Hubly Data Security and Privacy

Overview

At Hubly, customer trust is our top priority. Hubly continually monitors the evolving privacy regulatory and legislative landscape to identify changes and determine what tools our customers might need to meet their compliance needs. Maintaining customer trust is an ongoing commitment. We strive to inform you of the privacy and data security policies, practices, and technologies we’ve put in place. Our commitments include the following:

- Access: As a customer, you maintain full control of the content that you upload to the Hubly services under your Hubly account, and responsibility for configuring access to Hubly services and resources. We provide an advanced set of access, encryption, and logging features to help you do this effectively (e.g., Hubly Identity and Access Management, Hubly Organisations and Hubly CloudTrail). We provide APIs for you to configure access control permissions for any of the services you develop or deploy in an Hubly environment. We do not access or use your content for any purpose without your agreement. We never use your content or derive information from it for marketing or advertising purposes.
- Storage: You choose the Hubly Region(s) in which your content is stored. You can replicate and back up your content in more than one Hubly Region. We will not move or replicate your content outside of your chosen Hubly Region(s) except as agreed with you.
- Security: You choose how your content is secured. We offer industry-leading encryption features to protect your content in transit and at rest, and we provide you with the option to manage your own encryption keys. These data protection features include:
    - Data encryption capabilities available in over 100 Hubly services.
    - Flexible key management options using Hubly Key Management Service (KMS), allowing customers to choose whether to have Hubly manage their encryption keys or enabling customers to keep complete control over their keys.
- Disclosure of customer content: We will not disclose customer content (see *How does Hubly classify customer information?* below) unless we're required to do so to comply with the law or a binding order of a government body. If a governmental body sends Hubly a demand for your customer content, we will attempt to redirect the governmental body to request that data directly from you. If compelled to disclose your customer content to a government body, we will give you reasonable notice of the demand to allow the customer to seek a protective order or another appropriate remedy unless Hubly is legally prohibited from doing so.

- Security Assurance: We have developed a security assurance program that uses best practices for global privacy and data protection to help you operate securely within Hubly, and to make the best use of our security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments.

What is customer content?

We define customer content as software (including machine images), data, text, audio, video, or images that a customer or any end user transfers to us for processing, storage, or hosting by Hubly services in connection with a customer's account, and any computational results that a customer or their end-user derives from the foregoing through their use of Hubly services. For example, customer content includes content that a customer or their end-user stores in Hubly Simple Storage Service (S3). Customer content does not include account information, which we describe below. Customer content also does not include information included in resource identifiers, metadata tags, usage policies, permissions, and similar items related to the management of Hubly resources. The terms of the Hubly Customer Agreement and the Hubly Service Terms apply to your customer content.

What is account information?

We define account information as information about a customer that a customer provides to us in connection with the creation or administration of a customer account. For example, account information includes names, usernames, phone numbers, email addresses, and billing information associated with a customer account. The information practices described in the Hubly Privacy Notice apply to account information.

Who owns customer content?

As a customer, you own your customer content and select which Hubly services can process, store, and host your content. We do not access or use your customer content for any purpose without your agreement. We do not use customer content or derive information from it for marketing or advertising.

Who controls customer content?

As a customer, you control your content:

You determine where your customer content will be stored, including the type of storage and geographic region of that storage.

You choose the secured state of your customer content. We offer customers industry-leading encryption features to protect your content in transit and at rest, and we provide you with the option to manage your own encryption keys.

You manage access to your customer content, and access to Hubly services and resources through users, groups, permissions, and credentials that you control.

How do you use my customer account information?

The Hubly Privacy Notice describes how we collect and use account information. We know that you care how account information is used, and we appreciate your trust that we will do so carefully and sensibly.

What happens when Hubly receives a legal request for customer content?

We are vigilant about our customers' privacy. We will not disclose customer content unless we're required to do so to comply with the law or a binding order of a governmental body. If a governmental body sends Hubly a demand for customer content, we will attempt to redirect the governmental body to request that data directly from the customer. Governmental and regulatory bodies need to follow the applicable legal process to obtain valid and binding orders. We review all orders and object to overbroad or otherwise inappropriate ones. If compelled to disclose customer content to a government body, we will give customers reasonable notice of the demand to allow the customer to seek a protective order or another appropriate remedy unless Hubly is legally prohibited from doing so. It is also important to point out that our customers can encrypt their customer content, and we provide customers with the option to manage their own encryption keys.

We know that transparency matters to our customers, so we regularly publish a report about the types and volume of information requests we receive on the Hubly Information Requests webpage.

Where is customer content stored?

The Hubly Global Infrastructure gives you the flexibility of choosing how and where you want to run your workloads, and when you do you are using the same network, control plane, APIs, and Hubly services. If you would like to run your applications globally you can choose from any of the Hubly Regions and Availability Zones. As a customer, you choose the Hubly Region(s) in which your customer content is stored, allowing you to deploy Hubly services in the location(s) of your choice, in accordance with your specific geographic requirements. For example, if an Hubly customer in Australia wants to store their data only in Australia, they can choose to deploy their Hubly services exclusively in the Asia Pacific (Sydney) Hubly Region. If you want to discover other flexible storage options see the Hubly Regions webpage.

You can replicate and back up your customer content in more than one Hubly Region. We will not move or replicate your content outside of your chosen Hubly Region(s) without your agreement, except in each case as necessary to comply with the law or a binding order of a governmental body. However, it is important to note that all Hubly services may not be available in all Hubly Regions. For more information about which services are available in which Hubly Regions, see the Hubly Regional Services webpage.

What is my role in securing customer content?

When evaluating the security of a cloud solution, it is important for you to understand and distinguish between the security of the cloud, and your security in the cloud. Security of the cloud encompasses the security measures that Hubly implements and operates. We are responsible for the security of the cloud. Security in the cloud encompasses the security measures that you implement and operate, related to the Hubly services you use. You are responsible for your security in the cloud. For more information, see the Hubly Shared Responsibility webpage.

What steps does Hubly take to protect my privacy?

At Hubly, our highest priority is securing our customers’ data, and we implement rigorous contractual, technical and organisational measures to protect its confidentiality, integrity, and availability regardless of which Hubly Region a customer has selected.

Hubly complies with ISO 27018, a code of practice that focuses on the protection of personal data in the cloud. It extends ISO information security standard 27001 to cover the regulatory requirements for the protection of personally identifiable information (PII) or personal data for the public cloud computing environment and specifies implementation guidance based on ISO 27002 controls that is applicable to PII processed by public cloud service providers. For more information, or to view the Hubly ISO 27018 Certification, see the Hubly ISO 27018 Compliance webpage.

Additionally, Hubly publishes a SOC 2 Type II Privacy report, based on the SOC 2 Privacy Trust Criteria establishes criteria for evaluating controls related to how personal data is collected, used, retained, disclosed, and disposed to meet the entity’s objectives. The Hubly SOC 2 Privacy Type II report provides third-party attestation of our systems and the suitability of the design of our privacy controls, as stated in our Privacy Notice. The scope of the privacy report includes information about how we handle the content that you upload to Hubly and how it is protected in all of the services and locations that are in scope for the latest Hubly SOC reports. The SOC 2 Type II Privacy report can be downloaded through Hubly Artifact in the Hubly Management Console.

Who should I contact if I have questions about Hubly and data protection?

We recommend that customers with questions regarding Hubly and data protection contact their Hubly account manager. If customers have signed up for Enterprise Support, they can also reach out to their Technical Account Manager (TAM) for support. Hubly account managers and TAMs work with Solutions Architects to help customers meet their compliance needs. Hubly can’t provide legal advice to customers, and we recommend that customers consult their legal counsel if they have legal questions regarding data protection.

We also have teams of Enterprise Support Representatives, Professional Services Consultants, and other staff to help with privacy questions. You can contact us with questions here.

How does Hubly use information used in resource identifiers and other items related to the management of Hubly resources?

Hubly uses that information to provide Hubly services, and protect and improve the customer experience. For example, Hubly uses resource identifiers to help customers generate cost and usage reports, which can be used to break down Hubly spend by cost centre, and IAM permissions to determine whether a specific user can purchase reserved instances. When customers contact Hubly for technical assistance, Hubly may also analyse resource identifiers and permissions to help resolve their issues.