**Data Protection Information for Bids and Tenders**

**AMX system supports GDPR and DPA2018 in the way it captures, receives, stores and processes data.**

**Data Security:** Data in AMX is protected by passwords at log-in using role-based access control (RBAC) throughout to control permissions and data access. Time out is set by the client. AMX data is encrypted both in transit and at rest.

**Data Controller**: The client determines the purpose for which the data is processed AND the means of processing.

**Data Processors:** After the client cleanses their data for AMX to upload then only the client keys and maintains the data moving forward. Clients are able to manipulate their data into reports.

**Data Sensitivity/Personal Data**: AMX, as an asset management system, does not define the data that a client captures, however, there are tools in place to aid identification and management of sensitive data. Attributes can be tagged as data protected or sensitive and only users with appropriate permissions can view of edit the data.  Where databases are provided to AMX for Support purposes the AMX obfuscation tools are used to remove and PII (Personally Identifiable Information).

**Data Hosting**: AMX uses Microsoft Azure for all hosting solutions, which provides robust data security features to protect client systems including multi-layered security with built-in threat protection, encryption at rest and in transit, and role-based access control (RBAC) to enforce least-privilege access. Where clients require, Azure includes network security features such as firewalls and the Azure Security Centre offers continuous monitoring, compliance management, and AI-driven threat detection. These features help our clients safeguard sensitive data while maintaining compliance with industry regulations.

**Data Retention**: The client determines data retention policies for live systems, however, once contracts are terminated, client data is held for 30 days before deletion from all AMX servers.

**Data Subject Requests**: All data in AMX can be reported upon to support Data Subject Requests by users with appropriate permissions. The client would be responsible for verifying the requestor to the data.

**Data Protection Impact Assessment:** The client is responsible for completing their own DPIA as part of implementation as whilst core AMX data is not PII, the client may choose to capture and process this information to support operations.

**Information Commissioners Office (ICO):** AMX carries out regular ICO self-assessments to check for changes that may impact the classification of Data Controllers and Data Processors.

***ICO Definitions***

*“****’personal data’*** *means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.*

* *race;*
* *ethnic origin;*
* *political opinions;*
* *religious or philosophical beliefs;*
* *trade union membership;*
* *genetic data;*
* *biometric data (where this is used for identification purposes);*
* *health data;*
* *sex life; or*
* *sexual orientation.*

***Special category data****is personal data that needs more protection because it is sensitive. In order to lawfully process special category data, you must identify both a lawful basis under Article 6 of the UK GDPR and a separate condition for processing under Article 9. These do not have to be linked.*

***Data Protection Information Assessment required for: -***

1. ***Systematic and extensive profiling with significant effects****:*

*“(a) any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.”*

1. ***Large scale use of sensitive data****:*

*“(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10.”*

1. ***Public monitoring****:*

*“(c) a systematic monitoring of a publicly accessible area on a large scale.”*

*Last updated: 12/03/25*