# How to get started on the SAP Data Privacy Journey

Paul Wood
Chris Burfitt

# Agenda

- About Proceed
- How to get started on meeting data legislation for SAP data
- The Recommended approach
- Best practice SAP data protection tools and services to consider
- How Telia are using SAP ILM on their GDPR journey

# About Proceed

We are SAP experts in **archiving**, **decommissioning** and **content management** for enterprise businesses

**14**
Offices worldwide

**700+**
Customer projects worldwide

Over
**20 YRS**
Experience as leading specialists

## Proceed and SAP

- SAP Gold partners
- Global SAP Master Services Agreement
- Delivering pre-sales and services for SAP
- Taken 100+ SAP customers to SAP HANA, saving them over £150m on the way

**Plus, we have built an extensive partner network to support our projects:**

SAP, OpenText, Easy Software, Microsoft Azure, Virtustream, Google Cloud, Amazon Web Services, KPMG, SNP, Syniti and T-Systems

opentext™ | Partner Services Silver

SAP Gold Partner

# Proceed Customers

## Industry

- Retail
- Manufacturing
- Food and drink
- Finance
- ICT & Telecoms
- Energy & Utilities
- Pharmaceuticals
- Aerospace and aviation
- Automotive
- Electronics
- Media

## Some of our customers

# How to get started on the SAP Data Privacy Journey

# Getting Started

## Understand the problem that needs to be solved

- What does the Organisation want to change or make happen?
- Understand the value of solving the problem - how much is the problem is currently costing? What Is the risk if the problem is not solved (cost or reputational)?
- What is the business case? Who are your project sponsors?
- Connect with your users, identify what they think is the problem and the solution

## Understand wider context

- Identify if the problem and solution is part of a bigger process or user journey
- Understand context across the Organisation – problems often involve multiple departments and external organisations (interfaces to pension provider or learning provider, for example).
- Develop a picture of what that wider 'journey' looks like for the Organisation
  - Understand if other teams are working on similar problems within the Organisation. For example, discovery might reveal that another part of the Organisation has already implemented something similar for another system / department.
  - Identify industry best practice / vendor best practice that can be applied

proceed

# Getting Started (Cont.)

## Getting Ready

- Are your users ready for the project?
- Make sure you understand the resource requirements
- Are your key stakeholders engaged?
- Define your success criteria / outcomes
- Define critical success criteria that will be used to measure success

## Understand constraints

- Legislation or industry specific regulations
- Organisation / Policy / Contracts that might need to be reviewed or changed
- Technology that needs to be upgrade, or additional technology required
- Existing processes that need to change, or new processes that are required
- Break down and prioritise risks, assumptions and questions

## Share outcomes

- Produce a discovery report with implementation recommendations – this will form the foundation of your implementation design.

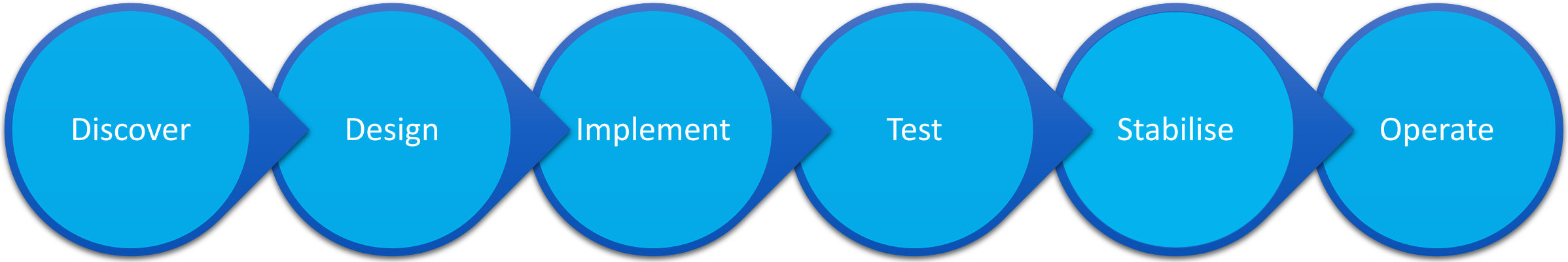
proceed

# Key Stakeholders

- **Policy / legal compliance:** Representatives from the business who understand the legal requirements for data retention
- **Data owners:** Representatives from the business who can make the decision on when to destroy specific types of data e.g. customer, vendor, business partner and employee.
- **Data governance / data protection:** The team or person from the business responsible for data protection compliance
- **Functional consultants:** The SAP consultants who deal with the types of data being discussed day to day
- **Reporting experts:** Reporting users including users of BW, and non-SAP systems where SAP data might be sent to for analysis etc.
- **Interface experts:** Representatives who understand the 'upstream' and 'downstream' systems i.e. systems that send data to SAP ECC and CRM, or systems that receive data from SAP ECC and CRM)
- **Key super-users:** End users who are considered to be the expert end users in their area who can articulate how the system is used and communicate the project aims and objectives to their colleagues, and also bring queries and concerns from their colleagues to the workshops to ensure they are covered off in the Blueprint
- **System / network administrators:** Those who understand how data can be downloaded and shared

# Recommended approach

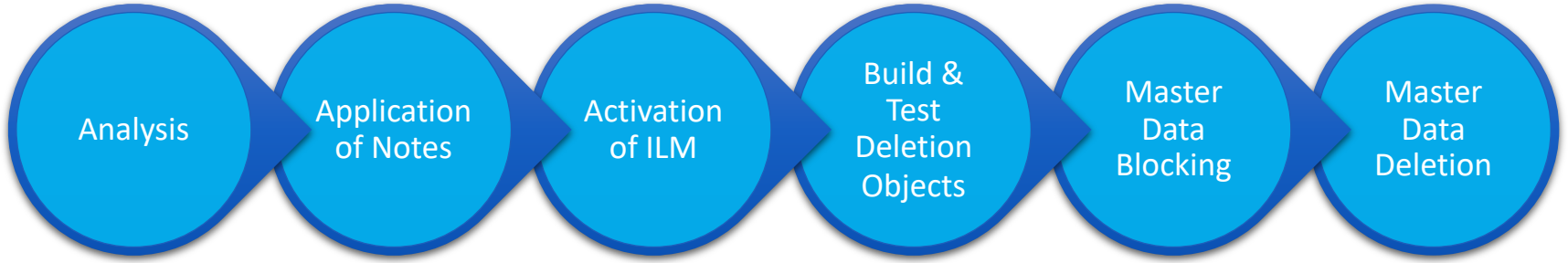
# Strategic Approach

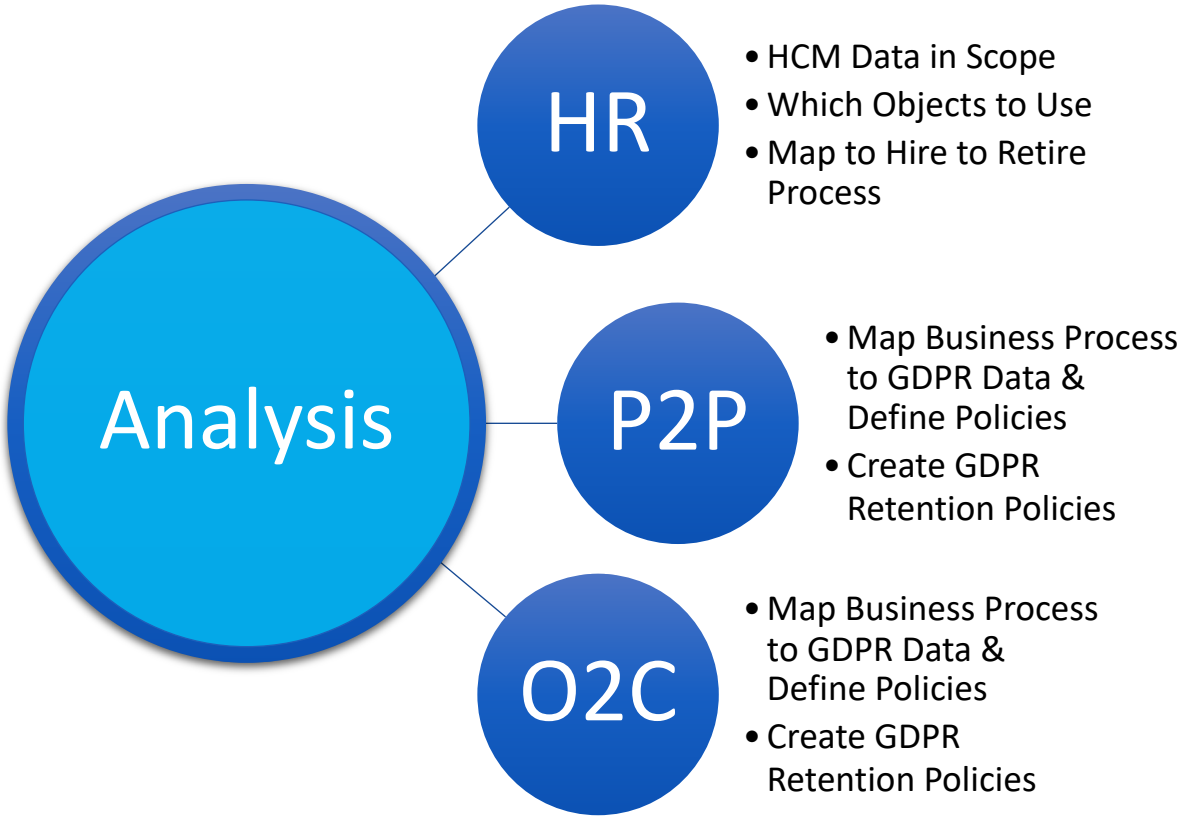



ILM = Information Lifecycle Management

# Phased Approach to ILM for GDPR

# Setting Up ILM - Analysis Phase




**Key Deliverables**

Blueprint for GDPR

Mapping Against Business Processes

Project Planning

proceed

# SAP ILM Free or Fee?

## Free

- Only to delete, block or archive Personally Identifiable Information (PII)
- Cannot be used for non PII data
- Cannot be used for decommissioning
- Limited Policy Setup
- Does not come with any storage option

## Fee

- Delete, Block or Archive any information in your SAP system
- Can be used for decommissioning
- Extensive Policy Setup
- Comes with SAP IQ

proceed

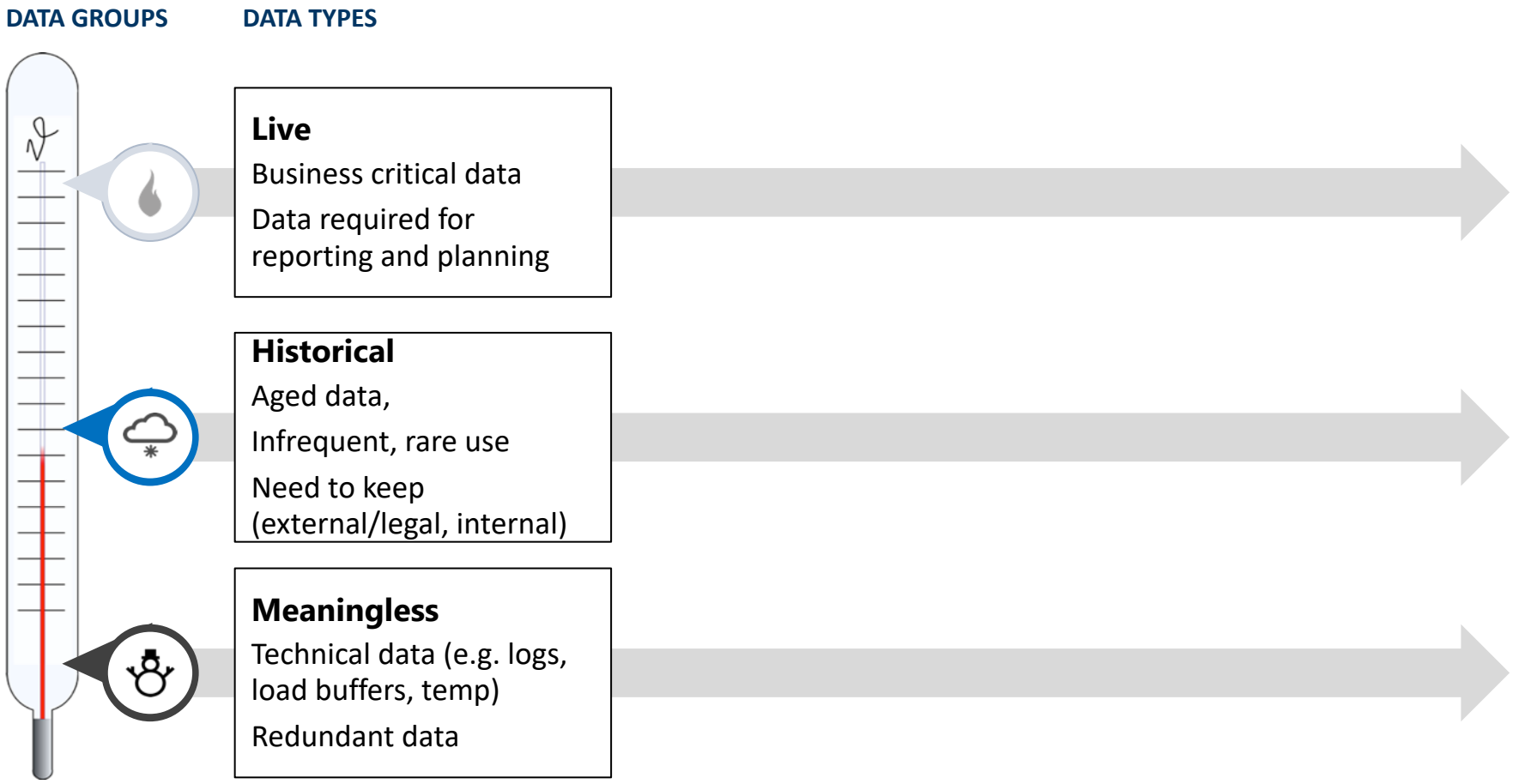
# Best practise SAP data protection tools and services to consider

# Key Foundations of Data Protection Compliance

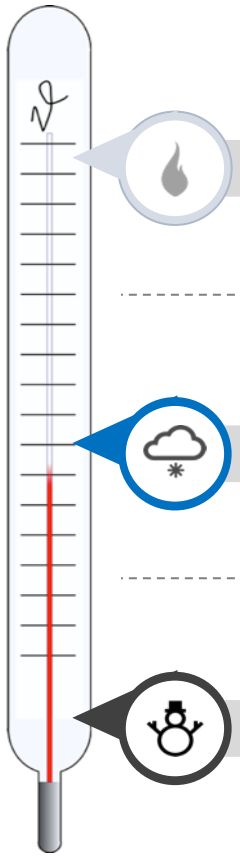
- **Purpose limitation (Principle b of the EU GDPR)**
- An Organisation must be clear about what the purpose for processing
- Organisations need to record the purpose as part of your documentation obligations and specify them in privacy information
- Organisations can only use the personal data for a new purpose if either this is compatible with the original purpose, or they obtain new consent, or they have a clear obligation or function set out in law.
- **Data minimisation (Principle c of the EU GDPR)**
- Organisations must ensure the personal data they are processing is:
  - Relevant – has a rational link to that purpose; and
  - Limited to what is necessary – Organisations should not hold more than they need for the stated purpose.
- **Storage limitation (Principle 3 of the EU GDPR)**
- Organisations must not keep personal data for longer than they need it.
- Organisations must justify how long they keep personal data. This will depend on the purposes for holding the data.
- Organisations need a policy setting standard retention periods
- Organisations should periodically review the data they hold, and erase or anonymise it when they no longer need it.
- Individuals usually have a right to erasure if the Organisation no longer needs the data.
- Organisations can sometimes keep personal data for longer for public interest archiving, research, or statistical purposes.

proceed

# Gauging the Data ‘Temperature’



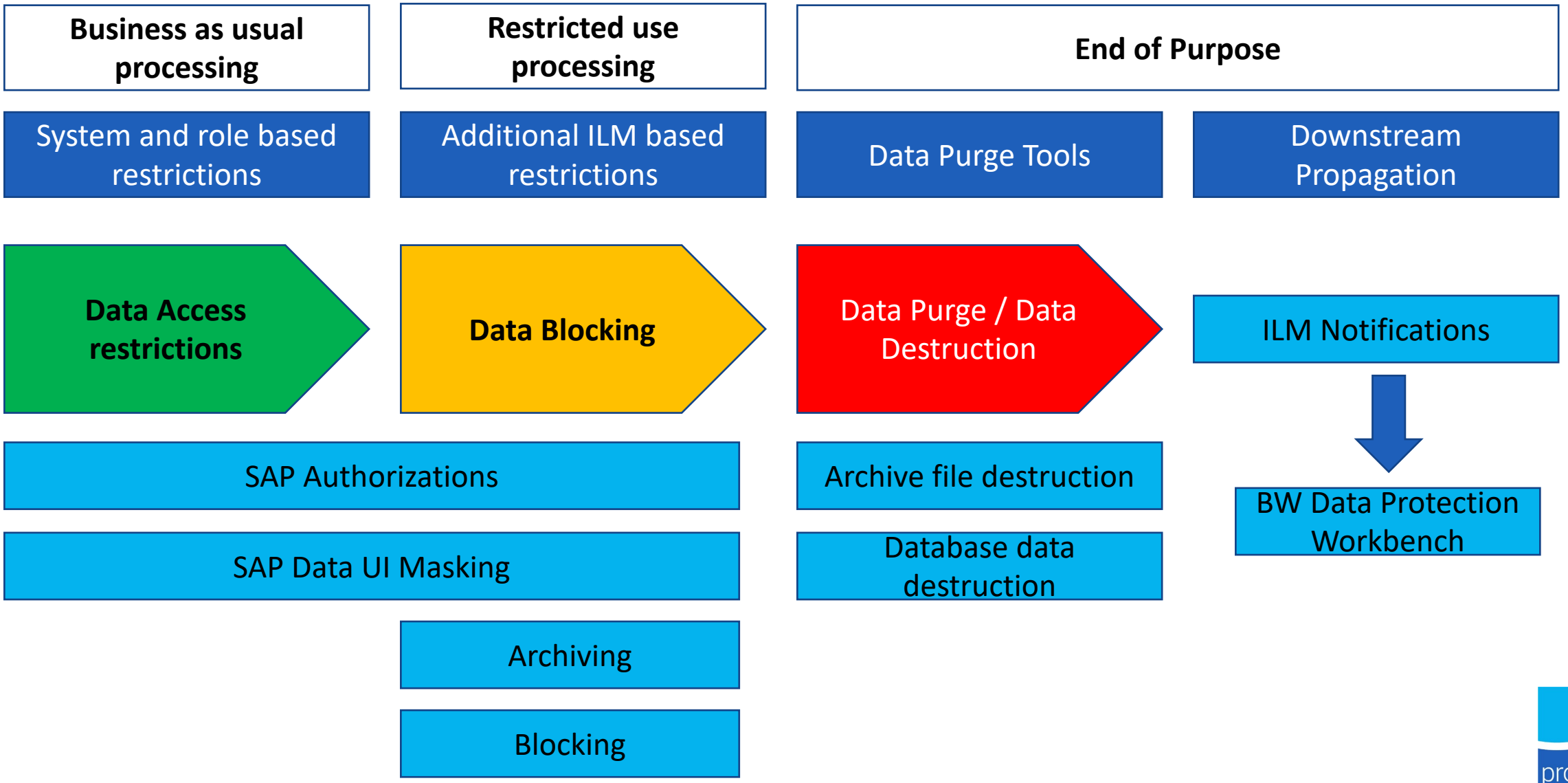
# Response to ‘Temperature’



| DATA GROUPS | DATA TYPES | GOALS | SCOPE OF ACTIONS | | |
|---|---|---|---|---|---|
| Live | **Live**<br>Business critical data<br>Data required for reporting and planning | Information “at your fingertips”<br>Speed and high availability is key | ▪ Performance optimization, Tuning<br>▪ In-memory<br>▪ Ensure SLAs are met | Business setisfaction | Keep in Live, mask or block if required |
| Historical | **Historical**<br>Aged data,<br>Infrequent, rare use<br>Need to keep (external/legal, internal) | Keep & store<br>Reduce cost | ▪ Set up central policies<br>▪ Use appropriate storage: Archiving, ILM, Smart data access | TCO & data access | Archive, mask or block if possible |
| Meaningless | **Meaningless**<br>Technical data (e.g. logs, load buffers, temp)<br>Redundant data | Purge, delete & housekeeping | ▪ Set up central policies<br>▪ Perform housekeeping<br>▪ Automation | TCO | Destroy |

proceed

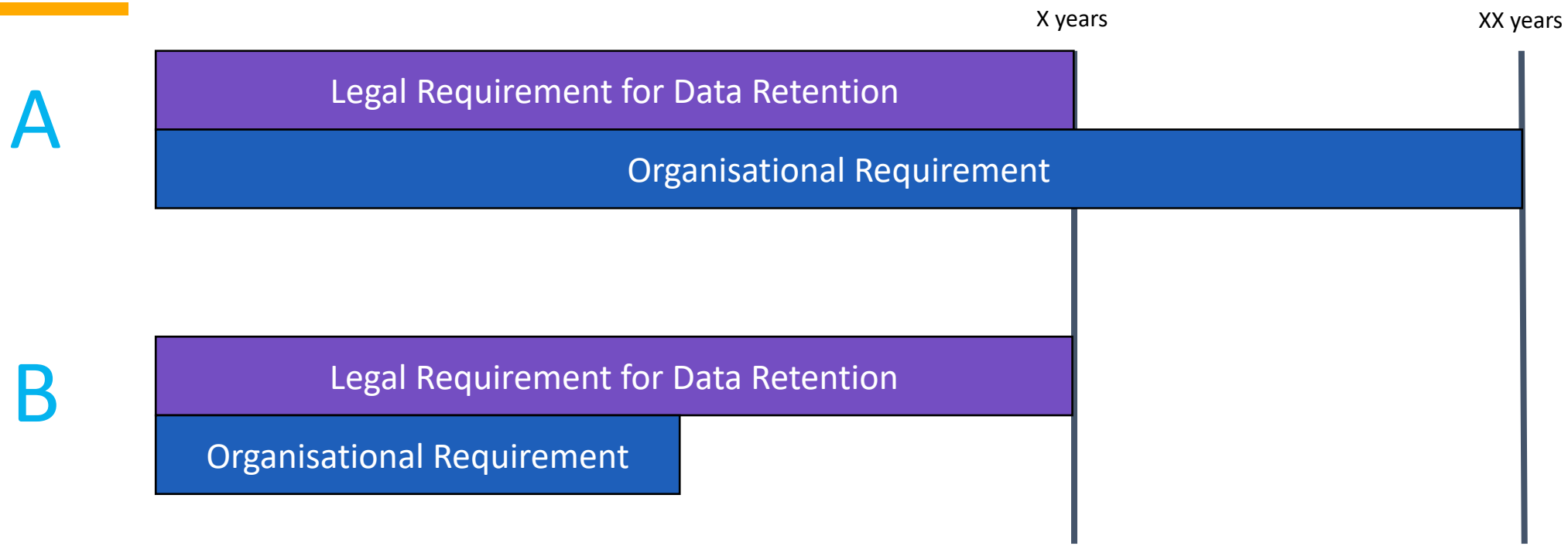
# Data Lifecycle and Data Access in an SAP ECC System



# What is End of Purpose (EOP)?

- Personal data is collected and stored for a specific processing purpose. Example:
  - To fulfil the purpose administrators need access to the personal data for a specific period of time – 7 years for example.
  - For the specific processing purpose you need name, address and bank details
  - After this primary purpose ends you may still need the data for reporting purposes (e.g., statistical analysis).
  - Even after the primary purpose is fulfilled other legal obligations might have to be taken into consideration, e.g., tax legislation, health and safety or statute of limitations.
- When data reaches the end of the primary purpose, data should be blocked for most users.
- When data reaches the end of purpose, i.e. there is no remaining justifiable purpose for the data, the data should be destroyed.

# Considerations for Retention

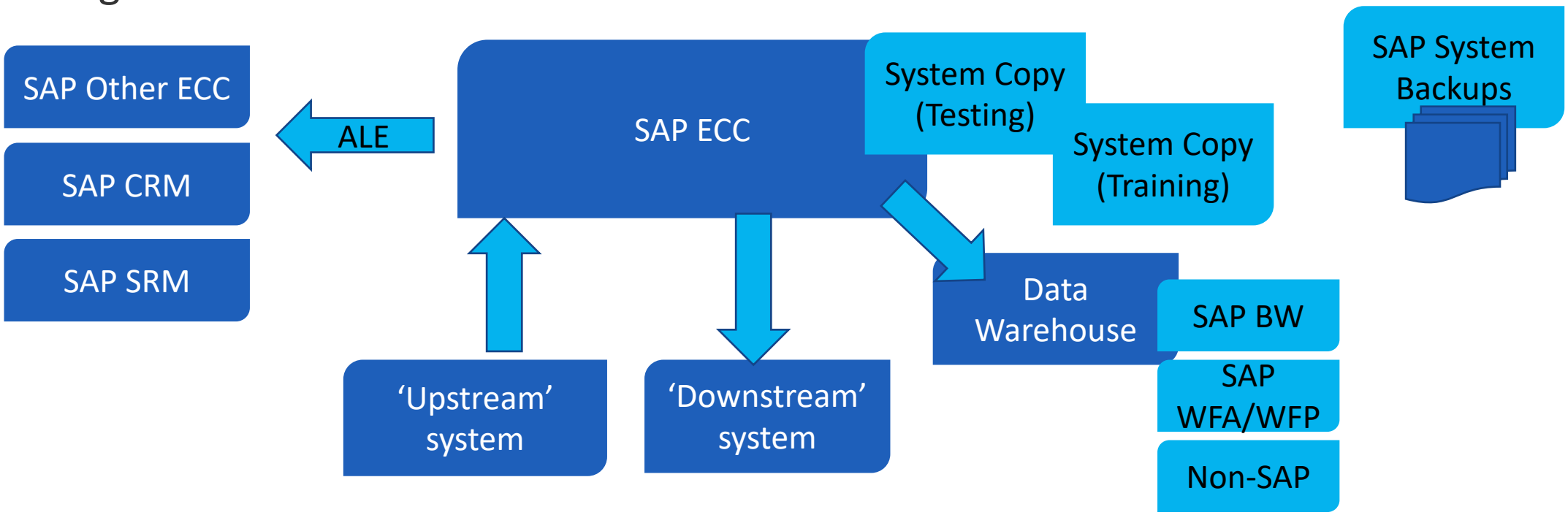



Example A:
The minimum retention is the legal requirement, however, there is an Organisational requirement to retain the data for a longer period.

Example B:
The minimum retention is the legal requirement. No Organisational requirement to keep longer so can be immediately considered for deletion once minimum retention period is reached.

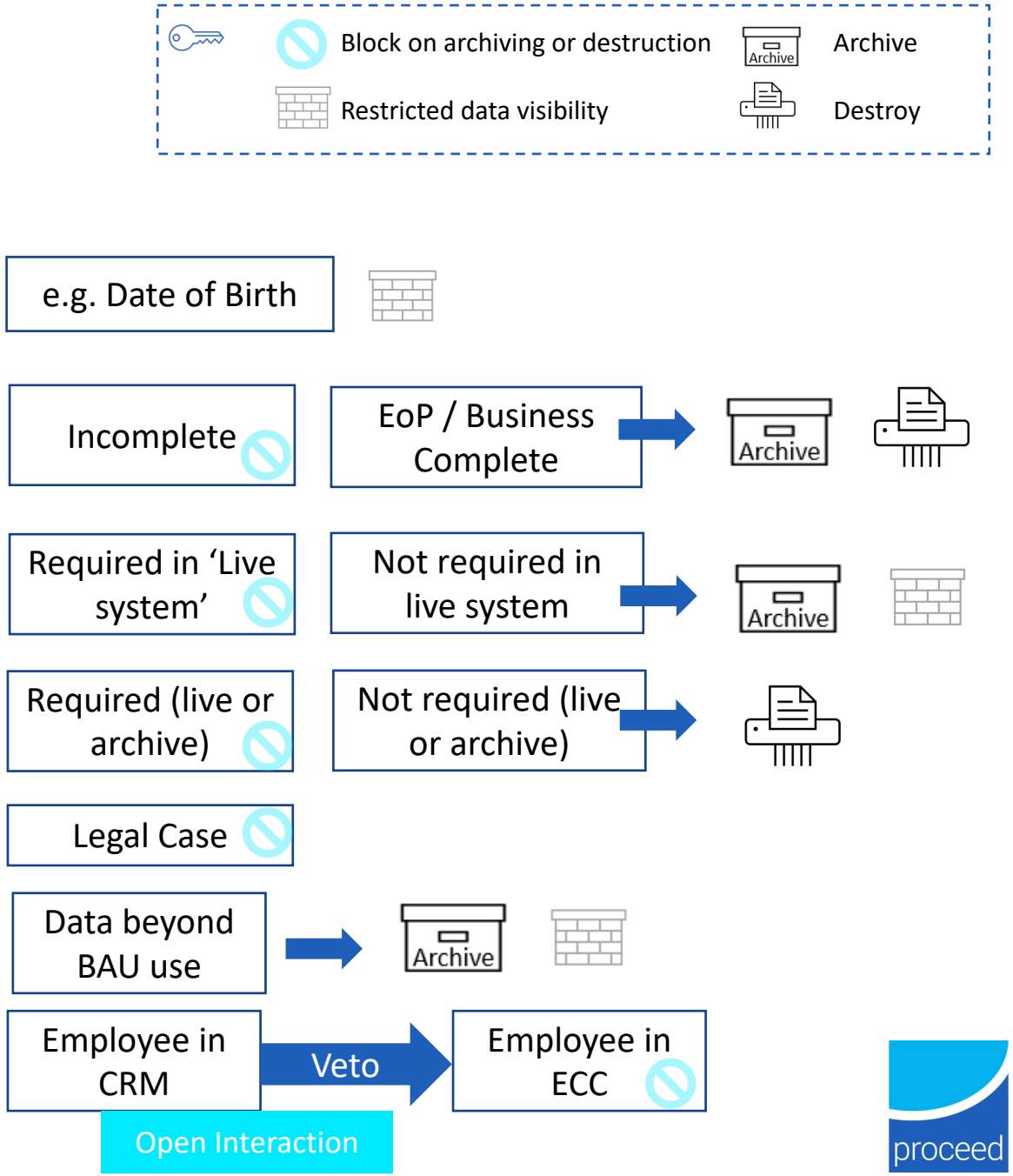
# Holistic Data Approach

- All systems that hold the specific type of data need to be considered in the approach.
- Some of the systems will ‘inherit’ the new status quo due to being system copies. Other systems like data warehouses and linked systems may need specific strategies.

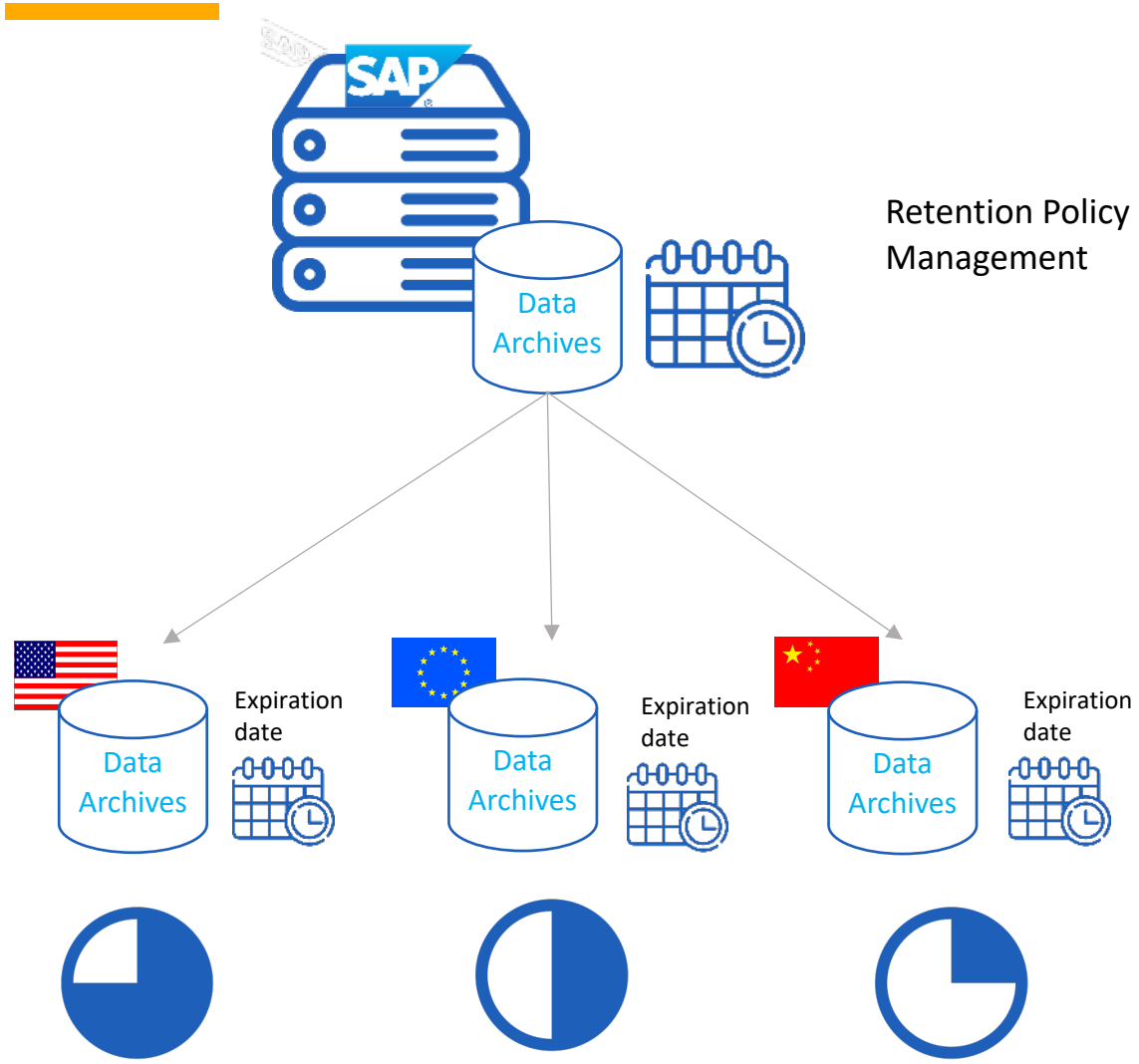


# Data Protection Toolset

- UI masking for data that user needs to see existence of, but does not need to see values
- End of purpose checks / business complete checks for archiving and destruction
- Residency rules i.e. rules controlling when data can be archived
- Retention policies i.e. policies controlling when data can be destroyed
- Legal Hold
- Blocking
- Destruction veto where another system still needs the data



# SAP Information Lifecycle Manager




## Manage and enforce retention policies

- Set policies for automatic data retention and subsequent destruction
- Retain data according to set policy
- Responsibly destroy data when expiration date has been reached

## Maintain Separate Archives per Retention Period

- Create multiple data archives for each data expiration data

## Perform e-Discovery

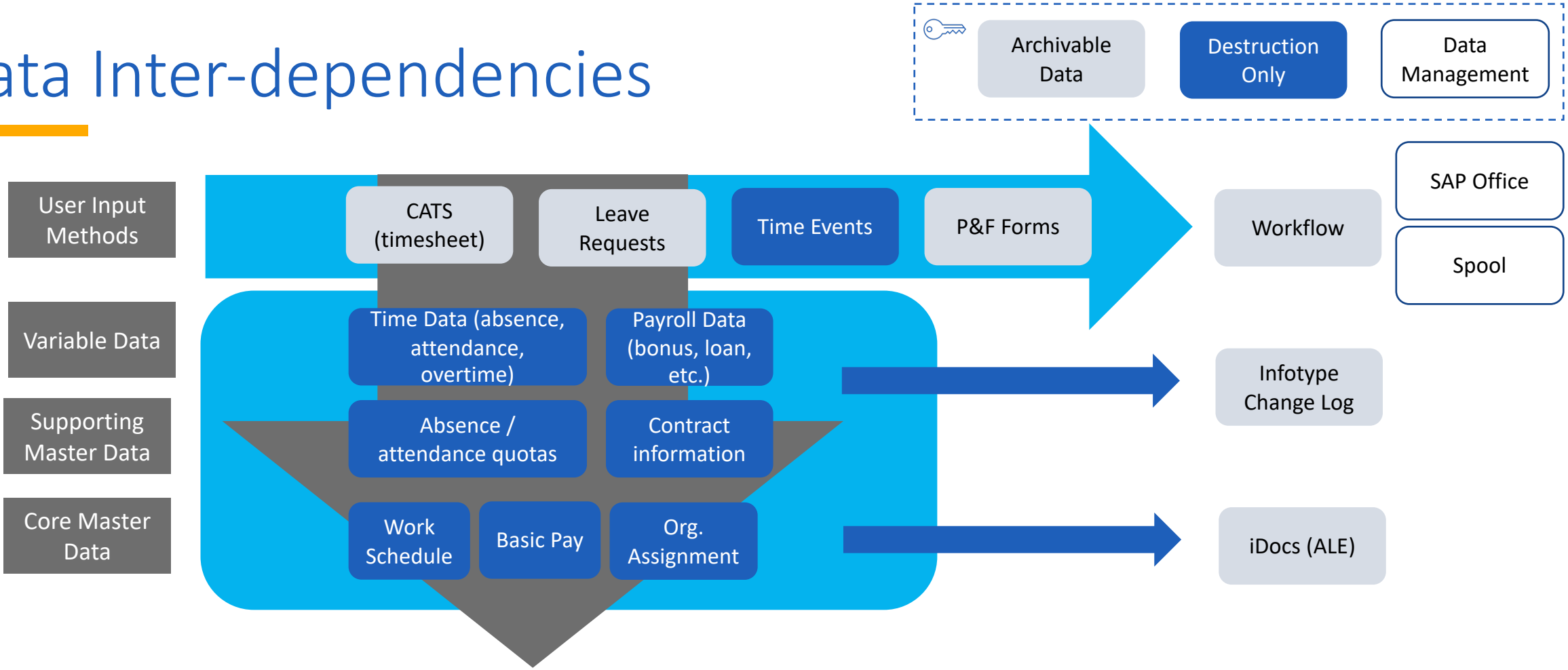
- Search for information in response to legal requests

## Apply Hold on Data

- Automatically prevent data deletion or destruction
- Apply holds to archives and current database

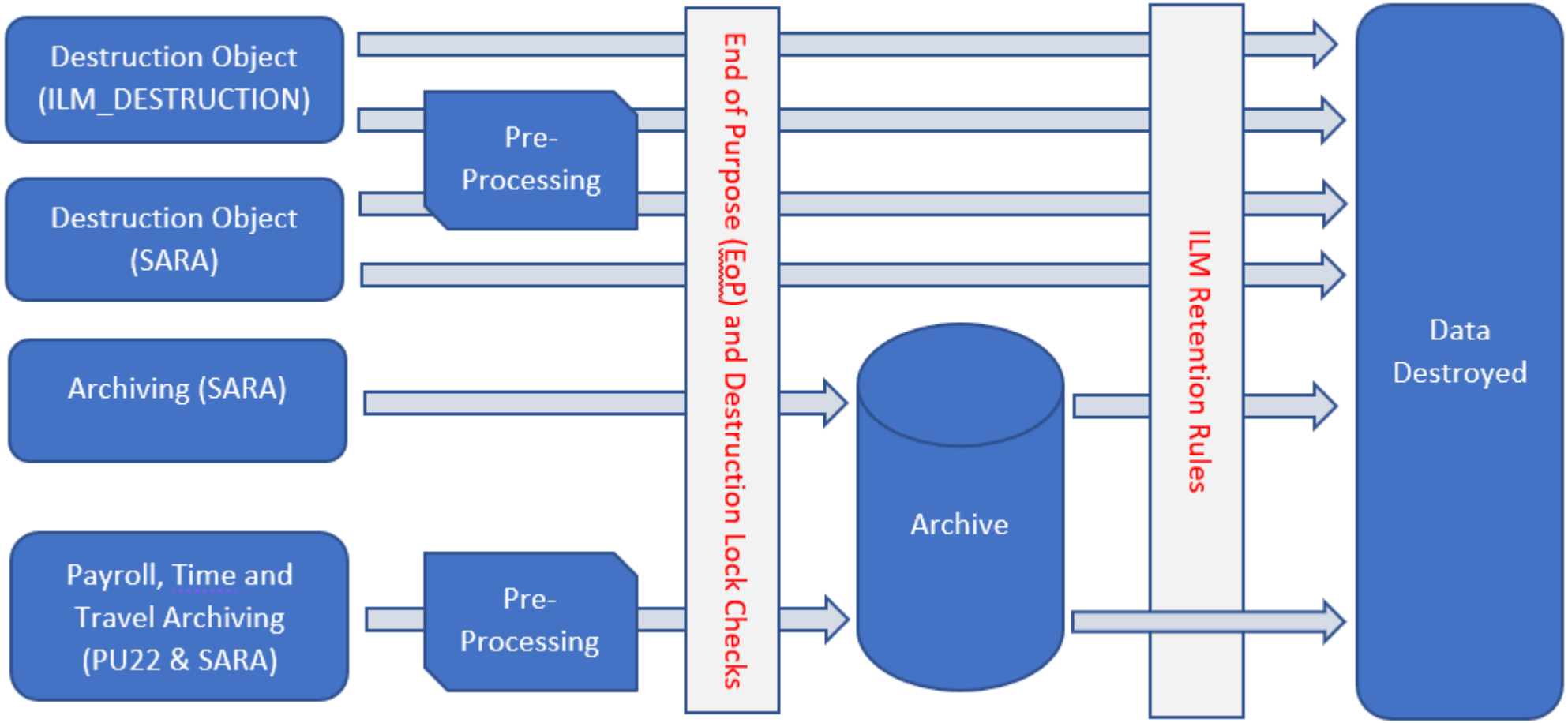
proceed

# Data Inter-dependencies



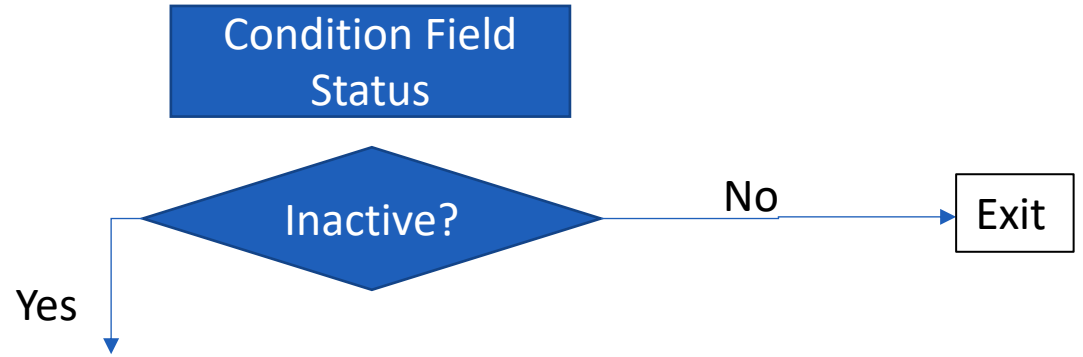

Archiving payroll or time prevents further changes in the archived period

# Overview of Types of Archive and Destruction in SAP ECC

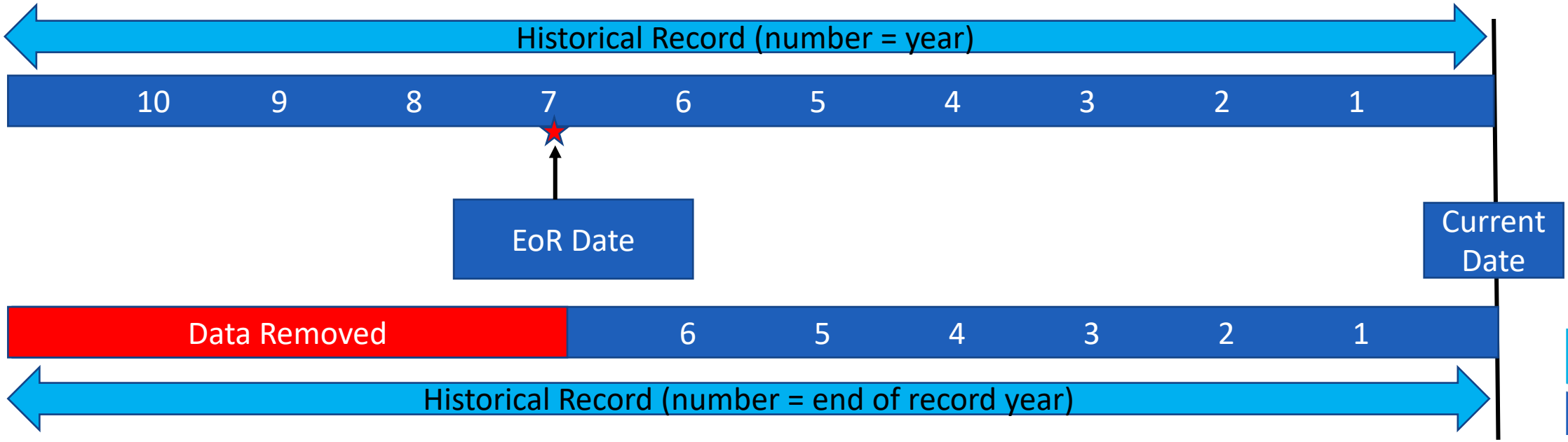



proceed

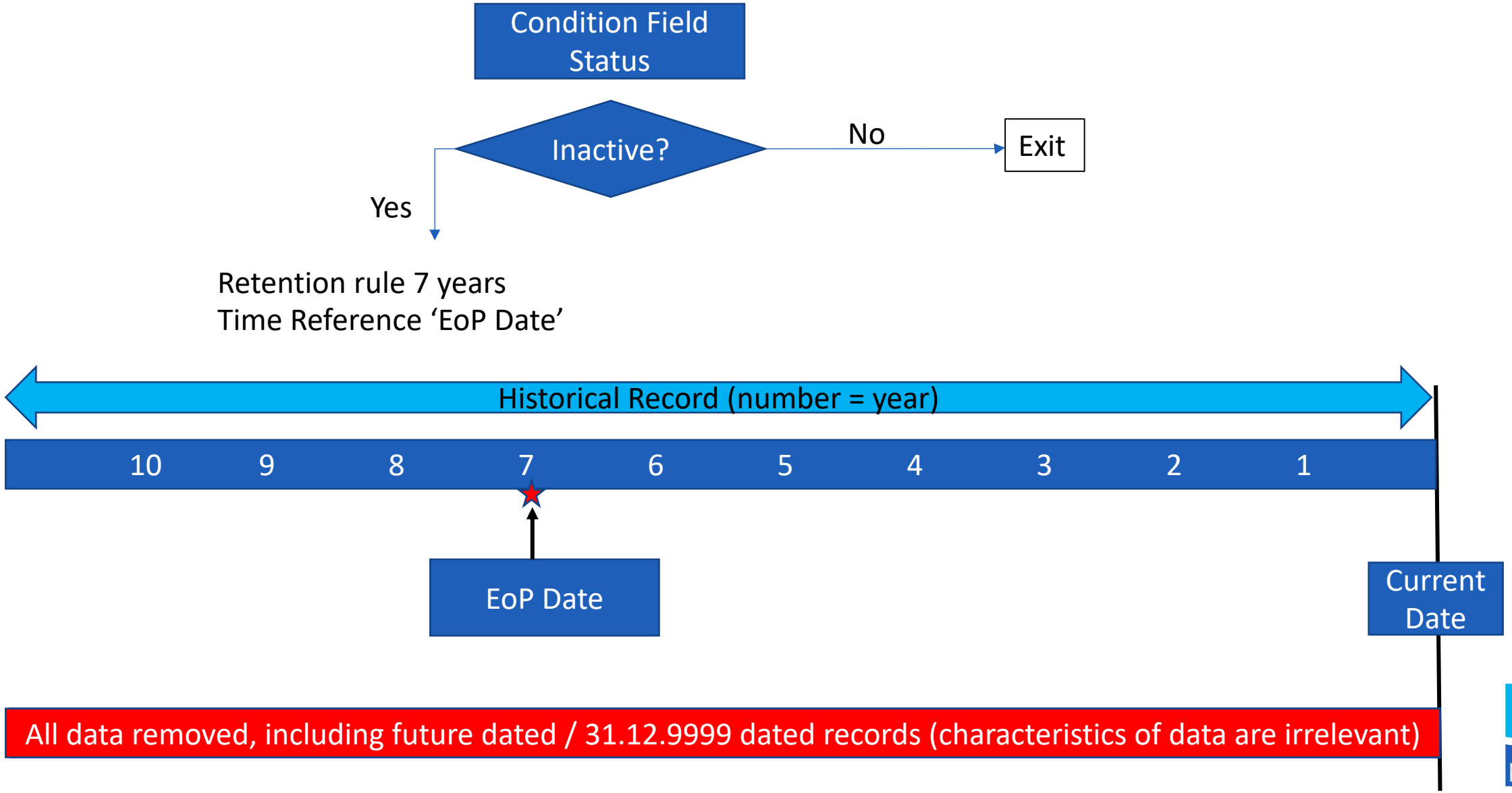
# Example: Destruction by ‘End of Purpose’ Date




Retention rule 7 years
Time Reference ‘End of Record’



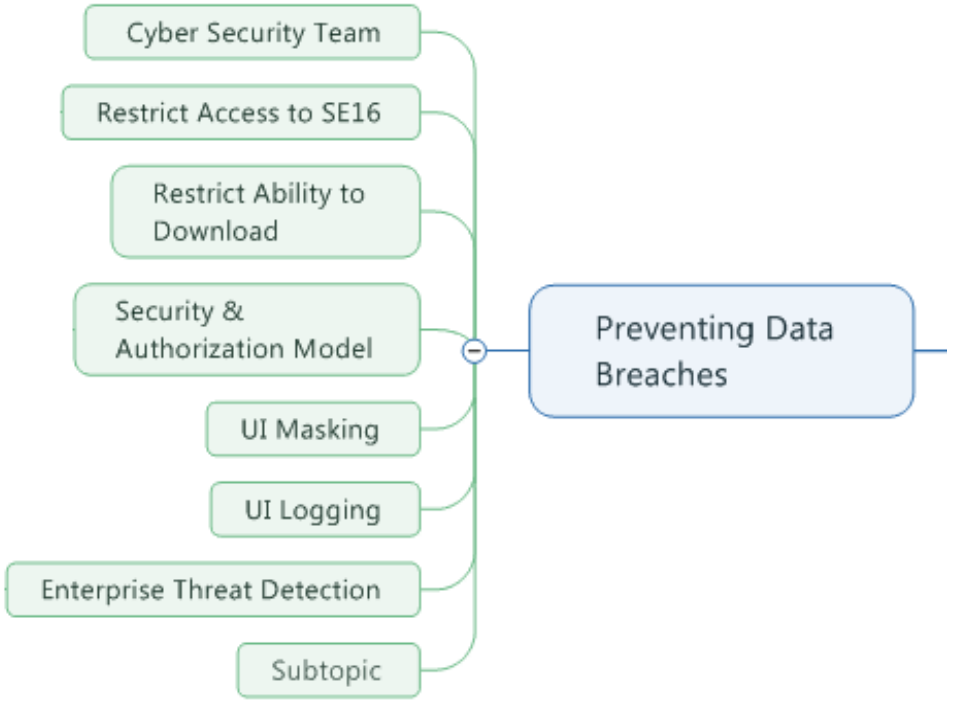
# Example: Destruction of all Related Data by Status



# Preventing data breaches

# Preventing Data Breaches

1. Restrict Access to SE16.
2. Restrict Access to being able to Download data from an SAP Transaction.
3. Ensure the Security & Authorisation Model is fit for purpose and has clearly defined processes for both provisioning and provisioning access.

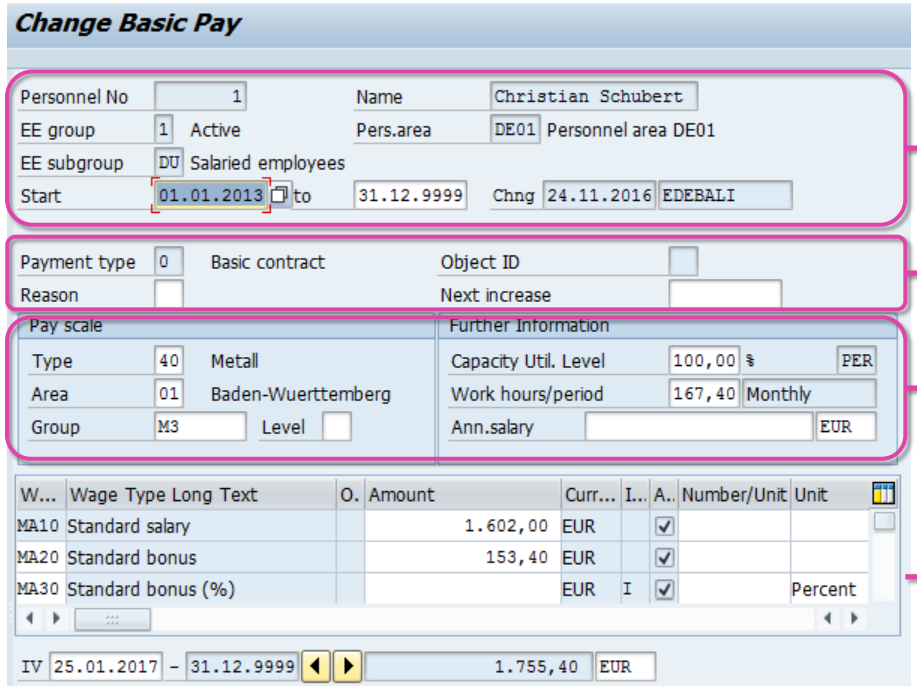


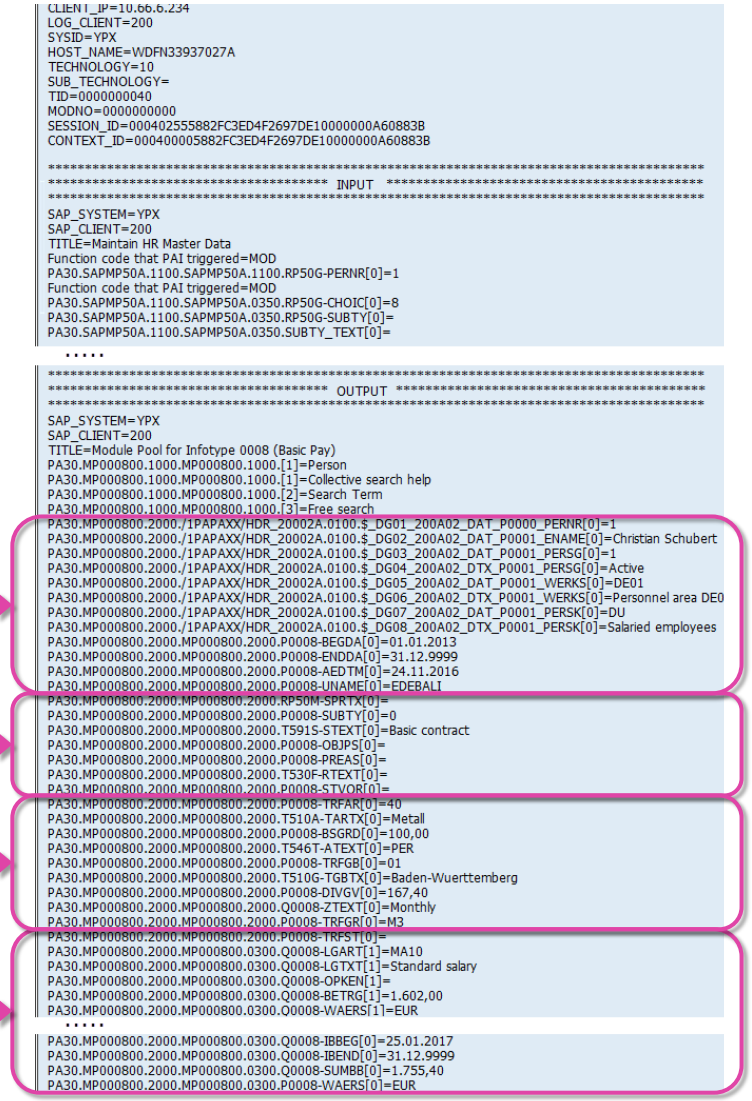
# Additional Tools Available from SAP UI Logging

- Logging **based on roundtrips** (frontend→server→frontend)
- filtering options to **control log file size**
- **efficient analysis:** log data organized with unique <name> →value pairs
  - on demand: **detailed analysis** of log file via Log Analyzer
  - real time: **configurable alerts/notifications**
  - automated: **integrated with ETD** → usable as powerful data source

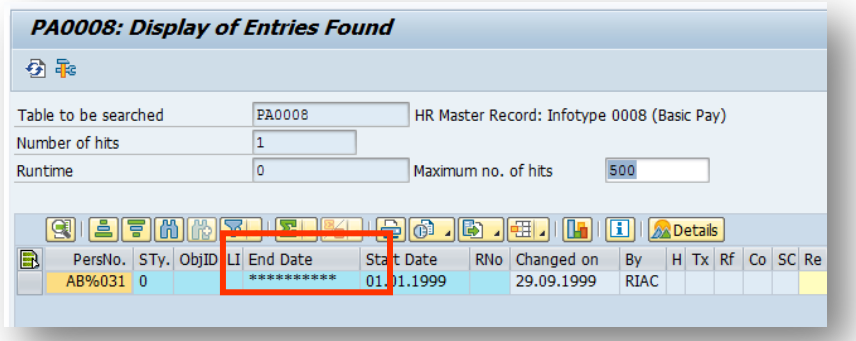
transaction: PA30
"Maintain HR Data"

Infotype 8
"Basic Pay"



# Additional Tools Available from SAP UI Masking






- Multiple uses:
- Minimal impact on ‘live data’ and ‘historical data’ systems
- Common core business areas such as HR, procurement, CRM, ERP, reporting
- UI Masking SAP only

proceed

# How Telia is using SAP ILM on their GDPR journey

# Telia Case Study

Telia needed to enhance their GDPR compliance to keep in-line with regulations which have already been announced and future directives internationally, thus ensuring personal data is readily available when required, but only visible to the approved employees within the business. With the right to be forgotten easily actionable and requirement to block customers, vendors, and business partners information when data rules set in SAP ILM for GDPR had been reached.


## What Proceed did:

Telia engaged with Proceed Group to implement SAP ILM and set up GDPR rulings which automates many of the processes required to meet the data regulations across the countries they service.

- Implemented ILM on SAP CRM and S/4HANA systems
- Enabled blocking to take place
- Blocking business partners in CRM and replicated in S/4
- ILM implementation took 7 months

proceed

# Questions



# Thank You

Paul Wood
Regional Lead

paul.wood@proceedgroup.com
+45 (0) 89 88 47 52