Security & Data Protection

Omnyfy's PaaS infrastructure provides multiple levels of security and data protection to deliver a highly secure marketplace platform for your organisation.

Data Storage	Omnyfy adopts a "Near Home" infrastructure policy, meaning that your marketplace is always hosted in a region closest to the country in which your marketplace operates. For GDPR and Australian Privacy Legislation compliance, marketplaces for the EU region are hosted within EU Data Centres, and marketplaces for Australia are always hosted within Australia East or South East Data Centres.
PCI-DSS	PCI-DSS Compliant Platform when using Omnyfy's integrated Stripe payment solution.
Encryption	256bit TLS1.2 encryption for data in transit.
Infrastructure Provider	Global PaaS infrastructure deployed on Amazon AWS.
Failover and DR	For Performance and Ultimate tiers, Omnyfy providers live Failover with multi-zone server clusters.
Recovery Time Objective	High availability solution with guaranteed up-time for Performance and Ultimate Tiers. We ensure your marketplace is always available, however if there is an issue we have agreed Recovery Time Objectives in any given month so that you'll be up and back-running in no time. RTO of 30 minute or less in case of Performance Tier. RTO of 5 minutes or less in case of Ultimate Tier.

Response Point Objective	Never lose any data. Omnyfy delivers 0 minute RPO using multi-server clusters to ensure that even if there is an incident or impact on a server, your marketplace will still be up and running*. RPO of 0 minutes for both Performance and Ultimate Tiers **Note: Multi-Region marketplaces must select Ultimate PaaS tier in order to avail of the 0 minute RPO commitment. Does not apply to marketplaces using Performance Tier in a multi-region configuration.*
Backup	30 Days rolling
Sub-Processor Compliance	GDPR Sub Processor Compliance Agreement included.
Admin Authentication	Authentication for Admin and Vendor users are governed by the application level policy which includes: • Strong password policy • Password expiry and forced password update policy • Lockout policy for failed re-try • Prevent re-use of past 5 passwords
2 Factor Authentication	2FA for Administration and Vendor Users is available as an added module option.
Infrastructure Security	Omnyfy adopts WAF to protect against non essential applications running on our clusters.
Monitoring	24/7 Infrastructure and Application monitoring.

Content Security compliments the Omnyfy team on the excellent efforts on securing their web applications."

Content Security