GDPR Compliance for Synantix Supported Customers

Introduction

This document references the General Data Protection Regulation known as GDPR, that comes into force on the 25th May 2018.

The extent to which GDPR compliance is applicable to Synantix as suppliers to its' customers covers business application software, software implementation, support and maintenance services.

This document describes Synantix compliance measures.

Implementation and Deployment, Support and Maintenance

- The Data Controllers employed by Synantix customer organisations are responsible for implementing the necessary technical and organisational policies to demonstrate and ensure that any data processing performed is carried out in compliance with the GDPR. Synantix will comply with customer data security protocols as directed by the customer, both during implementation/deployment and during the process of providing a software application support and maintenance update services.

- Synantix does not store or copy personal data from a customer's server environment as a product of software implementation, support and maintenance.

- Synantix does not act a Data Controller or Data Processor at any point in the implementation, support and maintenance of customer systems

- Synantix supplied software is installed and run on servers within our customers' own organisational control. Where software is installed and run on servers hosted in an external data centre, control may also lie with the company who manages those hosted environments.

Synantix Systems iDocuments software - Product Security

Synantix supplied software products have a number of tools and configuration options which can be utilised to further protect employee and other personal data against unauthorised or unlawful processing. These tools apply to the latest software release and include:

- Single Sign On - Linking Synantix supplied software logins to Active Directory and other SSO directories allows for centralised control and policy enforcement.
- Password Control - The supplied software can enforce password expiry, minimum length and format to improve overall system security
- Access Profiles - These can be used to restrict the options available to administrators relating to employee and user data
- General Authorisations – selected personal data can be secured and protected by pre-defined authorisation. Users have access only to their own personal data and only authorised personnel within the organisation structure have access to user's data.
- System Access Log – Users with special authorisation may access and review details about logs to the application such as which users logged into the system and when.
- Change Log - Users with special authorisation may check details of changes to certain data fields where those changes have been through an authorisation process.
- Access to personal data - Users are allowed self-service access to certain personal data fields and request changes to those data fields by means of an authorisation process. It is responsibility of the Data Controller to ensure that changes to or erasure of certain personal data is not in conflict with any regulations.
- Right to be forgotten – iDocuments includes a 'Forget' function which may be used for 'Dormant' users. Once you no longer need their personal data in the system for the purpose for which it was collected, the 'Forget' function can be used by authorised administrators to automatically encrypt relevant personal data.