FIRSTWAVE
CLOUD SECURITY TECHNOLOGY

FIRSTWAVE PRIVACY DATA SHEET

V2.1 FEBRUARY 2020

FirstWave Privacy Data Sheet

FirstWave is an Information Security service provider, developing and running the 'Cloud Control Security Platform' (CCSP) cloud delivered email, web and network security "as a Service" (SecaaS) to customers ranging from large telcos and government departments with millions of seats to SMBs with less than 50 seats.

FirstWave develops and manages security solutions with emphasis on data and network security, privacy, accessibility and, where required, data sovereignty.

FirstWave's Privacy Policy[1] and a range of security, operations and compliance policies and processes align Privacy and Data Protection regulations globally including the Australian Privacy Principles, the Privacy Act 1988 (Cth), the General Data Protection Regulation (GDPR EU), Payment Card Industry (PCI) requirements, best practice guidelines including ISO 27001, ISO 9001 and the Information Security Manual (ISM).

FirstWave's Privacy Policy outlines:

- How we collect personal information
- What personal information we collect
- The purpose of the collection of personal information, its use and disclosure, including overseas disclosure
- How we store personal information
- How we control access to personal information
- How consumers can access and correct personal information
- How consumers can ask questions and lodge complaints

FirstWave's ISO certified Information Security Management System (ISMS) includes a range of controls, policies and processes that collectively ensure that FirstWave's internal systems align with the Privacy Policy, regulation and InfoSec best practice.

[1] https://www.firstwavecloud.com/uploads/9/8/0/7/98070208/fw_privacypolicy_resaved.pdf

FirstWave's Processing of Personal Information

Definition of Personal and Sensitive Information

In many jurisdictions, the definition of personal data has been expanded to reflect the growth and development of technology and the novel ways that the technology is used.

Under most of the world's privacy legislation, email and email addresses are considered to be "Personal" information and must be handled accordingly. In many jurisdictions, IP addresses can become personal data when combined with other information or when used to build a profile of an individual, even if that individual's name is unknown.

In jurisdictions like Australia, metadata about an individual's web browsing is not considered to be personal information, while in other jurisdictions it is considered to be personal and sensitive information. FirstWave aims to meet the strongest and strictest regulation and best practices globally.

Personal Data Processing from various activities

In its provision of email, NGFW and web security services, FirstWave may collect, hold and process the following data:

Table 1: Personal Data Processed by FirstWave for Administrative Purposes

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	Customer administrator(s) contact information: • Administrator(s) Name • Email Address • Phone Number • Billing/Physical Address	• Product administration • Account management • License management • Billing • General product support and administration.
Platform Usage Telemetry	• Contact information for applicable administrator(s) • Phone Number • Physical Address	• Product support and operations. • Product Licensing • Product capacity management, performance and enhancements • Billing

Table 2: Personal Data Processed by FirstWave to Perform Email Security Functions

Personal Data Category	Types of Personal Data	Purpose of Processing
Email Envelope Header	• Sender • Recipient • Host/IP address	• Identify Envelope Sender, Envelope Recipient (e.g. jsmith@company.com) for security purposes. • Identify IP addresses for security purposes.
Email Data Header	• From • To • Subject • Reply-to Headers (including CC/BCC) • Name/Title of Attachment	• Identify the From, To, Subject, Reply-To headers (e.g. Jane Smith <jsmith@company.com>) • Attachment name/title for security purposes.
Email Body	• Personal data in Email body • Personal data in email attachments	• Evaluate email content for threats and apply any customer created policies.
Sender Domain Reputation Data	• Sender Email Address and Display Name	• Global threat intelligence research.

Table 3: Personal Data Processed by FirstWave to Perform Web and NGFW Security Functions

Personal Data Category	Types of Personal Data	Purpose of Processing
Web Use, Inter-network and External traffic	• Source and Destination IP Addresses • Pages visited and when • User data and possibly user login details with auto-fill features • URLs attempted access • URLs accessed • IP address, internet service provider, device hardware details, operating system and browser version • Cookies and cached data from websites • IP packet content*	• Identify URLS and IP addresses for security purposes. • Security analytics, forensics, general product functionality and usage. • Audit logs • Global threat intelligence research • Inspection of packets for malicious content detection (*when customer configured to perform this function)

In processing this information, FirstWave treats all of its customer's data and metadata as "Protected" classified personal and sensitive information.

Retention of data and metadata

FirstWave's systems are configurable and consequently, retention periods are flexible based on customer requirements. By default, the following retention periods apply:

Emails, email metadata:	8 days (moving to 32 days)
Mail logs:	Up to 7 years
Firewall logs:	12 Months (if not rolled from FIFO)
Platform logs:	12 Months (if not rolled from FIFO)
System logs:	12 Months

Cross Border Transfers

Personal Data Processed by FirstWave for Administrative Purposes is stored in the Salesforce cloud. Personal Data Processed by FirstWave for Security Purposes is stored with our infrastructure services providers, in various locations globally. At times, data may be located at a customer or end user's premises, or with their service provider, as part of a private cloud solution.

Generally, a customer will be provisioned to the nearest FirstWave public platform. The public platform infrastructure runs on Amazon Web Services (AWS) in the following regions:

Data Centre	Locations
Amazon Web Services (AWS)	The AWS infrastructure for the FirstWave platform runs in the following regions: • Americas: Oregon, USA • Americas: Virginia, USA • EMEAR: Frankfurt, Germany • EMEAR: London, UK • APJ: Sydney, Australia • APJ: Mumbai, India
Telstra CSX Generation 2 Cloud	The CSX infrastructure for the FirstWave platform runs in the following regions: • Australia: Sydney, NSW • Australia: Melbourne, Vic

Telstra Data Centre	The Telstra Data Centre infrastructure for the FirstWave platform runs in the following regions:
	• Australia: Sydney, NSW
	  ○ Pitt St
	  ○ Paddington

Equinix	The Equinix Data Centre infrastructure for the FirstWave platform runs in the following regions: • Australia: Sydney, NSW

Access, Correction and Deletion

Customers may request access to the personal information we hold about them by contacting our Privacy Officer. If personal information we hold is incorrect, we will upon request correct it or where we are satisfied that the information is inaccurate, out of date, incomplete, irrelevant or misleading, take such steps as are reasonable in the circumstances to ensure that the information is corrected.

Customers may request deletion of the personal information we hold about them by contacting our Privacy Officer.

Storage and Transit Security of Personal Information

Where we hold personal information, we take reasonable steps to ensure that the information is secure and may only be accessed by authorised persons, using both physical and technical means, in accordance with industry practice, including the use of secure servers with strong password protection and strict access controls.

Personal Data Category	Type of Encryption
Registration Information	Data at rest disk level (AWS Full Volume Encryption) Data in transit TLS encryption
Platform Usage Telemetry	Data at rest disk level (AWS Full Volume Encryption) Data in transit TLS encryption
Email Data	Data at rest disk level (AWS Full Volume Encryption) Data in transit TLS encryption
Web Data	Data at rest disk level Data in transit TLS encryption
NGFW Data	Data at rest disk level Data in transit TLS encryption

We review and update our security procedures regularly, in order to renew and improve those procedures. In limited situations, where a customer or end user has requested assistance, FirstWave technical staff may have access to customer or end user data, which may include personal information, for troubleshooting and technical assistance, but only to the extent necessary for the completion of those services and subject to applicable confidentiality and privacy restrictions.

We may be asked to archive or store information, including personal information, as part of the services we provide for customers and end users. If any personal information that we hold is no longer required for the purpose for which it was collected and no applicable law requires us to retain that information, we will take reasonable steps to anonymize or destroy the information in accordance with applicable law. The FirstWave platform may be used to automatically remove data after a retention period has ended.

Compliance with the EU General Data Protection Regulation (GDPR)

FirstWave has performed an extensive assessment of the impact of the GDPR and has found its systems and processes to be compliant with the regulations.

FirstWave's systems, policies and processes are considered to be EU General Data Protection Regulation (GDPR) compliant, supported by certification to ISO 27001 and 9001 covering classification, confidential handing of sensitive and personal information and security of processing.

In the context of the GDPR, FirstWave is considered to be a Data Processor and in general, the reseller/customer is a Data Controller.

In the context of the GDPR, the responsibilities of the Data Protection Officer rest with the Chief Risk Officer.