MDS *ap*

MDS *ap* GDPR-Compliance Solution Offering for SAP Customers

Introduction to GDPR

It is one of the biggest changes to hit the digital privacy landscape in 20 years. In May 2018, the EU General Data Protection Regulation (GDPR) will be valid for any organization that collects, processes or controls EU citizen's data, even if they are outside of the EU. It also significantly extends the definition of personal data to include anything that can identify an individual. That could mean pictures, IP addresses, and biological, economic or social information.

Responsibility is further placed on the data controllers, who will be held jointly liable with the data processors. Organizations in both categories must be able to demonstrate compliance and show that they have technical and organizational measures in place to ensure it is enforced and to avoid large fines.

High-level GDPR requirements business will be facing

Rights of data subjects

Data subjects have the right to:

a. Access their data
b. Rectification, erasure (right to be forgotten) and restriction of processing
c. Data portability
d. Object to the use of their data
e. To know recipients or categories of recipients of personal data

Accountability

Those processing personal data are obligated to:

a. Implement appropriate technical and organizational measures to ensure and be able to demonstrate that processing is performed in accordance with the GDPR
b. Obtain consent from the data subject for certain processing activities
c. Implement appropriate data protection policies and processes
d. Maintain a record of processing activities
e. Notify certain personal data breaches to the supervisory authority
f. Notify the data subject of certain personal data breaches
g. Designate a data protection officer where appropriate
h. Ensure accuracy of personal data collected and keep up to date
i. Lawful basis for processing: Data can only be processed if there is at least one lawful basis to do so

Data protection by design and by default

Implement appropriate technical and organizational measures that:

a. Are designed to implement data protection principles, such as data minimization and pseudonymisation, in an effective manner and to integrate necessary safeguards of processing.
b. By default, do not make personal data accessible without the individual's intervention to an indefinite number of natural persons.

Data breach reporting

In the case of a personal data breach:

a. Controllers must notify the supervisory authority no later than 72 hours after having become aware of the breach.
b. Processors shall notify the controller without undue delay after becoming aware.
c. Communicate the data breach to the data subject (exceptions apply).

Anonymisation and pseudonymisation

Pseudonymisation and anonymisation techniques should be applied:

a. As part of the principles of "data protection by design and by default" when processing personal data.
b. To data archived for the purpose of public interest, scientific or historical research or statistics.

Data protection requirements introduced by GDPR will impact the majority of businesses across all sectors. But even more drastically, implications and the impact of GDPR data privacy requirements on most of the organizations will be both holistic and technically challenging.

Journey to GDPR compliance will mandate an end-to-end approach, involving both business and IT perspectives, and demanding solutions that could only be addressed through an enterprise scale architecting or re-architecting legacy systems and business processes of an organization.

Yet, organizations still have the opportunity to turn this compliance challenge into a competitive advantage by considering and designing their GDPR compliance project as a means of improving their maturity in their digital transformation and enterprise architecture.

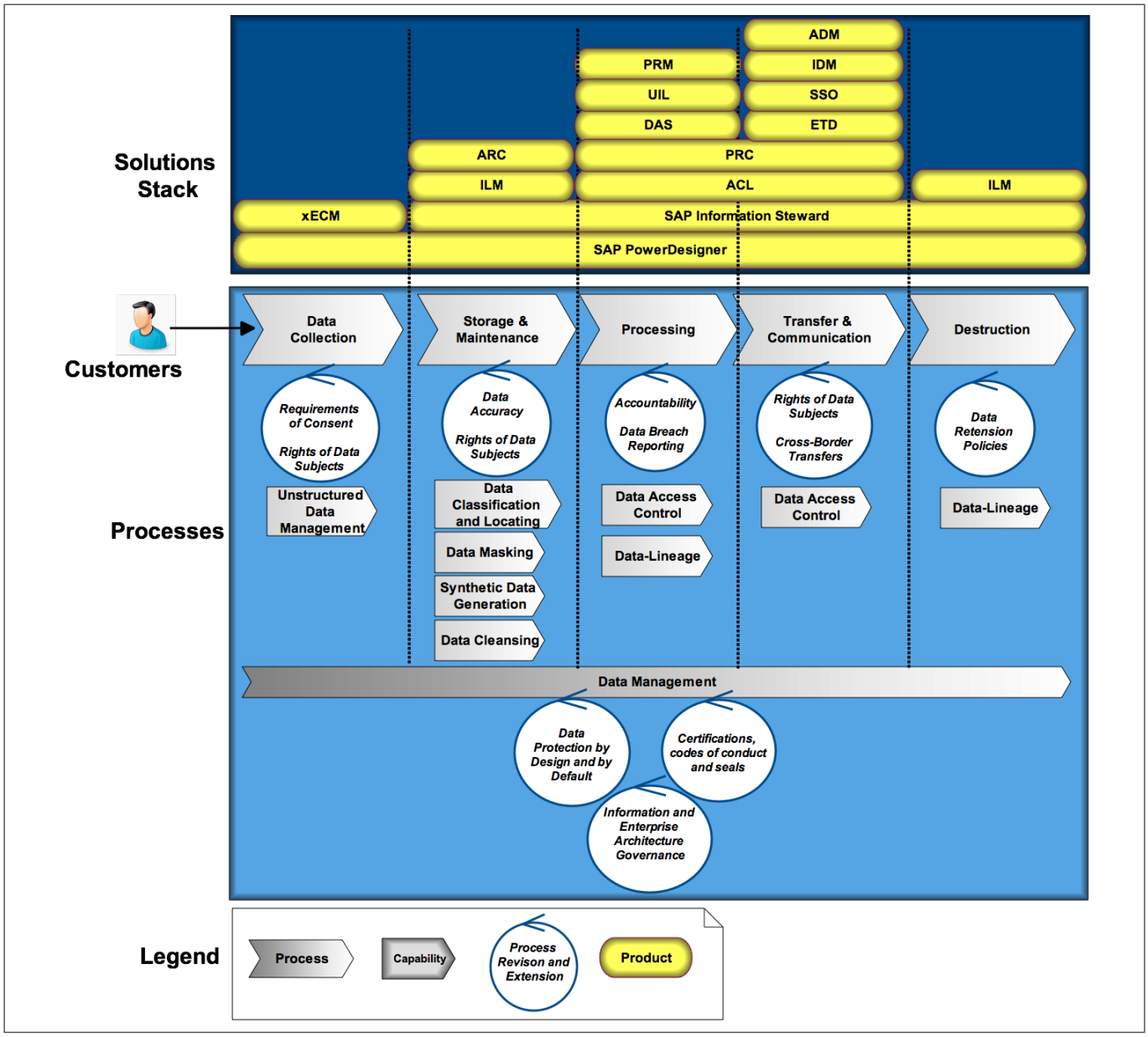
Solution overview– how MDS *ap* can help

Reference Architecture for GDPR Compliance

Taking into consideration each company is different, there are still steps in GDPR project implementation each company should consider:

1. Analysis
2. 1st phase – Process Analysis
3. Data profiling
4. Personal Data tagging
5. Impact Analysis
6. Design of the new processes required by GDPR regulation rules
7. Monitoring and management of the processes-implementation of the tool
8. Documentation
9. Implementation of access management to control administrator access
10. Implementation of identity management
11. Project and innovation lifecycle management
12. Implementation of Data masking

Powered by solutions ecosystem supported by SAP, GDPR compliance challenges and the required holistic solution approach for SAP customers could be summarized by our **reference architecture for GDPR compliance:**



Complex requirements of GDPR compliance pose challenges on enterprise data management which could only be answered by a thorough approach, including people, processes, and technology. Challenges as set forth by GDPR compliance and their solutions enabled by technological ecosystem supported by SAP offerings can be considered at different stages of data management life-cycle as follows:

Personal Data Collection Process

- Requirement to obtain consent from the data subject for certain data processing activities mandate that **personal data collection** is digital right from the start. Collected data may spread over biometric and documental media, as well as application data. These possibly unstructured or semi structured personal data collected may be required to be structured, or else processable by **content management tools,** in order to comply with GDPR.
- **SAP Extended Enterprise Content Management (xECM)** by OpenText will help organizations connect structured or unstructured content involving personal data with business processes in a securely controlled manner. Its data and document archiving system will provide a consistent, auditable, defensible and secure records management environment for any kind of unstructured content.

Personal Data Storage & Maintenance

- Ad hoc erasure and portability requirements on personal data (see **Requirement On Rights of data subjects,** and **Data protection by design and by default)** will compel an organization to have a **mature data-lineage capability**, and then the ability to trace, modify or delete personal data accross possibly distributed operational, warehouse, archive and redundant systems and environments. Ability to modify personal data distributed accross such diverse storage environments mandates a storage architecture supporting a highly **flexible and dynamic data-referential integrity.**
- Implementation of requirements of accountability (See Accountability, which require to ensure accuracy of personal data collected and keep up to date (chap.2, Article.5,1.d)) require capabilities to maintain accuracy of personal data. Acquirement of these capability mandates to implement a data-cleansing process possibly in combination with business processes for verifying correctness of collected personal data on a regular basis.
- **SAP Information Steward** meta data management module can provide tools to discover personal data, provide dynamic and interactive diagraming tools to analyze relationships between personal metadata, allowing to make impact and lineage analyses on personal data. Data insight module (profiling, monitoring data quality) can support organizations ensure quality (including accuracy) of personal data on diverse locations of entire organization by enabling to monitor data quality through scorecards. It also helps to quickly asses data quality issues and tune a solution for them. Through cleansing package builder module, data or business analysts, information stewards could easily define cleansing packages to parse and standardize personal data.
- **SAP NetWeaver Information Lifecycle Management (ILM)** product facilitates defining ILM (Information Lifecycle Management) rules (for example, retention rules) for the purpose of mapping legal requirements and their application to live and archived data. It also enables storage of data on an ILM-certified WebDAV server (to guarantee non-changeability of the data and to protect it from premature destruction)
- **SAP Archiving by OpenText (ARC)** enables your organization to maintain those personal data that is not functionally required by your applications, but that should still be maintained for legal reasons or by your business requirements.

Personal Data Processing

- Fulfilment of requirements on personal data processing (see Accountability, Data protection by design and by default, Data breach reporting, Anonymisation and pseudonymisation) both for user and application based (i.e., executed by users or applications) processes will mandate complex adaptations on the legacy systems of many organizations processing personal data. First and foremost, a holistically applicable means of scanning and discovering personal data across the full spectrum of diverse platforms will be a must-have. Then, creation or extension of a data classification schema reliably discriminating personal data will be a precondition of implementing most of the requirements of GDPR compliance. Once data classification schema adapted, next challenge is to profile and discover user and application based processes processing personal data. Finally, the hardest implementation requirement is to modify all these user or application based process and the related portfolio of applications in order to comply with data processing requirements as set forth by GDPR. These implementations include:

» Audit-trailing and logging personal data-access through user and application based processes. In implementing audit-trailing and logging capabilities, organizations will need solutions to assist not only in identifying the personal information, but also helping to detect and track the usage context of personal data (including both legal or business functional usages) during the whole data operation lifecycle.

» Introduction of new policies, or else revision of existing policies relevant to personal data access security.

» Masking (unmasked) personal data-in-motion or at-rest whenever possible without effecting current application and business logic.

» Inhouse application development (SDLC) process of most organizations will be effected significantly by requirements of GDPR compliance. During application test and development processes, data can spread across test and development as well as complex environments. (Testers might copy data to diverse environments or application release process may require different data staging environments). Across all these diverse development environments, it is mandatory to be able to know how long the data is used for and that it's used with consent and for a legitimate purpose. To ensure requirements of privacy and accountability on personal data under development and test environments, organizations having SDLC processes may apply pseudonymisation and anonymisation techniques. After pseudonymisation and anonymisation requirements applied (See Anonymisation and pseudonymisation), test data should still remain "logically usable", retaining its referential integrity in a meaningful and effectively identifiable manner. Moreover, in practice and in general, a huge amount of data needs to be masked in test environments (esp. stress-performance testing environments).

- In order to discover personal data access on an application or a user based process level, **SAP Information Stewards** meta data management module can be employed to discover any reference to personal data, aided with dynamic and interactive diagraming tools to analyze relationships between personal metadata and other types of metadata.
- Yet to obtain more complete and real-time control on personal data access layers across both application based and user based processes, you could make use of **SAP Access Control (ACL),** which will allow organizations to manage their data access policies and to monitor for compliance of these access across all layers. (SAP Access Control is an add-on to SAP NetWeaver, and works with SAP applications and non-SAP applications.)
- For many organizations, personal data on the move to data-warehouse environments will be a significant part of personal data processing. **SAP DataServices (DAS)** can provide your organization with very flexible controls on personal data on the ETL (extract, transform, load) processes targeting warehouse or other data staging environments. **SAP Data Services** combines industry-leading data quality and integration into one platform. With **SAP Data Services,** your organization can transform and improve data from anywhere into anywhere. Thanks to its integrative approach, you can have a single environment for development, runtime, management, security and connectivity of personal data.
- In implementing audit-trailing and logging capabilities relevant to personal data, **UI Logging (UIL)** will help, which could provide logging all user interactions with any kind of sensitive data based on user interfaces and user roles interacting.
- Finally, a holistic layer of compliance control on personal data access policies (which are expected to be enacted by controllers on the enterprise-wide) is enabled by **SAP Process Control (PRC)** and **SAP Process Mining by Celonis(PRM). SAP Process Control** is full-fledged policy-compliance management tool integrated with **SAP Access Control (ACL),** enabling to implement your organizations risk management and internal audit processes relevant to sensitive data. **SAP Process Mining by Celonis(PRM)** will help organizations discover and visualize all business processes across the enterprise and analyze operative process data created by your IT systems. This would make **mining of your processed data historically** possible, enabling your controllers to discover process variances and incompliant data flows.

Personal Data Transfer & Communication

- By requirements of Rights of data subjects („data controller shall provide the data subject with the recipients or categories of recipients of personal data, if any"(chapter.3,Article.13-1.e)) and cross-border data transfers and binding corporate rules, any personal data in-motion within or across organizational borders bound to be detectable and controllable. Such transfers or communications may involve unstructured or semi structured data formats (biometrics, e-mails, documents, file transfers etc) in addition to structured ones, possibly moving across geographically diverse sites within the organizational boundaries or across B2B or B2C channels over various communication protocols and media (ftp, web, private, hybrid, or public cloud etc). Across all channels of personal data movement, highly sensitive, precise, holistic and high performance data movement control and DLP (data loss prevention) capabilities should be in place to make sure nobody inadvertently sends information tagged as GDPR-related to third parties that are not authorized, and to make all these communications reportable and accountable from GDPR-perspective.
- **SAP Access Control (ACL)** and **SAP Process Control (PRC)** will monitor and then obtain a complete control on personal data transfers and communications within and across organizational borders over an enterprise scale. Their advanced policy management capabilities support the management of the overall data access/transfer/communication policy lifecycle, including the distribution and attestation of policies by target groups. These combined capabilities help reduce the cost of compliance and improve management transparency and confidence in overall compliance management processes.
- For securing personal data in-motion **UI Field Security (UIF)** can be used to mask sensitive personal data on user interface layers before they could be communicated with other parties.
- To secure personal data against application or user process level risks and vulnerabilities across all different channels of communication, **SAP Enterprise Threat Detection (ETD)** and **SAP NetWeaver single sign-on (SSO), SAP Identity Management (IDM), SAP Audit Management (ADM)** can be used. **SAP Enterprise Threat Detection (ETD)** will detect potential attacks on SAP systems at the application level by gathering and analyzing log data. Whether the threat is external or internal, **SAP Enterprise Threat Detection** will alert you to potential attacks in real-time. You have the opportunity to investigate and either dismiss the alert or pursue an actual incident. **SAP NetWeaver single sign-on (SSO)** will enable your organization to eliminate the need for multiple passwords and user IDs. You can lower the risks of unsecured login information, reduce help desk calls, and help ensure the confidentiality and security of personal and company data. **SAP Identity Management (IDM)** provides central role-based identity management for provisioning user and access data within your heterogeneous system landscape. It enables you to control all identities within your organization, not only for employees, but also for contractors, customers, partners, and other identities that need to access your organization's applications. **SAP Audit Management** provides a fully mobile enabled, end-to-end audit management solution. Your organizations audit departments can use it to build audit plans, prepare audits, analyze relevant information, document result, form an audit opinion, communicate results, and monitor progress.

Personal Data Destruction

- In order to ensure a minimal period of storage (in line with both the rights of data subjects and the necessities of their organizations business requirements) on personal data storage environments, data retention and destruction policies bound to more flexible while at the same be more granular and sensitive to personal data.
- **SAP Information Steward Metadata module** will help organizations locate where these personal data reside on an enterprise scale, while **SAP Information Steward Data insight module** will enable to set up policies of personal data retention in accordance with the categories of personal data, legal basis of their retention and rules on retention period enforced by regulations.
- Moreover, by capabilities of **SAP NetWeaver Information Lifecycle Management (ILM),** your organization could implement the following advanced **personal data retention management functions:**
  1. Defining ILM rules for the purpose of mapping legal requirements and their application to live and archived data.
  2. Putting legal holds on data that is relevant for legal cases in order to prevent early destruction.
  3. Destroying data while taking legal requirements and legal holds into account.

Overall Personal Data Management Process

- Controllers are to justify that "the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility" are in line with both the rights of data subjects and the necessities of their organizations business requirements. Moreover, controllers are also to supervise processes supporting or implementing these requirements by ensuring existence of "… a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing."
- Fullfilling duties of controllers within an organization as specified by GPDR, as well as implementing requirements of Certifications, codes of conduct and seals and of Data protection by design and by default includes establishment of policies, processes, procedures based on a holistically defined data management and data governance architecture, under which both business and IT perspectives and stakeholders are addressed with an enterpise architecture modeling approach.
- SAP PowerDesigner with its integrated approach to data architecture and enterprise architecture will help organizations not only discover, profile, classify personal data and regulate policies, processes, procedures on management of personal data within scope of GDPR, but it will also support governance and maintainence of GDPR compliance through its advanced capabilities of reverse-engineering, meta-data governance, model-driven SDLC support, data movement modeling, holistic impact and lineage analysis accross entire modeling perspectives of information and enterprise architecture of an organization.

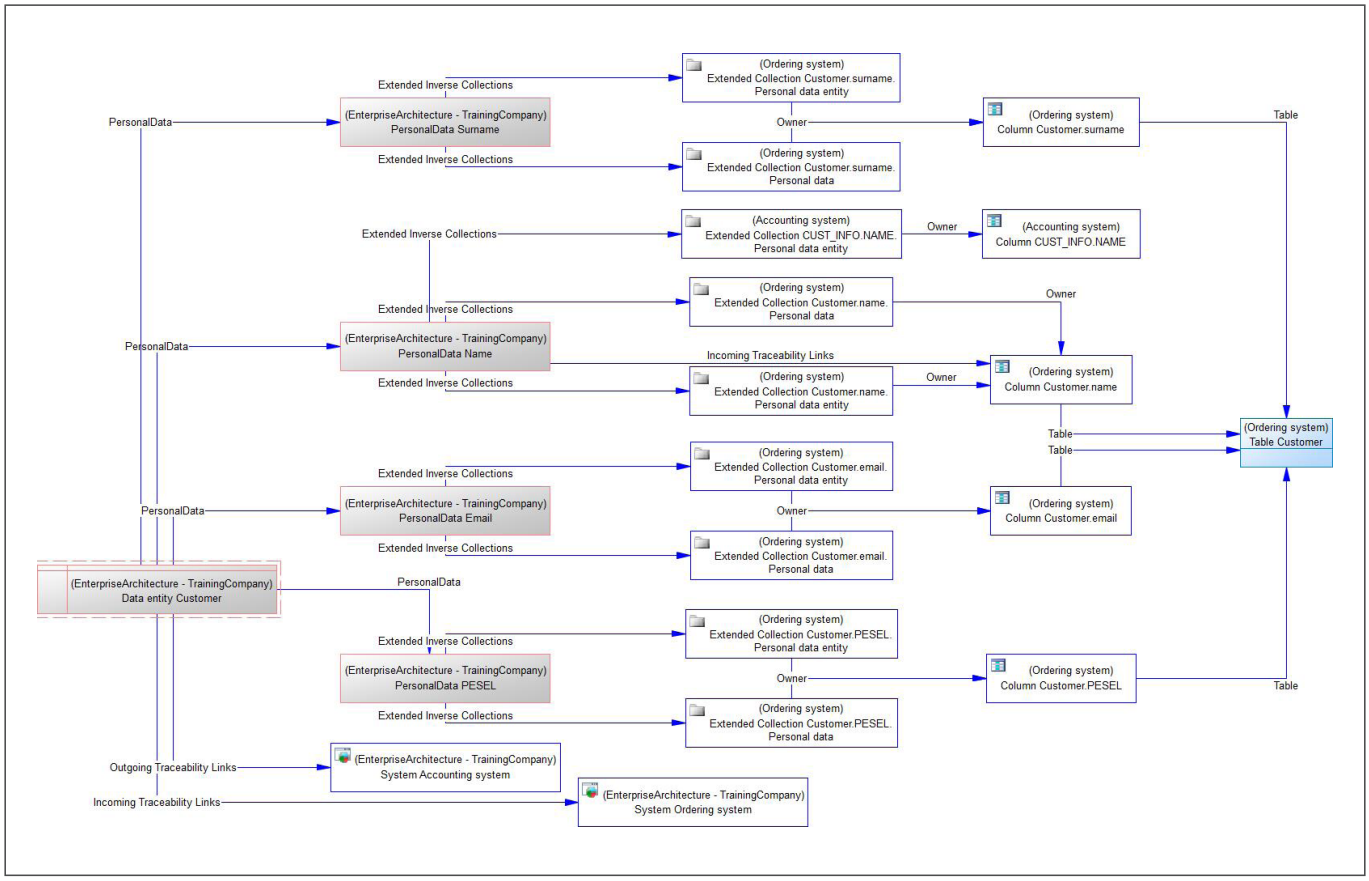
GDPR implementation in SAP PowerDesigner

SAP PowerDesigner provides tools for the many different areas, including in particular:

- Enterprise architecture
- Strategy
- **Business proces modelling**
- **Applications, systems and technologies**
- Business intelligence and information architecture
- **Data modeling and data architecture**

SAP PowerDesigner case tool (with GDPR extension) can be used for:

- Describing processes maintaining personal data (data sets) and how they work with them
- Describing interfaces for transferring personal data
- Documenting the purpose of processing these data in a given system/database, processing period and documenting the risk assessment of their storage
- Documenting structures of current systems in data models
- Tagging the places (tables, columns) where personal data are stored
- Connecting personal data described from the process point of view to their storages described in data models
- Performing impact analysis on particular data sets (example below)

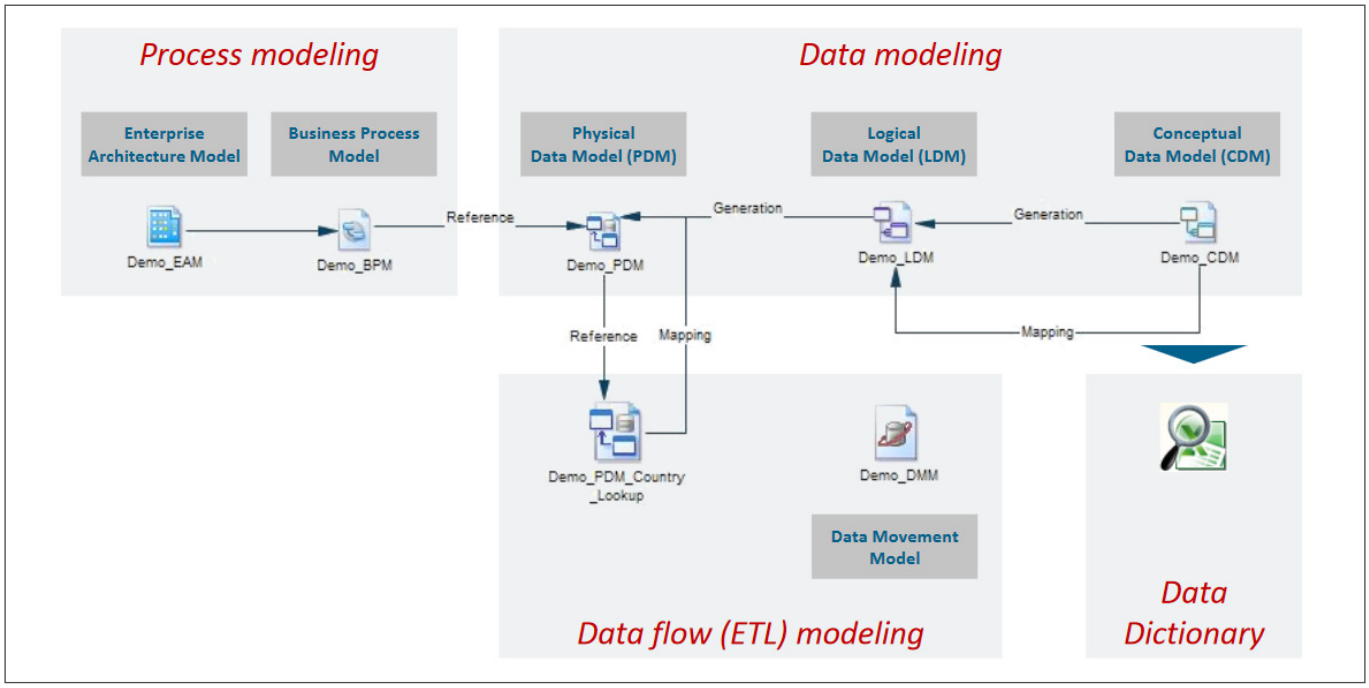


- Automated preparation of queries for gathering personal data related to specific person
- Documentation of applied data protection mechanisms in the organization
- When introducing new systems or making changes in the IT environment - analyzing the impact of the change on the protection of personal data in the enterprise

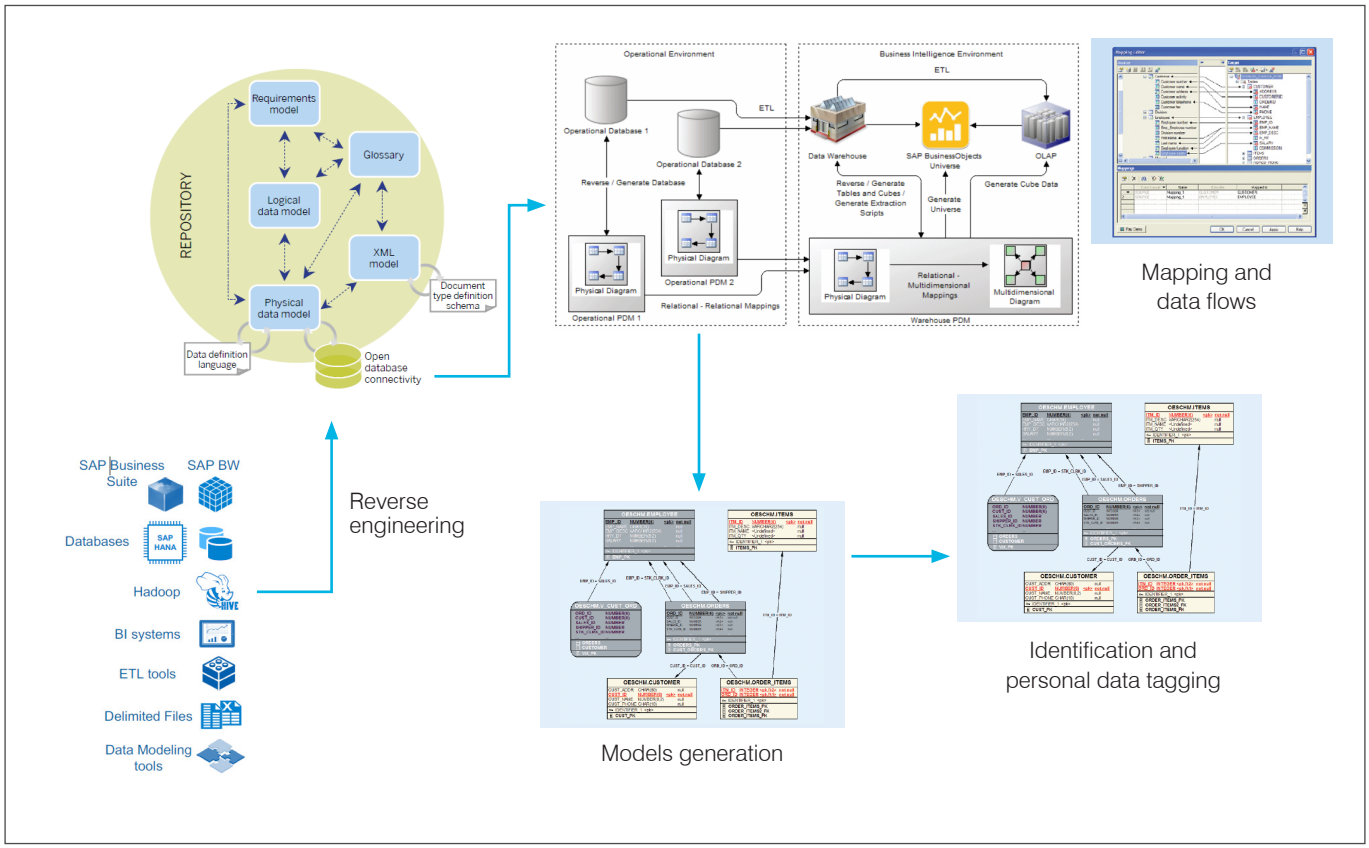
SAP PowerDesigner allows to visualize the information architecture. It provides tools for tagging and documentation of the storage of sensitive data - at the data model of applications using transactional and analytical databases (data warehouses, data marts):

- Reverse engineering of data models from databases to physical models
- Make models / table lists available to users for analysis and identification of sensitive data
- Report (document format or portal-accessible) - Provide information about models / tagged sensitive data to users

SAP PowerDesigner supports the GDPR regulation in the areas of Process, Data, Data Flow Modelling as shown in the schemas below:



Physical data model, data mapping, and data flows designed in SAP PowerDesigner can be seen in the picture below.



Products and key features

SAP PowerDesigner

- **Solution Class**
  - » **Enterprise Information Management**
- **Capabilities**
  - » Model and manage data across enterprise (requirements, enterprise architecture, business processes, data, data movement and technical architecture modelling)
- **SAP PowerDesigner** is a graphical enterprise modeling solution supporting standard methodologies and notations and providing automated code reverse engineering and generation through customizable templates. **PowerDesigner** provides powerful reporting capabilities, is highly extensible, and offers a scalable enterprise repository solution with strong security and versioning capabilities to aid multi-user development.

SAP Extended Enterprise Content Management (xECM)

- **Solution Class**
  - » **Enterprise Information Management**
- Capabilities
  - » Connect structured data and unstructured content with business processes
  - » ILM-certified, compliant data and document archiving
  - » Consistent, auditable, defensible and secure records management
- SAP xECM by OpenText creates an integrated, enterprise-wide information grid that transforms Personal Productivity, Process Productivity, and Control:
  - » Process Productivity: By integrating Enterprise Content Management with SAP Business Suite/S/4HANA where work actually takes place, SAP xECM by OpenTextcan connect disparate business processes and information sources to share content in order to improve insight, efficiency and throughput.
  - » Personal Productivity: SAP xECM by OpenText gives a new generation of knowledge workers access to their files anywhere, on any device, providing effortless sharing and collaboration without resorting to unsecured consumer applications.
  - » Control: SAP xECM by OpenText delivers transparent, automated, enterprise-wide governance to produce industry-leading security, privacy and compliance –effectively maximizing information value while minimizing risks.
  - » The solution allows customers to unify data from transactions, SAP S/4HANA software, and unstructured content, reduce regulatory compliance risk, personalize interactions with customers, enable collaboration in globally disperse teams.

SAP NetWeaver Information Lifecycle Management (ILM)

- Solution Class
  - » Enterprise Information Management
- Capabilities
  - » Enhanced data archiving
  - » Retention management
  - » Compliant archiving
- SAP Information Lifecycle Management enhances the traditional SAP data archiving technologies with information lifecycle management capabilities, covering retention, holds and destruction based on rules. SAP ILM uses ILM-specific, enhanced data archiving functions. Typical featuresare as follows:
  - » Lifecycle Management of data with the following Retention Management functions:
    - * Defining ILM rules (for example, retention rules) for the purpose of mapping legal requirements and their application to live and archived data.
    - * Putting legal holds on data that is relevant for legal cases in order to prevent early destruction.
    - * Destroying data while taking legal requirements and legal holds into account.
  - » Storage of archived data on an ILM-certified WebDAV server (to guarantee non-changeability of the data and to protect it from premature destruction)

SAP Information Steward

- **Solution Class**
  - **Enterprise Information Management**
- Capabilities
  - Discover, assess, define, monitor and improve data quality
  - Manage metadata
  - Maintain enterprise-wide business glossary
  - Cleanse data
- SAP Information Steward provides business analysts, data stewards, and IT users with a single environment to discover, assess, define, monitor, and improve the quality of their enterprise data assets through the various modules:
  - Data Insight: Profile data, create and run validation rules, monitor data quality through scorecards, and create data cleansing solutions based on your data's content-type identification results and SAP best practices for your specific data.
  - Metadata Management: Catalog the metadata across their system landscape, analyze and understand the relationships of their enterprise data.
  - Metapedia: Define business terms for data and organize the terms into categories.
  - Cleansing Package Builder: Define cleansing packages to parse and standardize data.
  - Match Review: Review results of automated matching on a regular basis and make any necessary corrections. Match Review maintains a list of records in the My Worklist tab that involves reviewers' actions for match decisions.

SAP Archiving by OpenText (ARC)

- **Solution Class**
  - **Enterprise Information Management**
- Capabilities
  - Compliant data archiving
- You archive data to remove from the database data that the system no longer needs, but which must still be accessible. You use a specific archiving object to archive specific data. Data archiving builds the basis for Retention Management delivered by SAP NetWeaver Information Lifecycle Management.

SAP Process Mining by Celonis (PRM)

- **Solution Class**
  - **Enterprise Information Management**
- Capabilities
  - Process mining on historical business process data
  - Discover process variances and incompliant process flows
  - Track personal data flow in businessprocesses
- SAP Process Mining by Celonis helps organizations to discover and visualize all business processes across the enterprise and analyze operative process data created by IT systems, providing greater business process transparency and optimization. Its highly efficient algorithms can analyze vast amounts of data inside the SAP HANA platform in real time, contributing to an end-to-end operational intelligence platform.

SAP Access Control (ACL)

- **Solution Class**
  - **Governance, Risk and Compliance**
- Capabilities
  - Access request management
  - Access risk analysis and management
  - Compliance certification review
  - Role management
  - Role mining
  - Emergency (super user) access management
  - Access control repository
  - Periodic access and SoD reviews
  - Reports and analytics

- SAP Access Control is an enterprise software application that allows organizations to manage their access governance policies and to monitor for compliance. SAP Access Control is an add-on to SAP NetWeaver, and works with SAP applications and non-SAP applications, such as SAP Finance, SAP Sales and Distribution, Oracle, and JDE.The application provides a framework for managing application authorization functions such as:
  - Access Requests (ARQ)–You can implement your company's policies for creating and maintaining access requests in ARQ. Users can create requests to access systems and applications. Approvers can review the requests, perform analysis for user access and Segregation of Duties (SoD) risks, and then approve, reject, or modify the requests.
  - Access Risk Analysis (ARA)–You can implement your company's policies for SoDand user access risk in ARA. Security analysts and business process owners run reports to determine if violations of SoDor user access policies have occurred. They can identify the root cause of the violations and remediate the risks. Compliance persons can use this function to monitor compliance with company policies.
  - Business Role Management (BRM)–In an SAP landscape, users' authorizations to applications are managed through the use of roles. Role designers, role owners, and security analysts can use BRM to maintain roles and analyze them for violations of company policies.
  - Emergency Access Management (EAM)–You can implement your company's policies for managing emergency access in EAM. Users can create self-service requests for emergency access to systems and applications. Business process owners can review requests for emergency access and grant access. Compliance persons can perform periodic audits of usage and logs to monitor compliance with company policies.
  - Periodic Reviews of User Access and Segregation of Duties (SoD)–You can use the application to carry out your company's policies on periodic reviews for compliance. Security and business process owners identify policies that require periodic reviews and define review processes. Reviewers perform the reviews and then security and business process owners determine if corrective actions are required.

SAP Process Control (PRC)

- **Solution Class**
  - **Governance, Risk and Compliance**
- Capabilities
  - Compliance management
  - Policy management
  - Integration with Access Control, Risk Management and Internal Audit Management
- SAP Process Control is an enterprise software solution for compliance and policy management.
- The compliance management capabilities enable organizations to manage and monitor their internal control environments. This provides the ability to proactively remediate any identified issues, and then certify and report on the overall state of the corresponding compliance activities.
- The policy management capabilities support the management of the overall policy lifecycle, including the distribution and attestation of policies by target groups.
- These combined capabilities help reduce the cost of compliance and improve management

SAP Audit Management (ADM)

- **Solution Class**
  - **Governance, Risk and Compliance**
- Capabilities
  - Audit management
- SAP Audit Management powered by SAP HANA provides a fully mobile enabled, end-to-end audit management solution. The audit department can use it to build audit plans, prepare audits, analyze relevant information, document result, form an audit opinion, communicate results, and monitor.

SAP Identity Management (IDM)

- **Solution Class**
  - **Information Security**
- Capabilities
  - Central user provisioning

  - » Approvals workflow
  - » Rules-and roles-based provisioning
  - » Password management
  - » Audit and monitoring
  - » Standards-based support for identity federation
- SAP Identity Management provides central role-based identity management for provisioning user and access data within your heterogeneous system landscape. It enables you to control all identities within your organization, not only for employees, but also for contractors, customers, partners, and other identities that need to access your organization's applications.
- SAP Identity Management can connect to any number of different applications and ensure that the identity information is updated correctly in each of these applications. It provides a unified view of the virtual identity of users.

SAP NetWeaver Single Sign-On (SSO)

- **Solution Class**
  - » **Information Security**
- Capabilities
  - » Authentication via single sign-on
  - » Secure login
  - » Identity provider
  - » Security token service
  - » One-time password authentication
  - » Policy scripts
  - » Password manager
- SAP Single Sign-On enables companies to eliminate the need for multiple passwords and user IDs. You can lower the risks of unsecured login information, reduce help desk calls, and help ensure the confidentiality and security of personal and company data.

SAP Enterprise Threat Detection (ETD)

- **Solution Class**
  - » **Information Security**
- Capabilities
  - » Real-time log monitoring
- SAP Enterprise Threat Detection enables you to do real-time evolution of security threats in your IT landscapes by leveraging SAP and non-SAP log data. SAP Enterprise Threat Detection detects potential attacks on SAP systems at the application level by gathering and analyzing log data. Whether the threat is external or internal, SAP Enterprise Threat Detection alerts you to potential attacks in real-time. You have the opportunity to investigate and either dismiss the alert or pursue an actual incident.
- SAP Enterprise Threat Detection provides graphical tools to enable you to navigate the log data. With the log data, you can support forensic analysis or gain new insights into your system landscape. From these new insights, you can create new attack detection patterns and run them regularly against log data as the log data comes in. Any matches to the patterns generate alerts.

UI Field Security (UIF)

- **Solution Class**
  - » **Information Security**
- Capabilities
  - » Masking of sensitive data
- User interface field security provides selective masking to sensitive fields on user screens based on user roles.

UI Logging (UIL)

- **Solution Class**
  - » **Information Security**
- Capabilities
  - » Logging of user interactions
- Solution for logging all user interactions to document when and by whom sensitive information has been accessed. Solution variants are available for Web Dynpro ABAP, Web Client UI, SAP NW BW Access, RFC and Web Services.

About MDS *ap*

MDS *ap* is the successor of Sybase Products with over two decades of history in the EMEA emerging markets. As a SAP Gold Partner, we are dedicated to helping you run businesses better leveraging technologies from SAP as well as from other complementary solution providers. Our technology expertise includes Business Analytics, Data Management, Enterprise Performance Management (EPM), Group Finance Management, Mobility, Omni-Channel Banking, Enterprise Architecture as well as SAP Cloud Solutions. The winning combination of our technical skills, real case experience and industry domain knowledge has allowed us to help many global and regional customers improve business performance and achieve growth targets.

MDS *ap*

www.mdsaptech.com

MDS *ap* Offices

Abu Dhabi – UAE
32nd Floor, ADDAX Building,
Al Reem Island P.O. Box 45652, Abu Dhabi
Tel: +971 2 613 0969

Dubai – UAE
Suite 358, Building 17,
Dubai Internet City P.O. Box 62631, Dubai
Tel: +971 4 39143918

Doha – Qatar
D'Ring Roads, Building No.75,
Street No.250 Airport Area, P.O. Box 22421, Doha
Tel: +974 4440 5000

Riyadh – Saudi Arabia
Al Anouf Building - Malaz - 1st Floor,
Al Ihsa'a St. P.O. Box 295903, Riyadh 11351
Tel: +966 1 479 7623

Kuwait City – Kuwait
Dar Al-Awadh Mall - 2nd floor / IO Center Ahmed
Al Jaber Street - Sharq
P.O. Box 29927 - Safat 13160
Tel: +965 2232 2926

Beirut – Lebanon
Berytech Technological Pole - ESIB-Mar Roukoz
P.O. Box 116 - 5004 - Beirut
Tel: +961 4533 162

Istanbul – Turkey
Nurol Plaza, Buyukdere Cad. No:257
Kat:12 34398 Maslak, Istanbul
Tel: +90 212 3512730

Ankara – Turkey
Bilkent Plaza A-3 Blok No:48
Bilkent - Ankara
Tel: +90 312 266 33 00

Prague – Czech Republic
V Parku 2326/18
148 00 Praha 4 Chodov
Tel: +420 2840 00711

Warsaw – Poland
ul. Woloska 5, Taurus Building
02-675 Warszawa
Tel: +48 2221 25428

Budapest – Hungary
Záhony u. 7., Graphisoft Park C Building
1031 Budapest
Tel: +361 4303 500

Bratislava – Slovakia
Apollo Business Center II, Block C Prievozská 4B
821 09 Bratislava
Tel: +421 2323 32501

For more information on MDS *ap* please visit us at:
www.mdsaptech.com