Standards, process & legal conformity

Login & provisioning

MyWiFi's "Provision" product is suitable for all businesses, enabling them to completely separate their guest and staff WiFi environment. Highly secure, this uses automatic certificate provisioning instead of WPA or other encrypted WiFi SSID's, which are intrinsically insecure for a BYOD environment.

Seamless roaming

Our social WiFi solution doesn't require repeat login. Once a customer logs into MyWiFi for the first time, using either social media authentication or filling in the registration form, the system remembers them.

Data protection

Personal data about individuals that is collected through venues is handled in accordance with the Data Protection Act 1998. This data is stored in line with the requirements of the act and MyWiFi are registered with the Information Commissioner's Office.

Data retention

To comply with the Data Retention (EC Directive) Regulations 2009, which assists in the prevention and detection of organised crime and terrorism, certain communication data must be retained by service providers. MyWiFi stores this data in line with the requirements of the regulation on secure third party Amazon web servers.

Illegal online activity

The Digital Economy Act 2010 targets online copyright infringement by end users, covering illegal or inappropriate downloading and file sharing. MyWiFi helps venues demonstrate that they have taken the necessary steps to prevent copyright infringement, by guest WiFi users having to register and accept terms and conditions which cover inappropriate use.

Security & protection

Internet security can be one of the biggest concerns for venues offering WiFi services. Using MyWiFi will ensure that you adhere to the legal requirements of being a public hotspot provider, such as those in the Digital Economy Bill.

All users logging onto the network will be routed through the MyWiFi solution, which complies with current laws and guidelines for providing a public WiFi hotspot. MyWiFi have ISO 27001 certification.

Our hosting infrastructure is wholly contained within Amazon's cloud services which are fully PCIDSS and ISO 27001 compliant.

Content filtering

All venues that use our content filtering, are also automatically compliant with the IWF (Internet Watch Foundation) Watchlist, thanks to Open DNS' membership with the IWF. This means that all URL's collected will be checked at a venue level in real time.

Every website request made within a venue, is routed via MyWiFi's DNS filtering servers. These servers check against the list of blocked sites and if a request is not allowed, it redirects the request to a landing page explaining that this site has been blocked.

Usage tracking

All current usage tracking is done by DNS requests and usage data is stored for at least the minimum legal period and is logged against the individual's MAC address/access details. Reports in the portal show which sites have been most requested and blocked, and which categories of domains have been most requested and blocked.

Analytics & reporting

MyWiFi's reporting feature is available with our Enhanced licence and comes with an array of report types including: number of visitors; type of device used; time spent in the premises; a list of websites that customers browse in venue, time of visit, customer gender, age and email address.

Frequency of reporting

Reporting is available in real-time via our cloud-based system, 24/7, 365. You can view reports online, export them as PDFs and download data into CSV format. Our API function means you can also set up the data to sync with your own data pool.

Safe harbor

All data is stored in Amazon cloud services and stored in four places globally, in line with legislation and best practice. EU data is stored in Dublin, US data in the US and APAC data in Singapore.