Privacy Compliance Policy

Policy Owner: Ariel Deschapell

Effective Date: 7 September 2023

Application

This policy applies to all employees, contractors, and vendors while doing business with Hydra Host, Inc. and others who have access to personally identifiable information (PII) also referred to as consumer information ("personal data") in connection with Hydra Host, Inc.'s operating activities.

Policy

Hydra Host, Inc. is committed to protecting the security, confidentiality, and privacy of its information resources including California consumers' personal data in accordance with the requirements set forth in ISO 27701 and all relevant privacy frameworks, laws and regulations. Personal data shall only be processed when there is a legal basis to do so, data shall be managed to ensure that security, confidentiality, and privacy are maintained, and data will be used only for authorized purposes. All employees and contractors of Hydra Host, Inc. share the responsibility for safeguarding personal data to which they have access.

When performing commercial activities in support of Hydra Host, Inc. products and services that impacts consumer personal data (PII), Hydra Host, Inc. may engage in certain activities which may require it to receive, store, process, transmit, create, or access and use data which may trigger compliance requirements with the provisions applicable to privacy regulations. This policy and the data privacy and information security policies adopted hereunder are intended to support the mission of Hydra Host, Inc. and to facilitate data processing activities that are important to Hydra Host, Inc. by:

- Ensuring compliance with requirements imposed by relevant data privacy regulations
- Providing for the establishment of data privacy policies that set forth, among other things, the required technical, physical, and administrative safeguards to maintain the security, confidentiality, and privacy of personal data
- Setting forth the roles and responsibilities necessary for Hydra Host, Inc. to meet its obligations with respect to activities related to the processing of personal data

Hydra Host, Inc. shall post a public-facing Privacy Notice (i.e. Privacy Policy). The notice shall be available at or before the point of collection, shall be easy to read and shall:

- use plain language and avoid jargon
- use a format that is readable including on small screens
- be available in the languages in which the company conducts the business
- be reasonably accessible to consumers with disabilities in accordance with Web Content Accessibility guidelines version 2.1.
- contain a meaningful description of categories of personal information collected
- the business purpose for collection
- include a link titled "Do-Not-Sell-My-Personal-Information" if the business sells personal information of California residents
- include a link to the privacy policy (if different)

If the company sells the personal information of California residents, a notice of right to opt-out of the sale of personal information shall:

- be posted on the web page to which the consumer is directed after collecting the "Do-Not-Sell-My-Personal-Information" link
- be provided within a mobile application such as through the settings menu
- be provided through an offline method if the company does not have a website
- be provided orally if the information is collected over the phone

Notice of right to opt-out shall include:

- description of consumer's right to opt-out the sale of their personal information
- an interactive form by which consumers can opt-out
- offline or alternative methods to opt-out

If the company markets goods or services in the EU or UK, the Privacy Notice shall include:

- Name and contact information for all GDPR Article 27 Local Representatives
- Name and contact information for the Data Protection Officer (DPO), if applicable

Roles and Responsibilities

Policy Adoption

Hydra Host, Inc. shall, in cooperation with relevant stakeholders, develop and adopt necessary and appropriate data privacy policies, which will include, among other things, the technical, physical, and administrative safeguards required to ensure the confidentiality, integrity, and privacy of personal data, and protect personal data against reasonably anticipated threats or hazards and unauthorized uses or disclosures. All relevant Hydra Host, Inc. stakeholders shall cooperate with Hydra Host, Inc. in the development and implementation of the policies.

The Hydra Host, Inc. Information Security and Data Privacy Policies are a component of the policies and implement controls which support compliance with all relevant data privacy regulations.

Responsible Person

Ariel Deschapell, Head of Product, [ariel@hydrahost.com], 786-763-1069 has been assigned responsibility for overall oversight of Hydra Host, Inc.'s Data Privacy Compliance Program, also known as the Privacy Information Management System (PIMS).

Data Protection Officer (DPO)

Ariel Deschapell, Head of Product, [ariel@hydrahost.com], 786-763-1069 has been assigned the role of Data Protection Officer (DPO) for the Hydra Host, Inc.'s Data Privacy Compliance Program, also known as the Privacy Information Management System (PIMS).

In accordance with Article 39 of the GDPR, the DPO shall perform the following tasks:

1. Inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
2. Monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
3. Provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
4. Cooperate with the supervisory authority;

5. Act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

Implementation

Data Protection and Regulatory Compliance

All personal data requires a legal basis for processing, and will be accessible on a strict need-to-know basis. Personal data is to be kept confidential and must be protected and safeguarded from unauthorized access, modification and disclosure.

- Storage and Transmission: Personal data must be encrypted, with strong cryptography, whenever stored on or transmitted by Hydra Host, Inc. systems
- Disposal: Paper records must be securely shredded prior to disposal. Electronic media must be securely wiped, sanitized or physically destroyed prior to disposal or reuse
- Awareness Training: Relevant personnel will receive appropriate training on their information security and data privacy responsibilities with regard to relevant regulations and the handling of personal data as well as the Consumer (Data Subject) Access Request (DSAR) procedure. Relevant persons shall be trained to properly direct consumers in the exercise of their privacy rights.
- Hydra Host, Inc. will not transmit personally identifiable information (PII) to any third-party or vendor until an appropriate Data Protection Addendum (DPA), or sufficient contract language, has been fully executed by Hydra Host, Inc. and the third-party.
- Hydra Host, Inc. shall not sell the personal information or minors or of persons who have previously opted out of sales, without explicit permission and shall not ask for permission for at least twelve (12) months after a consumer has opted-out
- Hydra Host, Inc. shall ensure that no service providers continue to sell PII after a consumer has opted out
- Hydra Host, Inc. shall not use PII provided for the purposes of opting-out of a sale for any other purpose
- Hydra Host, Inc. shall not deny goods or services or otherwise discriminate against (i.e. charge different prices, or offer different levels of service) persons for exercising their privacy rights
- Hydra Host, Inc. shall provide at least two methods for consumers to submit data access requests including an email address or webform
- Responses to access requests shall cover at least the preceding twelve (12) months
- Hydra Host, Inc. shall locate data in all relevant systems in response to access requests
- A public-facing Privacy Policy shall include a description of consumers' rights and shall be updated at least every twelve (12) months
- PII collected for the purposes of responding to a SAR shall not be used for any other purpose
- Hydra Host, Inc. shall not sell any PII without posting a "Do Not Sell My Personal Information" link on the company homepage and Privacy Policy for consumers to opt-out of any sale.
- Hydra Host, Inc. shall provide at least two methods for opting out of sales of PII which are consistent with the manner in which the company typically interacts with customers
- Hydra Host, Inc. will allow consumers to opt-out of sales via web browser plugin or other privacy setting
- When Hydra Host, Inc. offers an opt-out of a specific use, it shall also offer a global opt-out
- Hydra Host, Inc. shall ensure that opt-out requests are honored as soon as feasibly possible and within fifteen (15) days in all cases
- Hydra Host, Inc. shall establish a process for consumers to submit requests via an authorized agent
- Hydra Host, Inc. shall ensure that a written contract is established with all service providers that prohibits the service provider from retaining, using, or disclosing the personal information for any purpose other than the specific purpose specified in the contract

- Service providers shall only use, retain or disclose PII for the following purposes:

1. to provide service on behalf of the controller

2. to employ another service provider

3. to improve service quality

4. to detect security incidents and or fraud

5. to comply with the law or law enforcement

- Hydra Host, Inc. shall inform consumers of the company's privacy practices at or before any PII collection. The Privacy Notice shall be made available via a link titled "privacy" on the company's homepage.
- Hydra Host, Inc. shall deny access requests where the requestor's identity cannot be reasonable verified
- Hydra Host, Inc. in any case where the company has a legal basis for denying a consumer request, it shall provide an explanation of its decision to the consumer including a reference to the relevant laws or regulations
- Hydra Host, Inc. shall provide a individual response to each requestor and not refer them to a policy or provide a generic response
- Hydra Host, Inc. may de-identify personal information in response to a request for deletion
- Hydra Host, Inc. shall not be required to delete personal information from backups unless the backups are restored, accessed or disclosed
- Hydra Host, Inc. may retain records of completed deletion requests for compliance purposes
- Hydra Host, Inc. shall deny fraudulent requests with an explanation as to why they believe the request is fraudulent
- Opt-out processes shall require minimal steps and no multi-step opt-out process shall not have more steps than the opt-in process
- Opt-in processes shall have two steps: an opt-in request followed by a verification of the request
- When a consumers who have opted-out attempt to use a service that requires opt-in, the company shall inform the consumer how to opt-in
- When the company collects personal information that a consumer would not reasonably expect from a mobile device then it shall provide a just-in-time notice containing a summary of categories collected and a link to the full notice.

Breach Notification

Notification of any reportable unauthorized use or disclosure of personal data will be sent to affected parties, Data Controllers, and relevant regulators in accordance with all applicable notification requirements and the Incident Response Policy.

Identity Verification

Hydra Host, Inc. shall establish and document a reasonable method for verifying the identity of a requestor which shall not require a fee from the consumer.

The company shall implement reasonable security measures to detect and prevent fraudulent identity-verification activity.

Where a consumer maintains a password protected account with a company, the company may verify their identity using existing authentication practices.

Before providing categories of personal information, the company shall verify the identity of requesters to a "reasonable degree of certainty." Before providing specific pieces of personal information or honoring a deletion request, a company shall verify the identity of requesters to a

"high degree of certainty," depending on the sensitivity of the personal information or the risk of harm from an unauthorized deletion request.

A company shall consider the following criteria when determining a verification method:

- whenever feasible identifying information provided by a requestor should be matched with identifying information already maintained by the company, or use a third-party identification service
- avoid collecting unnecessary personal information
- consider the sensitivity of information requested, the risk of harm to the consumer, the likelihood of fraud, the manner in which the business interacts with the consumer and the availability of verification technology.

A company shall avoid personal information unless needed to verify the identity of the requestor. A company shall delete personal information collected for the purpose of verification as soon as possible after processing the request.

If there is no reasonable method by which a company can verify the identity of the consumer to the degree of certainty required by this section, the business shall state so in response to any request and explain why it has no reasonable method by which it can verify the identity of the requestor. If the company has no reasonable method by which it can verify any consumer, the company shall explain why it has no reasonable verification method in its privacy policy. The company shall evaluate and document whether a reasonable method can be established at least once every 12 months.

Agent Verification

When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. The business may also require the consumer to do either of the following:

- Verify their own identity directly with the company.
- Directly confirm with the company that they provided the authorized agent permission to submit the request

Request Verification for Minors

Process for Opting-In to Sale of Personal Information

When the company has actual knowledge that it sells the personal information of a consumer under the age of 13, it shall establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. This affirmative authorization is in addition to any verifiable parental consent required under COPPA, if applicable. (2) Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include, but are not limited to:

- Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the company by postal mail, facsimile, or electronic scan
- Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;
- Having a parent or guardian call a toll-free telephone number staffed by trained personnel;
- Having a parent or guardian connect to trained personnel via video- conference;
- Having a parent or guardian communicate in person with trained personnel; and
- Verifying a parent or guardian's identity by checking a form of government- issued identification against databases of such information, as long as the parent or guardian's identification is deleted by the business from its records promptly after such verification is

complete.

The process for validating requests on behalf of minors and verifying the identity of parents or guardians shall be described in the public-facing Privacy Policy.

Consumer (Data Subject) Access Requests (DSAR/SAR)

Subject to the exceptions noted below in this policy, Hydra Host, Inc. will comply with any SAR concerning the following rights of the consumer:

- Access (a copy of the personal data undergoing processing)
- Rectification of personal data (correction of data stored or processed)
- Erasure ('right to be forgotten')
- Notification regarding rectification or erasure
- Objection to processing (withdrawal of consent to processing)
- Right to opt-out of any sale of PII (i.e. Do Not Sell requests)

SAR/DSAR Response Requirements:

Responses to access requests shall include the following data points as appropriate.

- Categories of PII collected
- Categories of PII sold and disclosed to third parties

SAR when Hydra Host, Inc. is the data controller:

- A SAR must be made using the link on Hydra Host, Inc.'s privacy page hydrahost.com/privacy. If the consumer has a password-protected account on Hydra Host, Inc. systems, the company may provide an "interface" or self-service mechanism that the consumer is instructed to use to initiate the SAR process.
- A SAR can also be made using the email address privacy@hydrahost.com.
- A SAR may be made using the webform available on the company website hydrahost.com
- Where required, the consumer must provide reasonable evidence of their identity in the form of valid identification, for example, email verification.
- When submitting the SAR via the interface, the consumer must identify the SAR type that is being requested, e.g., erasure.
- If a SAR is submitted by an agent, the submission must include the identification of the consumer as well as a signed authorization from the consumer. Hydra Host, Inc. must make reasonable efforts to verify the identity of the consumer and legitimacy of all requests submitted by authorized agents.
- If a SAR is received which does not meet Hydra Host, Inc. criteria, the Hydra Host, Inc. shall inform the consumer or agent how to correct the SAR in order to receive a response from Hydra Host, Inc.

SAR when Hydra Host, Inc. is the data processor:

- The SAR must be submitted via the user interface in the Hydra Host, Inc. Services.
- Hydra Host, Inc. shall direct the consumer to the relevant Controller in accordance with all contractual commitments.

SAR requirements:

- The date by which the SAR is submitted, identification is verified, and the specification of the SAR request type must be recorded; Hydra Host, Inc. will acknowledge any manual requests within 10 business days. The acknowledgement will describe the verification process and when the consumer should expect a response.

- Hydra Host, Inc. has thirty (30) days from the initial request date to complete the request. If the company cannot respond within thirty days, it shall provide notice to the consumer. In California, the company may extend the response timeline up to an additional forty-five (45) days.
- The SAR application will be documented and can be audited using Hydra Host, Inc.'s internal processes.
- Hydra Host, Inc. shall ensure that deletion and correction requests are sent to subprocessors as needed.

Hydra Host, Inc. as the data controller

- Collect the data specified by the consumer
- Verify the identity of the consumer by confirming contact through two different communication mediums.
- Search all databases and all relevant filing systems (manual files) in Hydra Host, Inc., including all back up and archived files, whether computerized or manual, and including all email folders and archives. Hydra Host, Inc. maintains a record that identifies where personal data in Hydra Host, Inc. is stored.
- Hydra Host, Inc. will maintain a record of requests for data and of its receipt accessible by Hydra Host, Inc.'s, General Counsel, and/or any other designated Hydra Host, Inc. representatives. Hydra Host, Inc. will also keep a record of processing to include dates.
- Provide consumers an online mechanism for making requests and all such requests will be logged.
- Hydra Host, Inc. will acknowledge the SAR within ten (10) days of the initial request and respond to any SAR within 30 days of the initial request.
- SARs from employees or previous employees will be coordinated with HR and the employees' current or previous departmental leadership.

SAR Exemptions

- Hydra Host, Inc. may withhold information requested under SAR in accordance with any exemption under applicable law. Any such exemption must be reviewed and approved by the Data Privacy Officer or General Counsel.

Compelled Disclosure

Hydra Host, Inc. governs the compelled disclosure of customer Personally Identifiable Information pursuant to valid third-party legal demands for such information, such as court orders, search warrants, subpoenas, government investigations, and similar demands, and is incorporated by reference into Hydra Host, Inc.'s Privacy Policy.

In no cases shall personal information be voluntarily provided to law enforcement or any regulatory agency without the express written consent of the Data Controller or Data Subject.

Upon receipt of legal demands for information,Hydra Host, Inc. will immediately notify the General Counsel, CEO, and Data Privacy Officer (DPO).

Hydra Host, Inc. shall immediately notify any relevant Data Controllers unless prohibited by law.

The Chief Legal Officer in connection with the CEO and Data Privacy Officer will determine the Hydra Host response to law enforcement and affected third parties, including data subjects.

If determined to be appropriate by legal, and executive management, the Hydra Host, Inc. will investigate the demands, and if it is determined at Hydra Host, Inc.'s sole discretion that they are valid, we will search for and disclose the information that is specified and that we are reasonably able to locate and provide. Hydra Host, Inc. shall not process overly broad or vague demands, and will not disclose information that is not specifically demanded, except in response to follow-up demands.

Hydra Host, Inc. may contact customers if we are compelled to disclose their information pursuant to valid legal demands for such information, but we are not required to do so, and in some instances, we may be legally prohibited from doing so.

All external communications with customers, regulators and law enforcement shall be approved by Hydra Host, Inc.'s General Counsel, and Data Privacy Officer as appropriate.

Enforcement

The Head of People, Chief Information Security Officer and Legal Counsel are responsible for the enforcement of this policy.

Employees who may have questions should contact their HR representative or supervisor as appropriate.

Disciplinary Action

Failure to comply with any provision of this policy may result in disciplinary action, including, but not limited to, termination.

Records Retention and Metrics

A record of all consumer requests shall be maintained for at least twenty-four (24) months and shall include the following elements:

- request date
- nature of request
- request method
- date of company response
- nature of company response
- basis for any denial

Records of consumer requests shall not be shared with any third party except as necessary to comply with a legal obligation.

A company that buys, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall maintain and publish the following metrics:

1. the number of requests "to know" received and processed

2. the number of requests "to delete" received and processed

3. the number of requests "to opt-out" received and processed

4. the median number of days to respond

The company shall include a link to these metrics in its privacy policy and shall update this information by July 1st annually, and shall implement a documented privacy training policy.

Disclosures Log

A record of all non-standard disclosures of PII to third parties, including compelled disclosures to law enforcement and/or regulators shall be logged in Appendix A

Special Cases

Household Requests

Where a household doesn't have a password protect account with a company, the company shall not disclose or delete household personal information unless the following conditions are satisfied:

- all consumers of the household submit a joint request
- the company individually verifies all members of the household
- the company verifies that each requestor is member of the household

If a member of a household is under 13, a company must obtain a verifiable parental consent before complying with a request.

Reporting

All suspected violations or potential violations of this policy, no matter how seemingly insignificant, must promptly be reported either to <recipient(s) or policy violation reports, e.g., Legal Counsel, or Hydra Host, Inc.'s Data Privacy Officer immediately, or via the incident reporting process at abuse@hydrahost.com.

As long as a report is made honestly and in good faith, Hydra Host, Inc. will take no adverse action against any person based on the making of such a report. Failure to report known or suspected wrongdoing of which you have knowledge may subject you to disciplinary action up to and including termination of employment.

Applicable Laws, Regulations and Standards

- ISO 27701 Privacy Information Management System (PIMS)
- SOC 2 Privacy Criterion
- General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Colorado Privacy Act
- Connecticut Data Privacy Act
- Virginia Consumer Data Protection Act
- Utah Consumer Privacy Act

Version History

Version	Date	Description	Author	Approved by
[1.0]	7 Sep2023	Initial policy	Larkin Rogers	Ariel Deschapell

Appendix A - Third-Party PII Disclosure Log

Third-Party	PII Disclosed	Reason	Date	Time	Compelled?	Notes