



See Good. Do Good.

---

## Privacy Policy - Cloud

Document Number: IT003

Last updated: 13 July 2020

# Contents

GenVis Privacy Policy - Cloud	<b>4</b>
1. Introduction	<b>4</b>
1.1 Definitions	4
1.2 Consent	6
2. About Our Services	<b>6</b>
2.1 Using Our Services	6
2.2 Children	7
3. The Data We Collect	<b>7</b>
3.1 Content Data	7
3.2 Non- Content Data	8
3.2.1 Personal Information	8
3.2.2 Sensitive Information	8
3.2.3 Account and Usage Information	8
3.2.4 Log Files	8
4. Using Your Non-Content Data	<b>9</b>
4.1 General Use	9
4.2 Creation of Anonymous Data	9
4.3 Use of Credit Card Information	9
4.4 GenVis Partners, Sharing and Third Parties	10
4.5 Data Retention	10
4.6 Government Requests	10
5. General Data Protection Regulations (GDPR) Compliance	<b>11</b>
5.1 The Roles of GenVis	11
5.2 Lawful basis for processing Personal Information	11
5.3 Lawful basis for processing of special categories of Personal Information	11
6. Your Rights and obligations	<b>11</b>
6.1 Rights to Your Data	11
6.2 Accessing Your Personal Data	12
6.3 Your obligations when using Our Services	12
7. Security and Access to Your Information	<b>12</b>
7.1 GenVis Security	12
7.2 Security Breaches	13
7.4 Secure Access	13
7.5 Storage of Your Information	13
8. Your GenVis Team	<b>14</b>
9. Post Termination of Account	<b>14</b>

9.1 Deletion of Data	14
9.2 Data Retrieval	14
10. Additional Information	<b>14</b>
10.1 Accountability	14
10.2 To Unsubscribe from Our Communications	14
10.3 Change of Control	14
10.4 GenVis' Compliance and Dispute Resolution	15
10.5 Changes and Contact Information	15

# GenVis Privacy Policy - Cloud

Last Updated: 11 June 2020

## 1. Introduction

We at GenVis (Genvis Pty Ltd) are committed to protecting Your privacy obligations.

All GenVis cloud-based products and services are aligned to the data protection and privacy requirements applicable to Our Customers. They are designed with privacy and security at the core and enable customers to implement necessary controls when processing and handling data.

This privacy policy applies to GenVis Customers accessing and using Our websites, Cloud Products, Software (Mothership, Hallo, Zero, Kudo, ION and Milli) and features (collectively “Our Services”) accessed via the Cloud, and governs Our data collection, processing and usage practices.

This policy also outlines Our Customers choices regarding use, access and removal of personal information.

### 1.1 Definitions

The below table defines a common set of terms that has been developed to assist in reading and interpreting this policy.

Further information can be found in the GenVis Data Classification policy [here](#).

Term	Definition
Cloud	Means web services hosted on the cloud, either on the customer’s cloud account or on GenVis’s cloud account.
Data	Is defined as all information owned, held, used or created by a customer or vendor, or created on behalf of a customer or vendor, that is stored using, or inputted into GenVis products and services.
Data Access	Data access refers to a User’s ability to access or retrieve data stored within a database or other repository.
Data Classification	Is the assigning of Data to a category that then determines the extent to which the Data needs to be controlled and secured.
Data Collection	Is a systematic gathering of Data for a particular purpose from various sources.
Data Controller	Means the natural or legal person, public authority, or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Data.
Data Processor	Means a natural or legal person, public authority or any other body which processes Personal Data on behalf of the Data Controller.
Content	Refers to all Data including without limitation text, photos, images, audio,

	video and any other materials uploaded to GenVis services by a user.
GDPR	General Data Protection Regulation (EU) 2016/679 of the European Parliament
Insight Data	Insight Data refers to anonymised and aggregated statistical, analytical and historical Data developed by GenVis and used to support artificial intelligence / machine learning, decision making and/or research.
Non-Content	refers to Data, configuration and usage information about a customer's Mothership account and users, captured during account creation, management and support activities.
Personal Information	<p>includes a broad range of information, or an opinion, that could identify an individual. Personal information may include:</p> <ul style="list-style-type: none"> <li>● an individual's name, signature, address, phone number or date of birth</li> <li>● sensitive information</li> <li>● credit information</li> <li>● employee record information</li> <li>● photographs</li> <li>● internet protocol (IP) addresses</li> <li>● voice print and facial recognition biometrics (because they collect characteristics that make an individual's voice or face unique)</li> <li>● location information from a mobile device (because it can reveal user activity patterns and habits)</li> </ul>
Processing	Means any operation or set of operations which is performed on Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Sensitive Information	<p>Is a subset of personal information that includes information or an opinion about an individual's:</p> <ul style="list-style-type: none"> <li>● racial or ethnic origin</li> <li>● political opinions or associations</li> <li>● religious or philosophical beliefs</li> <li>● trade union membership or associations</li> <li>● sexual orientation or practices</li> <li>● criminal record</li> <li>● health or genetic information</li> <li>● some aspects of biometric information</li> </ul>
Security	Is the preservation of confidentiality, integrity and availability of Data.

User	A user either within a customer organisation, a GenVis member of staff or a third party who has authorized access to GenVis resources or a GenVis product.
We	Genvis Pty Ltd

## 1.2 Consent

We obtain consent to process Our Customers information when We are required to do so by law, as described in this Privacy Policy.

If at any time after setting up an account with GenVis, You wish to update Your Personal Data, change Your mind about sharing Your Personal Data with us, wish to cancel Your Account or would like to request that GenVis no longer uses Your information, You can withdraw Your consent to collect and use this data by contacting us in writing at [support@genvis.co](mailto:support@genvis.co)

By using Our Services, You acknowledge that You have read and understood this Policy and agree to be bound by its terms and conditions.

GenVis may occasionally update this Policy and will update the “Last Updated” information displayed on our website. Your continued use of Our Services signifies Your agreement and acceptance to any such changes.

If You do not agree with Our practices described in this Privacy Policy, You should not use Our Services.

If You have any questions about this privacy policy please write to us at:

Email: [support@genvis.co](mailto:support@genvis.co)  
 Postal mail: GenVis  
 18 Southport St,  
 West Leederville  
 Western Australia, 6007

You can opt-out of tracking on Our Services by disabling cookies or preventing Your browser from accepting new cookies.

To prevent data collected specifically by Mixpanel, users can visit <https://mixpanel.com/optout/> to opt out.

## 2. About Our Services

Our Services, including to but not limited to Mothership, Zero, Hallo, Kudo and Milli, encompass software that is designed to analyse, extract and summarise intelligence from previously recorded video footage, live camera feeds or other data sources. In addition, We operate/use several websites, including those used for marketing and customer support and for delivery of Our Services.

### 2.1 Using Our Services

As a business, individual or organisation, You may use Our Services to analyse video footage of Your premises, properties, offices, stores, homes or other locations where You have the right to do so. You may also use Our Services to collect data from sensors, including video cameras, smartphone or tablet cameras or other devices,

to use along with other data, such as purchases, weather, and third-party information to improve Your operations.

This Privacy Policy includes the Data that is gathered by You through Your use of Our Services, through Your engagement with Our websites, GenVis and Our team.

## **2.2 Children**

Under GDPR, “processing of the personal data of a child” is only allowed by law when the child is at least 16 years old. If a child is under 16 years of age, companies must obtain consent from the child's parent or legal guardian to collect and process their data.

Our Services are not intended for, and may not be used by persons under 16 years of age. By using Our Services, You represent that you are 16 years and older, and You are responsible for ensuring that all Users are at least 16 years old.

Any use or access to Our Services by anyone under 16 who is not directly supervised by an adult is strictly prohibited.

When using Our Services to collect and process data of individuals under 16 years, you represent that you have obtained the necessary consent from a parent or legal guardian, and as such have the right to process the data.

GenVis does not knowingly collect personal information from persons under 16.

## **3. The Data We Collect**

Through the provision of Our Services to Our Customers, GenVis collects a range of Data that can be classified as either Content Data or Non-Content Data.

### **3.1 Content Data**

By accessing Our Services, Customers may provide us with or create, Data and content, including text, photos, images, audio, video, other materials and personal information. Content Data refers to all such Data uploaded to or created in GenVis services by a User.

GenVis personnel cannot access or use Your Content Data without Your explicit permission.

GenVis will only access and use Content Data, with Your permission, for the limited purposes of providing GenVis Services to You, improving GenVis products, developing new AI capabilities, and as otherwise set out in Our Terms of Service and in this Privacy Policy - Cloud.

Where, through the use of Our Services You require support or assistance, GenVis administrators are only able to access Content Data, with Your explicit permission, for a limited period of time and only for the purpose for which You provide your permission.

## 3.2 Non- Content Data

By accessing and using Our Services, and setting up an account with GenVis, You may provide us with or create Non-Content Data including:

1. Personal information
2. Sensitive information
3. Account and usage information
4. Log files

### 3.2.1 Personal Information

When You purchase or evaluate Our Services We collect Personal Information such as Your name, company name, email address, billing address, credit card information and information about any transactions, both free and paid.

This personal information is accessed and collected by various means including, but not limited to:

- correspondence by telephone or by email with GenVis
- via Our website [www.genvis.co](http://www.genvis.co) from cookies and third parties
- via Our mobile applications

We collect the email addresses of those who communicate with us via email, aggregate information on pages visitors access, and information volunteered by the visitor (such as survey information or form submissions).

We also use third party services for analytics, customer support, and other promotional purposes, including Mixpanel, Hosted Libraries) and others.

### 3.2.2 Sensitive Information

Our Services include optional product features that utilise facial recognition technology. Only the features of Our Services that use facial recognition technology generate and collect sensitive information, which is limited to:

- biometric information that is used for the purpose of automated biometric verification or biometric identification; or
- biometric templates.

When activated at Your request, these features can be used to generate identifying markers such as facial signatures of individuals where You have the legal right or permission to do so. This information can then be used by Our Services to identify individuals when they appear in video footage and live camera streams.

This information is collected and stored only when requested by Our Customers and no other forms of sensitive information are collected, processed or stored by Our Services.

### 3.2.3 Account and Usage Information

Account and usage information refers to the information collected by GenVis from Your use of Our Services. This may include information about how You use Our Services, Your interactions with Our Services, and information regarding requests that You have made for support services. GenVis may provide support through phone or email, and phone conversations with the GenVis Support Team may be recorded and/or monitored.

### 3.2.4 Log Files



When You use Our Services or view content provided by Us, We automatically collect information about Your computer hardware, software and smartphone You are using. This information can include Your IP address, browser type, domain names, the files viewed on Our sites, operating system, access times and referring website addresses.

## 4. Using Your Non-Content Data

### 4.1 General Use

We collect Your Non-Content Data for the purpose of providing Our Services to You. In general, We use the information We collect to provide, maintain, protect, and improve Our Services. This may include:

- Facilitating the creation and securing of Your GenVis Account;
- Identifying You as a User of Our Services;
- Improving Our Services, Our websites and how We operate Our business;
- Understanding and enhancing Your experience of Our Services;
- Providing and delivering the services You request;
- Responding to Your comments or questions;
- Resolving Your support incidents;
- Sending You related information, including confirmations, invoices, technical notices, updates, security alerts, support and administrative messages;
- Communicating with You about promotions, upcoming events and news about products and services offered by GenVis.
- Linking or combining it with other information We get from third parties, to help understand Your needs and provide You with better service; and
- Protecting, investigating and deterring fraudulent, unauthorized or illegal activity.

When We collect personal information We will, where appropriate and where possible, explain to You why We are collecting the information and how We plan to use it.

The information We collect is not shared with or sold to other organisations for commercial purposes, except to provide the services You have requested, when We have Your permission, or under the circumstances described in this policy.

### 4.2 Creation of Anonymous Data

We may create anonymous data records from any personal information collected by Us or supplied to Us by You by excluding information that makes the data personally identifiable to You (such as Your name).

We use this anonymous data to monitor trends and to analyze usage patterns of Our Services so that We may improve Our Services. We reserve the right to use anonymous data for any purpose and disclose anonymous data to third parties, in Our sole discretion.

### 4.3 Use of Credit Card Information

If You give us credit card information We use it solely to collect payment from You. We use a third-party service provider to manage credit card processing. This service provider is not permitted to store, retain or use the information You provide except for the sole purpose of credit card processing on Our behalf.

#### 4.4 GenVis Partners, Sharing and Third Parties

We work with a global network of partners who provide consulting, implementation, training and other services around Our Services. Some of these partners also help us to market and promote Our Services, generate leads for us, and resell Our Services.

We receive information from these partners, such as billing information, billing and technical contact information, company name, what GenVis Services You have purchased or may be interested in, evaluation information You have provided, what events You have attended, and what country You are in.

You may direct Us to share Data We collect with third-party service providers such as security companies or vendors who provide services for customer relationship management, marketing program management, business intelligence and analytics, workforce management, and loss prevention.

GenVis contracts with trusted third-party service providers, such as cloud based hosting infrastructure providers AWS and Azure, to host Our servers and databases and to provide other services to Us.

It is Our policy to request that Our service providers agree not to access or use any information or Data they may have access to while providing services to Us other than as specified by Us and for the purpose for which it was originally collected.

Neither AWS nor Azure accesses or uses Your Data for any purpose other than as legally required for maintaining their respective services. You can read more about AWS's privacy policy [here](#) and Azure's privacy policy [here](#).

#### 4.5 Data Retention

We retain Your Data for as long as needed to provide You Our Services, comply with Our legal obligations, resolve disputes, and enforce Our agreements, and where We have an ongoing legitimate business need to do so.

When We have no ongoing legitimate business need to process or store Your personal information, We securely delete the information or anonymise it. We will delete this information from Our servers at Your request.

GenVis data retention policies instruct for the secure disposal of Your Data when such data is no longer necessary for the delivery and support of Our Services and in accordance with applicable regulations.

#### 4.6 Government Requests

Notwithstanding anything to the contrary in this policy, We may preserve or disclose Your Data if We believe that it is reasonably necessary to comply with a law, regulation, or legal request or to protect the safety, property, or rights of GenVis or others. However, nothing in this policy is intended to limit any legal defences or objections that You may have to a third party or government request to disclose Your information.

If a government, domestic or foreign, or third party demands Your Data stored by GenVis, it is required to follow the applicable legal process, serving GenVis with a court order for Your Data or a subpoena for information.

GenVis would redirect any such requests to You and if compelled to disclose Data, GenVis would notify You and provide a copy of the demand, unless legally prohibited from doing so. GenVis is also willing to work with You to apply for a protective order or motion, if required and where appropriate.

## 5. General Data Protection Regulations (GDPR) Compliance

### 5.1 The Roles of GenVis

To comply with GDPR regulations:

1. GenVis acts in the role of Data Processor in relation to the collection and processing of Customer Content Data. Our Customers control and own all rights, title, and interest in and to their Content Data and GenVis obtains no rights to the Customer Content Data.
2. GenVis is a Data Controller for Non-Content Data. GenVis collects, controls, and processes Non-Content Data to provide Our Services and to support the overall delivery of GenVis Products including business, operational, and security purposes. With Non-Content Data, GenVis may analyze and report anonymized and aggregated data to communicate with external and internal stakeholders.

### 5.2 Lawful basis for processing Personal Information

Under the GDPR (Article 6), GenVis may only process Your personal information lawfully if GenVis has at least one of six lawful bases for processing this information. Currently, GenVis relies on at least one of the following legal bases to process personal information under GDPR:

- “the data subject has given consent to the processing of his or her personal data for one or more specific purposes.”
- “processing is necessary for the performance of a contract to which the data subject is a party.”

### 5.3 Lawful basis for processing of special categories of Personal Information

Under the GDPR (Article 9), GenVis may only process Your sensitive information lawfully if GenVis has at least one of ten lawful bases for processing this information. Currently, GenVis relies on the following legal basis to process sensitive information under GDPR:

- “the data subject has given explicit consent to the processing of the personal data for one or more specified purposes.”

## 6. Your Rights and obligations

### 6.1 Rights to Your Data

When using GenVis products, Your Data and information always remains Yours. GenVis contractually commits that Our Customers control and own all rights, title and interest in and to their Data. GenVis does not claim any ownership of their Data.

You are solely responsible for the uploading, sharing, withdrawal, management and deletion of Your Content Data. You grant Us limited access to Your Content Data solely for the purpose of providing and supporting Our Services to and for Your and Your Users.

Furthermore, You represent and warrant to GenVis that:

1. You own Your Content Data; and
2. Your Content Data, and Your and Your User’s use of this Content Data and Our Services, does not violate this Policy or applicable data protection laws and regulations.

You can download and/or have Your content permanently removed at any time by submitting a written request to GenVis.

Email: [support@genvis.co](mailto:support@genvis.co)  
Postal mail: GenVis  
18 Southport St,  
West Leederville  
Western Australia, 6007

## 6.2 Accessing Your Personal Data

GenVis acknowledges that You have the right to access any of the personal and sensitive information that is collected through Your use of Our Services. You control and are responsible for correcting, deleting or updating information We have collected from Your use of Our Services.

If You wish to access, correct, restrict or delete data collected about You or opt-out of future data collection, please contact us in writing at [support@genvis.co](mailto:support@genvis.co) and We will respond within a reasonable timeframe.

In order to protect Your Personal and Sensitive information We will require identification from You before releasing any requested information. As long as You have provided us with sufficient information to identify You and verify Your identity, We will use reasonable efforts to comply with Your request.

## 6.3 Your obligations when using Our Services

You are responsible for procuring all authorisations and consents required for You to use Our Services. This includes authorisations and consents to ingest data into Our Services, and process and distribute data through Our Services.

For some of Our customers, adhering to additional privacy and security regulations when using Our Services may be necessary and You may be required to obtain consent and provide opt in / opt out options for certain groups of people such as Your employees or customers before using Our Services in Your business.

You may also be required to record the type of data that We process on Your behalf through Your usage of Our Services and the reason for its collection.

Your specific requirements and obligations will depend on Your business type, model, how and for what purpose You intend to use Our Services.

We encourage all customers to find, review and understand applicable privacy laws in Your state or country to determine Your obligations.

# 7. Security and Access to Your Information

## 7.1 GenVis Security

The team at GenVis understand that the security of Your data is paramount. You trust us to keep it safe and We take that seriously.

We take care to ensure the latest security processes and protocols are adopted and embedded within Our solutions, aligning to industry standards and Our own best practices. The GenVis Security Program adheres to the ISO 27001 standard and is guided by the NIST<sup>1</sup> Special Publication 800-53.

Our Customers can rest assured knowing that GenVis has built the highest-level of security into Our applications and security practices to protect the confidentiality, integrity and security of Your Content and Non-Content Data against unauthorized access, use, modification, disclosure or other misuse.

When Your information is no longer needed for the purpose for which it was obtained, We will take reasonable steps to destroy or permanently de-identify Your Personal and Sensitive information.

For further information please refer to the GenVis Security Program [here](#).

## 7.2 Security Breaches

Our Services comprise network level firewalls to protect the perimeter and segregate the network appropriately, and web application firewalls to enhance the protection of the web application. Vulnerability scanning and intrusion detection systems constantly monitor and alert whenever anomalies are detected. All security information events are stored and GenVis is able to search this information for investigation purposes.

These measures ensure We can rapidly respond to any issues that arise and in the unlikely event of a security breach, We will promptly notify You of any unauthorized access to Your Data.

## 7.3 Secure Access

GenVis protects all Customer Data with strong logical access control mechanisms to ensure only users with appropriate business needs have access to data.

GenVis has built granular access control within its products to help customers grant the permissions needed by teams and individual team members, and control who within their organisation has access to what information.

GenVis customers are responsible for ensuring that the correct roles and permissions are assigned to authorised staff appropriately, according to need.

## 7.4 Storage of Your Information

The team at GenVis understand that ensuring Your data remains in and never leaves Your local region is likely to be a requirement for You.

GenVis only uses Your local region to store and process Your data ensuring that Your data remains localised and is never moved outside of that region.

GenVis will advise all customers prior to any intended changes to data processing and storage location, and will provide the following options:

- a) Customer can accept the movement of data
- b) Customer can elect to have all data remain in Australia
- c) Customer can elect to have all data deleted

---

<sup>1</sup> The National Institute of Standards and Technology

## 8. Your GenVis Team

GenVis team members are required to conduct themselves in a manner consistent with relevant laws, the company's guidelines and policies regarding confidentiality, business ethics, acceptable usage, and professional standards.

GenVis team members must complete security training at induction in addition to annual and role-specific security training.

In addition, GenVis team members undergo an extensive background check process to the extent legally permissible and in accordance with applicable local labor laws and statutory regulations.

## 9. Post Termination of Account

### 9.1 Deletion of Data

Upon termination of Your GenVis Account, We will retain and not delete any of Your Data for 30 days following the date of termination. During this 30-day period, You may retrieve Your Content only if You have paid all bills related to Your account and no charges remain unpaid. In addition, You will not incur any additional fees if You download Your Content from Our Services during this 30-day period.

Following this 30-day period, GenVis has no obligation to maintain or provide any of Your Data and will thereafter, unless legally prohibited, delete all of Your Content stored in Our Services.

You may request written proof that all of Your Content has been successfully deleted and removed from Our Services by sending an email to [support@genvis.co](mailto:support@genvis.co)

### 9.2 Data Retrieval

GenVis can provide Our Customers with assistance to retrieve data following termination. Requests for additional assistance to download or transfer Content may result in additional fees and GenVis cannot warrant or guarantee data integrity or readability in the external systems.

## 10. Additional Information

### 10.1 Accountability

GenVis is committed to maintaining compliance with relevant security and privacy standards to ensure the continued security, availability, integrity, confidentiality, and privacy of Our Services and Customer Data stored within.

### 10.2 To Unsubscribe from Our Communications

You may unsubscribe from Our marketing communications by clicking the "unsubscribe" link located on the bottom of Our emails, updating Your communication preferences, or by sending us an email at [hello@genvis.co](mailto:hello@genvis.co)

Customers cannot opt out of receiving transactional emails related to their account with us.

### 10.3 Change of Control

If GenVis is involved in a bankruptcy, merger, acquisition, reorganisation, or sale of assets, Personal information may be sold or transferred as part of that transaction. If another company acquires Our company, business or assets, that company will possess the Personal information collected by us and will assume the rights and obligations regarding Your Personal information as described in this policy.

#### **10.4 GenVis' Compliance and Dispute Resolution**

GenVis commits to resolve any complaints about Your privacy and Our collection, use, or disclosure of Your personal information. If You have any inquiries or complaints regarding this statement, You should first contact GenVis at:

Email: [compliance@genvis.co](mailto:compliance@genvis.co)

Postal mail: GenVis  
18 Southport St,  
West Leederville 6007,  
Western Australia

#### **10.5 Changes and Contact Information**

We periodically review and update this Privacy Policy. If We make any changes to this statement, We will change the "Last Updated" date above. If We make any material changes, We will notify You by email via the address specified in Your Account.