M-Files for Compliance White Paper

M-Files Benefits for GDPR Compliance

The EU General Data Protection Regulation (GDPR) is the most important change to European data privacy regulations in 20 years. Replacing the outdated Data Protection Directive 95/46/EC (DPD), GDPR aims to simplify and harmonise data privacy laws across Europe - giving EU citizens back control of their personal data. There are heavy fines for non-compliance, of up to €20m, or 4% of global annual turnover for the preceding financial year.

M-Files is a proven, high performing content and process management platform for regulatory requirement management - and it fits perfectly to governing and managing GDPR requirements. This summary paper lists the features and capabilities that are relevant to GDPR compliance, be that either when

- ***M-Files is used to assess and maintain an organization's GDPR compliance***, or
- ***when the M-Files system itself is used to store, access or process personal data***

M-FILES BENEFITS FOR PERSONNEL MANAGING GDPR COMPLIANCE

The following capabilities help Data Protection Officers (DPO) and other key personnel managing GDPR compliance and protecting the personal data:

- ***Comprehensive search capabilities*** allow discovering personal data or identifiers across vast collections of documents and data. With the introduction of the ***Intelligent Metadata Layer, or IML,*** such discovery capabilities are taken to a whole new level. M-Files can connect to existing systems, enabling search and discovery of personal data across multiple systems, file shares, repositories and databases. There's no need ever to migrate the documents or data into M-Files in order to discover and manage personal data. *For more info on this topic please go* here.

- The Intelligence services provide advanced ***natural language AI analysis that can help identify sensitive personal data***, such as health information, home addresses etc. For example, M-Files user organization could use such capabilities to connect to an existing document repository and search for a) anything about a specific person, b) anything about a specific company, or c) crawl through the entire repository for any files that look like they contain sensitive personal information. *For more info on this topic please go* here.

- M-Files provides ***transparency through folder-less metadata architecture***. For example, all the files, documents, emails and database records for a specific marketing campaign, some of which contain personal data, are found connected to marketing campaign object itself. There's no need to find the full collection of personal data and documents related to a certain topic in different locations, folders and spreadsheets. *For more info on this topic please go* here

- M-Files provide unique ***Metadata-driven Automatic Permissions*** which greatly simplifies effective data control. The M-Files system can be configured to set exact correct permissions for each document and database record based on its current metadata properties. For example, an employee contract with sensitive personal details is automatically visible only to the employee in question, the employee's current line manager (not ***all*** the line managers), and the HR department. All permission actions on documents and data take place automatically and instantly, reducing both the manual burden and the probability of human error. *For more info on this topic please go* here

- M-Files not only supports automatic permission management, but allows ***clear verification of the currently effective permissions***. That is: through configurable permission rules each document and database record 'knows' the full list of users who can see the data in question, and also reveals why this is so. For example: employee A sees a customer-related contract since she has Upper Management role in the system, and thus has access to all such documents. Employee B sees the same document since he's the current account manager for the customer in question. However, he has no access to other contracts for other customers. All this what-and-why information is instantly verifiable and auditable in the regular M-Files user interface. There's no need for guesswork

like "I wonder who can see this sensitive document….I better ask the IT department". *For more info on this topic please go* here.

- Daily document work is often done with many systems and tools simultaneously. Drafting is done with regular office tools, collaboration or co-authoring with another tool, draft versions are sent back and forth as email attachments, annotation/redlining or proofreading may require yet another tool, there's dedicated tools for digital document signature, and the final documents are published via dedicated portal tools, or locked away in a records management system. As a result, various copies of the same document, including personal information, are left in many places.

  With M-Files there can be ***a single instance of the document*** throughout its entire life cycle. All authoring, collaboration, approval, publishing and archival can be done in one place. Instead of draft versions, only links to the document are emailed out, leaving no document copies stored in obscure locations. This simplifies the protection of personal information. *For more info on this topic please go* here.

- Last but not least, M-Files provides dedicated ***M-Files GDPR solution***, a fully pre-packaged assessment & governance tool for organizations' GDPR compliance projects, handling of DPIA audits, GDPR-related procedures and policies, and the continuous activities to maintain GDPR compliance. Metadata architecture ensures requests, corrective actions, people and documents stay connected and only the right versions are being used. Attempting to do the same in Excel spreadsheets will always eventually fail since different items in different spreadsheets and file collections are disconnected and there's no control of changes over time. *For more info please find take a look at the* product datasheet.

GDPR-RELEVANT M-FILES PLATFORM CAPABILITIES

The following technical platform features may help protecting personal data:

- M-Files has comprehensive ***encryption capabilities***. M-Files can encrypt all the files and documents on the server, protecting the personal data from breaches or intrusions on the back end. The local cache in Mobile apps can be encrypted. Data connections are encrypted between M-Files server back end and any client device being used (Window desktop app, Web browser interface or Mobile apps) thus protecting the personal data in transit.

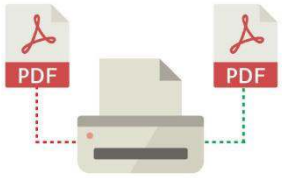
- M-Files provides ***time-stamped full audit trail and full version history***, showing who has logged into the system, and who has saved or modified what and when. *For more info on this topic please go* here.

- Data visibility ***control can be configured to the level of individual key personal identifiers***. For example, M-Files HR system can contain a single master inventory of all employees, visible to all. However, more limited HR-only permissions are applied

to employee's social security numbers and private email address.

- Data access can ***dynamically depend on the current state in a workflow process***. For example, in an M-Files CRM system moving a customer contact person to 'Not Current' state can automatically reduce its visibility. Or, if the person has specifically requested her/his data to be forgotten, moving the person record to a specific state can trigger record deletion.

- M-Files system can apply ***printing and content copy prevention*** rules for documents with sensitive personal data. This ensures documents stay in M-Files only i.e. they cannot be copied outside M-Files, saved on a user's Desktop via 'Save As' command in native viewer apps, sent out as an email attachment, or sent to a printer. Such actions can be prevented altogether, or only allowed to a certain group.



- M-Files allows setting ***automatic data retention rules***. For example, if a job application and its attached CV document is moved to state 'Not Chosen for Interview' an automatic rule is applied that destroys the application after 6 months.