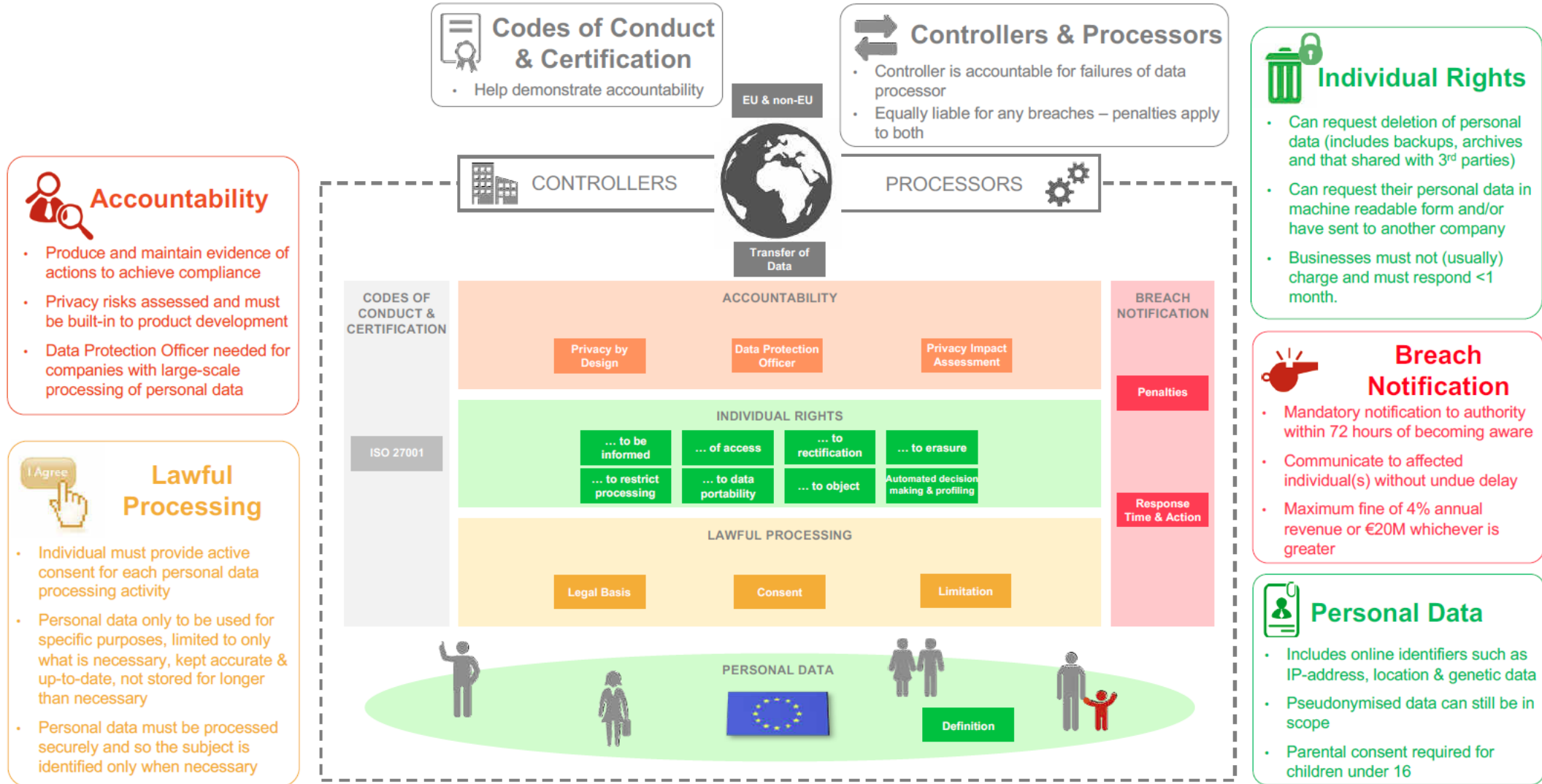


# Nástroje pre podporu GDPR nielen pre SAP systémy

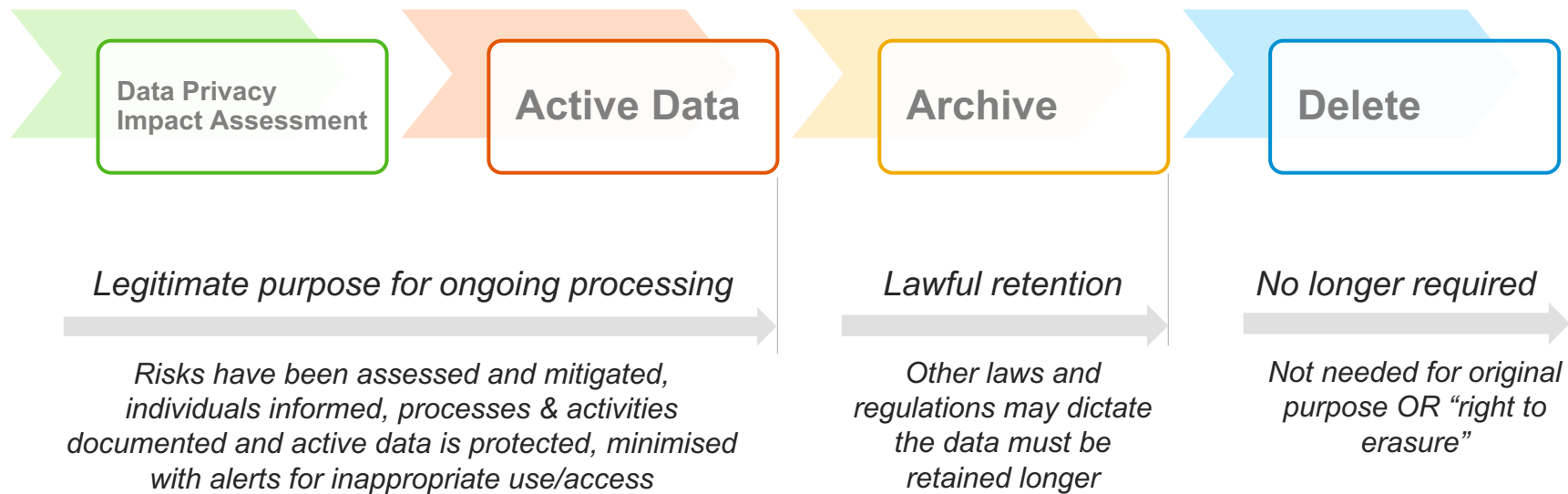
**Peter Mravčák**

Solution Architect  
SAP Slovensko s.r.o.

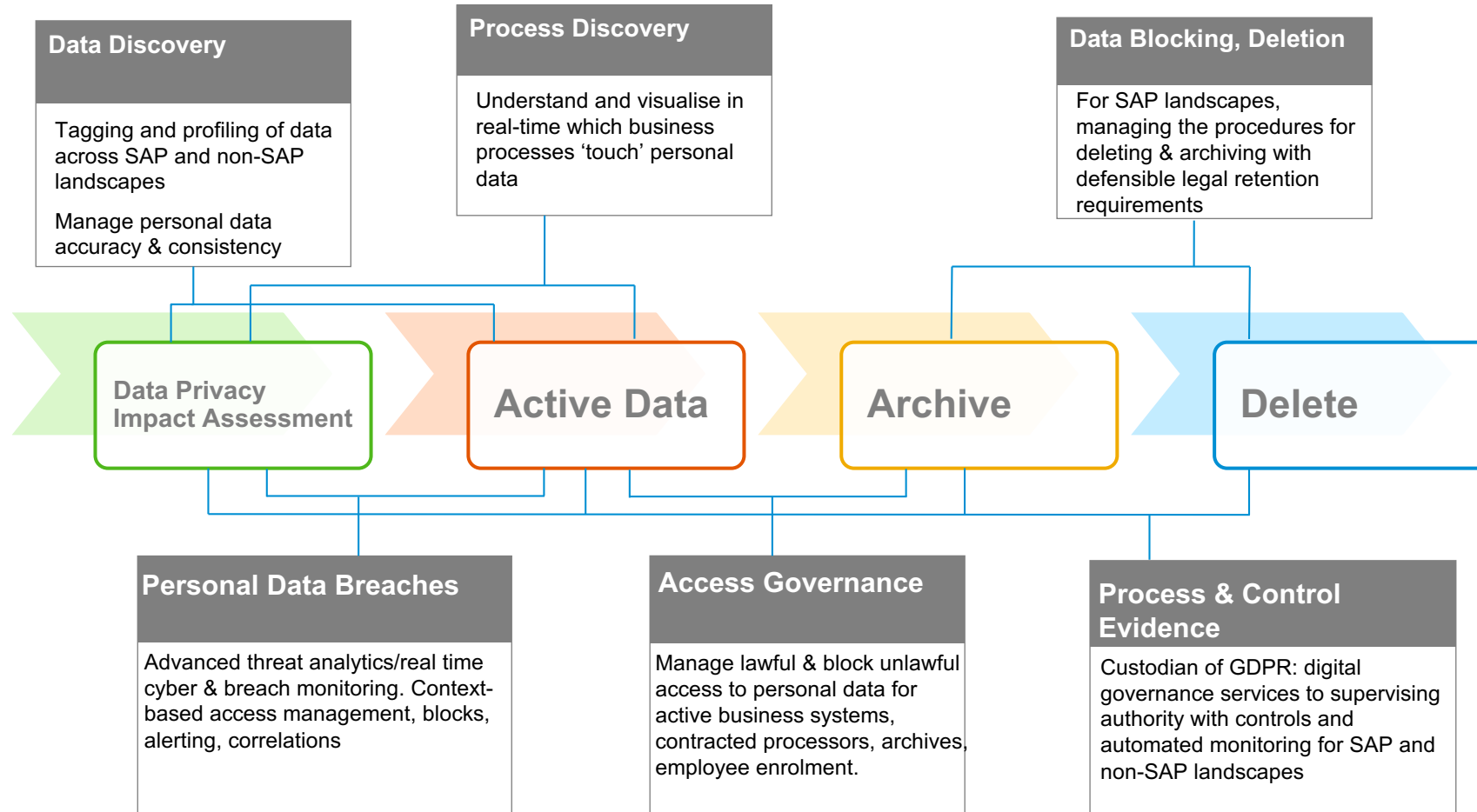
# GDPR Recap



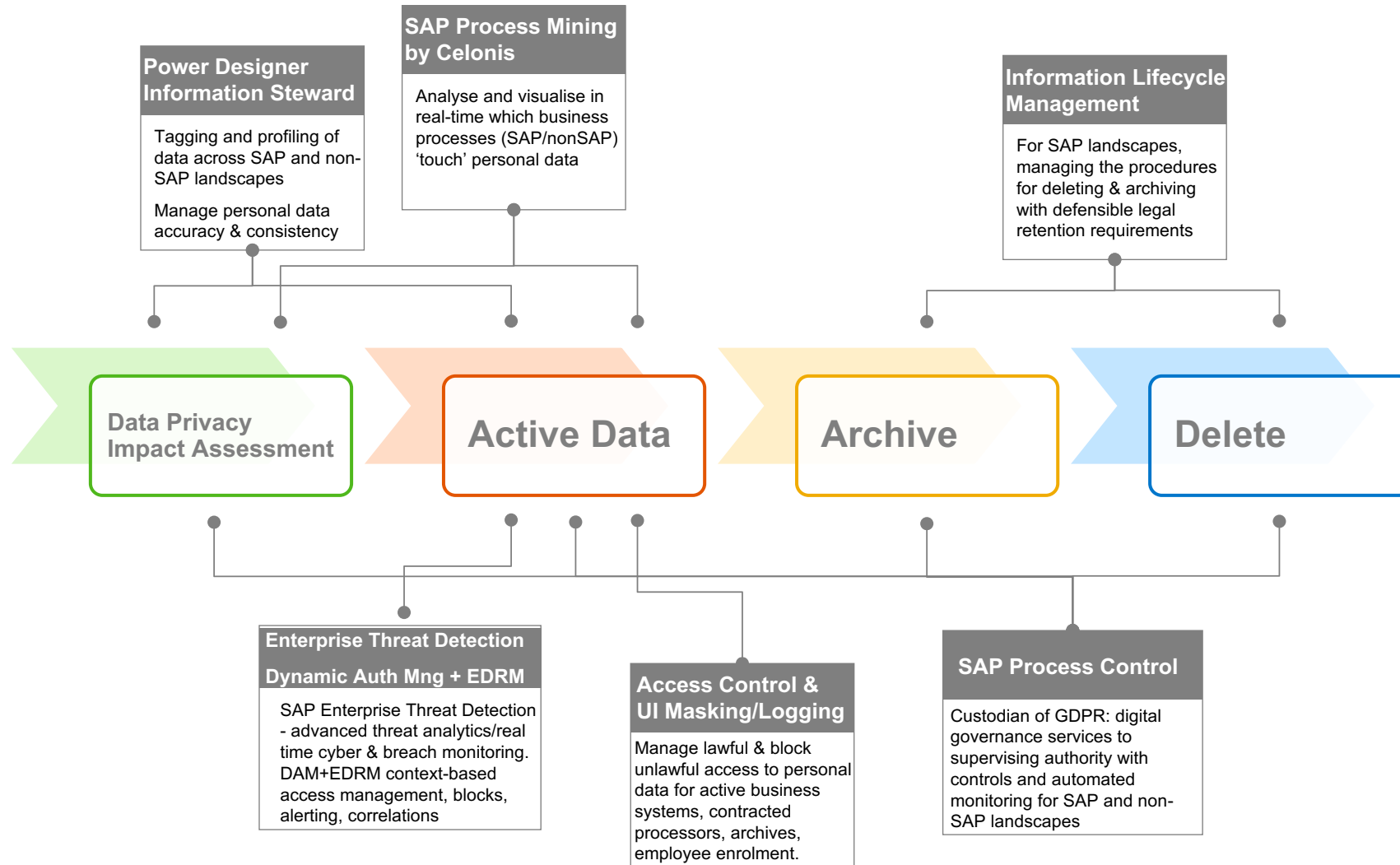
# Personal Data Lifecycle



# 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

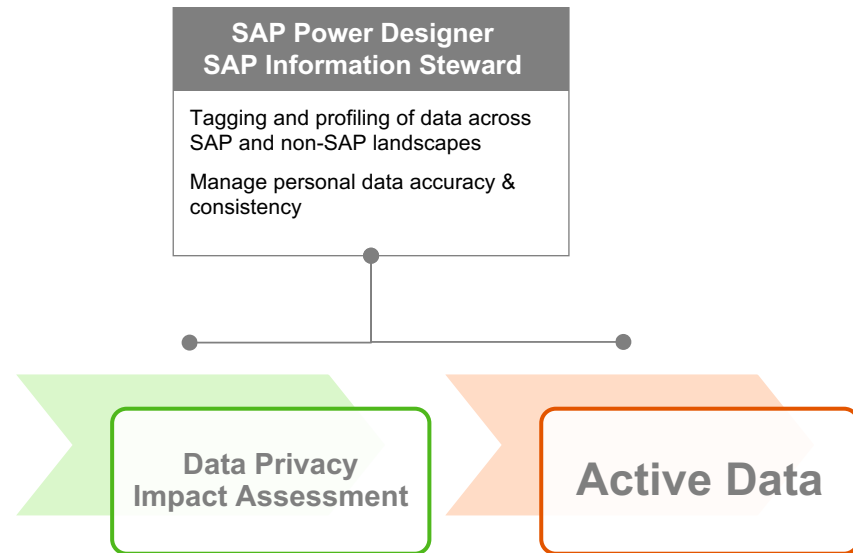
The screenshot shows the SAP Fiori Launchpad interface for a user named 'd)'. The browser address bar displays the URL: `https://cimg1.wdf.sap.corp:4301/sap/bc/ui5_ui2/ui2/ushell/shells/abap/FioriLaunchpad`. The page title is 'Home'. The navigation bar includes the following items: 'My Reports (Custom)', 'My Objects', 'Assessment Planning', 'Surveys', 'Compliance Manager (GRC)', 'Data Protection Office', and 'Work Inbox'. The 'Data Protection Office' section contains a grid of tiles: 'My Processes', 'Open Issues', 'Compliance Results by Organisation', 'GDPR Compliance Dashboard', 'Data Sources & Tags', 'Privacy & Impact Assessments', and 'Automated Access Monitoring'. The 'Privacy Risks' tile shows a count of 4 and the text 'Tests with HIGH Iss...'. The 'Data Breach' tile shows a count of 1. The 'Work Inbox' section contains 'Incidents' and 'Outlook' tiles.

**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

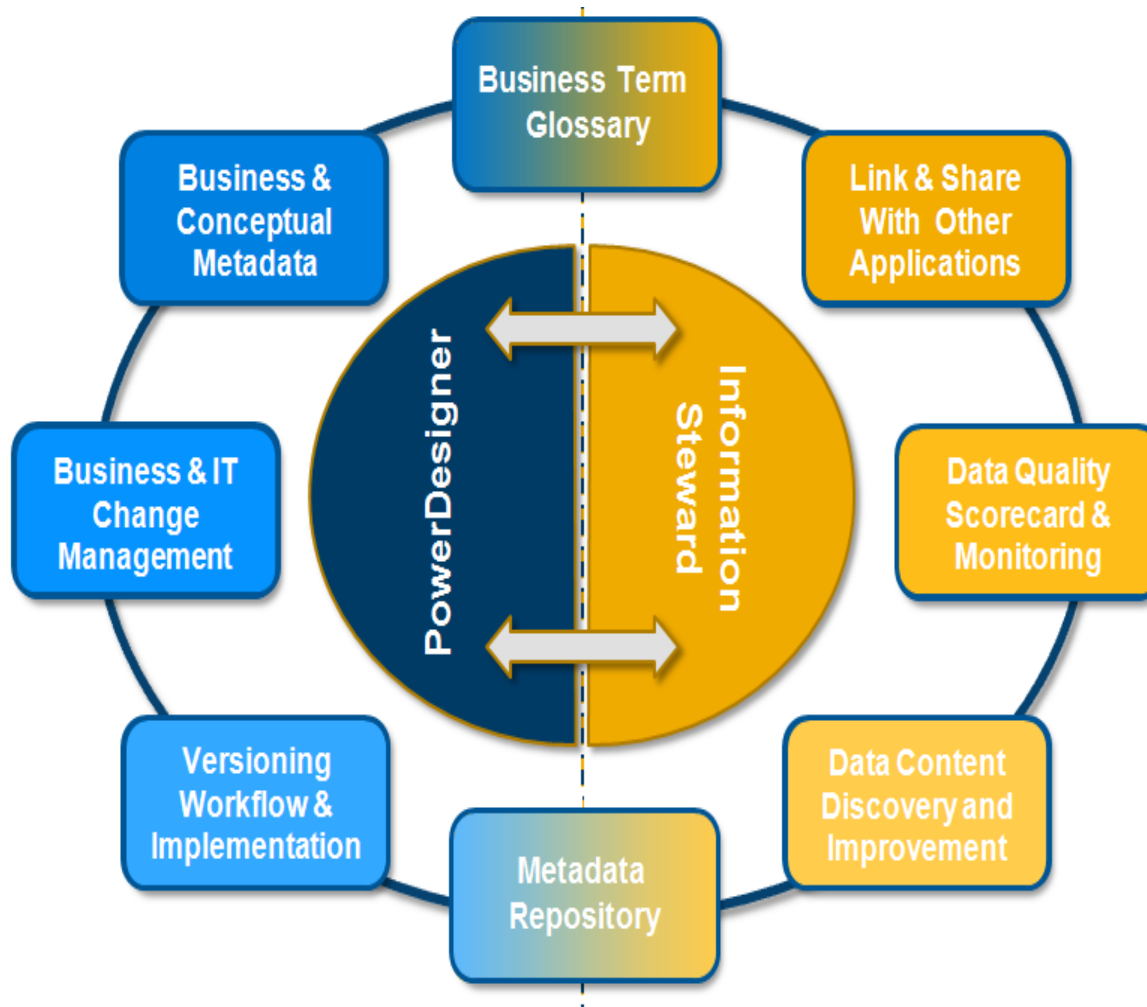


# Full Lifecycle Metadata Management

From Discovery, Quality and Monitoring to Architecture Driven Change

SAP Power Designer

Design time, define the environment

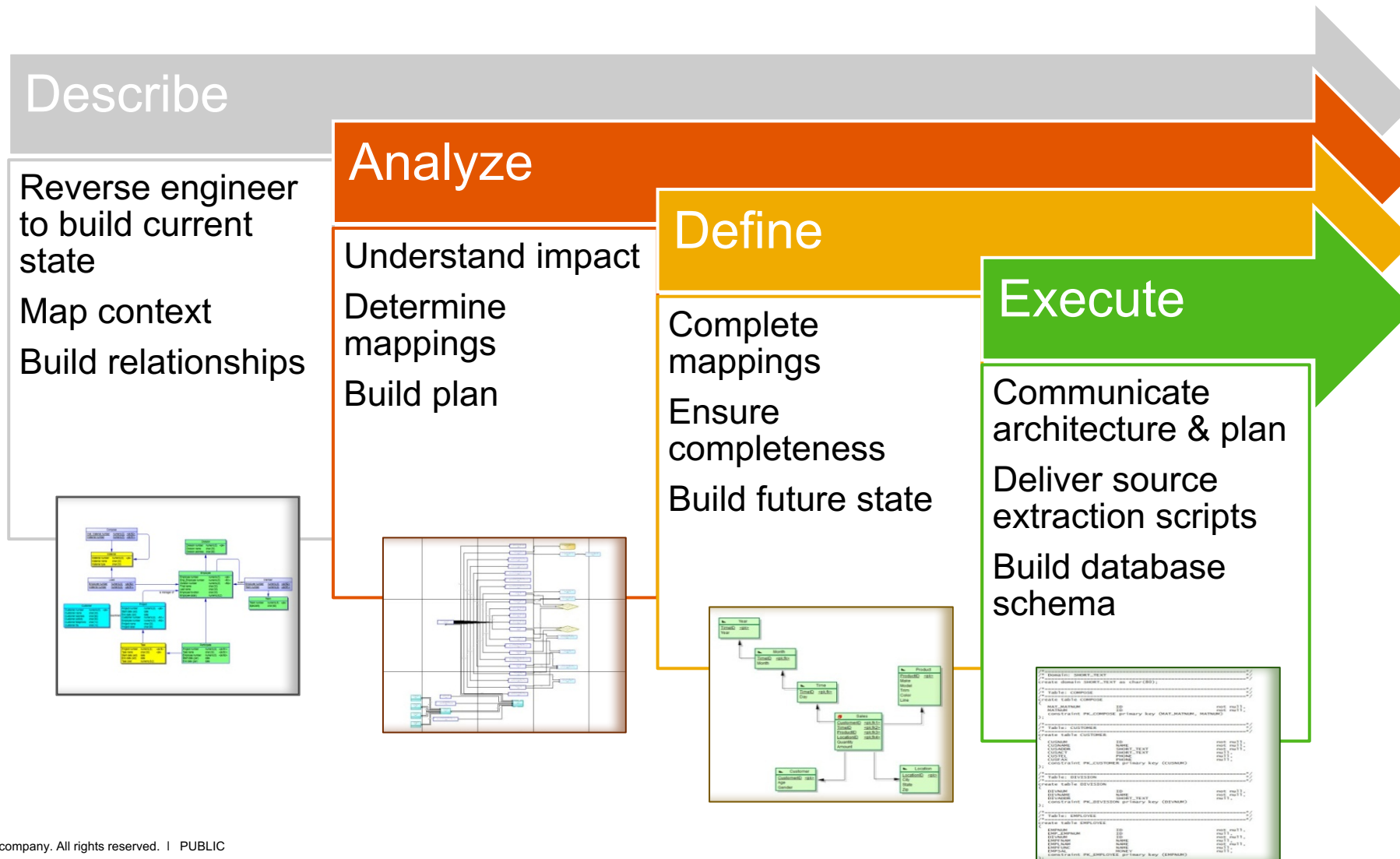


Operational time, apply to given landscape

SAP Information Steward

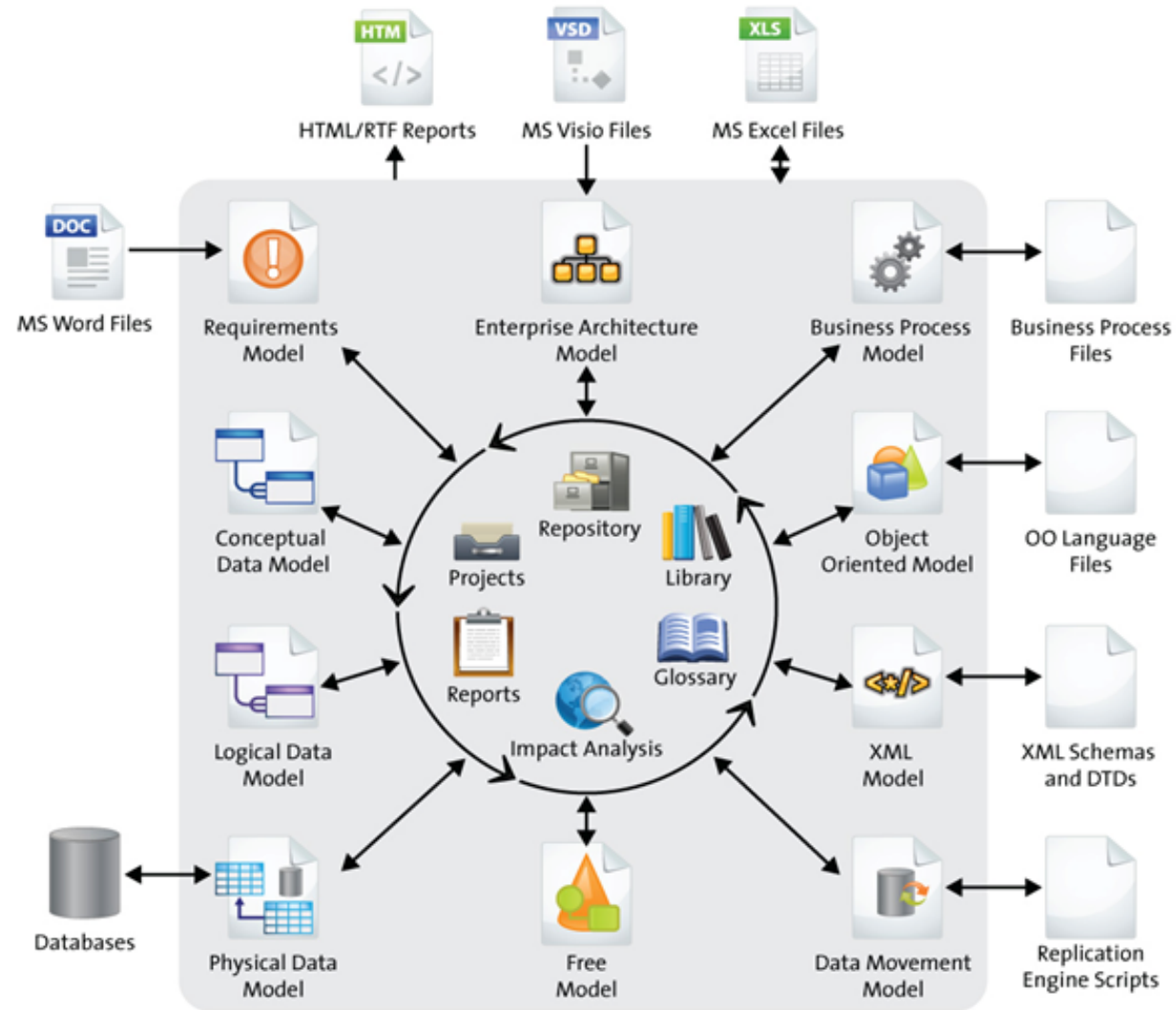
# SAP Power Designer

## Solution Business Overview



# 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



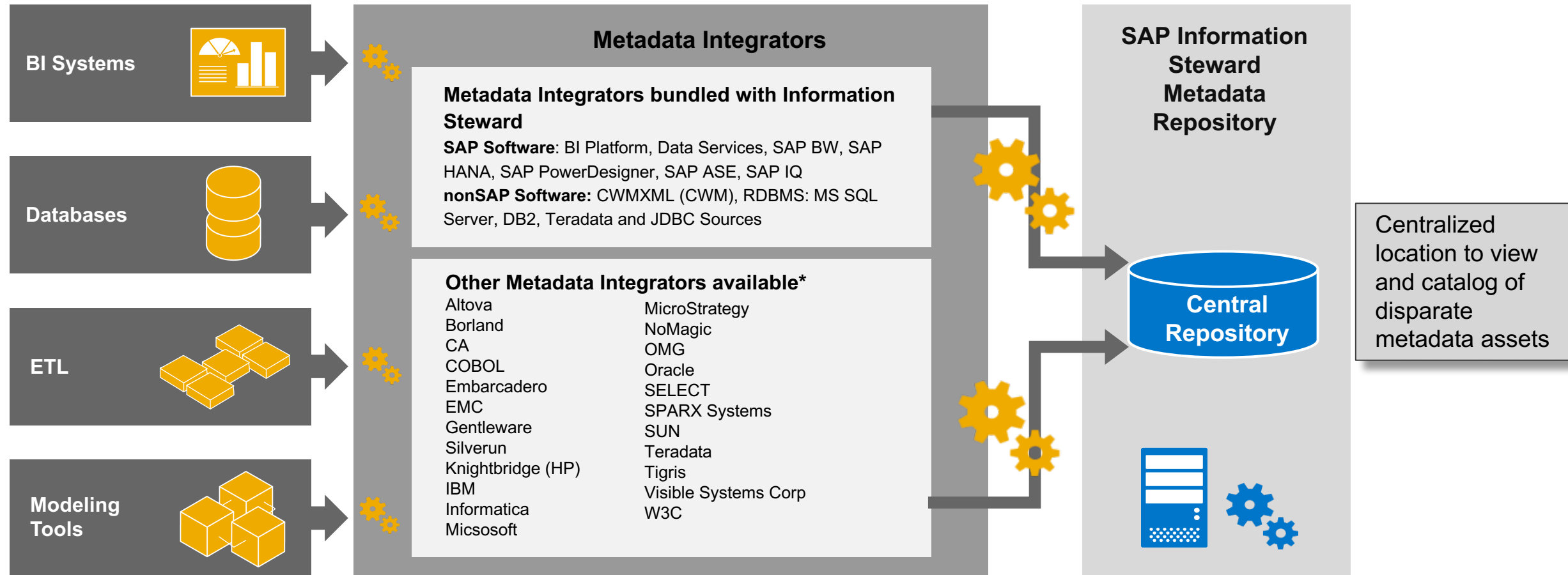
## Improve

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

The screenshot shows the SAP Information Steward interface. A table is displayed with columns 'Advisor' and 'Content Type'. A context menu is open over the 'Content Type' column, with 'Content Type' selected. A large grey arrow points from the 'Content Type' column in the table to the right-hand screenshot.

|                    | Advisor | Content Type |
|--------------------|---------|--------------|
| dbo.CALLS          |         |              |
| dbo.CallReason     |         |              |
| dbo.Categories     |         |              |
| dbo.City           |         |              |
| dbo.CityStrings    |         |              |
| dbo.CountryStrings |         |              |
| dbo.Customers      |         |              |

The screenshot shows the SAP Information Steward interface. A table is displayed with columns 'Advisor' and 'Content Type'. The 'Content Type' column contains a list of fields: Given Name1, Country, Phone, Email, Date, Family Name1, Title, Address, Locality, Region, and Postcode.

| Tables   | Advisor | Content Type |
|----------|---------|--------------|
| SEARCH   |         |              |
| DATABASE |         |              |
| TABLE    |         |              |
| FIELD1   |         | Given Name1  |
| FIELD10  |         | Country      |
| FIELD11  |         | Phone        |
| FIELD12  |         | Email        |
| FIELD13  |         | Date         |
| FIELD2   |         | Family Name1 |
| FIELD3   |         | Title        |
| FIELD4   |         | Address      |
| FIELD5   |         |              |
| FIELD6   |         |              |
| FIELD7   |         | Locality     |
| FIELD8   |         | Region       |
| FIELD9   |         | Postcode     |

# SAP Information Steward

## Out of the box Identification of Personal data

Content Types ✕

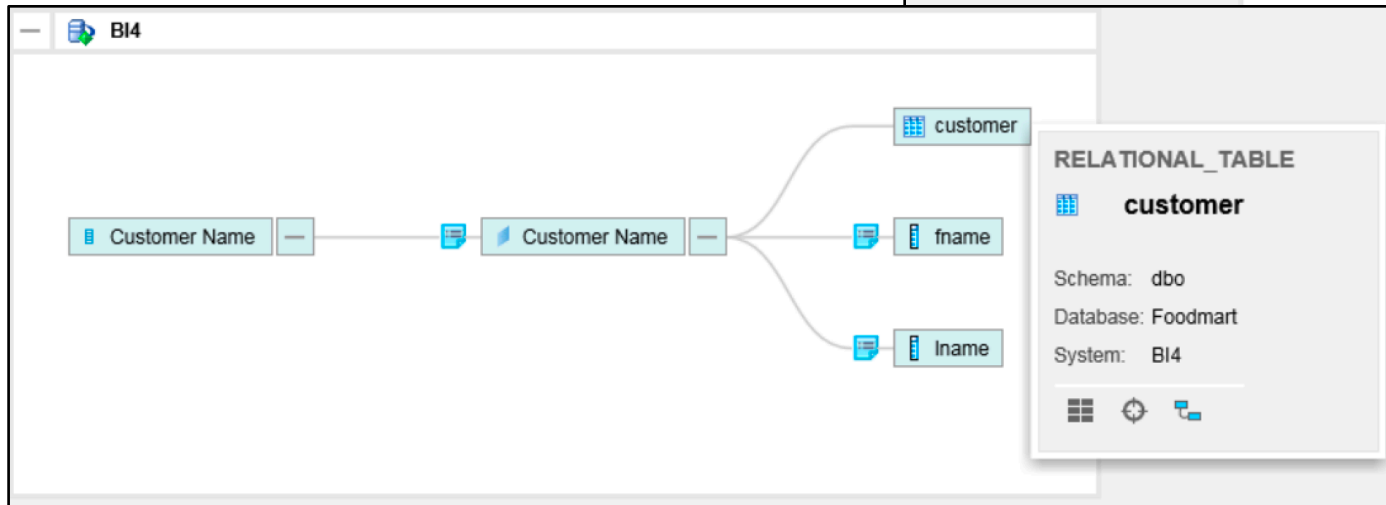
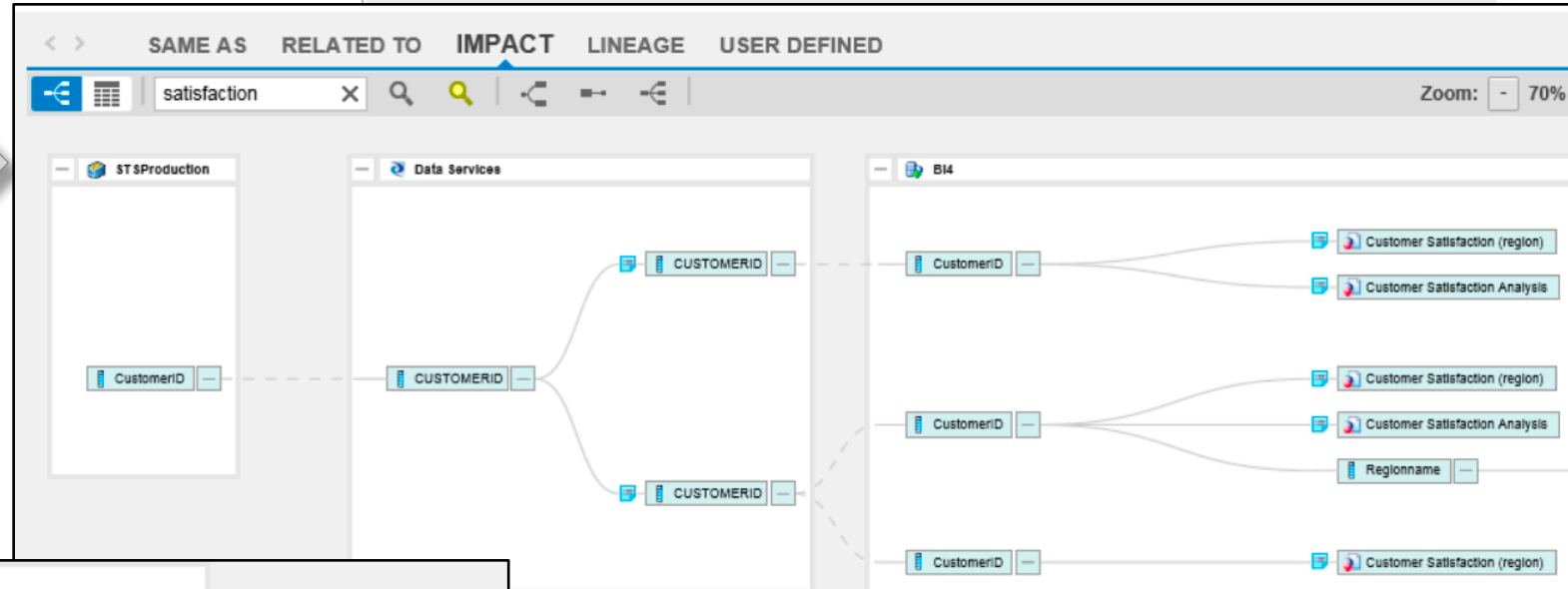
New Edit Delete Enable Show Dependencies Import Export Refresh

| 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

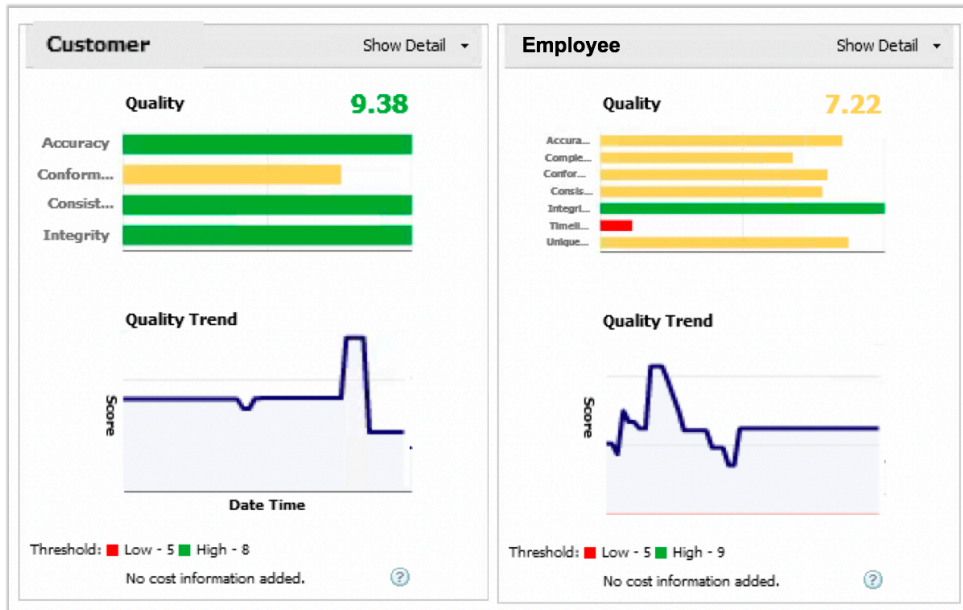


Data Lineage for data origins



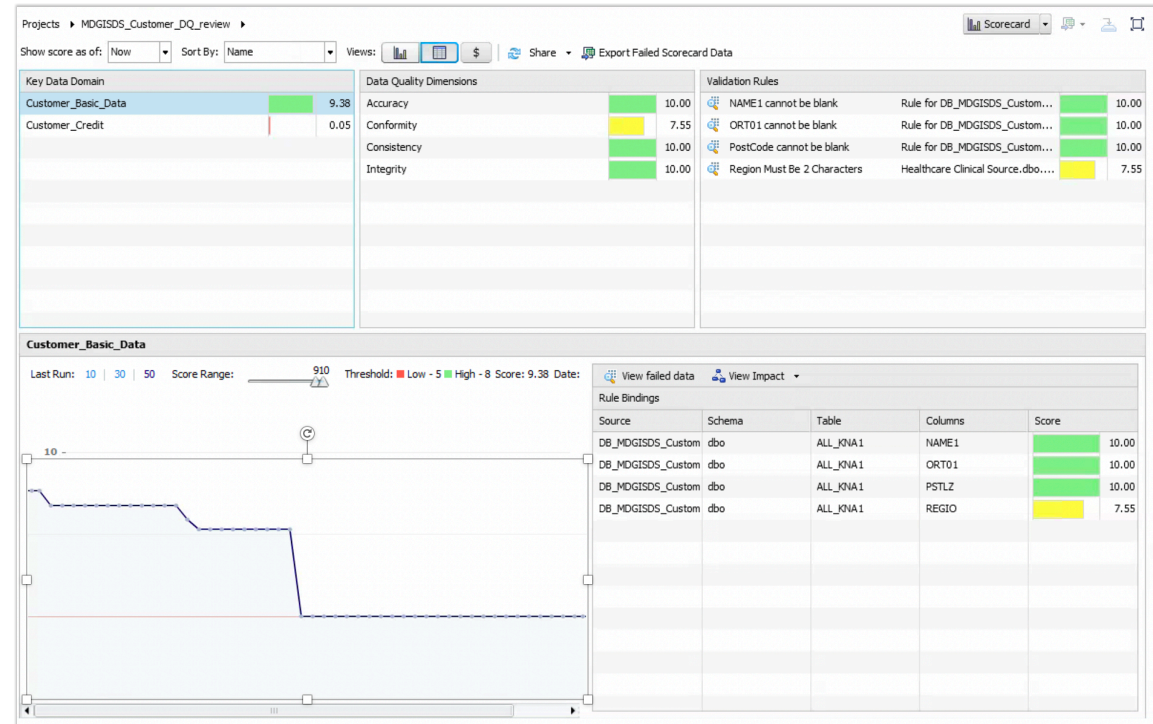
# SAP Information Steward

## Monitor and improve quality of data



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

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



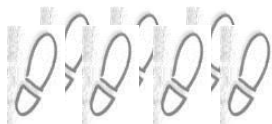
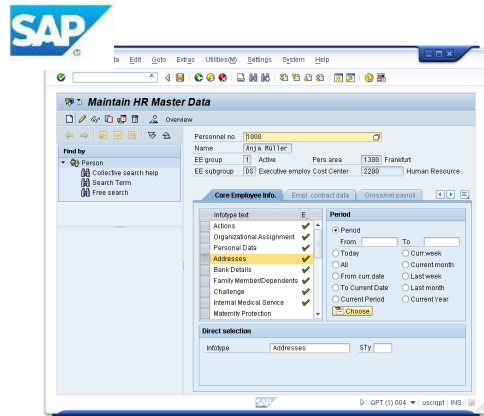
# SAP **Process Mining** by Celonis

# SAP Process Mining by Celonis

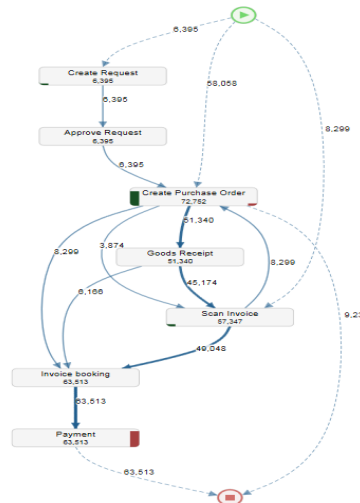
## Knowing what's going on in your business

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

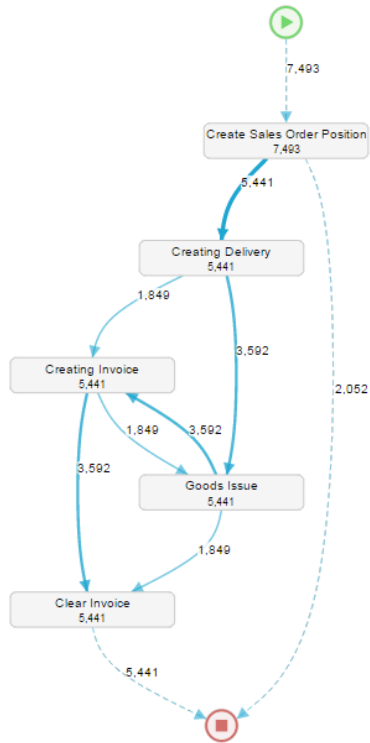
**System usage**

Compare process models to actual "As-Is" process

# Getting all Process Variations

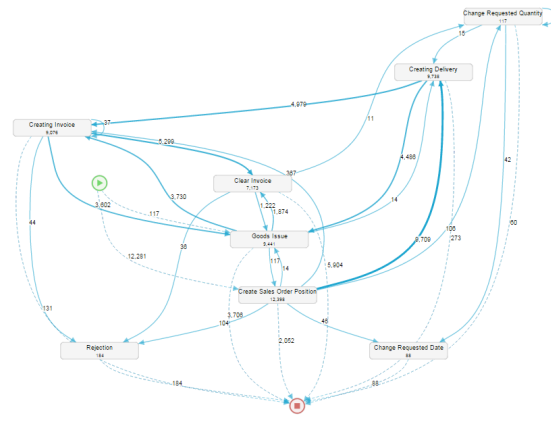
## See the happy paths

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**.



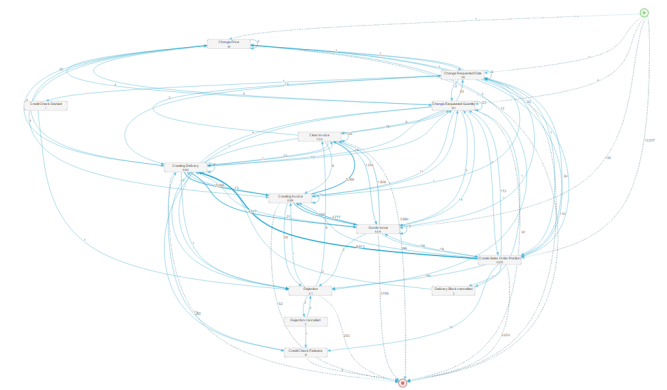
## Explore deviations

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

My Processes

Regulation: All Open

| Name                             |
|----------------------------------|
| CRG International, Inc.          |
| Data Protection Office           |
| CRG Business Units, Inc.         |
| Operations                       |
| Finance                          |
| Human Resources                  |
| Information Technology           |
| IT General Controls              |
| Access Management                |
| System Development Life Cycle    |
| GDPR                             |
| Records of processing activities |
| Documented Processing Activity   |
| Processor Processing Activity    |
| Controller Processing Activity   |
| IT Operations                    |

Self Assessment: Controller Processing Activity

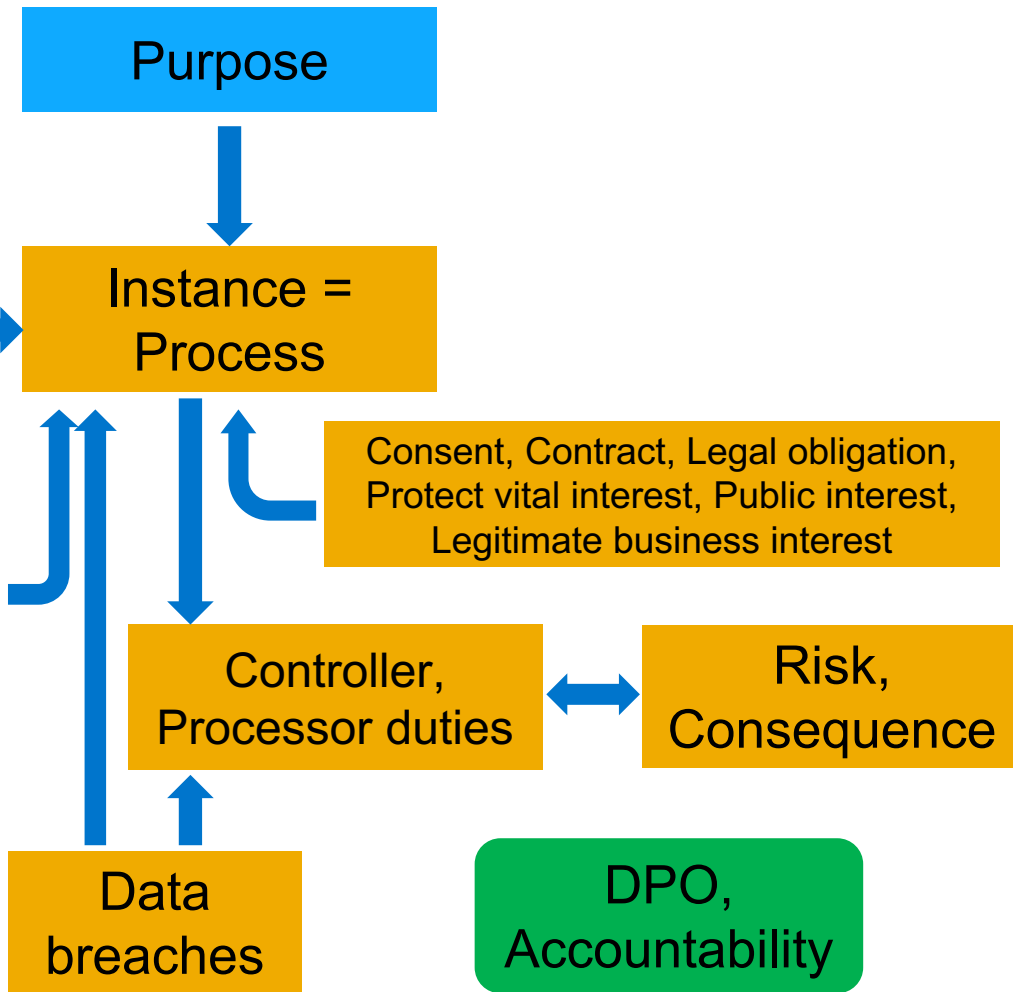
Assessment Period: Year 2017 Status: Draft

Organization: Data Protection Office Process: GDPR

Subprocesses: Records of processing activities

Submit

| Question  | Answer                            | Comment  |
|---|-----------------------------------|--|
| 1. Controller name  | John Treble                       |  |
| 2. Data Protection Officer name                             | SAP Customer Care                 |  |
| 3. Data Protection Officer email                            | SAP Customer Care                 |  |
| 4. IT System  | CRM                               |  |
| 5. Categories of Personal Data                              | Customer Data                     | Personal Data is not masked, evidence attached.                                    |
| 6. Retention period   | Private address                   | Process transferred via email with attached screenshots.                           |
| 7. Categories of Recipients                                 | Agency                            |  |
| 8. Purposes of Processing                                   | Provisional Campaign              |  |
| 9. Retention period and organizational measures implemented |                                   | Policy creation and physical block mechanisms proposed in comments below.          |
| 10. Time Limits for Erasure                                 | < 1 year                          | Consent was only provided for promotional campaigns, which was set to last 1 year. |
| 11. Location of server                                      | SAP SE Leon-Rot, Lic02.S042.Srv02 |  |



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

### Survey

**Save**

**General** Attachments and Links

\* Category: Policy Quiz

\* Title: GDPR: General Discovery and Awareness

Description: This survey is meant to gather some initial data to understand who handles, owns, or administers personal data of EU data subjects

Valuation: No Valuation

Active: Yes

### Questions

| Question  | Answer Type | Display condition |
|---|-------------|-------------------|
| GDPR General 1: Do you handle personal data related to EU data subjects?  | Yes/No/NA   |                   |
| GDPR General 2: For which categories of data subjects?  | Choice      | Yes               |
| GDPR General 3: Do you own or administer processes or systems that handle such personal data of EU data subjects? | Yes/No/NA   | Always Display    |
| GDPR General 4: Indicate processes or systems that you own or administer.   | Text        | Yes               |
| GDPR General 5: Have you attended GDPR awareness training?  | Yes/No/NA   | Always Display    |
| GDPR General 6: On what date did you attend GDPR awareness training?  | Text        | Always Display    |

# Data protection impact assessment (excerpt)

| Questions   |             |                   |   |
|---|-------------|-------------------|---|
| <input type="button" value="Add"/> <input type="button" value="Add As Child"/> <input type="button" value="Remove"/> <input type="button" value="Open"/> <input type="button" value="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

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

\* Name:  \* Valid From:

Description:  \* Valid To:

Transaction type:

Business Subprocess:

Industry-specific:  Yes  No

### User-defined fields

Purpose:  Category:

Lawful Processing: Consent  Legal Need  Personal Data:

Business Need  IT System:

# Ad hoc issues

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

### Ad Hoc Issue: Laptop with Personal Data Stolen

[Submit](#) [Assign Remediation Plan](#) [Close Without Plan](#) [Reassign The Issue](#)

Status Submitted Created By Ian Robb Created On 09/07/2017 Updated By Ian Robb Updated On 09/07/2017

[Issue Details](#) [Regulation](#) [Attachments and Links](#)

\* Name:

\* Description:

\* Priority:

Object Type:

Object Name:  [Open](#)

Owner:

Source:

\* Issue Date:

Due Date:

Audit Trail: [Audit Trail](#)

#### Notes

Ian Robb - 09/07/2017 03:32:17:

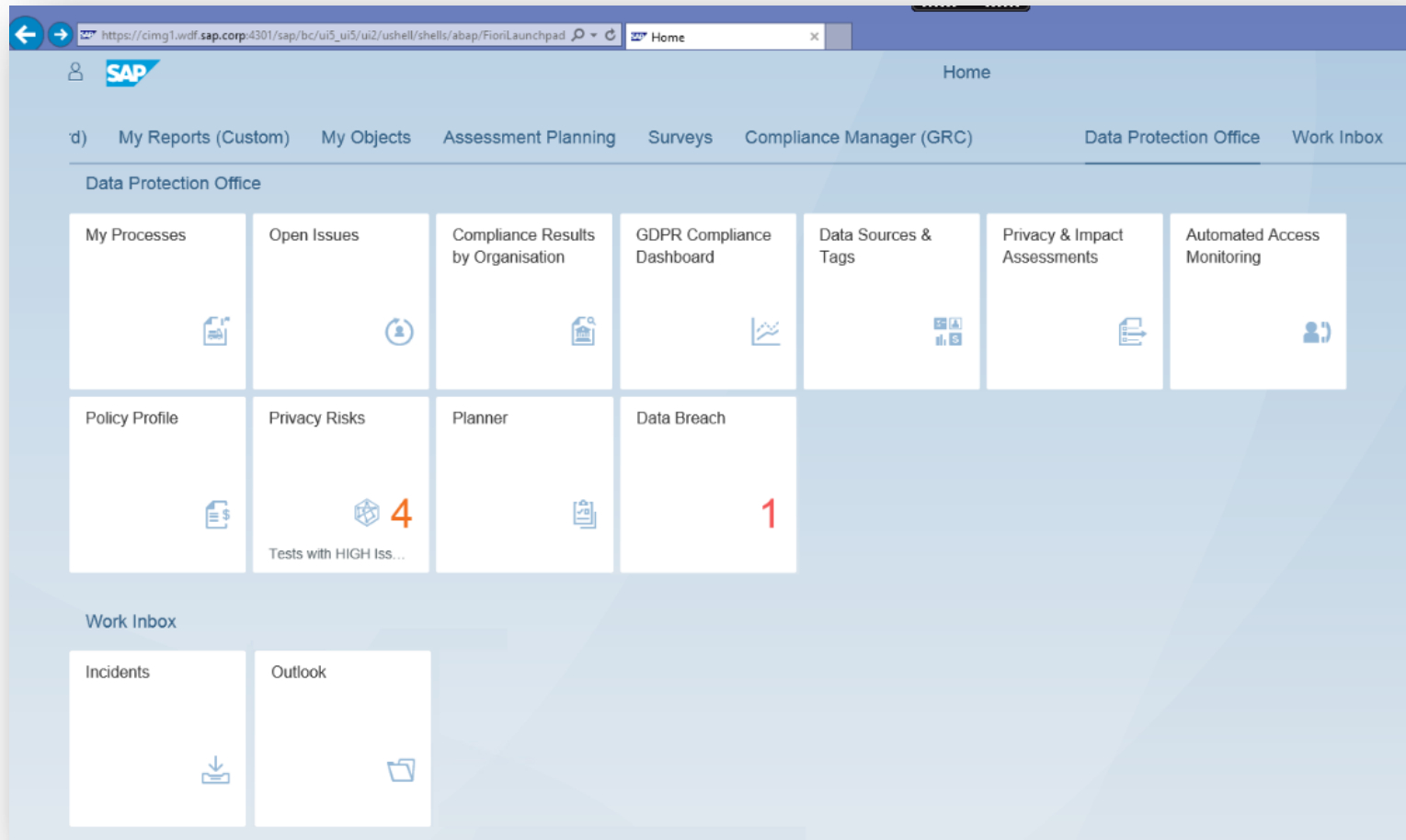
We should assume that physical recovery might not be possible

Ian Robb - 09/07/2017 03:30:37:

[Add Note](#)

# 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](mailto:peter.mravcak@sap.com)



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

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See <http://global.sap.com/corporate-en/legal/copyright/index.epx> for additional trademark information and notices.