PeopleSense INC.
ERP solutions and services

M-Files®

M-Files Security and Compliance

M-Files operates an ISO and SOC certified Quality and Information Security Management System to provide you a secure and high-quality service and takes a legal and ethical approach to its business practices at all times.

ISO/IEC 27001:2013

M-Files has been certified by an independent third-party to comply with the requirements of the standard ISO/IEC 27001:2013. Certification covers M-Files Cloud Operations.

SOC 2 and SOC 3

M-Files has been certified for compliance with the SOC 2 standard based on the Trust Services Criteria of the American Institute of CPAs (AICPA).

M-Files has also received SOC 3 certification, based on the same criteria (Trust Services Criteria of security, availability and confidentiality).

ISO 9001:2015

M-Files has been certified by an independent third-party to comply with the requirements of the standard ISO 9001:2015. Certification covers design, development, delivery and support of information management software and related services.

GDPR

M-Files complies with the GDPR both as a processor and as a controller of personal data. As a data processor M-Files complies with applicable GDPR regulations for all the relevant services delivered to customers. M-Files will also co-operate with our customers, to help them meet their GDPR obligations as data controllers.

We are committed to high standards of information security, data privacy, and transparency, and to managing data in accordance with GDPR. We have collected our privacy notices and other GDPR documentation in our Privacy Policy page.

READ M-FILES PRIVACY POLICY ▶

Anti-Slavery Position Statement

M-Files is committed to protecting against any slavery or human trafficking in our supply chain or in any part of our business. While M-Files business of providing intelligent information management solutions is not high risk with respect to slavery, human trafficking or other human rights issues, M-Files takes a zero-tolerance approach. Among other safeguards, it is M-Files business practice to comply with any applicable laws and to seek from its suppliers a contractual commitment to follow all applicable laws at any time, including the Modern Slavery Act 2015.

ISO/IEC 27017:2015

Used with ISO/IEC 27001 series of standards, ISO/IEC 27017 provides enhanced controls for cloud service providers and cloud service customers. M-Files cloud infrastructure provider Microsoft Azure has been certified to operate an Information Security Management System that confirms to the requirements of ISO/IEC 27017:2015.

ISO/IEC 27018:2014

ISO/IEC 27018 provides enhanced controls for public-cloud computing service providers acting as PII processors. M-Files cloud infrastructure provider Microsoft Azure has been certified to operate an Information Security Management System that confirms to the requirements of ISO/IEC 27018:2014.

ISO 22301:2012

ISO 22301:2012 Business Continuity Management Standard provides ensurance for commitment to business continuity and disaster preparedness. Certification demonstrates conformance to rigorous practices to prevent, mitigate, respond to, and recover from disruptive incidents. M-Files cloud infrastructure provider Microsoft Azure has been certified to operate a Business Continuity Management System that confirms to the requirements of ISO 22301:2012.

Records Management – SÄHKE2, DoD 5015.2, MoReq2, etc.

Sähke2 is a Records Management standard maintained by The National Archives of Finland. M-Files product (Asianhallinta) has been certified by an independent third-party to comply with the requirements of the SÄHKE2 requirements.

M-Files is formally certified for SÄHKE2 in Finland, and also supports the key requirements of other records management specifications, such as DoD 5015.2 and MoReq2.

FDA 21 CFR part 11

M-Files QMS meets or supports the requirements of U.S. 21 CFR Part 11 for both electronic records and electronic signatures.

Part 11 contains
– requirements that are about the computer system itself
– requirements that can only be met via local procedures or personnel

We have prepared a compliance statement document that clearly defines which ones we consider to be the latter type, together with some best practices or recommendations. As 21 CFR Part 11 final rule was originally published in 1997, some of its requirements also call for interpretation or clarification based on today's IT standards.

Eudralex Vol 4 Annex 11

M-Files Quality Management System (QMS) meets or supports the requirements of EudraLex Volume 4., Good Manufacturing Practice, Annex 11: Computerised Systems (2011).

The Annex 11 paper contains basically two types of requirements. First, certain requirements can be applied to an individual computer system that is in GMP related use. We have prepared a compliance statement document in which we explain how each such requirement is met with M-Files QMS. We clearly define where a certain requirement is met by the qualities of the software itself vs. where meeting the requirement requires also certain local process.

Secondly, Annex 11 contains requirements about how the organization should run its IT function as a whole. In the compliance statement paper, we explain how M-Files QMS supports meeting such requirements via several predefined processes and work practices.

HIPAA

M-Files software can be used to promote compliance with the Security Rule of U.S. Health Insurance Portability and Accountability Act of 1996, or HIPAA. Microsoft Azure and M-Files together can be validated to gain HIPAA compliant solution for customers.

We have prepared a compliance statement document which covers the two main, expected use cases of M-Files. In the first use case, M-Files itself is a repository containing HIPAA protected health information, and thus the system needs to have the proper security measures, controls and alarms. In the second use case M-Files is used as organization's quality management, SOP, training and personnel qualification tool, but does not contain any actual patients or their health information.

Some HIPAA rules clearly indicate certain qualities in the software system itself. For such cases we state how M-Files meets each requirement. Other HIPAA rules are about local processes, work practices and personnel. For several such rules, we propose a number of good practices and helpful tips about how M-Files can contribute to HIPAA compliance through its automation, notifications, alarms and access control features.

SOX-404

We state that M-Files Compliance Kit, the Quality, Compliance and Regulation specific extension to the M-Files core platform, has been developed and tested according to software industry known best practices by professional in-house development team. M-Files product development, testing, release and support are performed according to M-Files Corporation's Quality System.

Quality, Compliance and Regulation requirements have been taken into account in the design, development and testing of M-Files core software and its add-ons. Our regulatory awareness includes, but is not limited to, ISO 9001:2015, ISO 13485, 21 CFR Part 11, 21 CFR Part 820, Eudralex GMP Annex 11: Computerised systems, SOX-404, HIPAA and GDPR.

FIPS 140-2 Level 2

The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2) is a U.S. government computer security standard used to accredit cryptographic modules. Vendors can validate their cryptographic modules against this standard.

The cryptographic module that M-Files leverages (Microsoft Enhanced Cryptographic Provider) is validated to FIPS 140-2.

M-Files Server performs AES-256 encryption using the Microsoft Enhanced Cryptographic Provider (RSAENH) that is embedded to Windows Operating Systems. The RSAENH module encapsulates the AES algorithm in a cryptographic module accessible via the Microsoft CryptoAPI. M-Files has linked the RSAENH module dynamically into M-Files Server application and uses the Microsoft CryptoAPI for encryption. Hence, M-Files Server uses FIPS 140-2 validated cryptography.