functionality to ensure that it meets internal security requirements. Post-release, security service providers are used to to analyze and monitor the application and infrastructure for potential security issues.

Change Control

All new functionality requires extensive testing and peer-code review. Tugboat Logic provides explicit notice (via a what's new section) of changes impacting customer experience or usage and are committed to working with our customers to minimize any negative impact from changes.

Platform Security Architecture

Data encryption in HYP3R

Sensitive data is protected and encrypted in HYP3R, both in transit and at rest, to ensure the consumer information is protected. The HYP3R encryption keys are stored and managed in a logically separate area, away from the data. Role-based access control ensures that only the application process business logic can access the encryption keys encrypt & decrypt operations. The HYP3R data store cannot be accessed directly via the internet.

Platform Security Operations

Key Management

Decryption keys are segmented: stored within a secured environment separate from data and all access requires multiple layers of authentication.

Strong Authentication and session management

We require users to authenticate with every access of the HYP3R application. Passwords are never stored unencrypted in the HYP3R database and all communication between users and HYP3R is conducted using TLS (Transport Layer Security).

Activity monitoring and testing

We monitor employee, customer, and vendor behavior to guard against suspicious or unauthorized activity. We work with certified 3rd parties to conduct vulnerability scans at least quarterly and external penetration tests at least once a year.

Vulnerability Management and Monitoring

Our first priority is to protect your data and our systems. Where reasonable, we work to identify and remediate issues and minimize customer impact and interaction.
Any new incidents or vulnerabilities identified are immediately escalated to our security team, reviewed for applicability, risk ranked, and assigned to be resolved by the appropriate HYP3R personnel.

The latest security patches and secure configurations are applied to all operating systems, containers, applications, infrastructure, tools, etc. to reduce exposure to vulnerabilities. Our environments are scanned regularly using industry standard security tools. These tools are configured to perform application and network vulnerability scans, which test for vulnerabilities, patch level and misconfigurations.

Availability

Capacity Monitoring

HYP3R monitors for potential downtime thresholds. We continuously monitor our availability and uptime by reviewing and evaluating our current processing capacity and usage to meet our availability commitments and system requirements.

Backups

We maintain a robust and well-documented recovery plan. We run regular backups of any changes and conduct a full backup on a bi-weekly basis. Backups are replicated across multiple availability zones. Disaster recovery drills are conducted on at least an annual basis.

Risk Management

We conduct annual internal risk assessments to identify, prioritize and mitigate known risks. High impact risks are remediated upon discovery. The assessment process is documented and audited annually by an independent party as part of our third party audit processes. Findings and remediation are reviewed and approved by our internal security team and leadership.

See our Privacy Policy for further details.