SAP Innovation Forum Portugal
GDPR Compliance Program – Focus Use Cases

Dr. Neil Patrick – Director COE GRC & Security (EMEA)

10th May 2017

What is GDPR?

GDPR (EU Regulation 2016/679), effective 25 May 2018, gives **individuals control** and **protection** of their **personal data** in a **networked digital world**. Data controllers (why personal data is collected and used) and processors (process on behalf of controllers) are most affected. It simplifies prior EU regulation replacing the 1995 data protection directive.

Penalties up to

4% of annual global revenue /

€20million

whichever is greater

or

2% of annual global revenue /

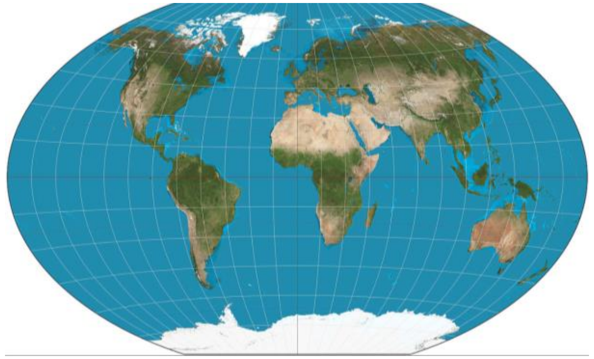
€10million

whichever is greater

"…effective, proportionate and dissuasive."

Applies to

EU and non-EU companies that manage/process personal data of individuals' activities in the EU



Protect other's personal data with the same respect you expect to have your personal data protected

Assist with GDPR Governance Principles

Document governance requirements for regulator and DPO

Evidence of processes from Article 5(1). What to do:

- Privacy by design and default
- Privacy impact assessments
- Engaging a DPO, transparency into state of compliance
- Controller selection process, data processed
- Manage third party contracts
- Evidence of pseudonymisation, encryption, breach management
- Route to approach certification

Customer GDPR programs fail because they do not have an attestable ***program***, with ***evidence*** of a ***(human) governance*** framework with controls in place.

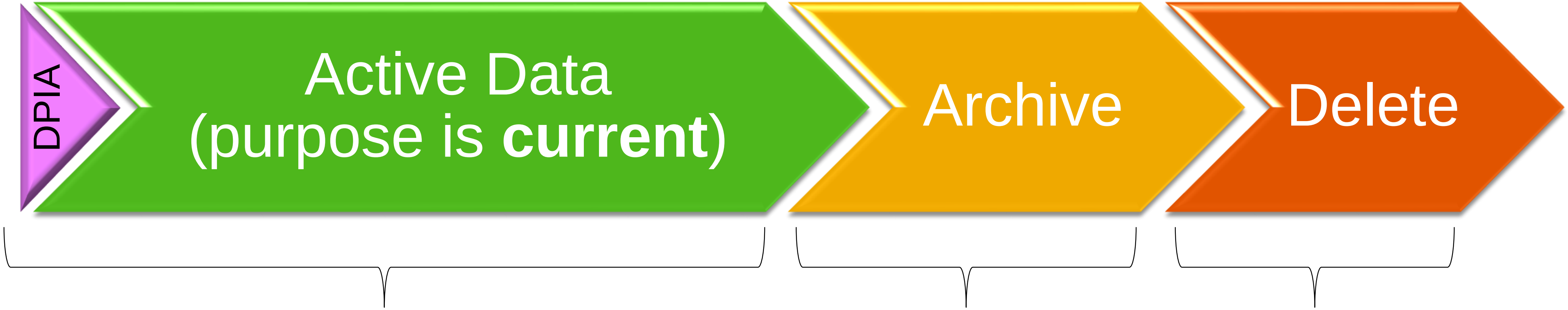
Art 5(2) “The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').”

Data Life and Terms

Active and Archive, cover non-SAP

There are phases of data use that need to be managed under GDPR

- Products from GRC & Security and DDM
- Different technologies apply at each stage
- Customers will have their own IT landscapes already



DPIA

Active Data (purpose is **current**)

Archive

Delete

Business as usual use of data, defined by purpose. Manage access, breach, accuracy, consent, portability, copy, minimization, with evidence

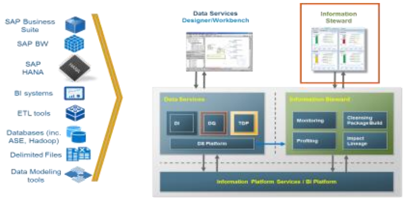
Purpose concluded, consent revoked: blocked archive, retention periods

Retention concluded: delete with evidence

Starting Point

Where is my data, what is my Risk?

Information Steward – Data Tagging



IS: Tagging non-SAP data across environments

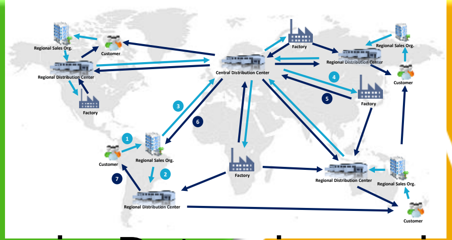
DPIA

Active Data

Archive

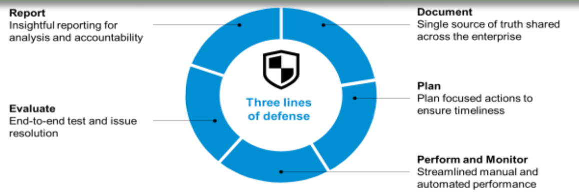
Delete

Celonis – Process Mining


Regional Sales Org.
Customer
Regional Distribution Center
Factory
Central Distribution Center
Factory
Regional Distribution Center
Regional Sales Org.
Customer
Factory
Customer
Regional Sales Org.
Factory
Regional Distribution Center
Regional Sales Org.
Customer
Regional Distribution Center

Celonis: Determine as-is data processes under GDPR

Process Control


Report
Insightful reporting for analysis and accountability
Document
Single source of truth shared across the enterprise
Three lines of defense
Plan
Plan focused actions to ensure timeliness
Evaluate
End-to-end test and issue resolution
Perform and Monitor
Streamlined manual and automated performance

DPIA

PC: Governance & evidence

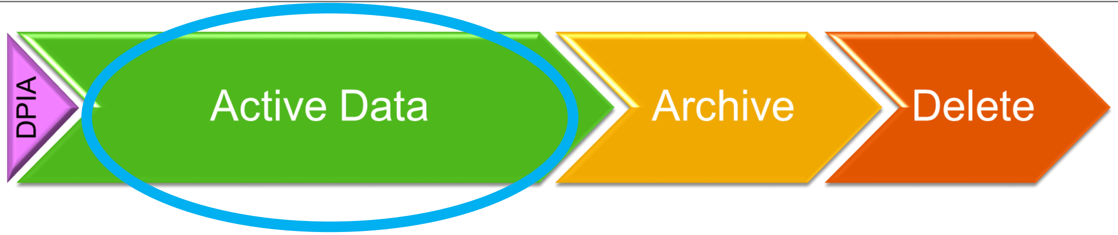
Talk Track: Information Steward, Process Control, Celonis

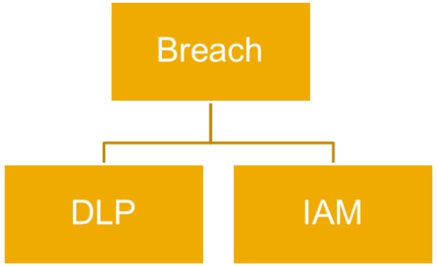
- Tagging of personal data
- Prepare for Portability
- Prepare for Consent
- Prepare for Deletion
- GDPR register documentation
- Process, purpose, owners
- ➢ Integrated DPIA
- ➢ Controller, Processor duties
- ➢ A5, 6, 9, 26, 27, 28, 29, 30, 33, 34, 35, 70,…..
- ✓ Mining personal data processes

Operationalise: Data Breach, Masking

How do I Stop Fines from Inappropriate Access/Loss?

- Data Breach: “accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data”
- Processing: “collection, recording, organisation, structuring, storage, adaptation or alteration, **retrieval**, **consultation**, **use**, **disclosure** by **transmission**, dissemination or *otherwise making available*, alignment or combination, restriction, erasure or destruction”





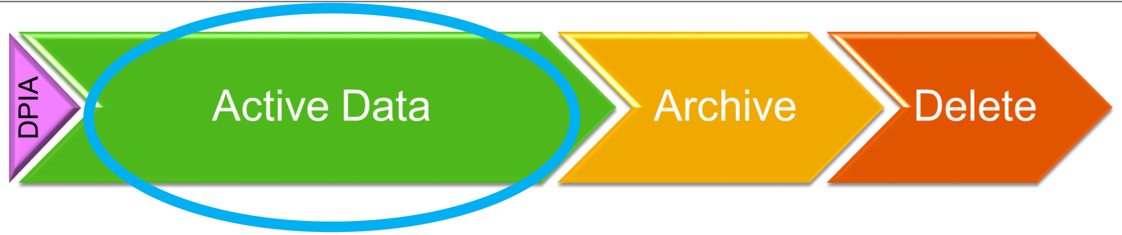
- Minimisation: adequate, relevant and **limited** to what is necessary in relation to the purposes for which they are **processed**

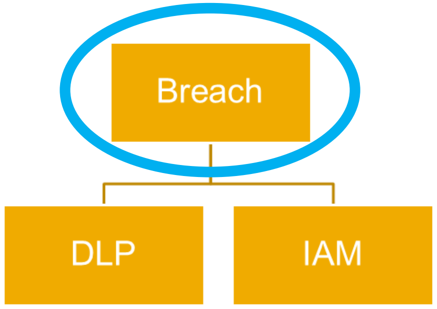
Operationalise: Data Breach, Masking

How do I Stop Fines from Inappropriate Access/Loss?

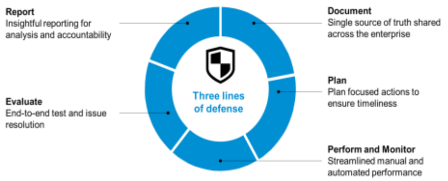
Board, controller and processor - Articles 70, 33, 34:

- Issue & supply guidelines, recommendations and best practices to encourage application of GDPR
- Controller has 72 hour notification window, processor notify a controller without undue delay
- Consequences of breach, measures (to be) taken, history





Process Control


Report
Insightful reporting for analysis and accountability
Document
Single source of truth shared across the enterprise
Three lines of defense
Plan
Plan focused actions to ensure timeliness
Evaluate
End-to-end test and issue resolution
Perform and Monitor
Streamlined manual and automated performance

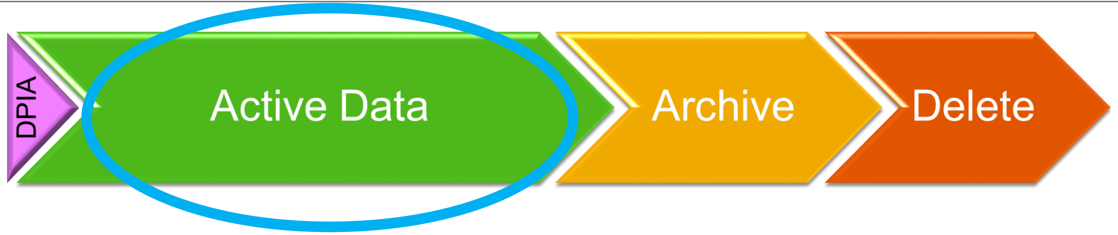
PC: Governance & evidence

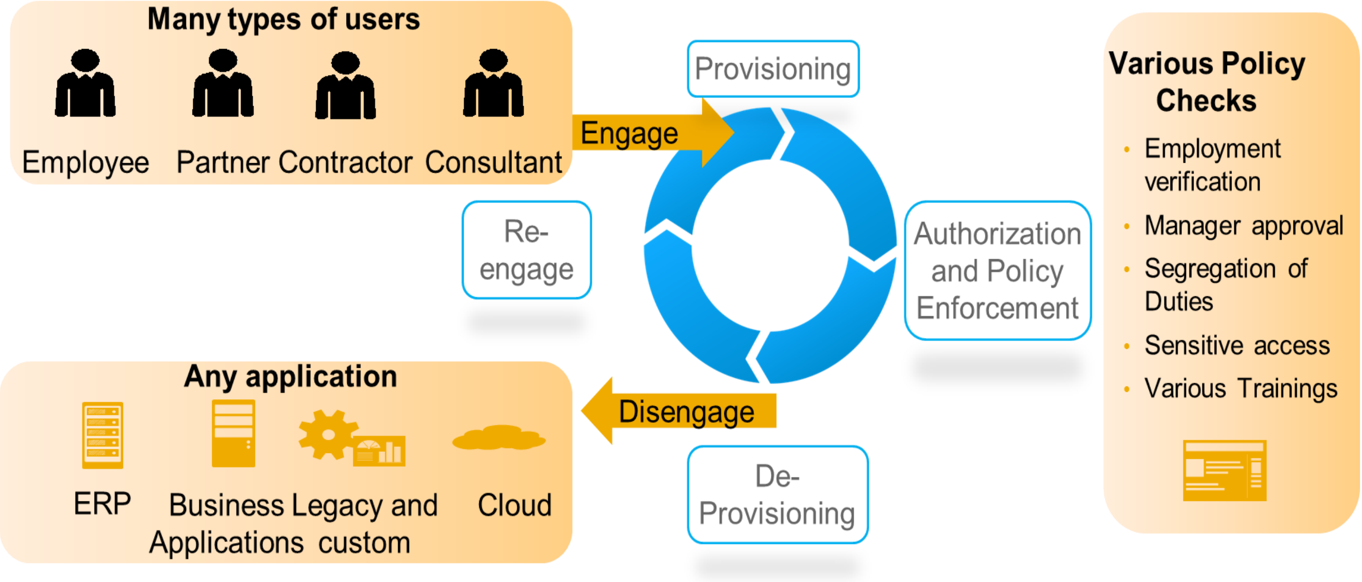
Talk Track: Process Control

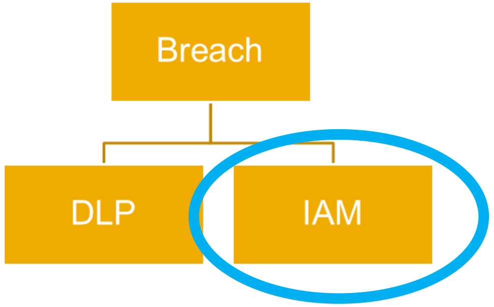
Operationalise: Data Breach, Masking

How do I Stop Fines from Inappropriate Access/Loss?

- ‘Legitimate’ access to personal data
- Role design, management
- Provision/de-provision per current role
- Alerts for inappropriate access



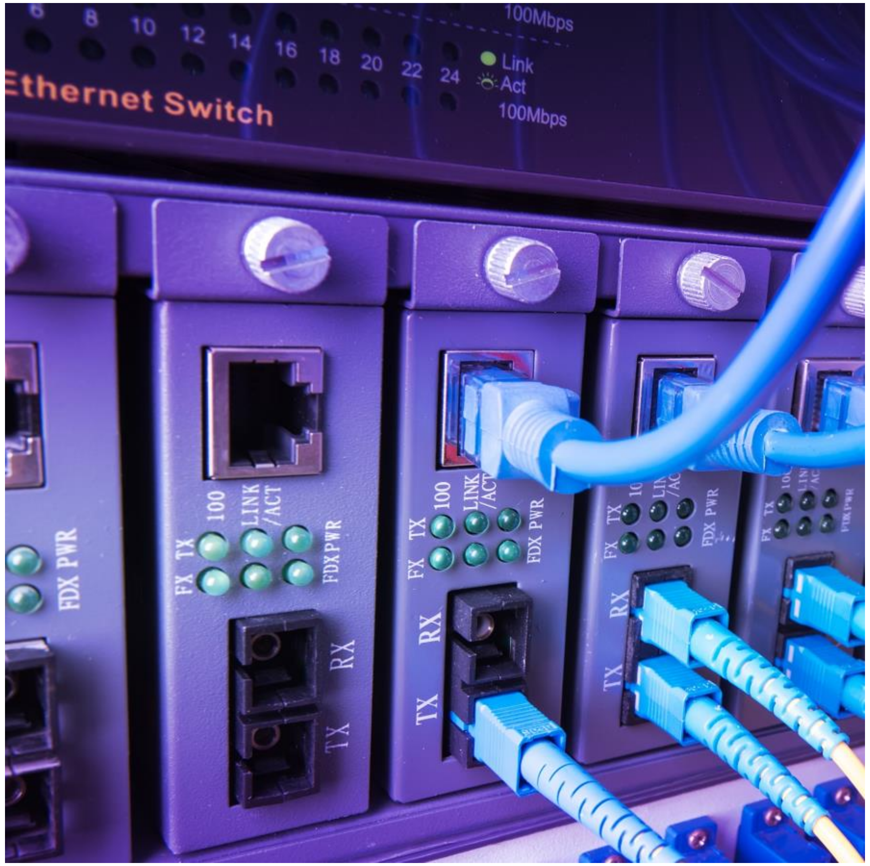


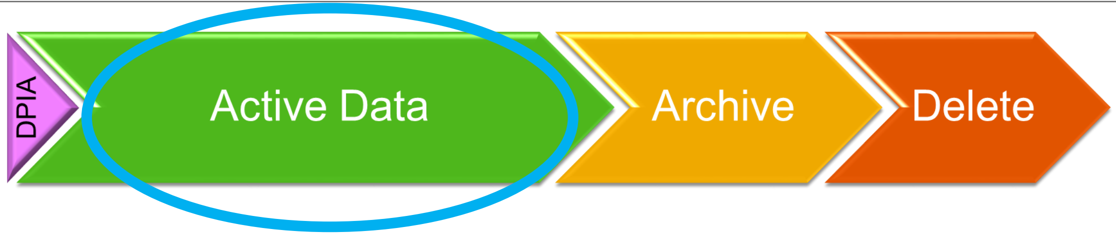


Talk Track: Access Control, Dynamic Authorisation Management, Access Violation Management (and IDM, SSO)

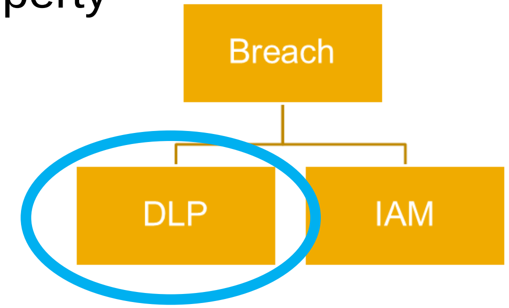
Operationalise: Data Breach, Masking

How do I Stop Fines from Inappropriate Access/Loss?





- Big data, real-time analysis
- Application level not infrastructure: location of personal data, Intellectual Property
- Patterns, alerts, investigation

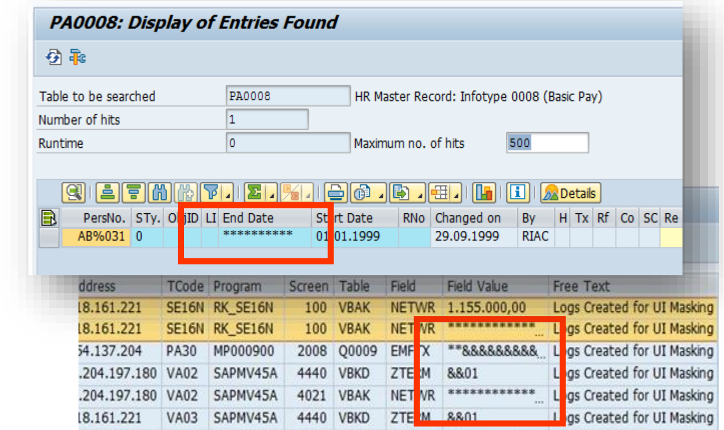


Business process level	SAP Fraud Management
Application level	SAP Enterprise Threat Detection
Infrastructure level	SIEM, Central Log Server

Talk Track: Enterprise Threat Detection, UI Logging, Dynamic Authorisation Management

Operationalise: Data Breach, Masking

How do I Stop Fines from Inappropriate Access/Loss?

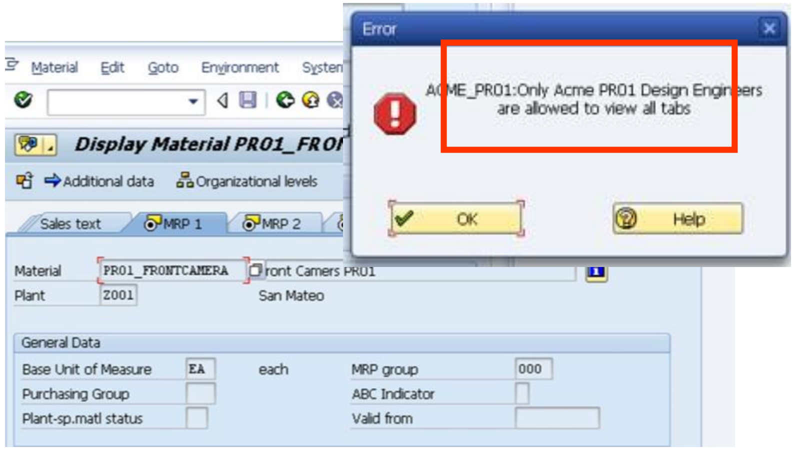


PA0008: Display of Entries Found

Table to be searched	PA0008	HR Master Record: Infotype 0008 (Basic Pay)	
Number of hits	1		
Runtime	0	Maximum no. of hits	500

PersNo.	STy.	ObjID	LI	End Date	Start Date	RNo	Changed on	By	H	Tx	Rf	Co	SC	Re
AB%031	0			**********	01.01.1999		29.09.1999	RIAC						

ddress	TCode	Program	Screen	Table	Field	Field Value	Free Text
18.161.221	SE16N	RK_SE16N	100	VBAK	NETWR	1.155.000,00	Logs Created for UI Masking
18.161.221	SE16N	RK_SE16N	100	VBAK	NETWR	************	Logs Created for UI Masking
54.137.204	PA30	MP000900	2008	Q0009	EMFTX	**&&&&&&&&&	Logs Created for UI Masking
.204.197.180	VA02	SAPMV45A	4440	VBKD	ZTERM	&&01	Logs Created for UI Masking
.204.197.180	VA02	SAPMV45A	4021	VBAK	NETWR	************	Logs Created for UI Masking
18.161.221	VA03	SAPMV45A	4440	VBKD	ZTERM	&&01	Logs Created for UI Masking



Display Material PR01_FRO

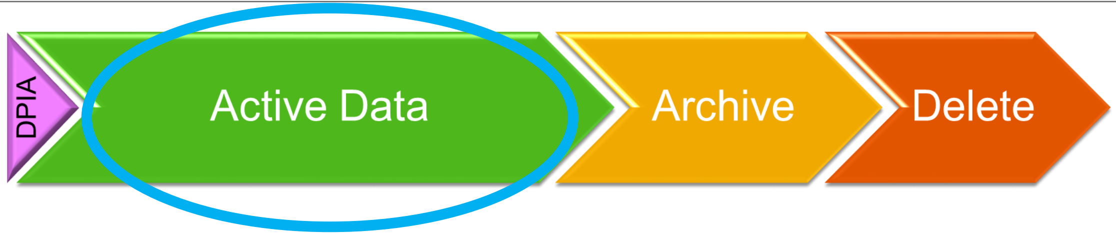
Error

ACME_PR01:Only Acme PR01 Design Engineers are allowed to view all tabs

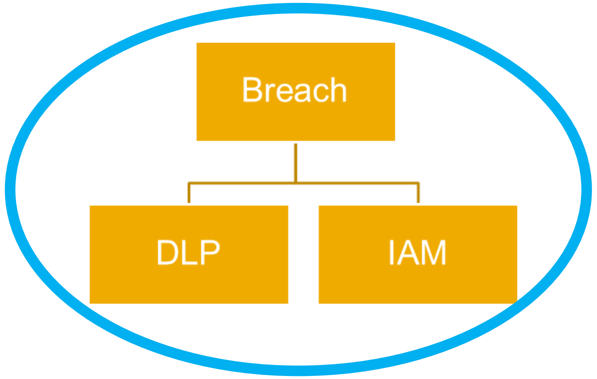
Material	PR01_FRONTCAMERA	Front Camers PR01	
Plant	Z001	San Mateo	

General Data

Base Unit of Measure	EA	each	MRP group	000
Purchasing Group			ABC Indicator	
Plant-sp.matl status			Valid from	



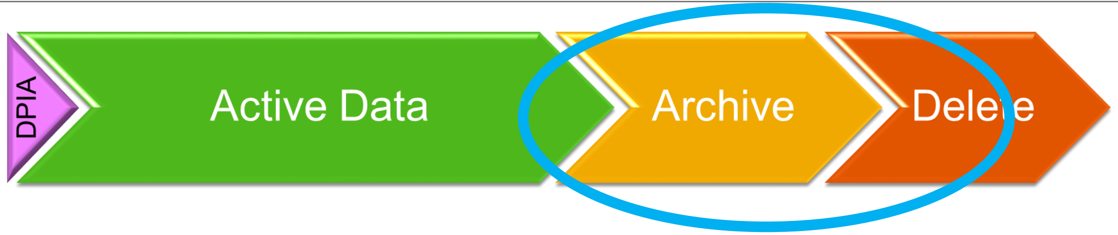
- Minimal impact on 'live data' and active 'historical data' systems
- UI Masking SAP only
- DAM is SAP and non-SAP
  - ERP, CRM, BW, PLM,
  - SharePoint, MSFT Exchange, Dynamics CRM, IBM FileNet, File Servers/Shares, Windchill, Enovia, Teamcenter, Skype for Business
  - SDK for others



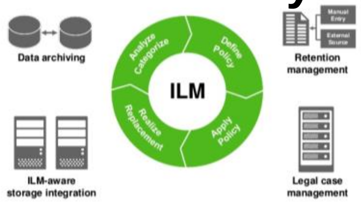
Talk Track: UI Masking, Dynamic Authorisation Management

Operationalise: Deleting, Blocking, Retention

‘Right to forget’

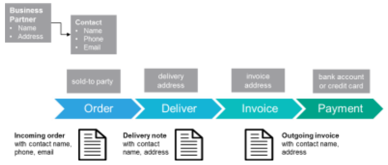


Information Lifecycle Management



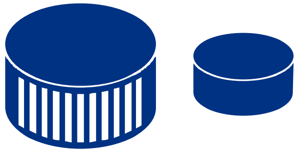
ILM: Tagged SAP data across environments, delete and block

OpenText™



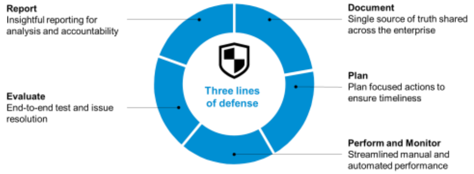
OT: ‘Digital Vault’, OCR, content tagging, storage, management

Other non-SAP



Processes for delete, block, retention

Process Control

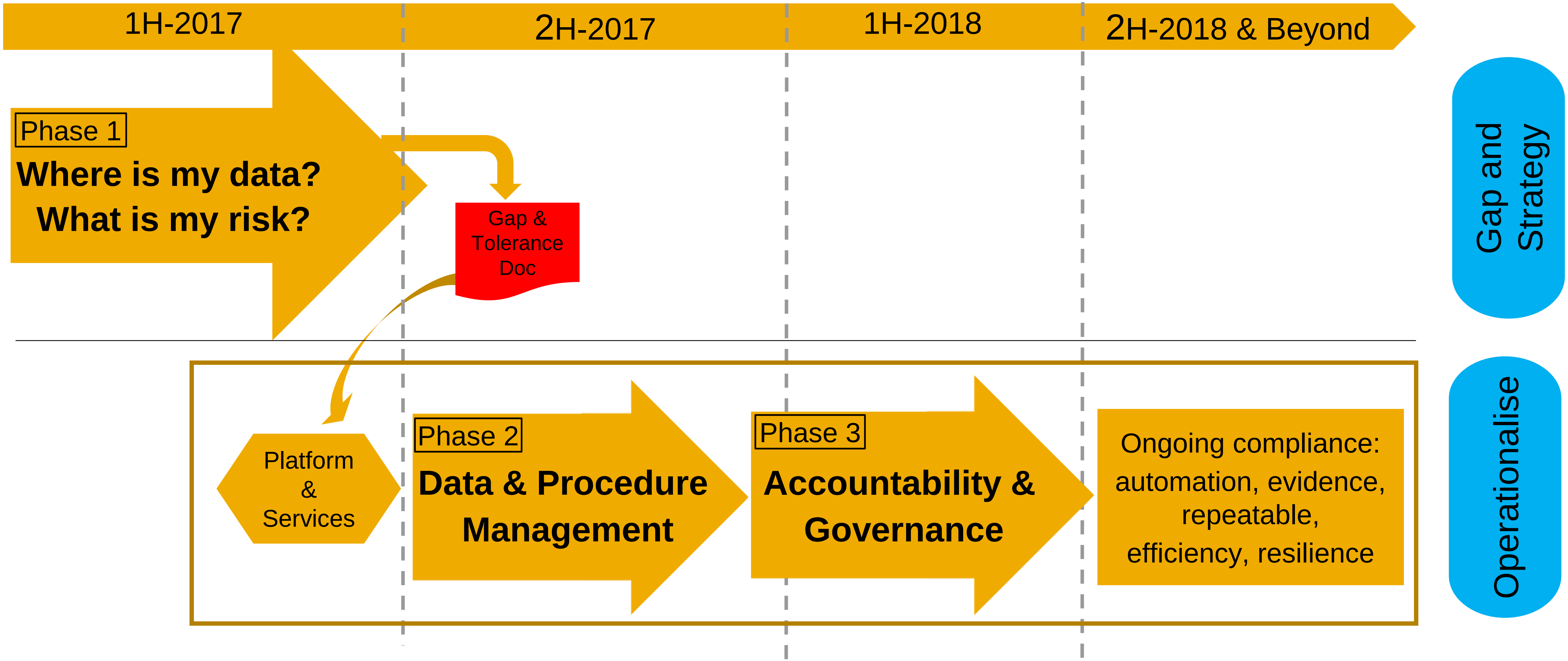


PC: Governance & evidence

- Deletion of SAP personal data, archive, retention, delete on expiration
- Archive SAP & non-SAP personal data, for legal purposes + retention periods, paper, OCR, unstructured data
- Other systems for non-SAP data
- Document systems & procedures for SAP, non-SAP: *Evidence* and *Governance* of (human) GDPR processes

Talk Track: Information Lifecycle Management, OpenText, Process Control

Example Conceptual Overall Project Plan



1H-2017

2H-2017

1H-2018

2H-2018 & Beyond

Phase 1

Where is my data?

What is my risk?

Gap & Tolerance Doc

Gap and Strategy

Platform & Services

Phase 2

Data & Procedure Management

Phase 3

Accountability & Governance

Ongoing compliance: automation, evidence, repeatable, efficiency, resilience

Operationalise

Core potential SAP Solutions – Phase 1

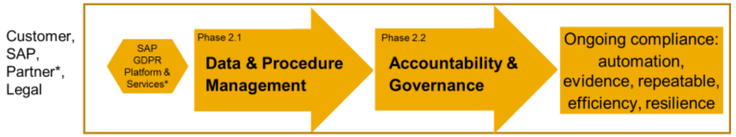
Requires services (SAP or partner) & Legal to Implement

Solution	Value in GDPR
PC	Custodian of GDPR compliance: digital evidence to the supervising authority. Breach management, compliant policies and privacy notices and procedures, lawful exclusions, DPIA results (and assessment), controls (with automated monitoring across SAP and non-SAP systems), audit evidence and action management, lawful purpose per process, third party management
IS	Data profiling and metadata management tool providing contiguous interrogation of the location of personal data across the estate for SAP and non-SAP systems, as well as assisting in managing personal data accuracy and consistency.
Celonis	Cutting edge HANA-powered process mining technology to understand and visualize which processes actually ‘touch’ personal data, as opposed to the ones you think do, with real-time cross-platform big data surveillance for SAP and non-SAP systems.

PC: Process Control; IS: Information Steward

Core potential SAP Solutions – Phase 2 & 3

Requires services (SAP or partner) & Legal to Implement



Customer, SAP, Partner*, Legal

SAP GDPR Platform & Services*

Phase 2.1 **Data & Procedure Management**

Phase 2.2 **Accountability & Governance**

Ongoing compliance: automation, evidence, repeatable, efficiency, resilience

Solution	Value in GDPR
OT	Flexible powerful ‘digital vault’ and delete regime. Already supports ILM functionality, in addition handles paper doc digitising and meta tagging, unstructured to structured data management.
IAM: AC,AVM DAM, UI-M	Manage lawful user access, blocking unlawful access to personal data. Cover active business systems, contracted processors, archives, employee enrolment. AVM connects to non-SAP.
DLP: ETD, DAM, UI-L	Monitor, log and categorise read access to personal data. HANA-powered ETD is a big-data real-time security event detection and management tool for application-level access processing and pattern analysis: real time breach, inappropriate access, investigation and remediation.
ILM	ILM is a powerful SAP-only tool for tagging personal data across multiple environments and managing the procedures for deleting and archiving with defensible legal retention requirements.
BI	Develop a dashboard as a ‘single place to go’ for real-time GDPR compliance status, drill-through into topic details.

OT: OpenText; ILM: Information Lifecycle Management; AC: Access Control; DAM: Dynamic Authorization Management; AVM: Access Violation Management, UI Tools: Masking & Logging; ETD: Enterprise Threat Detection; BI: Business Intelligence

Business Value in GDPR from SAP Solutions

Keys to GDPR ROI

1. Reduces cost of compliance (*not* just GDPR) and decreases likelihood of a fine
2. Reduces organizational and individual risk, leads to better to business planning/mission
3. Supports good data governance
4. Reduces cybersecurity & reputational risk
5. Smaller, better organized IT toolset
6. Addresses user privilege administration
7. Enables greater organizational agility

Protect Value

- Respect laws and regulations
- Reduce losses
- Improve governance and internal controls

Create Value

- Improve overall management
- Release ‘maintain the lights’ budget for innovation
- Enhance reputation, talent retention

Thank you

Contact information:

Rui Duarte
Solution Sales Executive, Portugal

r.duarte@sap.com
+351 911042266

Dr. Neil Patrick
Director COE GRC & Security (EMEA)

neil.patrick@sap.com
+44 7833 480 248