MDS *ap* GDPR offering

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.

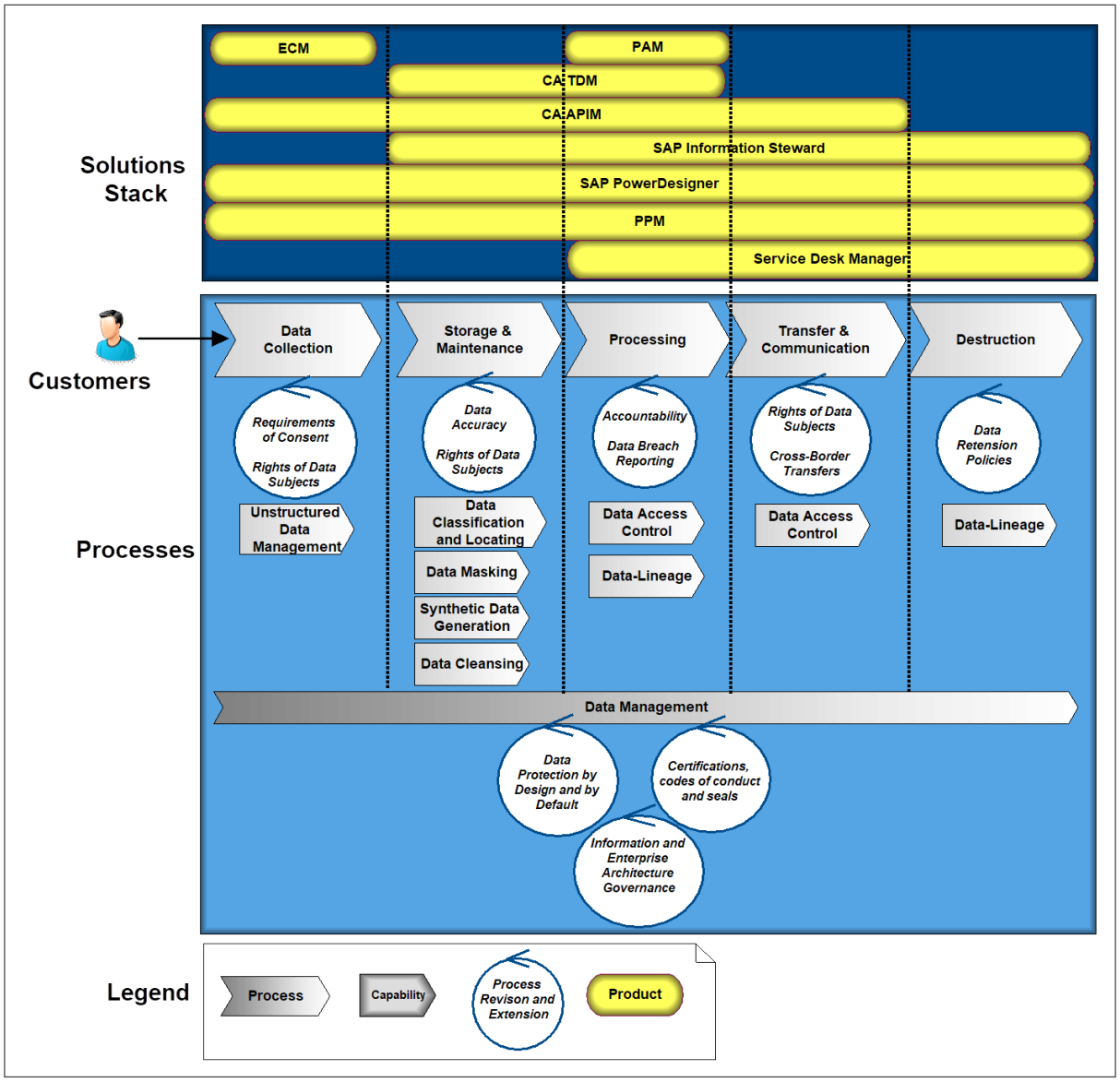
Solution overview – how MDS *ap* can help

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

Reference Architecture for GDPR Compliance

Powered by solutions ecosystem supported by SAP and CA, GDPR compliance challenges and the required holistic solution approach could be summerized 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 and CA offerings can be considered at different stages of data management life-cycle as follows:

1. Personal Data Collection

- Requirement to obtain consent from the data subject for certain 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 semistructured personal data collected may be required to be structured, or else processable by **content management tools,** in order to comply with GDPR.
- Moreover, an organization should be able to monitor all channels of personal data collection to ensure that they comply with the principle of obtaining explicit consent from data subjects for collecting their data. By using **CA API Management solutions,** organizations can avoid continuously checking and modifying their applications involving personal data collection (which is a risky and expensive process), and will be able to control behaviors from a rule-and-policy-oriented solution. In this way, the organization can incorporate rules for gathering consent, informing users about the information requested.

2. 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 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.

3. 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:
    1. 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.

2. Introduction of new policies, or else revision of existing policies relevant to personal data access security.
3. Masking (unmasked) personal data-in-motion or at-rest whenever possible without effecting current application and business logic.
4. 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). Accross 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).

Ad 1. Whether they're obtained maliciously or used inappropriately by a valid user, exploited privileged user accounts are the common thread of most data breaches, and therefore represent high risk for GDPR compliance. CA Privileged Access Manager is proven solution for privileged access management in physical, virtual and cloud environments enhancing security by protecting sensitive administrative credentials, controlling privileged user access, proactively enforcing policies and monitoring and recording privileged user activity across all IT resources. IT Security as well as Data Privacy Officer are then able to audit, notify and report all events and potential incidents instantly.

When organizations need to make their current applications accessing personal data compatible with this new regulation, while at the same time avoiding incurring the cost of modifying existing applications, their only option is to utilize from APIs. The CA API Management suite makes it simple for enterprises to address the challenges of information sharing in the application economy. The solution combines advanced functionality for back-end integration, mobile optimization, cloud orchestration and developer management, and is unique in its ability to address the full breadth of these enterprise API management requirements.

Ad 2. 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.

Ad 3. One way to avoid exposing personal data to test environments is to not provision it in the first place, even in a masked form. Synthetic data generation offers a technique that could enable organizations to transition to fully virtualized test environments by masking personal data while retaining their logical and referential usability constraints. CA Test Data Manager helps companies comply with requirements of personal data privacy by anonymizing or creating synthetic data for use in testing.

Ad 4. Data profiling features of CA Test Data Manager can also help locate personal data access points on test environments by identifying exactly where sensitive data is stored enterprise-wide, and by using statistical analysis to find personal data stored across multiple file formats and applications.

4. 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 accross organizational borders bound to be detectable and controllable. Such transfers or communications may involve unstructured or semistructured data formats (biometrics, e-mails, documents, file transfers etc) in addition to structured ones, possibly moving accross geographically diverse sites within the organizational boundaries or accross B2B or B2C channels over various communication protocols and media (ftp, web, private, hybrid, or public cloud etc). Accross all channels of personal data movement, highly sensitive, precise, holistic and high performance data movement control and DLP (data loss prevension) 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.

- In order to monitor and then obtain a complete control on personal data transfers and communications within and accross organizational borders over an enterprise scale, the CA API Management suite will help create unified control points, allowing an organization to regulate policies or processes required by Rights of data subjects and cross-border data transfers and binding corporate rules.

5. 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 retension 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 retension in accordance with the categories of personal data, legal basis of their retension and rules on retension period enforced by regulations.

6. 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

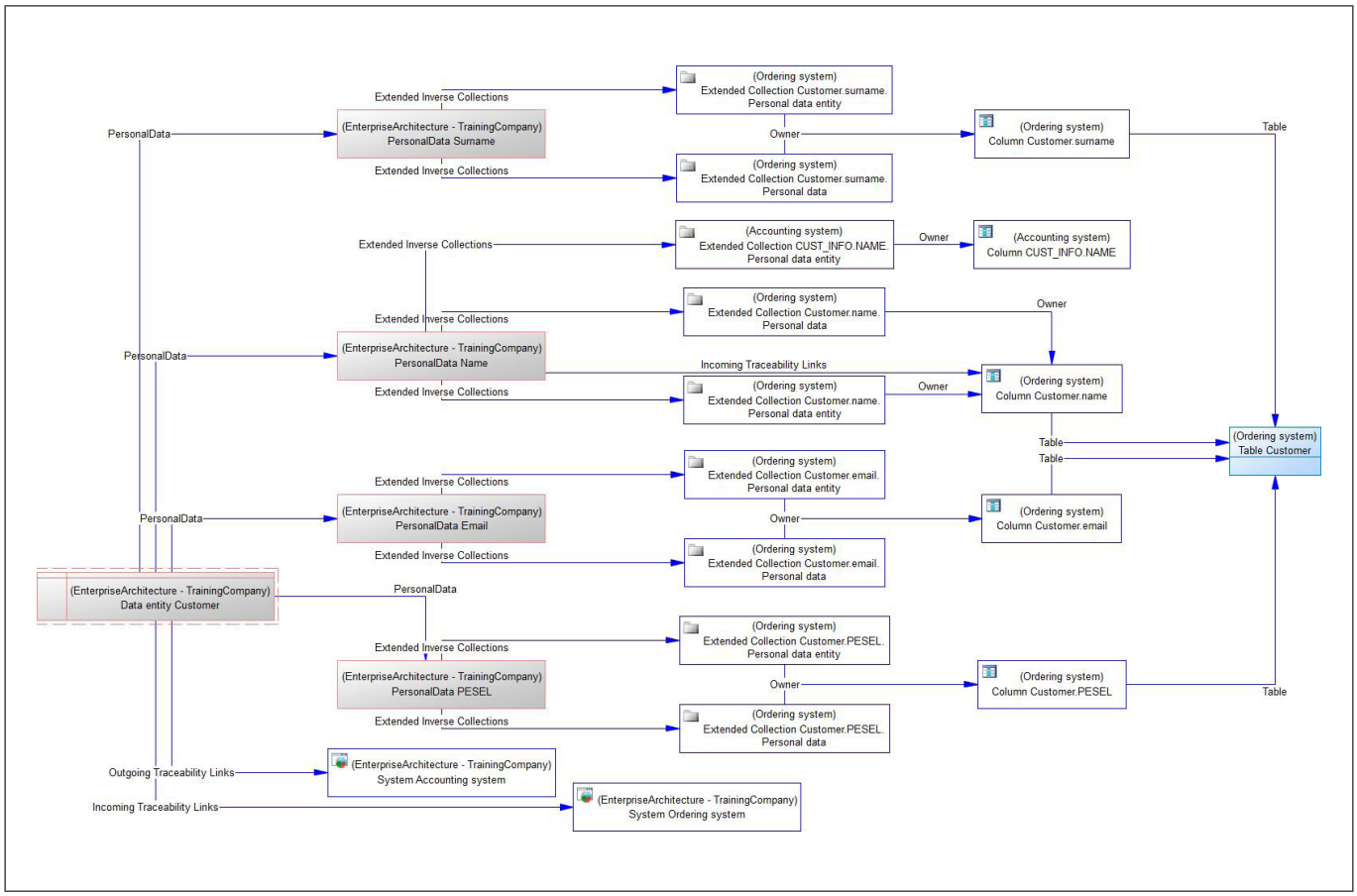
SAP PowerDesigner provides tools for the many different areas, including in particular:

- 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)

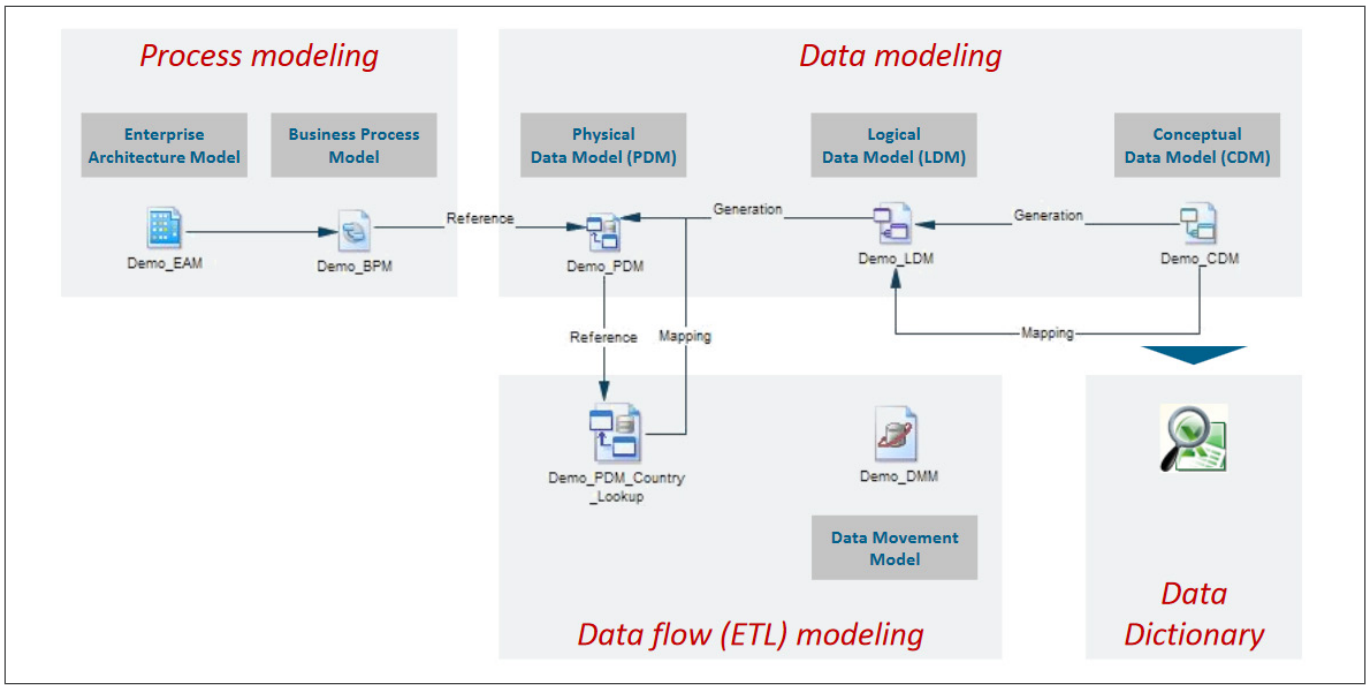


- Automated preparation of queries for gathering personal data related to specific person
- Documentation of applied data protection mechanisms in the organization
- When introducing new systems or making changes in the IT environment - analyzing the impact of the change on the protection of personal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

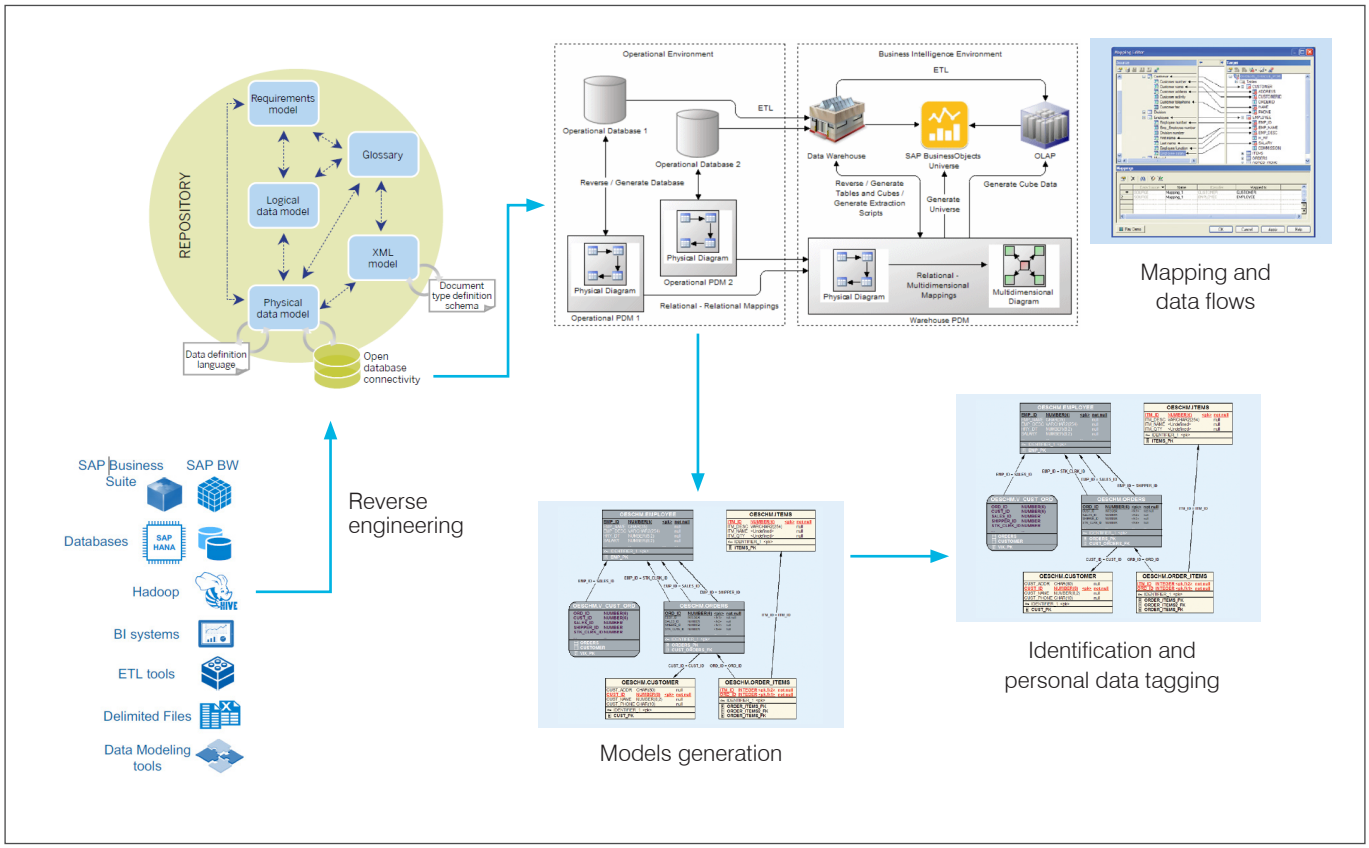
SAP PowerDesigner allows to visualize the information architecture. It provides tools for tagging and documentation of the storage of sensitive data - at the data model of applications using transactional and analytical databases (data warehouses, data marts):

- 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:

SAP PowerDesigner is a heterogeneous platform for modeling and description of the architecture, supporting documentation and change management in the company by delivering understandable visualization of complex architectural artifacts.

SAP Information Steward:
multisource platform for personal metadata discovery and data profiling allows access to databases, applications, ETL tools, BI tools and modeling tools, categorize and catalog personal data, creates technical metadata documentation and tagging, allows data governance and ownership.

GDPR Data Search Extension:
ActiveX Add-in for SAP Power Designer, which implements the functionality required to provide to data subject a copy of personal data concerning him or her which are processed by the organization in databases. This is done based on mining of physical database metamodels to search for the personal data of specific person based on unique search criteria. As a result, information is provided in commonly used electronic form – csv file generated.

Repository of consent:
Extension do GDPR Data Search Form mechanisms which is based on repository storing the information required to give to the data subject the right to obtain from the data processing entity confirmation if or not personal data concerning him or her are being processed.

This repository is prepared to include information like: the purpose of the processing, consents given by the data subject or other lawsuit purposes, the categories of personal data concerned, the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations, period for which the personal data will be stored.

CA API Management:
provides reliable connectivity between data, people, apps and devices. You can aggregate and orchestrate data from multiple data sources into modern REST APIs almost instantly. Whether your data is in legacy systems, disparate databases or the cloud, you'll be able to bring it all together to power new digital initiatives at scale in modern apps or SaaS applications.

CA Privileged Access Manager:
protection against personal and data breaches through careful monitoring of privileged user credentials. Helps secure data with a focus on trusted digital identities and breach alerts. Most security breaches involve the use or abuse of privileged credentials. The CA Technologies solution helps organizations continually monitor privileged user accounts, assess risk and detect malicious activity.

CA Test Data Manager:
the process of providing, distributing and managing test data for development teams. Helps companies comply with data privacy by anonymizing or creating synthetic data for use in testing. By using synthetic data, organizations will avoid the pitfalls associated with masking production data which is one of the GDPR requirements.

CA Project & Portfolio Manager:
enables to monitor and manage companywide compliance regulations, in addition to the traditional project management office that manages the implementation of IT projects. For most organizations, getting into compliance with these various regulations will require a massive project implementing and impacting business systems and processes.

CA Service Desk Manager:
drives all data subject's request workflows related to their GDPR rights across DPO and multiple Data Controllers while maintaining auditability of all steps and proactively enforcing due dates to avoid penalties for noncompliance; tracks security incidents related to personal data.

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