captivnet
global wifi solutions

HSMX GDPR READINESS STATEMENT

SUMMARY

The HSMX platform consists of a hardware appliance, a locally-installed operating system and an application designed to provide localised, on-premises guest WiFi and authentication services. HSMX has been available and has evolved over several years with regular updates and feature additions.

However, as the hardware appliance reaches its technical end-of-life, pus limitations on security support for the operating system become more restrictive, Airangel will no longer be able to develop and update the HSMX product. As a result, HSMX is now marked as end-of-life and will be replaced by Captivnet, a more feature-rich and scalable platform.

The Captivnet software platform is a Hybrid solution which can be deployed in the public cloud, private data centre, or on a local Fusion Hardware Appliance.These appliances have significantly greater processing capability, run the latest versions of the operating system and receives regular Captivnet feature and security updates. The replacement platform has been developed in-line with our ‘privacy by design’ and default principles. Furthermore, Captivnet includes all the necessary features for the forthcoming GDPR data protection regulation and to assist in demonstrating compliance.

It is acknowledged that although a GDPR-ready upgrade path is now available, some organisations may need additional time to migrate to the new platform. As such, this document outlines where the HSMX platform aligns with requirements and where manual or organisational processes will need to be implemented to support a compliant approach.

HSMX & GDPR

Requirement	Overview	GDPR Management
Data Minimisation	Limit the data collected to the minimum required to provide the service and ensure there is clear legal basis for the collection and processing.	Where a venue operator does not collect, store or process data that, in conjunction with any other data, can be used to identify a natural person, then GDPR principles and requirements do not directly apply.
Data Security	There is a requirement to protect personal data using encryption, anonymisation or other form of protection.	Although HSMX does not support data encryption at rest, the risk to a data breach can be reduced by locating the appliance in an access-controlled location, and implementation of a least-privilege approach to system user accounts.
Data Retention	Personal Data must be stored for the minimum time required to meet the requirements outlined within the data privacy policy	HSMX provides functionality for the venue operator to anonymise personal data, based on filters, including date. A manual process to check and delete redundant, obsolete or trivial data can be implemented, by using the ‘date delete’ option to remove expired accounts prior to a retention date.
Terms, Conditions and Privacy Notice	The Data subject must be presented with a clear statement of what data is being collected, for what purpose, and on what legal basis.	Review and update the terms, conditions and privacy notice displayed to guests. Request that these are accepted at each authentication and record any updates through a dated version-controlled document.
Consent Management	Where the basis for collecting data is based on consent, this must be freely given demonstrable and able to be withdrawn	This can be managed through the interface, and the guest settings amended accordingly, on a per user basis.
Subject Access Requests	The data subject has the right to access, rectify, erase, restrict or object to the processing of their data, and to have the data exported in a common, machine-readable format.	This can be managed through the interface, and the guest data amended and extracted accordingly. The venue operator should review their existing Subject Access Request policy and processes to ensure that data stored within HSMX is included within the data collection process, where appropriate