Privacy Policy

The privacy and protection of your data are important to us and because of that, this data protection policy explains what personal data SnapComms collects from you, through our interactions with you and through our products, and how we use that data.

We offer a wide range of internal communication solutions. References to our products in this statement include SnapComms services, website, apps and software.

This statement applies to our interactions with you and the SnapComms products.

What personal data do we collect/store?

We collect data to operate effectively and provide you the best experiences with our products and across our website. Some of this data is provided directly through the ways you engage with our website and platform, such as when you install the trial through the website, install the app through Google Play and App Store, contact us for support, sign up to our blog or marketing communications, or complete a form on our website.

We collect names, job titles, company names and contact details. We also record tracking behavior as to how the data subject engages with our website by, for example, using technologies like cookies. This helps us identify which content is most relevant through clicks and time on page and the interest level (marketing potential) of the opportunity.

You have choices about the data we collect. When you are asked to provide personal data, you may decline. But if you choose not to provide data that is necessary to provide a product or feature, you may not be able to use that product or feature.

We only process the data with your consent, or on another legal basis. We only require the minimum amount of personally identifiable information that is necessary to fulfill the purpose of your interaction with us: we do not sell it to third parties: and we only use it as this Privacy Statement describes. If you're visiting us from the European Union (EU), European Economic Area (EEA), Switzerland, or the United Kingdom (UK), please refer to this Privacy Policy. We comply with the EU-US Privacy Shield Policy and we are compliant with the General Data Protection Regulation (GDPR). No matter where you are, where you live, or what your citizenship is, we provide a high standard of privacy protection to all our users around the world, regardless of their country of origin or location.

We use third-party data analytics software to collect analytics information when you use the SnapComms Content Manager (Web Portal) and Mobile App. The software may record information such as page loads, click, focus, form submit, and change events to allow us to better fulfill our contractual obligations.

Have we obtained it fairly?

Yes. It is our policy that all data subjects have opted-in to receive our content.

We make it easy for all data subjects to withdraw consent at any time; all marketing emails include the option to unsubscribe from our marketing content in the email footer.

Why do we collect this data?

We collect the data of visitors who are interested in our software so that we can best engage with them on use evaluation and subsequent purchase of our solution. In addition, we believe our content can provide useful guidance relating to internal communications best practice. As such, we have a database of those who we believe would benefit from this content.

SnapComms uses data for providing and improving the solutions we offer and perform business operations. This includes conducting research, providing customer support, operating the solutions, maintaining and improving the performance of the solutions and developing new features.

How do we ensure accuracy of data?

We endeavor to ensure that personal data we hold is accurate and up to date. We will check the accuracy of any personal data at point of collection, through our double opt in process.

At the footer of all our marketing communications, we include a link to our communication preferences page. Here, you can contact us and inform of any rectifications.

How do we act upon any withdrawal or amendment of consent?

Individuals located in certain countries including European Economic Area have certain statutory rights, in relation to their personal data including the following rights:

- **Right to access your information.** You have the right to ask for receiving confirmation as to whether your personal data is being processed by SnapComms.
- **Right to obtain confirmation of information use.** You have the right to obtain information relating to whether or not your personal data is being processed by SnapComms.
- **Right to rectify information.** You have the right to either correct or update your information at any time.
- **Right to request a copy of your information.** When necessary you might request a copy of the personal information held by SnapComms.

- **Right to erasure.** If necessary you might request erasure of your Personal Data that SnapComms is processing at any time.
- **Right to consent.** If you are a European citizen/resident you have the right to give consent for SnapComms to control your data. At the same time, you have the right to rescind the consent. We use HubSpot as our platform for recording consent. This keeps a track of when consent was received, and how.
- **Right to data portability.** You have the right to request free of charge in a machine readable format a copy of your data held by SnapComms.
- **Right to object.** SnapComms may control your Personal Data for direct marketing
- purposes and you have the right to object or withdraw consent to SnapComms' use of your Personal Data for this purpose at any time
- **Right to be notified of a breach.** SnapComms has a formal incident management procedure which is invoked when interruptions to IT services adversely affect customers, internal staff or both. For incidents related to data breaches and according to GDPR regulations, SnapComms establishes a period of no more than 72 hours to notify the protection authority and its clients regarding the impact of it over their personal information.
- **Right to complain.** Regarding the use of your personal information, you might report a complaint with us or also lodge a complaint to a supervisory authority.

We act on any change to consent within ten working days. First, we must be notified by the data subject emailing: privacy@SnapComms.com

How does the use of legitimate interest apply?

Under the General Data Protection Regulation (GDPR), we are a 'data controller' of your personal information and have a lawful reason that we can use (or 'process') your data once you have initiated and actively expressed an interest in engaging our services. Examples of what we consider to be actively interested - and therefore potential to enter into a contract together - include: requesting a free trial, viewing a demonstration of the SnapComms solution, and requesting pricing.

How long do we hold data for?

SnapComms may retain your personal data depending on what it is and whether we have the need for running business reports.

How do we ensure the data is safe and secure?

The systems we use which record personal data are housed in cloud environments which are ISO 27001 and SOC 2 Type II Certified. Personal information that we transmit is protected by security and access controls, including username and password authentication, two-factor authentication, and data encryption where appropriate.

If SnapComms learns of a security systems breach, then we will attempt to notify you electronically so that you can take appropriate protective measures. SnapComms will also take necessary measures in compliance with the relevant regulations.

To request a copy of our data security protocols, email privacy@SnapComms.com

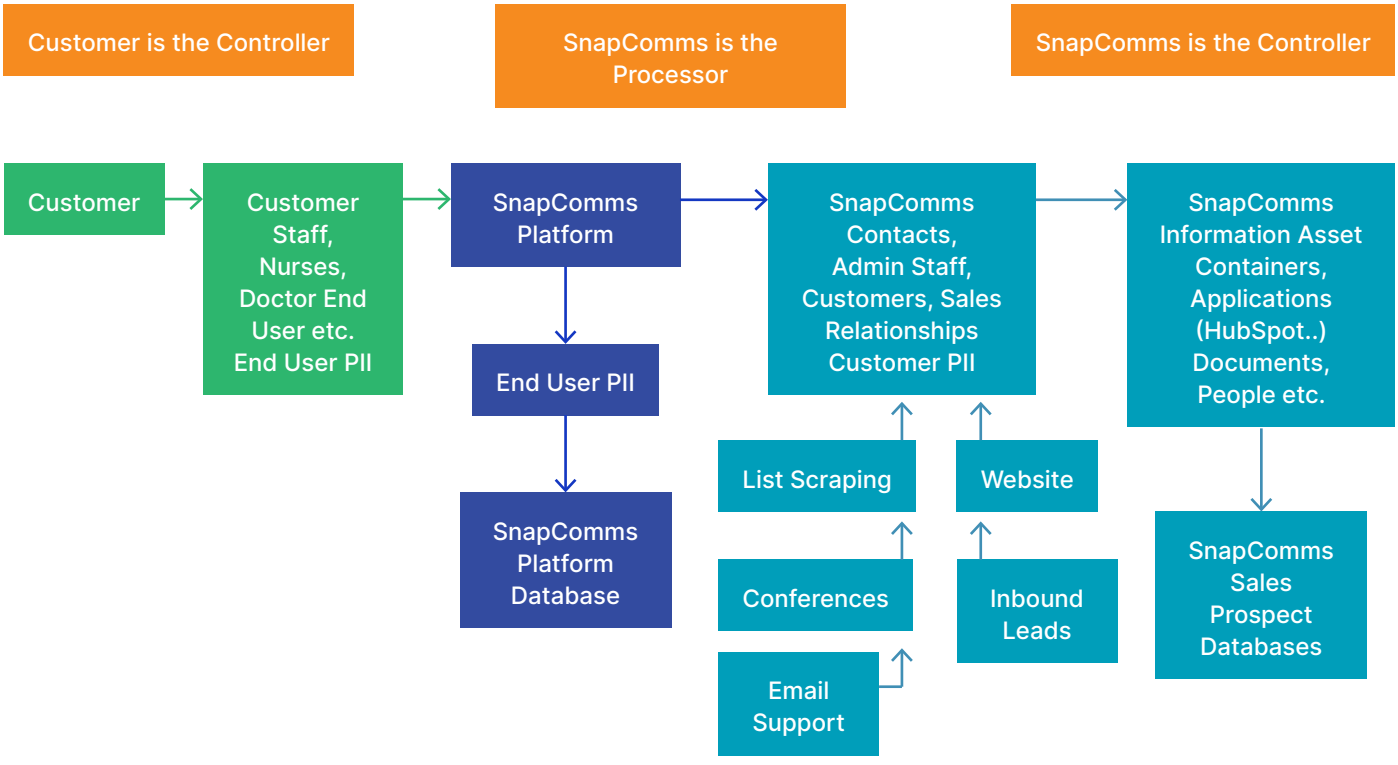
How do we share and disclose information?

SnapComms might share and disclose Information when necessary for the purposes previously stated in this policy to the following entities:

- **SnapComms employees.** When necessary for troubleshooting and technical support, SnapComms might disclose Personal Information to its employees.
- **Customer Access.** If required for business operations, SnapComms might disclose Personal Information to authorized users that have permission to access, modify or restrict access to personal information.
- **Approved suppliers and third party services.** Data is processed by HubSpot and Salesforce. You can view HubSpot's security and data protection policy here. You can view Salesforce privacy policy here.

Data processor vs data controller

The following diagram shows how SnapComms assumes the responsibility for being either Data Processor or Data Controller.



How do we use cookies?

SnapComms website use cookies to help us track your behavior on our website. You can view our cookie policy here.

What happens when you download our trial?

We receive and store information you enter on our website or give us in any other way. We use the information you provide for such purposes as responding to your requests, customizing future services, improving our products and communicating with you. View the Terms and Conditions of a SnapComms Trial here.

How to contact us?

To obtain a copy of your personal data, to correct inaccuracies or if you have any queries or concerns about how we handle your personal data, please contact: privacy@SnapComms.com or write to SnapComms, 159 Hurstmere Road, Takapuna, Auckland 0622.

General information security policy

SnapComms establishes as “General Information Security Policy” through its Information Security Management System, the preservation of confidentiality, integrity and availability of the information related to its customers and the organisation.

Confidentiality provides assurance that the information is gathered only by the authorised individuals. Integrity provides for maintenance of accuracy and validity of the information. Finally, availability guarantees the disposition of services for being used when needed.

Information is a critical factor in today’s business; consequently SnapComms management is committed to implementing, communicating and enforcing policies to protect information at different levels of the organisation as well as by suppliers and third parties.

SnapComms commits to continually improve its ISMS, to comply with applicable legal and other obligations to which it subscribes, and satisfy applicable expectations from interested parties.

SnapComms will control or restrict access so that only authorised individuals can view sensitive/confidential information. Access to customer information is limited to only those individuals who have a specific need to see or use that information.

Information will not be made available to outside parties without the written consent of the information owners.

SnapComms is committed to meet all Information Security requirements from its customers and the provision of the necessary resources to achieve this.

This policy is implemented through an information security management system according to standards, procedures and records.

To ensure compliance of employees, this policy is distributed through presentations, the SnapComms documentation platform and published on the website of SnapComms.

The compliance of this policy is controlled over time and breaches are subject to possible penalties.

ISMS Objectives

BRAVE

SNAPCOMMS VALUE	ISMS OBJECTIVE	MEASUREMENT
BOLD Showing a willingness to take opportunities; confident and courageous.	1- Be confident that all identified information security risks are assessed and treated to acceptable levels	1- All identified information security risks are assessed and treated to under level 6
RESOURCE AWARE & IMPACT-FOCUSED The capability of knowing the necessary resources for accomplishing its goals deciding configuration of its execution.	2- All employees are aware of and have competence to carry out their information security responsibilities	2- All SnapComms employees meet ISMS training and awareness requirements
ACTION ORIENTATED Willing to take practical action to deal with a problem or situation.	3- Ensure continual proactive and practical action to deal with Information security events or incidents or nonconformities	3- Keep nonconformities and incidents adequately treated within 30 days

VALUE-DRIVEN Enhancing value for the customer, for the business and for each other.	4- Enhance value for our customers by ensuring their private data and ours is protected at all times; and 5- Ensure continual compliance with legal and regulatory requirements	4- Achieve and maintain ISO27001 Accreditation 5- All legal, regulatory and contractual requirements are reviewed within required period
EVOLVING To develop and progress gradually.	6- Evolve and develop a strong information security focused image and develop market share through positive competitive differentiation	6- Identified new business won based on information security credentials 7- Produce 1 Case Study on ISMS at SnapComms within 6 months of after certification

Data security & privacy principles

Overview

SnapComms services include platform and software offerings. Technical and organisational security measures have been implemented for covering the services in compliance with international regulations and requirements related to the information security management system of the organisation.

SnapComms software as a service (SaaS) offerings provide standardised solutions from public and private cloud environments for which SnapComms manages administration, deployment, operation, maintenance and security of the solutions and the processed data pursuant the terms of the cloud service agreement. SaaS clients are responsible for assessing the suitability of the standard data security and privacy measures that SnapComms implements. The SnapComms hosted solution is a web-based solution. The network connectivity required for the SnapComms hosted solution is web traffic only (HTTPS).

The SnapComms client is a software program that is installed locally on users' computers or smartphones and is responsible for initiating regular communications with the SnapComms servers. The primary purpose of the client is for downloading and managing the display of content and information onto the users' screens.

SnapComms' specific management responsibilities for cloud services are set out in the relevant offering agreement. The data security and privacy measures designed to, among other things, defend SnapComms

cloud services against different risks such as un-authorised use of customer data and un-authorised access have been incorporated to each service description including any configurable options and other services that might be available through the content manager.

This document describes the SnapComms policies and best practices that are incorporated into SnapComms services.

Security policies

SnapComms security policies are reviewed as part of the Information Security Management System and refined as necessary to keep current with threats and in line with updates of standards such as ISO 27001, ISO 27002, and SOC 2 Type II.

SnapComms employees are required to complete specific training related to information security and data privacy as part of the Information Security Management System of the organisation and getting compliance with confidentiality and security requirements.

Security incidents are handled in accordance to ISMS requirements considering data breach notification requirements under applicable GDPR regulation. The core function of SnapComms' cybersecurity incident management practice is conducted by the SnapComms' Security Incident Response Team (SSIRT), which is managed by SnapComms' Information Security Manager who coordinates the investigation of suspected incidents to take the appropriate response plan.

Incident management

SnapComms has a formal incident management procedure which is invoked when interruptions to IT services adversely affect customers, internal staff or both. For incidents related to data breaches and according to GDPR regulations, SnapComms establishes a period of no more than 72 hours to notify the protection authority and its clients regarding the impact of it over their personal information.

Governance

SnapComms IT security policies are managed by the Information Security Manager and are an integral part of SnapComms' business. Compliance with internal security policies is mandatory and audited.

Access, intervention, transfer and separation control

The architecture of SnapComms cloud services maintains logical separation of customer data. Through internal rules and measures separate data processing, such as inserting, modifying, deleting and transferring. Access to customer data including any personal data, is allowed only by authorised employees in accordance with principles of segregation of duties, strictly controlled under identity and access management policies and monitored in accordance with SnapComms' internal privileged user monitoring and auditing program.

SnapComms' privileged access authorisation is individual, role based and subject to regular validation. Access to customer data is restricted to the level required to deliver services and support to the customers.

Transfer of data within SnapComms' network takes place on wired infrastructure and behind firewall.

Upon request or service termination, in accordance with the terms of the cloud service agreement, customer data is rendered unrecoverable in conformity with NIST guidelines for media sanitization unless other overriding legal requirements apply.

Service integrity and availability controls

SnapComms ensure its developers, technical support staff and network management teams are well versed with current industry best practice in terms of development and management of the SnapComms application. This includes awareness and understanding of the latest software and internet based security vulnerabilities (i.e. OWASP Top 10) which are reviewed and assessed on a regular basis.

SnapComms uses a suite of vulnerability scanning software from Veracode (http://www.veracode.com), a market leader in web application security technologies, to detect and identify points of vulnerability within the SnapComms software application. Advanced techniques used while the source code is executed provides a comprehensive means of vulnerabilities within the code-base.

Modifications to operating system resources and application software are governed by SnapComms change management process. Changes to network devices and firewall rules are also governed by the change management policies and are separately reviewed by security staff prior to implementation.

Each SnapComms cloud service has business continuity and disaster recovery plans, which are deployed, maintained, verified and tested in compliance with the ISO 27001 and ISO 22301 standards. Recovery Time Objectives (RTO) are established according to its architecture and intended use.

Security configuration and patch management activities are performed and reviewed regularly. SnapComms' infrastructure is subject to emergency planning concepts, such as disaster recovery and data mirroring. Business continuity plans for SnapComms' infrastructure are documented and regularly revalidated.

Activity logging and input control

SnapComms policy requires administrative access and activity in its cloud services' computing environments to be logged and monitored and the logs to be archived and retained in compliance with the information security management system. Changes made to production cloud services are recorded and managed in compliance with SnapComms change management process.

Order control

Data processing is performed according to offering agreement in which SnapComms describes the terms, functionality, support and maintenance of a cloud service offering and measures taken to maintain the confidentiality, integrity and availability of customer data.