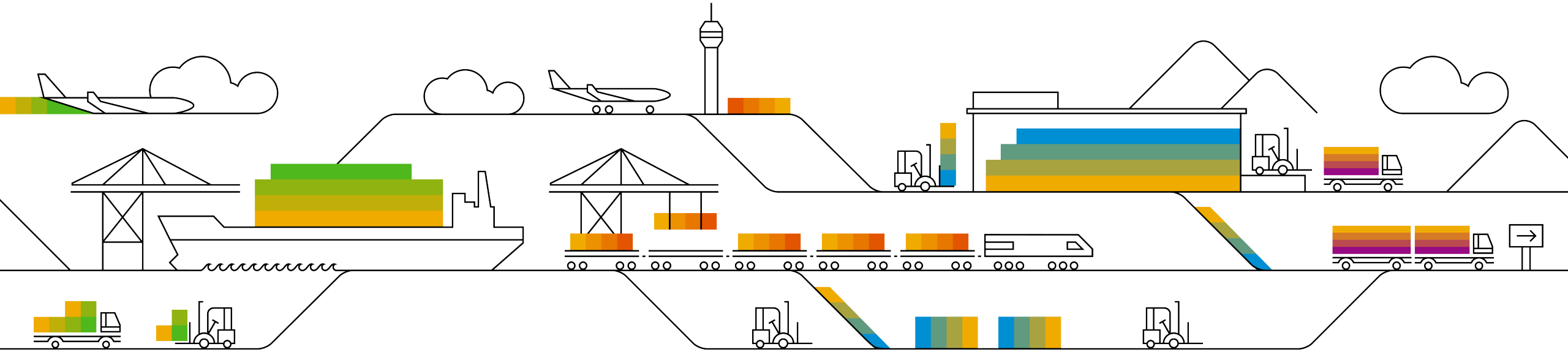


Nástroje pre podporu GDPR
nielen pre SAP systémy

Peter Mravčák

Solution Architect
SAP Slovensko s.r.o.

Run Simple

GDPR Recap

Codes of Conduct & Certification

- Help demonstrate accountability

Controllers & Processors

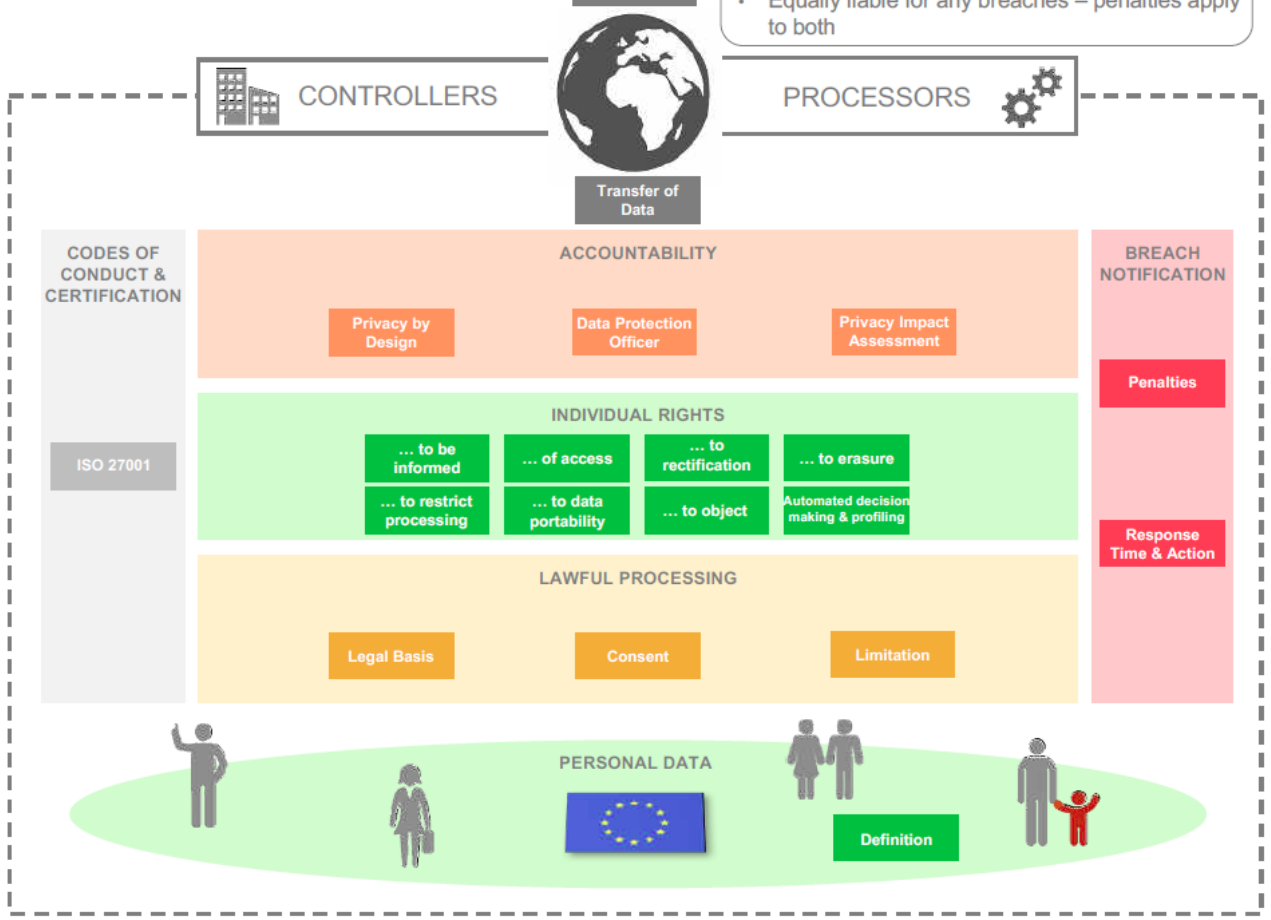
- Controller is accountable for failures of data processor
- Equally liable for any breaches – penalties apply to both

Accountability

- Produce and maintain evidence of actions to achieve compliance
- Privacy risks assessed and must be built-in to product development
- Data Protection Officer needed for companies with large-scale processing of personal data

Lawful Processing

- Individual must provide active consent for each personal data processing activity
- Personal data only to be used for specific purposes, limited to only what is necessary, kept accurate & up-to-date, not stored for longer than necessary
- Personal data must be processed securely and so the subject is identified only when necessary



Individual Rights

- Can request deletion of personal data (includes backups, archives and that shared with 3rd parties)
- Can request their personal data in machine readable form and/or have sent to another company
- Businesses must not (usually) charge and must respond <1 month.

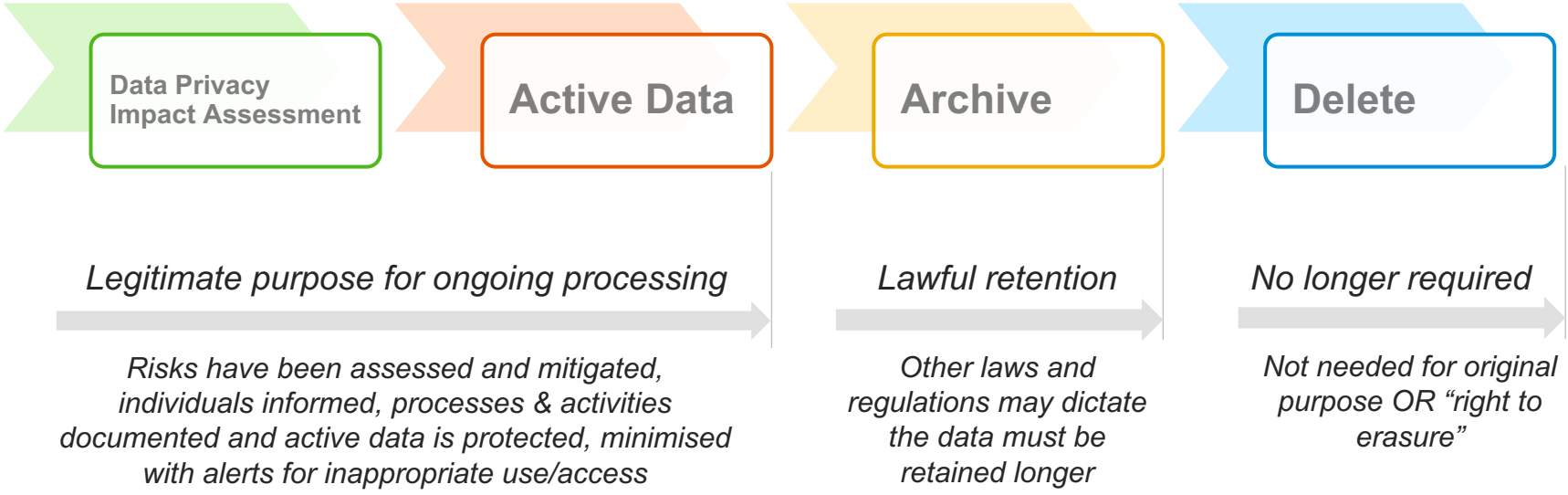
Breach Notification

- Mandatory notification to authority within 72 hours of becoming aware
- Communicate to affected individual(s) without undue delay
- Maximum fine of 4% annual revenue or €20M whichever is greater

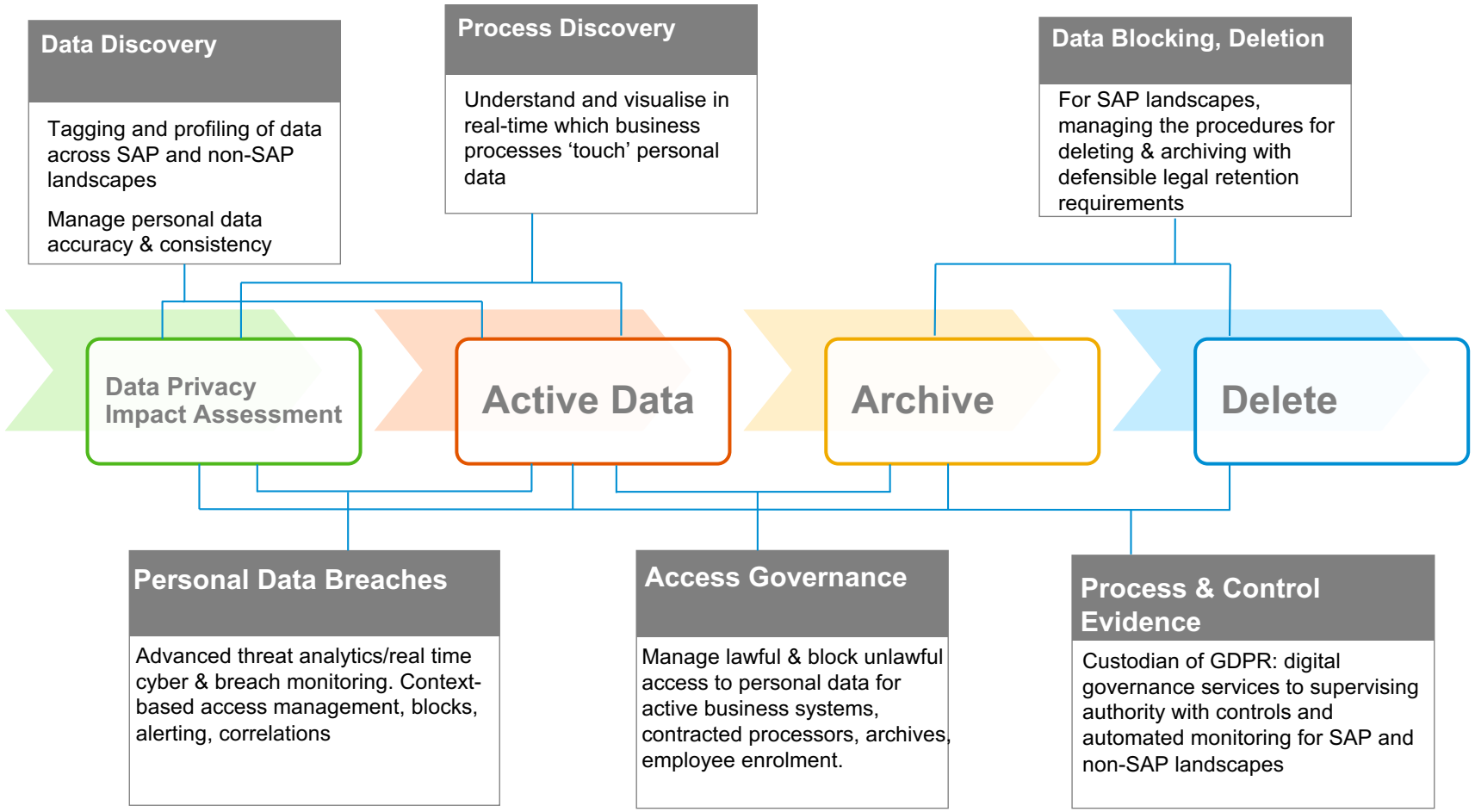
Personal Data

- Includes online identifiers such as IP-address, location & genetic data
- Pseudonymised data can still be in scope
- Parental consent required for children under 16

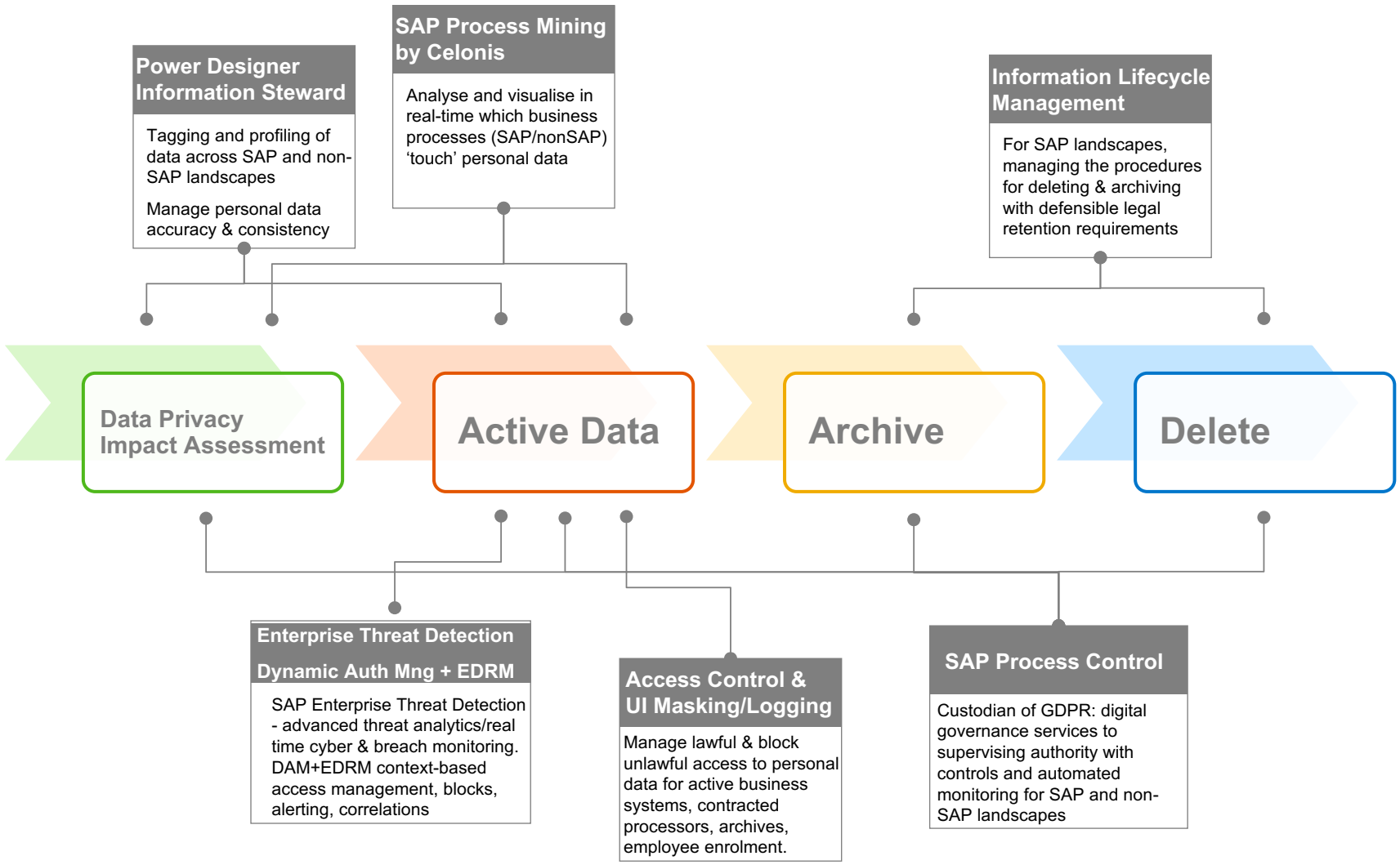
Personal Data Lifecycle



SAP Capabilities



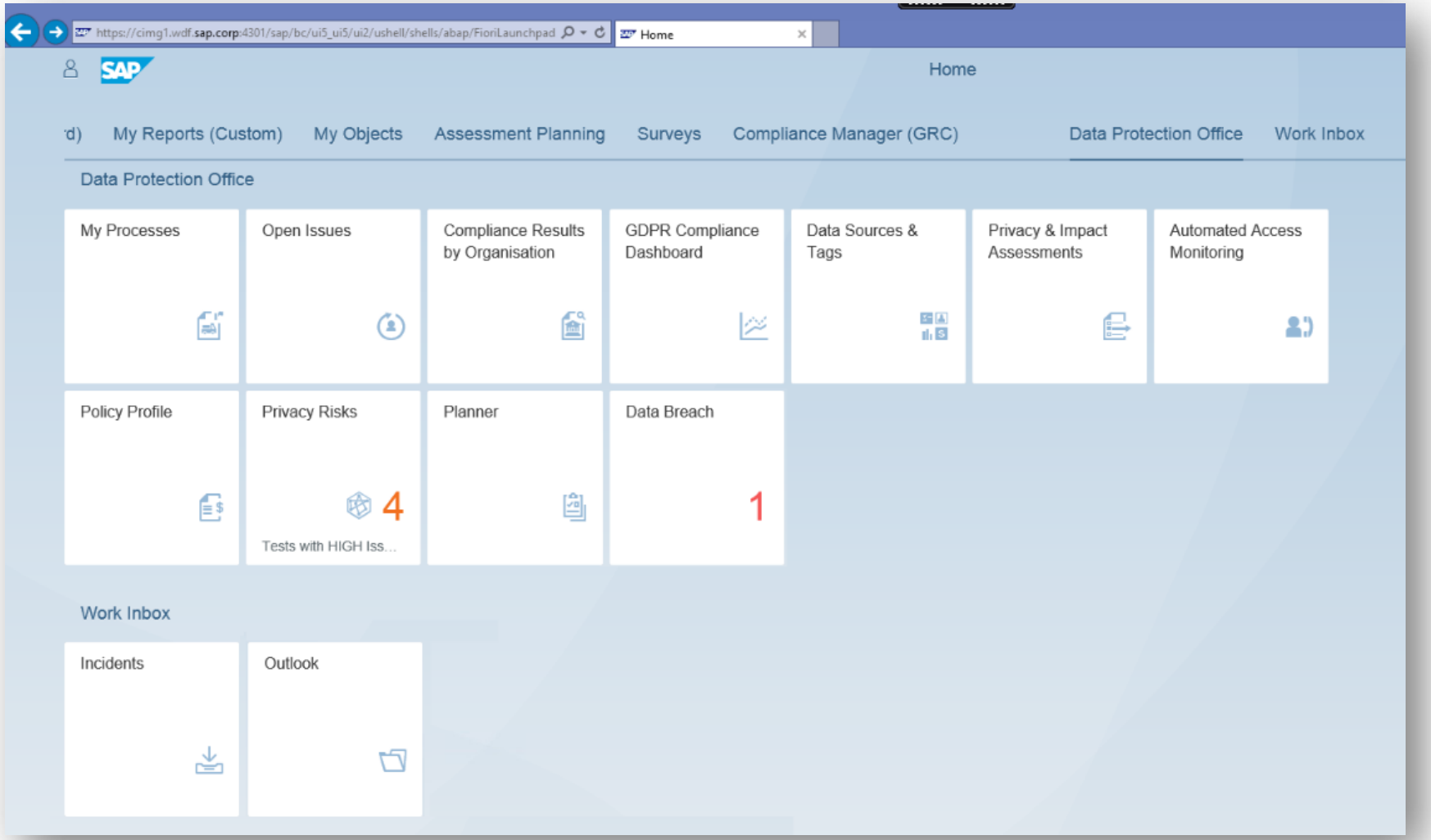
What are the major SAP products that help?



GRC & Security for GDPR

- "The controller shall … be able to demonstrate compliance with, paragraph 1 ('accountability')."
- Regulator: "Accountability, good governance, sustainable procedures"
- Privacy by design and default
- Privacy impact assessments
- Engage DPO - transparency into state of compliance
- Reduce Cost of Compliance: Process Control with ownership & automation
- Breach management

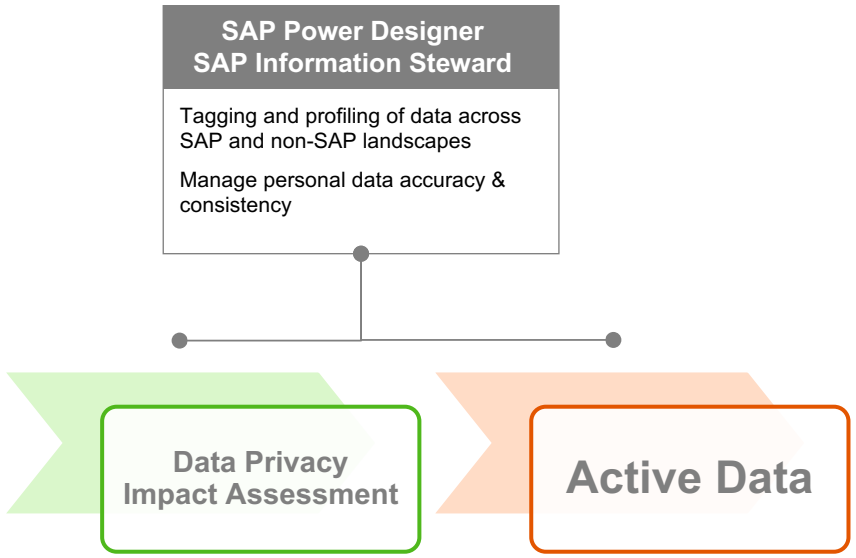
The Goal



SAP Power Designer
SAP Information Steward

Where Does Personal Data Exist In My Landscape?

SAP Power Designer / SAP Information Steward



Value for GDPR

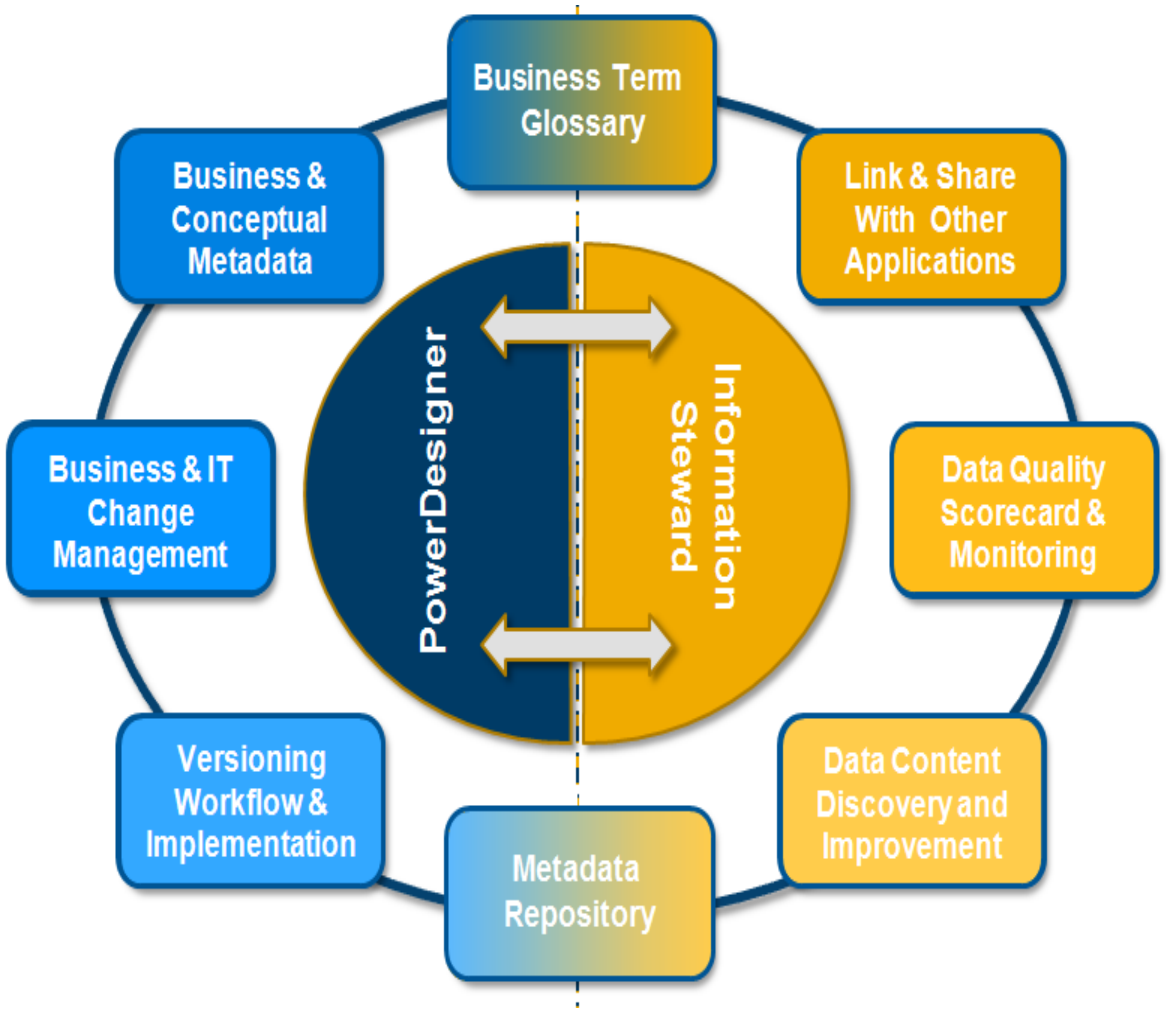
- Tagging and profiling of data across SAP & non-SAP landscapes
- Analyse repositories for personal data types
- Lineage analysis to create transparency on data flows
- Manage data accuracy & consistency

Full Lifecycle Metadata Management

From Discovery, Quality and Monitoring to Architecture Driven Change

SAP Power Designer

Design time, define the environment



Operational time, apply to given landscape

SAP Information Steward

SAP Power Designer

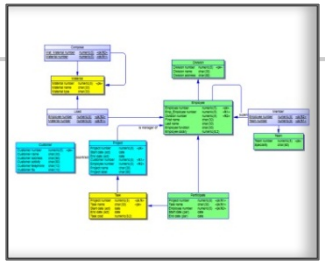
Solution Business Overview

Describe

Reverse engineer to build current state

Map context

Build relationships

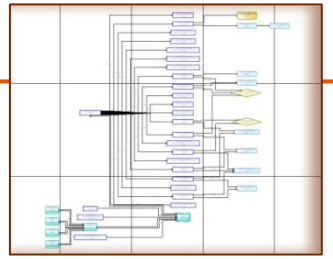


Analyze

Understand impact

Determine mappings

Build plan

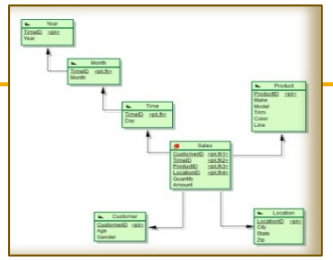


Define

Complete mappings

Ensure completeness

Build future state

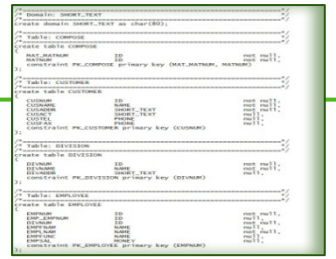


Execute

Communicate architecture & plan

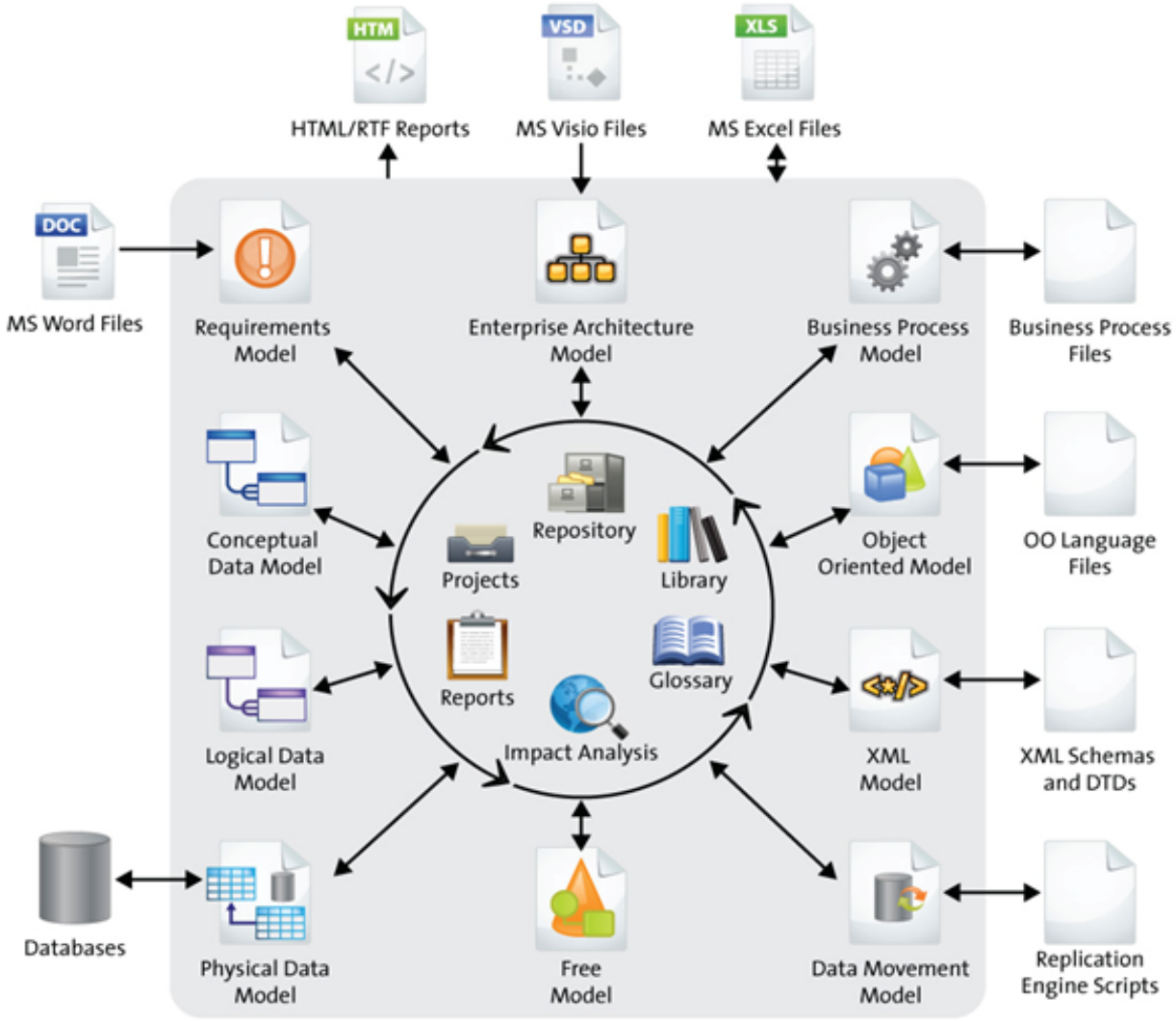
Deliver source extraction scripts

Build database schema



SAP Power Designer - Unified Enterprise Modeling

SAP's EA tool



SAP Information Steward

Discover, define, monitor, and improve quality of data assets

Discover

Understand and catalog enterprise data

Define

Rules and ownership

Monitor

Quality continuously

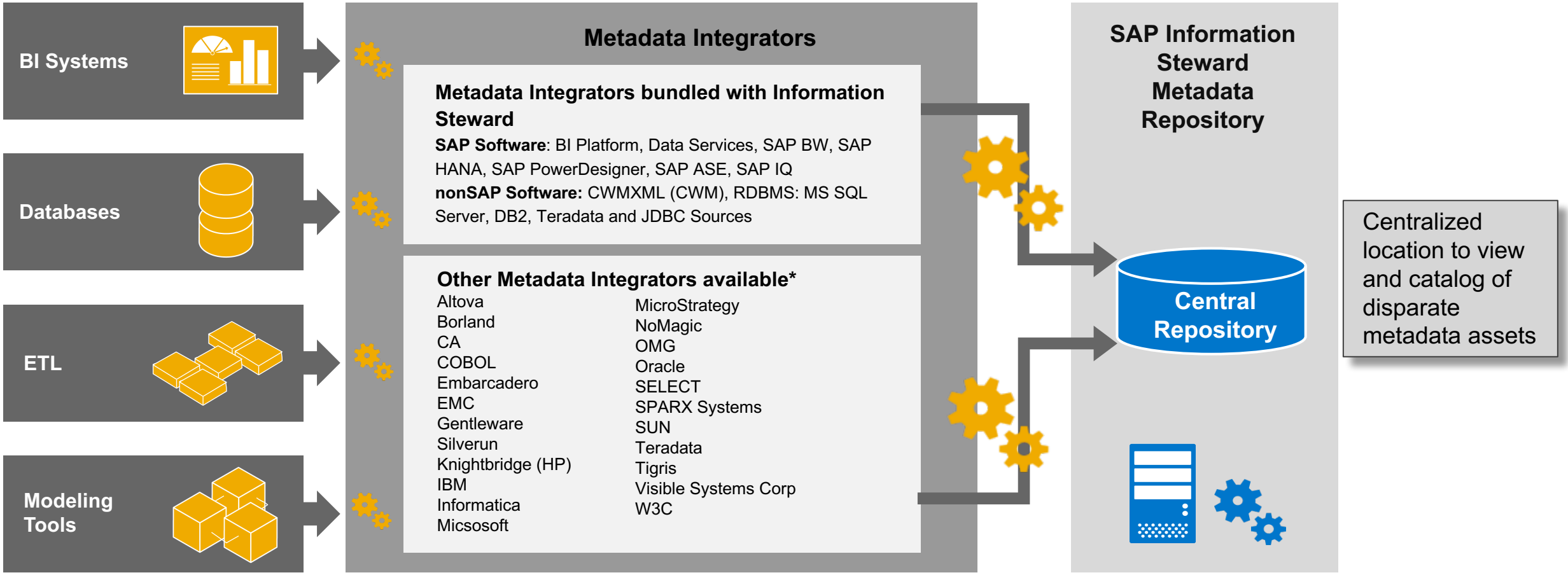
Improve

Data quality and governance

Empower business and IT users with a single environment to manage the quality of their enterprise data assets

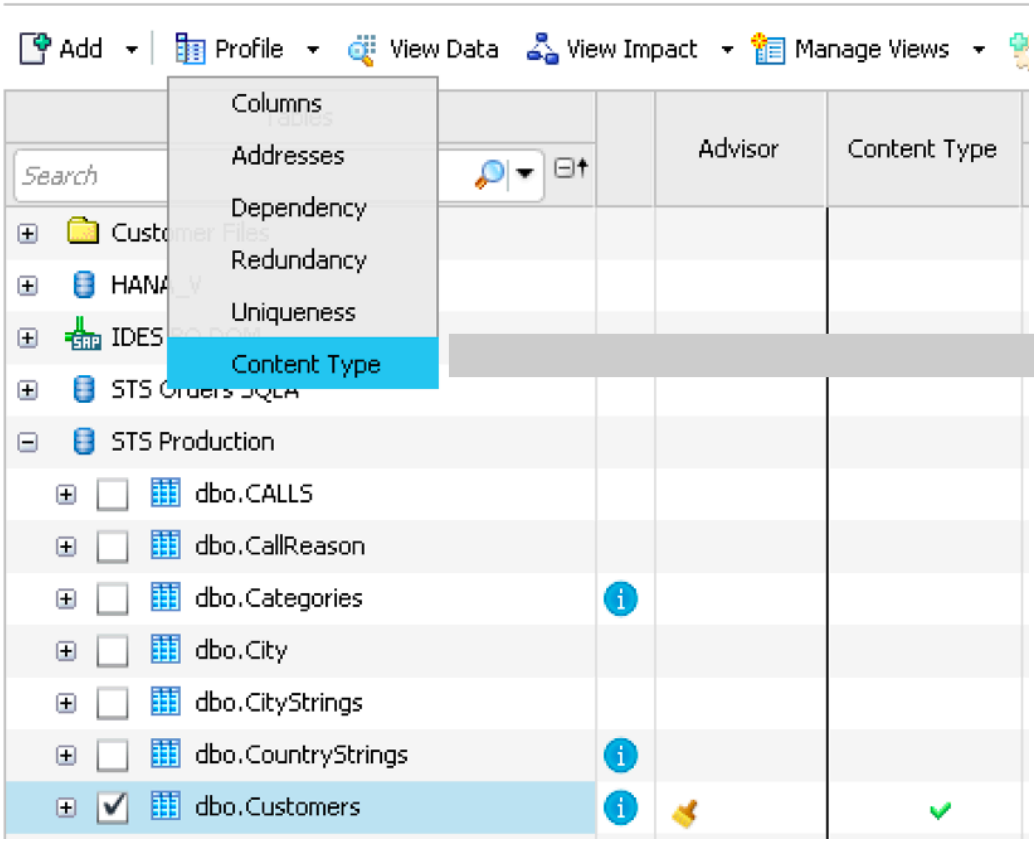
SAP Information Steward

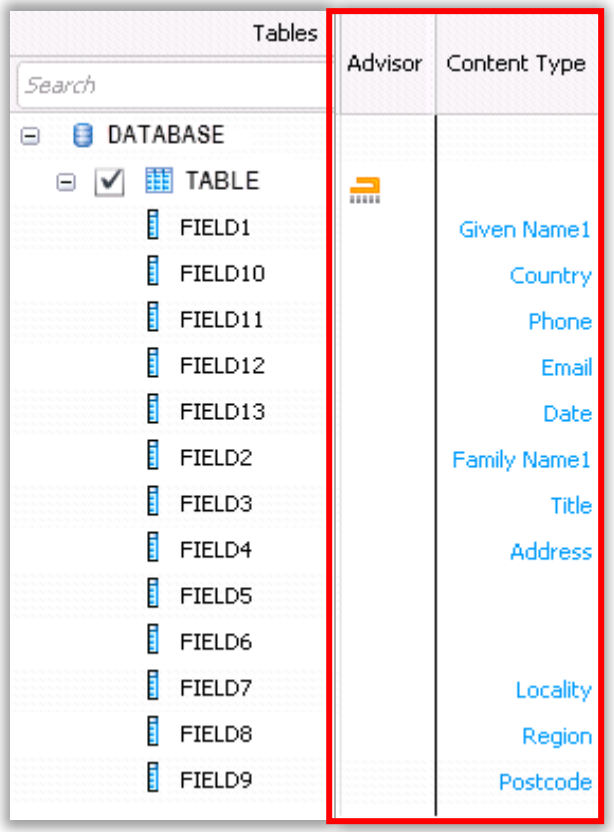
Metadata discovery & catalogue



SAP Information Steward

Identify content / data behind the column names





SAP Information Steward

Out of the box Identification of Personal data

Content Types

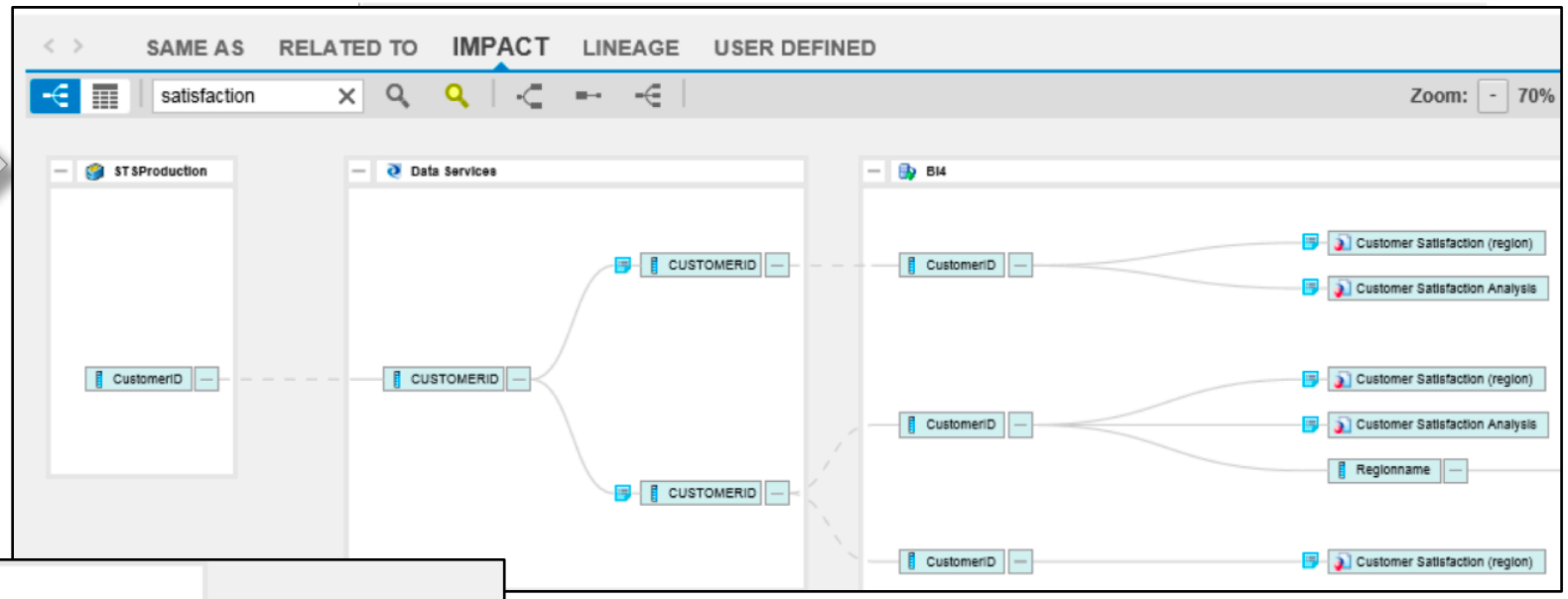
New | Edit | Delete | Enable | Show Dependencies | Import | Export | Refresh

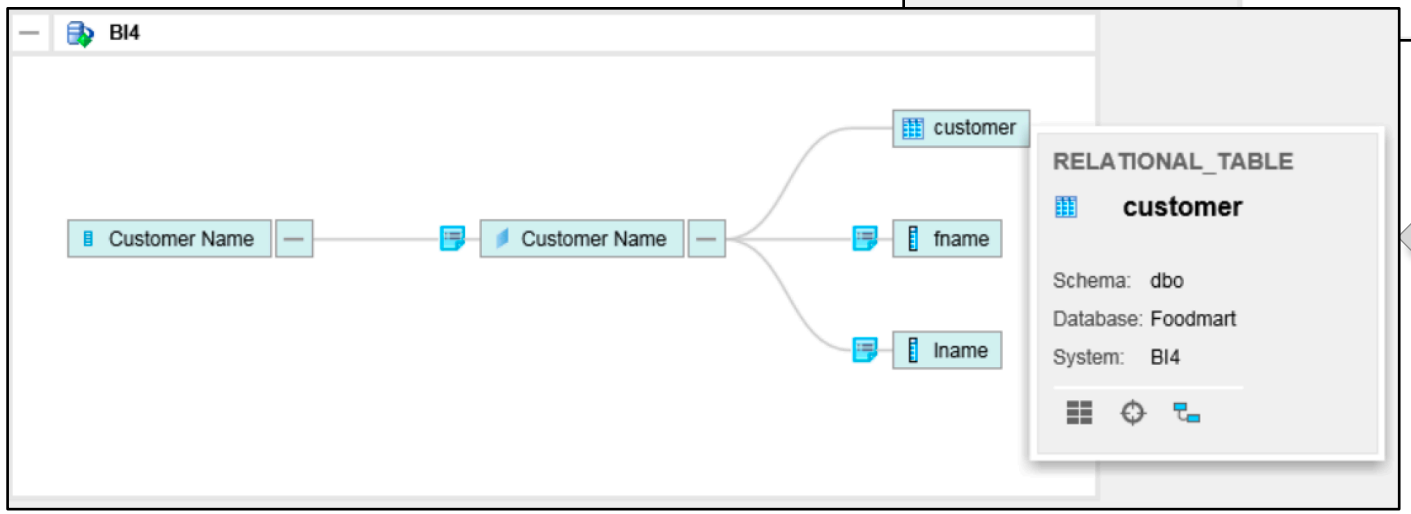
Name	Description	Custom	Enabled	Status
Address Line	All components that make up the street or postal address, such as 1050 Main Street.		✓	
Building Name	The building name for the address, which in some countries is a formal component in the address. For example, in the U.K. an...		✓	
City	City, town, suburb, or a subcity component such as district, neighborhood, or subdivision within a city.		✓	
City Region Postcode	City, region, and postcode combined in one column, such as Chicago IL 60640.		✓	
Country	Country, such as Ukraine or France.		✓	
Credit Card		✓	✓	
Date	A day of the month or year such as, 29 Oct, 2012 or 13/10/12.		✓	
Email	Electronic address used for exchanging digital messages.		✓	
Firm	Organization's name, location, or both.		✓	
First Name	Person's given name, such as Mary or Robert.		✓	
Full Address	The entire address in one column. The single address content type is valid only in Chinese and Japanese scripts. For example,...		✓	
Honorary Postname	Person's postname indicating certification, degree, or affiliation, such as CPA.		✓	
Last Name	Person's family name, such as Smith or Hamilton.		✓	
Maturity Postname	Person's postname indicating heritage, such as Jr. or III.		✓	
Person	Person's whole name combined in one column, such as Dr. Robert Hamilton III. This column may also include a person's title.		✓	
Person or Firm	Some records contain a person's name and some records contain an organization's name. For example, Person or Firm could b...		✓	
Phone	String of numbers that a phone user can dial to reach another phone.		✓	
Postcode	Postcode or ZIP Code.		✓	
Prename	Person's prename, such as Mr., Mrs., or Dr.		✓	
Product_Name		✓	✓	
Region	Region or state.		✓	
Secondary Address	Apartment or suite information, for example, the Apt 315 portion of 1050 Main St. Apt 315.		✓	
SSN	Nine-digit number assigned to U.S. citizens and residents issued by the United States Social Security Administration.		✓	
Street Name	Street description, for example, the Main Street portion of 1050 Main Street.		✓	

SAP Information Steward

Meatadata discovery & catalogue

Impact Analysis upstream use

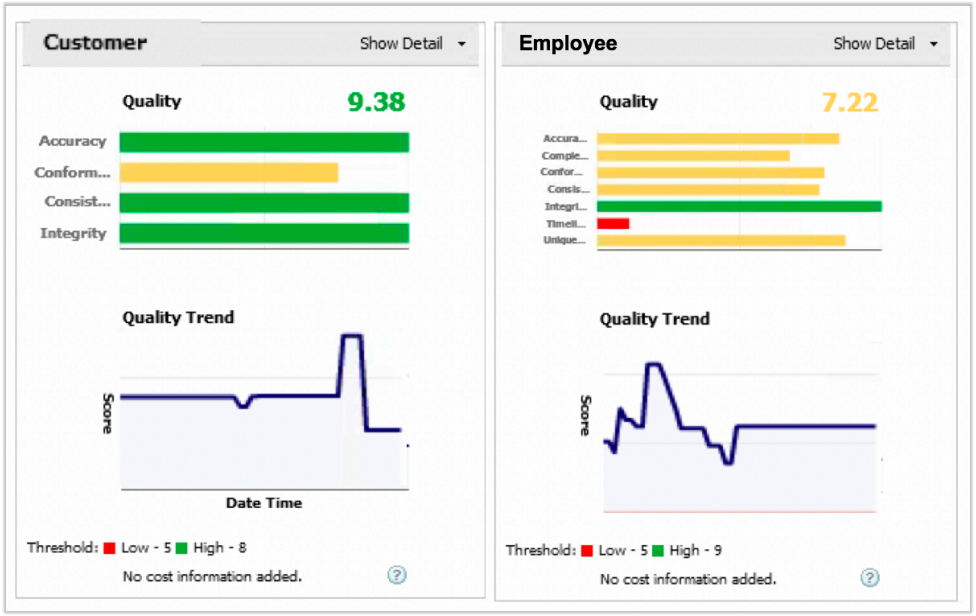




Data Lineage for data origins

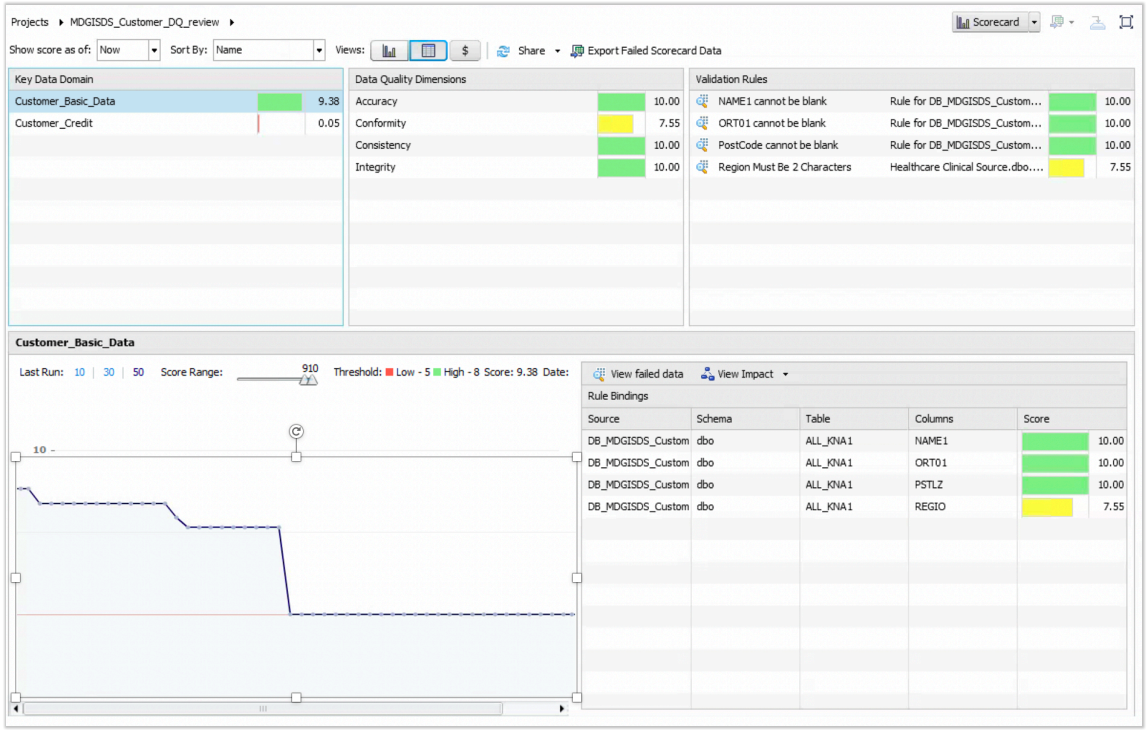
SAP Information Steward

Monitor and improve quality of data



Report on the accuracy of personally identifiable data using Data Quality scorecards

Drill down to explore problem areas, by rules, subject areas and systems.



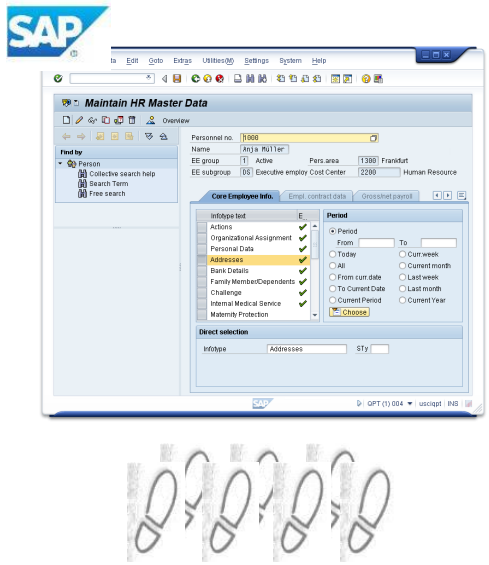
SAP Process Mining by Celonis

SAP Process Mining by Celonis

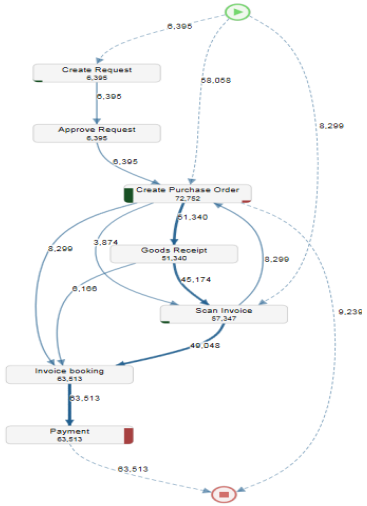
Knowing what's going on in your business

Analyze your business processes in real time and achieve the maximum level of transparency Process Mining (aka Automated Business Process Discovery) knows, analyzes and visualizes all of the process data saved in your IT systems.

Digital footprints from IT systems



Visualization of actual processes



Value for the customer

Efficiency
Identify bottlenecks and decrease cycle times

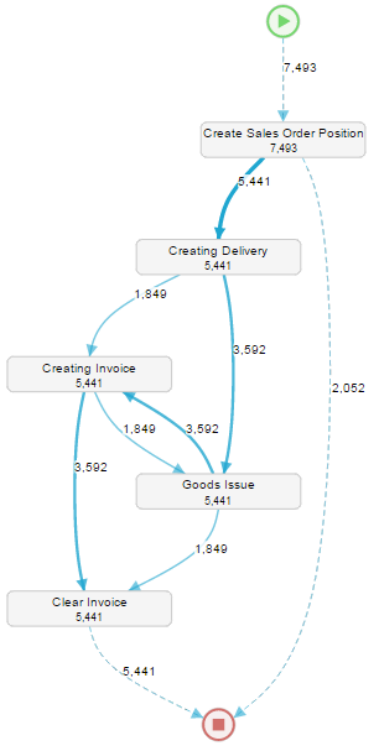
Compliance
Detect non-compliant processes or fraud

System usage
Compare process models to actual "As-Is" process

Getting all Process Variations

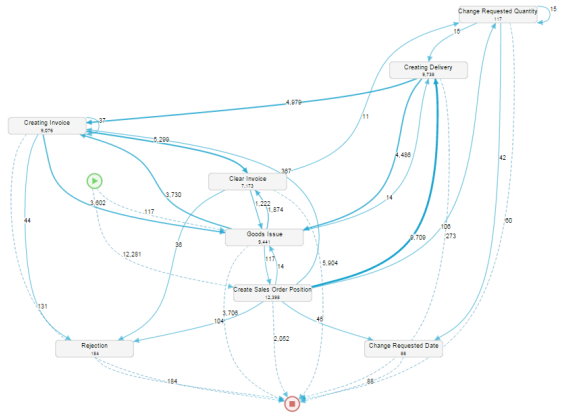
See the happy paths

The level of detail of the process can be **seamlessly adjusted.** The number of variants displayed can be reduced in order to show only the **core process.**



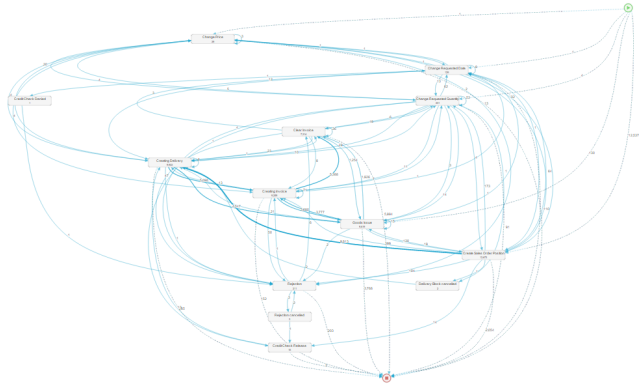
Explore deviations

Increasing the number of variants, i.e. the level of detail, the process will reveal **less common paths and activities**. This is great to spot **deviations** and **inefficient loops**.



Get the big picture

Going full-throttle on the process, one may display **100% data coverage**. Nothing escapes the watchful eye – especially if this augmented with **drill-down functionalities** to spot long-runners, unusual process paths, etc.



SAP Process Mining by Celonis
take

- Visualisation of complex business processes to identify:
  - The real “As Is”
  - Non Compliance
  - Inefficiencies

- Real Time monitoring not just a once off analysis

- Opportunity for significant process streamlining and/or savings

SAP Process Control

SAP Process Control

Reporty na podporu rozhodovania

Automatické monitorovanie systémov

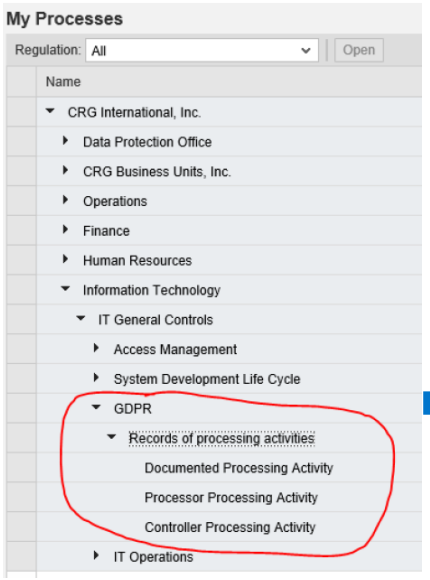
Dokumentácia kontrol a politík, prepojenie na regulácie

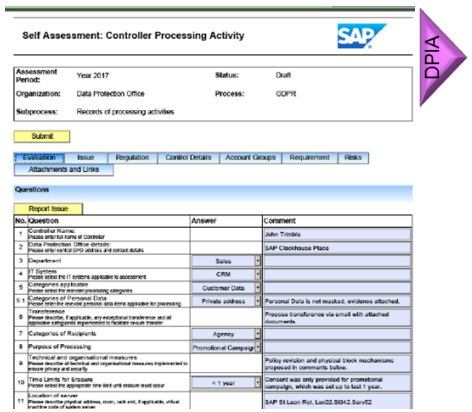
Periodické posúdenie rizík pre určenie rozsahu a testovacích stratégií

Vyhodnotenie kontrol, vytváranie a spracovanie výnimiek

SAP Process Control

Process Guardian





DPIA

Purpose

Instance = Process

Consent, Contract, Legal obligation, Protect vital interest, Public interest, Legitimate business interest

Controller, Processor duties

Risk, Consequence

Data breaches

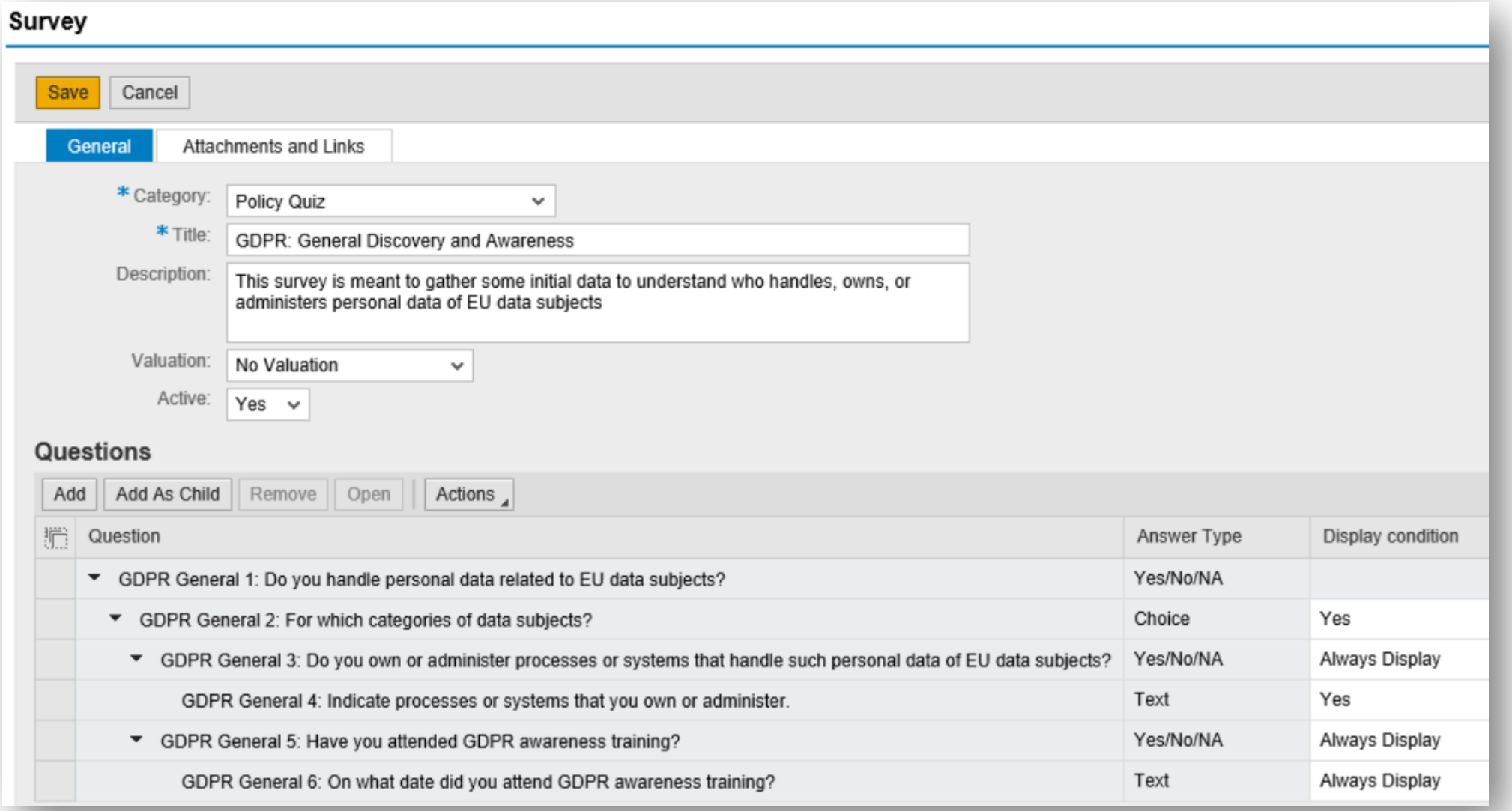
DPO, Accountability

Regulator wants *evidence* the following rights of the natural person are carried out on an on-going basis:

- Their data can only be processed if one of the grounds on the left can be shown - per process.
- Right to request blocking & deleting of their data from active procedures.
- The risk associated with processing their data has to be assessed.
- Only the defined and currently agreed processing in scope takes place.
- Data deleted as soon as all legal retention periods have passed, the data is blocked during retention for legal grounds, or if in dispute.

Discovery survey (policy quiz)

Example



Data protection impact assessment (excerpt)

Questions

Add | Add As Child | Remove | Open | Actions

Question	Answer Type	Display condition
GDPR DPIA1: Is the establishment of your activities in European territory?	Yes/No/NA	
▼ GDPR DPIA2: Do you handle information that can identify other people through one or more of the following activities: Web browsing, account management, delivery, payments…?	Yes/No/NA	
GDPR DPIA2a - Web browsing?	Yes/No/NA	Yes
GDPR DPIA2b - Account or subscription management?	Yes/No/NA	Yes
GDPR DPIA2c - Sales or service delivery?	Yes/No/NA	Yes
GDPR DPIA2d - Payments and transactions	Yes/No/NA	Yes
GDPR DPIA2e - Marketing and promotion	Yes/No/NA	Yes
GDPR DPIA3: For what purposes or legitimate interests do you process the information?	Text	
▼ GDPR DPIA4: Are you relying on consent to process information of individuals?	Yes/No/NA	
GDPR DPIA4a: How have you obtained the consent of individuals?	Choice	Yes
GDPR DPIA4b: If individuals have given their consent, can they withdraw it with ease and whenever they want to?	Yes/No/NA	Yes
GDPR DPIA4c: Are the consequences of withdrawal of consent significant for individuals?	Yes/No/NA	Yes
GDPR DPIA5: On what basis do you process the information?	Choice	
GDPR DPIA6: Is it possible for the individual to restrict the purposes for which you process the information?	Yes/No/NA	
GDPR DPIA7: Are decisions being made on the basis of the information you process?	Yes/No/NA	

Subprocess

Human Resource Management	Process
Benefits	Process
Hiring and Termination	Process
Employee Onboarding and Setup	Subprocess
Blocking / Deletion - rejected candiate	Control
Blocking / Deletion - rejected candiate	Control
Data Privacy Impact Assessment performed	Control
Purpose and lawful reasons documented	Control
Transference of data within policy	Control
Access to data is managed	Control
Retention of data is managed	Control
Consent is managed appropriately	Control
Procedure for rejecting candidates	Subprocess
Blocking / Deletion - rejected candiate	Control

Subprocess: Procedure for rejecting candidates

Parent Organization: Human Resources | Parent Process: Hiring and Termination | Allow Local Changes: Yes | ID: 50008709
Timeframe: Year 2017 | Effective Date: 01/01/2017

Save | Cancel

General | Controls | Regulations | Control Objectives | Account Groups | Risks | Attachments and Links

* Name: Procedure for rejecting candidates
Description: Procedure for rejecting candidates
Industry-specific: Yes / No

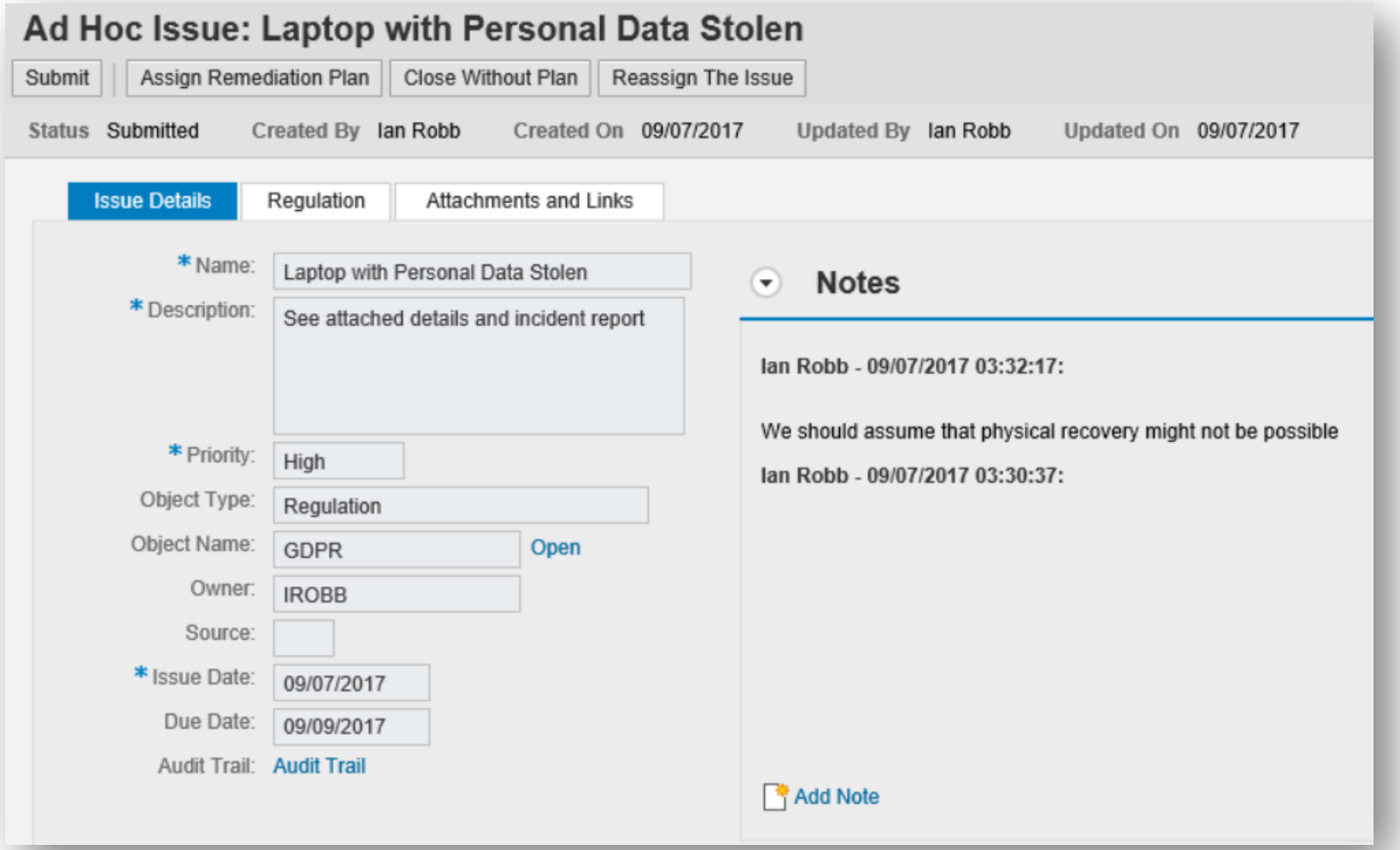
* Valid From: 01/01/2017
* Valid To: 12/31/9999
Transaction type:
Business Subprocess:

User-defined fields

Purpose: Recruiting
Lawful Processing: Consent X | Legal Need | Business Need X
Category: Applicants
Personal Data: Private address and telephone
IT System: Talent Management

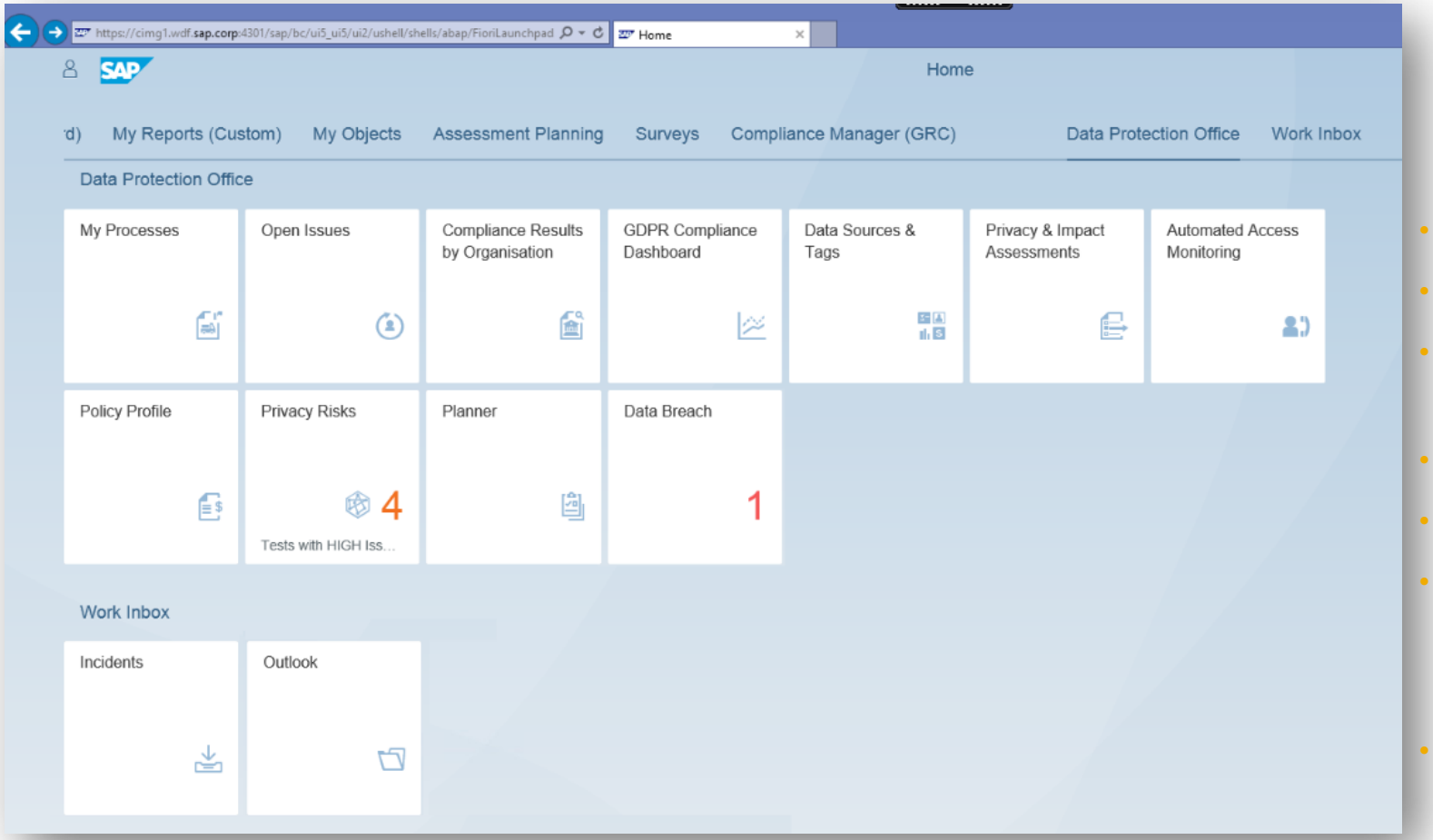
Ad hoc issues

Issues related to the GDPR can be documented as ad-hoc issues



SAP Process Control

System of record for DPO & Audit



- Process register that impact or are impacted by GDPR
  - Attach GDPR data type, presence of sensitive data (high risk)
  - Roles and responsibilities related to processes
- DPIA engine, results, linked to processes
- Lawful processing linked to processes
- Policy and legalisation compliance management
- Employee compliance
- Third party compliance
- Data breach register, governance thereof
  - Link breach to system to process to owner
- Evidence of technical controls in operation, design effectiveness
- Manual and automated controls
- Include control evidence from Access Control
- Link to level of risk and risks (ERM)

Summary

Business Value in GDPR from SAP Solutions

1. Reduces cost of compliance (*not* just GDPR), likelihood of a fine
2. Reduces organizational and individual risk, link to business planning/mission
3. Good data governance
4. Good data minimisation
5. Reduce cybersecurity & reputational risks
6. Smaller, better organized IT toolset
7. Address user privilege administration
8. Greater organizational agility

Ďakujem za pozornosť

Kontakt:

Peter Mravčák

Presales Solution Architect
SAP Slovensko s.r.o.

peter.mravcak@sap.com

Run Simple

© 2017 SAP SE or an SAP affiliate company. All rights reserved.