Conversify Data Security Policy

Conversify is dedicated to protecting all customer data using industry best standards. This Security Statement is aimed at being transparent about our data governance framework, security infrastructure, and practices, to help reassure you that your data is appropriately protected.

General Overview

We specialise in helping organisations reach and engage their customers through all direct channels, utilising strategic guidance, data leverage and high impact designs. To achieve this we use transactional and engagement data to analyse and influence customer behaviours. This data includes 'Personally Identifiable Information' (PII) which falls under the Australian Privacy Act (or 'Personal Data' as it is defined by the GDPR). As such, Conversify handles, uses, and manages data in accordance with the Australian Privacy Principles (APPs) and the General Data Protection Regulation (GDPR), including the Notifiable Data Breach schemes.

We work closely with our clients, staff, and vendors to ensure that all parties understand their responsibilities with respect to privacy and security. We only collect as much data as is required to provide our services in an efficient and effective manner. We do not share data or disclose personal Identifiable information to non-authorised parties. We only use (process) customer data in accordance with our agreed scope of services. We have technical and organisational measures to ensure a high level of security and confidentiality.

Our most important priority is the security and privacy of customer data.

Data encryption is employed to ensure customer data is received, stored, and processed in a fully secure environment. Our servers are protected by our security platform of high-end firewall systems with threat detection. Regular scans are performed to ensure that any vulnerabilities are quickly identified and patched. All services have quick failover points and with redundancy, and complete backups performed daily. Access to systems is severely restricted to specific individuals, whose access is monitored and audited for compliance.

Conversify uses Transport Layer Security (TLS) encryption (also known as HTTPS) for all transmitted data. Our solutions are hosted in world-class data centres that are independently audited using the industry standard SOC SSAE No. 18 method. As we may provide solutions for you to access this data, it is important for your users to adhere to sound security practices by using strong passwords and restricting access to their accounts to authorised persons.

Handling of Security Breaches

Despite best efforts, no method of transmission over the Internet and no method of electronic storage is perfectly secure. We cannot guarantee absolute security. However, if Conversify learns of a security breach, we will notify affected clients so that they can take appropriate protective steps. Our breach notification procedures are consistent with our obligations under the Australian Privacy Act 1988 Notifiable Data Breaches scheme and GDPR.

- Security Incident Response Plan: our team are trained to identify, investigate, and respond to security issues
- Incident Report: A description of the incident, the data accessed, the identity of affected third parties, if any, and such other relevant information will be provided

Your Responsibilities

Keeping your data secure also depends on you ensuring that you maintain the security of your integrated systems, and that user accounts are using sufficiently complicated passwords.

External Party Security Standards

Individual clients may have External Party Security Standards (EPSS) to ensure compliance to their own IT security policies, procedures, risk management practices and other measures. If required, we will work with your information security team to identify any risks which could adversely impact your strategy, operations or reputation. Conversify currently complies with the following EPSS:

- Suncorp Group (Banking & Insurance)
- Bank of QLD (Banking)

Document Intent

This Security Statement is aimed at being transparent about our security infrastructure and practices to help reassure you that your data is appropriately protected. Additional information can be made available on request under a NDA.

Physical Security

All Conversify systems and infrastructure are hosted in secure data centres. These data centres include all the necessary physical security controls (e.g., 24×7 monitoring, cameras, visitor logs, entry requirements).

Data Residency

Conversify does not store or process customer data on servers located outside of Australia without the prior written consent of clients.

Network Security

- Testing: System functionality and design changes are verified in an isolated test environment and subject to functional and security testing prior to deployment to active production systems.
- Firewalls: We use Palo Alto firewalls to secure our network boundary and DMZ zones, restricting access to all non-required ports.
- Threat Detection: Advanced threat detection monitoring and automatic block malicious traffic patterns. External IP addresses are banned after certain number of incorrect authentication attempts.
- Malware and Virus Protection: Centralised CyberSecurity Application (ESET) provides high level of protection from malware/viruses, with boundary protection file blocking based on threat analysis
- Access Control: Secure VPN, 2FA (two-factor authentication), and role-based access is enforced for systems management by authorised staff.
- Logging and Auditing: Central logging systems capture and archive internal systems access including any failed authentication attempts.
- Encryption in Transit: By default our solutions use Transport Layer Security (TLS) enabled to encrypt traffic. This ensures that all data in transit is safe, secure, and available only to intended recipients.

Vulnerability Management

- Patching: Latest security patches are applied to all operating systems, applications, and network infrastructure to mitigate exposure to vulnerabilities.
- Third Party Scans: Our environments are regularly scanned using security tools. These tools are configured to perform application and network vulnerability assessments, which include tests for patch status and misconfigurations of systems and sites.
- Penetration Testing: External organisations perform penetration tests at least annually.

Organisational & Administrative Security

- Information Security Policies: We maintain internal information security policies, including incident response plans, and regularly review and update them.
- Employee Screening: We perform background screening on all employees,
- Training: We provide security and technology use training for employees.
- Service Providers: We screen our service providers and contract them with appropriate confidentiality and security obligations if they deal with any data.
- Audit Logging: We maintain and monitor audit logs on our services and systems.
- Access Control: Customer data access in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis.
- Authentication: Staff access to systems is controlled by an authentication method involving a minimum of a unique user ID/password combination. Privileged users and administrators must use multi-factor authentication.
- Remote Network Access: Where available, is secured by multi-factor authentication VPN.

Software Development Practices

- Stack: We primarily code in Python and PHP, with SQL Server and MySQL for databases running on Windows and Linux operating systems,
- Coding Practices: Our engineers use best practices and industry-standard secure coding guidelines which align with the OWASP Top 10.
- Deployment: We deploy code multiple times during the week, giving us the ability to react quickly in the event a bug or vulnerability is discovered within our codebase.

Availability

- Power: Servers have redundant internal and external power supplies. Data centres have backup power supplies.
- Uptime: Continuous uptime monitoring, with immediate escalation to Conversify staff for any downtime.
- Failover: Our production databases are replicated in real-time and can failover in less than an hour.
- Backup Frequency: Backups occur daily at geographically disparate sites.

Deletion of Data

After contract termination, following the return of any data required, data is securely overwritten or deleted within 90 days. Back-up data may be retained for an additional 6 months after the deletion of data after which it is securely overwritten or deleted. This process is subject to applicable legal requirements. Without limiting the ability for customers to request return of their data submitted.

External Links

- Privacy Act 1988 & Privacy Amendment (Notifiable Data Breaches) Act 2017
- Australian Privacy Principles guidelines
- General Data Protection Regulation (GDPR)
- Guide to the General Data Protection Regulation (GDPR)
- OWASP Top Ten

Appendix A - Personally Identifiable Information (Australian Privacy Act)

Conversify uses Personally Identifiable Information to analyse behaviours and direct communications to customers. We only collect and store as much of this data as is required to provide our services in an efficient and effective manner. In compliance with the Privacy Act we do not collect or store any 'Sensitive Data' as defined by the Act.

How does the Privacy Act define 'personal information'?

> *B.79 'Personal information' is defined as any 'information or an opinion about an identified individual, or an individual who is reasonably identifiable:*
> - *whether the information or opinion is true or not; and*
> - *whether the information or opinion is recorded in a material form or not' (s 6(1))*
>
> *B.80 Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details, employment details and commentary or opinion about a person.*

The Privacy Act generally affords a higher level of protection to 'sensitive information' given the mishandling of it can generally have a more detrimental impact on the relevant individual.

> *B.132 'Sensitive information' is a subset of personal information and is defined as:*
> - *information or an opinion (that is also personal information) about an individual's:*
> - *racial or ethnic origin*
> - *political opinions*
> - *membership of a political association*
> - *religious beliefs or affiliations*
> - *philosophical beliefs*
> - *membership of a professional or trade association*

As an example, APP 3, which deals with the collection of solicited personal information, prohibits (with some exceptions) the collection of sensitive information unless the individual to whom it relates consents to the collection and the information is reasonably necessary for the collecting entity's functions or activities.

The collection of non-sensitive information is otherwise generally permitted where it is reasonably necessary for the collecting entity's legitimate functions or activities.

Appendix B - Personal Data (GDPR)

Conversify uses Personally Identifiable Information to analyse behaviours and direct communications to customers. We only collect and store as much of this data as is required to provide our services in an efficient and effective manner. We do not collect or store any 'Sensitive Personal Data' as defined by the GDPR.

This definition is critical because EU data protection law only applies to personal data. Information that does not fall within the definition of "personal data" is not subject to EU data protection law.

How does the GDPR define 'personal data?

> *The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.*
>
> *This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.*
>
> *The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.*
>
> *Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.*

The GDPR affords a higher level of protection to 'sensitive personal data' which are special categories of personal data that are subject to additional protections. In general, organisations require stronger grounds to process Sensitive Personal Data than they require to process "regular" personal data.

> *The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9).*
>
> *Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*
>
> *Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).*