computer workware

Beneficiary Designation forms eSignature Solution

Beneficiary Designation Forms eSignatures Solution

This document provides eSignatures solution implementation details.

Members can eSign beneficiary designation forms on the portal.

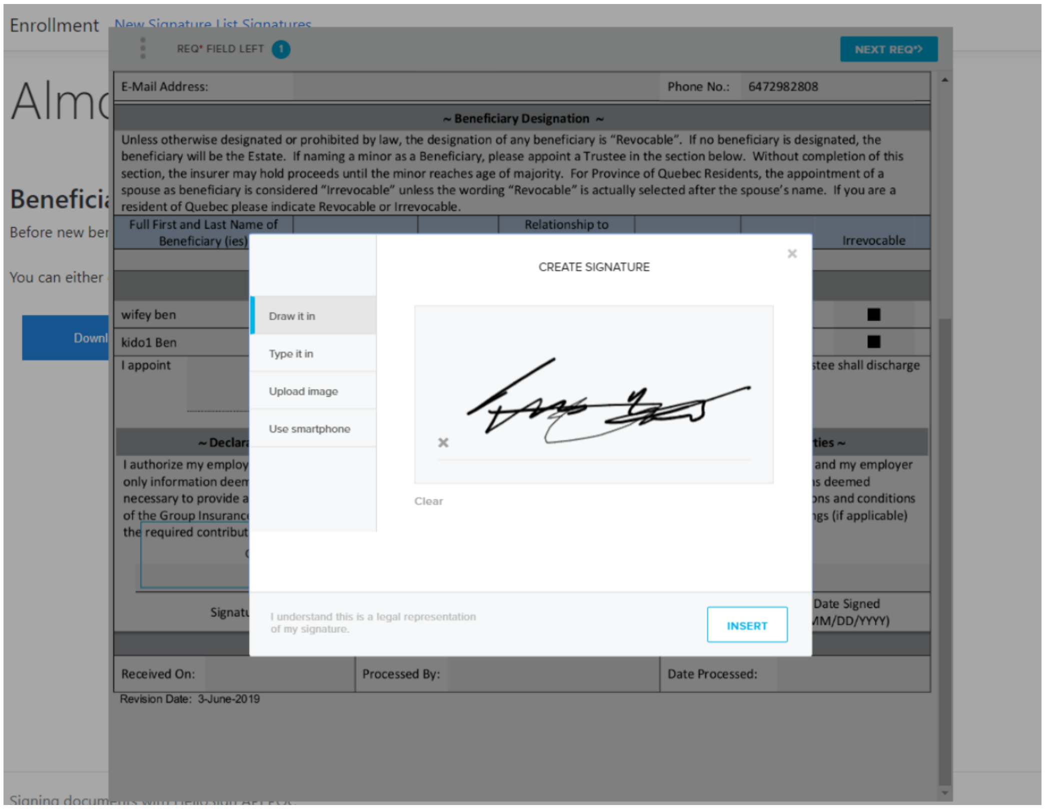
eSignature service is provided by HelloSign, a Dropbox Company.

Overview

This solution allows members to eSign beneficiary designation forms on the member benefits portal at a time of enrollment, life event, or new hire.

The solution implements embedded flow, so members can provide their signatures without leaving a portal.

The signature can be drawn, typed, or uploaded as an image.



E-Mail Address: | Phone No.: 6472982808

~ Beneficiary Designation ~

Unless otherwise designated or prohibited by law, the designation of any beneficiary is "Revocable". If no beneficiary is designated, the beneficiary will be the Estate. If naming a minor as a Beneficiary, please appoint a Trustee in the section below. Without completion of this section, the insurer may hold proceeds until the minor reaches age of majority. For Province of Quebec Residents, the appointment of a spouse as beneficiary is considered "Irrevocable" unless the wording "Revocable" is actually selected after the spouse's name. If you are a resident of Quebec please indicate Revocable or Irrevocable.

Full First and Last Name of Beneficiary (ies)	Relationship to	Irrevocable
wifey ben		■
kido1 Ben		■

I appoint ... stee shall discharge

~ Declara ... ties ~

I authorize my employ ... only information deem ... necessary to provide a ... of the Group Insuranc ... the required contribut ... and my employer ... s deemed ... ons and conditions ... ngs (if applicable)

Signatu ... Date Signed (MM/DD/YYYY)

I understand this is a legal representation of my signature.

Received On:	Processed By:	Date Processed:

Revision Date: 3-June-2019

Technologies Used

eSignatures service is provided by HelloSign, a Dropbox Company. More details at https://www.hellosign.com/trust

HelloSign is a global company, serving over 150 countries, having over 6 million users and providing services for 8 years.

Data Storage Location

All documents are stored in Canada, Ontario. After documents are signed they are deleted from HelloSign servers and stored by Computer Workware Inc. (a Canadian corporation) in the Ontario data centre.

Encryption

All documents are stored behind a firewall and authenticated against the sender's session every time a request for that document is made. All communications use SSL (Secure Sockets Layer) encryption and all data is stored in a SOC 1 Type II, SOC 2 Type 1 and ISO 27001 certified data centre. Documents are stored and encrypted at rest using AES 256-bit encryption.

Applicable Provinces

eSignatures are configurable by a province. Depending on a province legislation eSignatures can be enabled or disabled.

Authentication and Intention

Documents are "signed" by the correct person

Only authenticated users can access the member benefits portal. In order to sign up for the member portal, the operator has to invite a member to the portal by sending an invitation to a member's email address. Then only a member with access to their email and knowledge of their personal information can sign up and access the portal.

An electronic signature is maintained by a sole user control

Only authenticated users with access to their account can sign their beneficiary forms.

Signers consent that eSigned documents are legally binding

Upon eSigning documents, users actively consent that their electronic signature is legally binding.

Electronic documents are organized the same way as non-electronic documents

Beneficiary designation forms available for members to sign are also available for download and offline signing in exactly the same format.

Documents can be reviewed before and after signing

Users can review and access electronic versions of documents before applying their electronic signature. After documents are eSigned they are also available for download and print by members.

Integrity and Non-Repudiation of the Electronic Signature

Documents eSigned are the same as the document stored in the system

After the user electronically signs a document it is getting stored in a system immediately. Signing and download of documents happen over an encrypted channel. This ensures that documents downloaded are the same as stored in the system.

Specific user data is captured

When the user eSigns the document the following information is captured: time-stamp and IP address.

Signatures are not modifiable after delivery

After the eSignature is collected the document is getting stored on the server in a PDF format. Signed documents cannot be altered by users.

Electronically signed documents can be downloaded

After documents are signed they can be accessed, downloaded and printed by portal users and system operators.

Electronically signed documents are part of the disaster recovery program

eSigned documents are backed up to the disaster recovery site. There is no expiration time after which documents are getting deleted in the system.

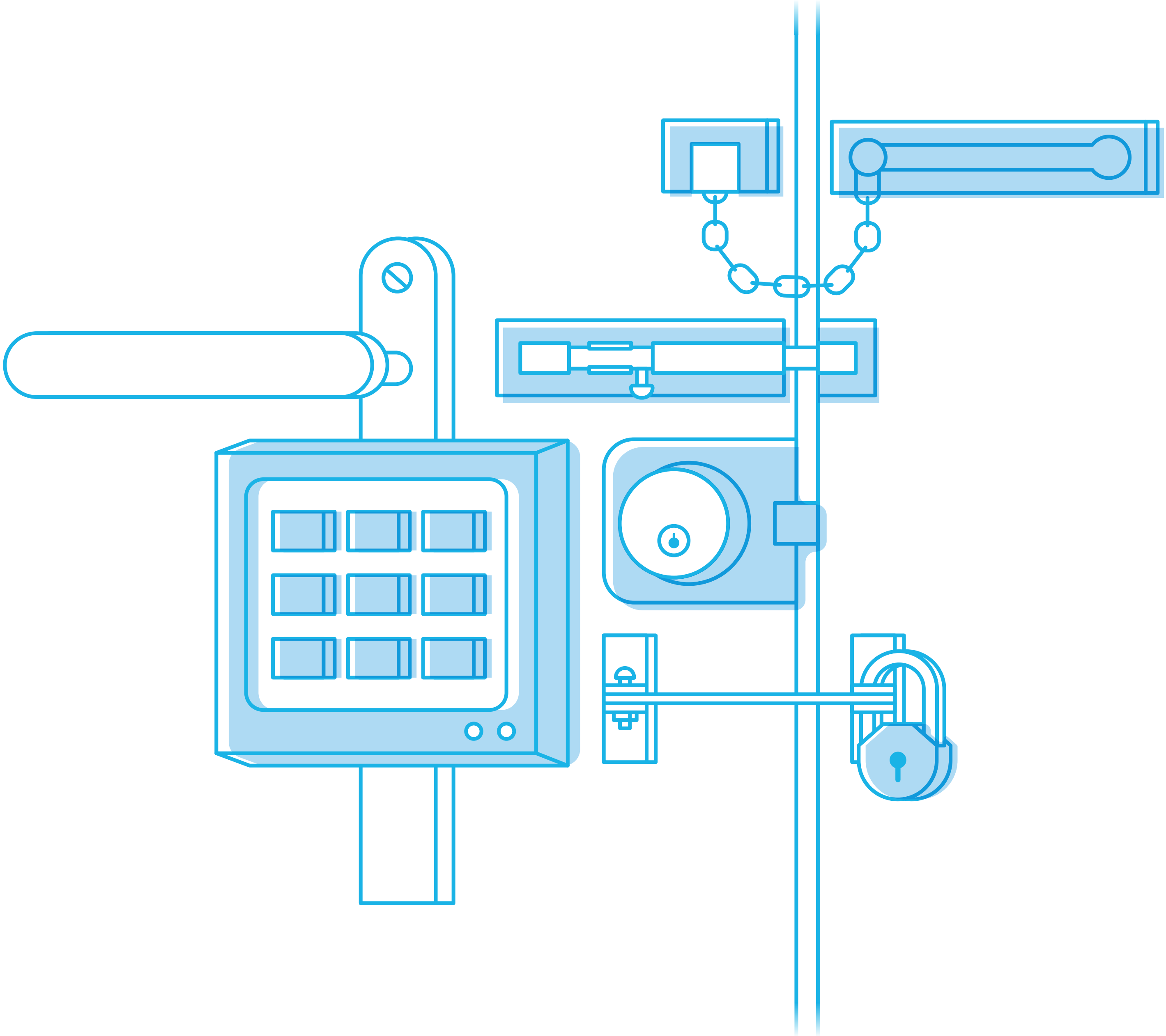
DocuSign vs HelloSign Security

Comparison of security and reliability features of DocuSign and HelloSign:

Feature	DocuSign	HelloSign
AES 256-bit encryption at rest	V	V
Communications are encrypted using TLS	V	V
Backups encrypted	V	V
HTTP Strict Transport Security	V	V
2 levels of the document encryption	V	V
99.9% uptime	V	V
2-Factor Authentication	V	V
Court Admissible Audit Trail	V	V
Security Monitoring	V	V
Physical Security	V	V
Personnel Security	V	V

HELLOSIGN

HelloSign Security, Legality and Privacy



- Bug Bounty Program
- Breach Notification Policy
- Security & Risk Management Committee

COMPLIANCE

In order to meet the most stringent security and compliance needs of our customers around the world, it's imperative that we comply with the industry standards that matter most.

We're proud to be a SkyHigh CloudTrust provider with the highest rating of "Enterprise-Ready", given only to those cloud services that fully satisfy the most stringent requirements for data protection, identity verification, service security, business practices, and legal protection.

HelloSign is compliant with the following:

SOC2 Type I
HIPAA
The U.S. ESIGN act of 2000
The Uniform Electronic Transactions Act (EUTA) of 1999
The new eIDAS regulation for the EU of 2016 (EU Regulation 910/2014), which replaces the former European EC/1999/93 Directive

LINKS TO IMPORTANT RESOURCES

Below, you will find additional links to important resources.

HelloSign Terms of Service

HelloSign Privacy Policy

HelloSign Security Information

Statement of Legality

Table of Contents

Introduction

Welcome to the HelloSign Security, Legality and Privacy Guide!

Our mission at HelloSign is to make our customers awesome. In order to ensure our customers know that they're sending signatures in confidence, we've established top-of-the-line security measures.

To help highlight our passion for security we've built the following Security Guide to share with our HelloSign community. This guide addresses many of the the questions we've been asked over the years regarding our security processes. Security isn't static, it's a fluid task that must constantly be addressed. Rest assured we work tirelessly to make the HelloSign platform safe and sound for our users.

– Neal O'Mara, Co-Founder & Chief Technology Officer at HelloSign

HelloSign Security, Legality and Privacy

DEDICATED AND EXPERIENCED SECURITY TEAM

Every employee at HelloSign, from office operations to our CEO, is dedicated to security and protecting our customer data in all that we do.

HelloSign has a formal information security program in place under the Head of Security with a team of experienced security professionals dedicated to overseeing all of our security practices, policies and procedures with the safety of our customers' data at the forefront of all efforts.

We also have an Information Security governance structure in place with an Information Security and Risk Management Committee which meets periodically to review security-related initiatives at the product, the infrastructure, and at the company level.

RELIABILITY

When you're doing business, you need us to be there for you. That's why we strive to hit at least 99.9% uptime all the time. And you can always see our current availability at our status site. We also offer 9 9's of durability with data automatically replicated in multiple data centers for the protection of your data.

All customer files have a hot backup in a different AWS region and all of our source code and server configurations are stored in source control, allowing easy replication to new regions. This ensures your data remains secure and protected.

AUTHENTICATION

It's extremely important that we verify a user is who they say they are before being allowed to either issue a document for signature or execute a signature. To that end, we have several capabilities that ensure strong authentication of individuals.

- **2-Factor Authentication**
  Users are able to set up 2-Factor Authentication (using SMS), which requires the entry of a unique code sent to that individual via mobile, along with their username and password.

- **Password-protected signature requests**
  Users can enable a 4-12 digit pin code that signers need to enter in order to view a document.

- **OAuth**
  The HelloSign API supports OAuth as a means of authenticating API calls on behalf of a user.

- **Unique key-based authentication for the API**

- **All passwords are hashed and salted with an adaptive hashing algorithm**

- **Sessions are timed out.**

- **All authentication data is encrypted**

PERMISSIONS

It's imperative that you can control who can do what within the system. Different roles carry different access rights, both in the HelloSign API and in the end user product. For example, Administrators control team-wide settings, billing information, and the roles of others.

Role-based security

Enables different levels of permissions for different members of a team, ranging from administrative rights to members who have only permissions to view templates and issue signature requests.

Signer-specific access codes

Can be assigned to each individual being asked to sign as an extra layer of security.

ENCRYPTION

All documents are stored behind a firewall and authenticated against the sender's session every time a request for that document is made. All communications use SSL (Secure Sockets Layer) encryption and all data is stored in a SOC 1 Type II, SOC 2 Type 1 and ISO 27001 certified data center. Your documents are stored and encrypted at rest using AES 256-bit encryption.

In addition, each document is encrypted with a unique key. As an additional safeguard, each key is encrypted with a regularly rotated master key. This means that even if someone were able to bypass physical security and access a hard drive, they wouldn't be able to decrypt your data.

- **All HelloSign documents are encrypted at rest using AES 256-bit encryption**
- **For any document in transit to be signed, all communications are encrypted using SSL/TLS**
- **All backups are encrypted**
- **HSTS is enabled (HTTP Strict Transport Security)**
- **HelloSign uses 2 levels of document encryption**
  Each document is encrypted using a unique key (a document encryption key or DEK), and that DEK is then encrypted using a master key that is regularly rotated.

PROTECTION OF CUSTOMER DATA

In addition to providing encryption (as outlined above), we take every measure to ensure your documents are protected and that customer data is handled with appropriate security, privacy, and confidentiality. Specific capabilities include (but are not limited to):

Data Deletion/Destruction

At the request of a customer, HelloSign will expunge all data for a customer who wants it stored only in their own storage system of choice or who leaves the HelloSign service.

Payment Info

We process all payments through payment provider Stripe, a PCI Service Provider Level 1 service. HelloSign does not store customer credit card information on its servers.

Our privacy policy can be found here.

COURT ADMISSIBLE AUDIT TRAIL

Each signature on a contract is imposed and affixed to the document. When you request a signature, HelloSign affixes an audit trail page to the document itself. The audit trail contains a globally unique identifier, or GUID, that can be used to look up a record in our database that shows who signed a document and when. These records include a hash of the PDF document which we can compare to the hash of a questionable PDF document to determine whether or not it has been modified or tampered with. Our statement of legality can be found here.

The non-editable audit trail ensures that every action on your documents is thoroughly tracked and time-stamped, to provide defensible proof of access, review, and signature.

Here are a list of all audit-tracked events in HelloSign:

- Document Uploaded
- Document Viewed
- Document Removed
- Document Sent
- Document Signed
- Signer Email Address Updated
- Signer Access Code Authenticated
- Signature Request Canceled

APPLICATION SECURITY

HelloSign has a formal application security program in place with all code being scanned for security vulnerabilities using an industry-leading static code analysis tool. To further enhance application security, HelloSign runs a bug bounty program to make sure that any vulnerabilities found by security researchers can be disclosed to us in a responsible manner. HelloSign also engages an independent third party to conduct penetration tests on its production environment.

SECURITY MONITORING

HelloSign uses a cloud native security platform to monitor the security of its production environment. HelloSign actively monitors for suspicious user activity, and tracks access to key secret and configuration files.

INFRASTRUCTURE

HelloSign uses Amazon Web Services (AWS) as its Infrastructure as a Service (IaaS) provider with Amazon data centers hosting our data within United States. HelloSign utilizes Amazon security features like Virtual Private Cloud (VPC), Security Groups, disk level encryption, etc., to ensure the confidentiality of our customer data in the cloud.

PHYSICAL SECURITY

HelloSign is hosted in a state-of-the-art SOC 1 Type II, SOC 2 Type I and ISO 27001 certified facility. Physical access is strictly controlled by professional security staff utilizing video surveillance, state-of-the-art intrusion detection systems, and other electronic means. Authorized staff must pass 2-Factor authentication no fewer than three times to access data center floors.

PERSONNEL SECURITY

All HelloSign employees undergo comprehensive background checks upon joining. All employees and contractors have to sign and follow a code of conduct and an acceptable use policy. All employees undergo information security awareness training upon joining and on an annual basis. Continuous information security awareness is maintained via monthly information security newsletters and security relevant notifications to HelloSign personnel.

INTERNAL POLICIES AND PROCEDURES

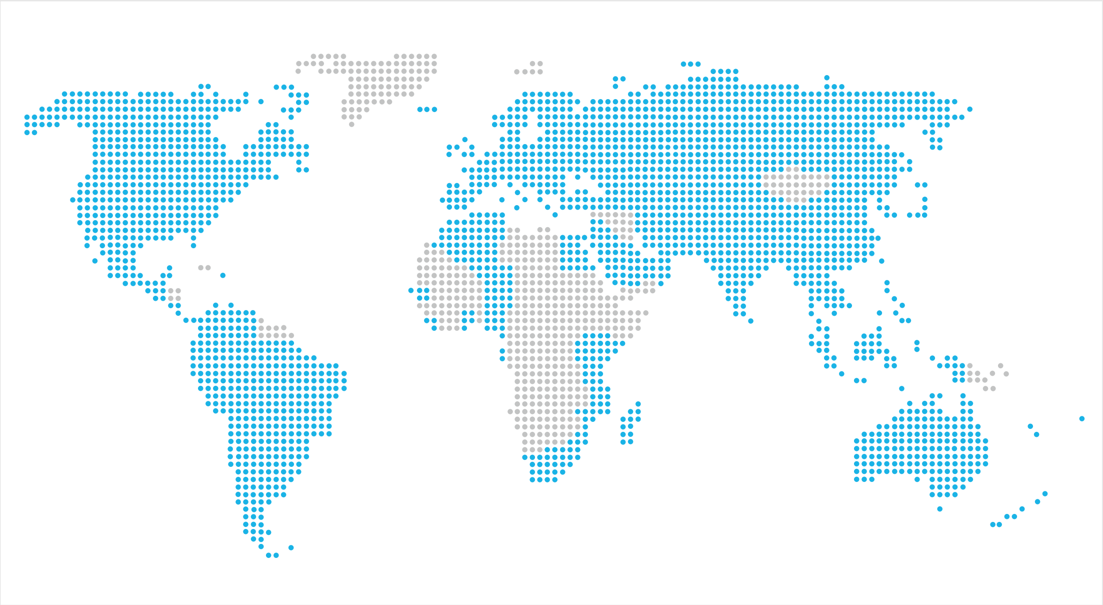
HelloSign adopts and adheres to several internal procedures that make sure the way we build, test, and release our software is with our customers' security and scalability needs in mind. Our policies ensure we comply with needed standards and regulations, and also mean we have business continuity and customer notification plans that satisfy the most rigorous of requirements. Here is a sample list of our internal policies and procedures , some of which may be shared under NDA if needed during an evaluation process:

- Information Security Policy
- Acceptable Use Policy
- Code of Conduct
- Background checks for all employees
- Endpoint encryption for all company owned/issued devices
- Release Management Procedure
- Change Management Procedure
- Release Notes
- Access Provisioning, Termination, and User Access Review Procedure
- Incident Response Plan
- Business Continuity and Disaster Recovery Plan
- Penetration Testing Program

HelloSign as a Global Company

Where are our customers? All over the world.

HelloSign is a global eSignature solution, helping over 150 countries get documents signed online. Our international partners include +1,000 employee companies and span hundreds of industries.



HelloSign Customers Across the Globe

150+ countries

SERVED BY HELLOSIGN

6,000,000+

HELLOSIGN USERS

8 years

OF OPERATIONS

Leading Countries

1. USA
2. UK
3. Canada
4. Australia
5. India
6. Germany
7. Israel
8. Netherlands
9. Singapore
10. Mexico

FAQ

What countries use HelloSign to legally sign documents?

We currently serve customers in the USA, United Kingdom, Canada, Australia, India and most countries around the world. Take a look at our customer map for a complete overview.

Are eSignatures legal in my country?

HelloSign powers the legal transmission of electronic signatures in accordance with international eSignature laws. To verify that your country supports electronic signatures, be sure to double-check your local legislation.

What efforts does HelloSign take to protect companies using eSignatures outside of the US?

As a trusted eSignature provider, we dedicate significant resources to protecting our international customers.

These include:

- Secure hosting on Amazon Web Services (AWS)
- Hosting in a state-of-the-art SAS70 Type II, SSAE 16 facility that has achieved ISO 27001 certification
- ‘Nine 9s’ of durability, with data automatically replicated in multiple data centers
- Authenticated audit trails
- Encrypted and secure backups for all data files
- Data integrity checks for all user documents
- Continuous penetration testing via a leading security firm
- Physically and logically separate corporate and production networks

What international support do you offer in the event of an outage?

Uptime for HelloSign is currently 99.99%. But in the event of an outage, we have protections in place to keep your data safe and secure. This includes a hot backup of customer files in a different AWS region. Additionally, all our source code and server configurations are stored in source control, allowing easy replication to new regions.

Do you accept different currencies as payment?

We accept valid payments through our PCI compliant payment processor, Stripe. Stripe accepts over 100 different currencies. You can view the full list by visiting: support.stripe.com/questions/which-currencies-does-stripe-support/
Please note you may be required to pay a bank conversion fee or a foreign transaction fee as indicated by Stripe’s terms and conditions.

Where is your data center?

AWS in Northern Virginia.

We take the security of your documents and data seriously. Questions? Concerns? Let us know. To learn more about HelloSign’s security, email us at **sales@hellosign.com** to talk with one of our eSignature experts.