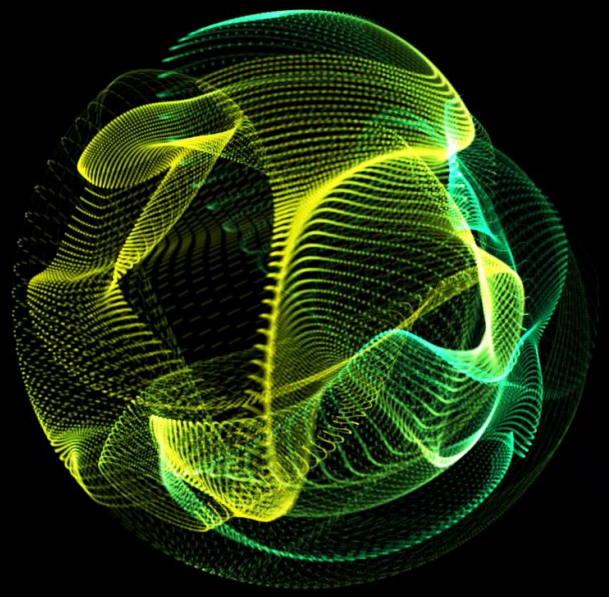
Deloitte.

SAP & Data Protection

2 sides of the same coin



Georgia Skouma (Deloitte BE)
Malene Fagerberg (Deloitte DK)

May 16th, 2022

Meet the moderators

Georgia Skouma

Director Deloitte Belgium

RELEVANT EXPERIENCE

Georgia is a Director with Deloitte Belgium Risk Advisory with a seniority of 24 years in legal advisory, incl. ICT law, information protection and privacy. Former lawyer of the Athens and Brussels Bars, Georgia has been supporting clients of the public and private sector in the design and implementation of Digital Transformation Programs and holistic strategies on data management.

gskouma@deloitte.com

Malene Fagerberg

Partner Deloitte Denmark

RELEVANT EXPERIENCE

Malene is an experienced Privacy leader with 15 years of work experience and implementation of data protecting/ privacy regulation and best practices. Background from Top-tier law firm and in-house experience with GDPR compliance from medical device company, B2B/B2C, financial institution and public sector. Named in Legal500 as data protection expert. Joined Deloitte in 2021 as Partner of Privacy.

mfagerberg@deloitte.dk

AGENDA

Table of Contents

Technology brings new CHALLENGES to data management. Data is a new DRIVER for business while its protection has become KEY. New regulations ARE EMERGING . . .

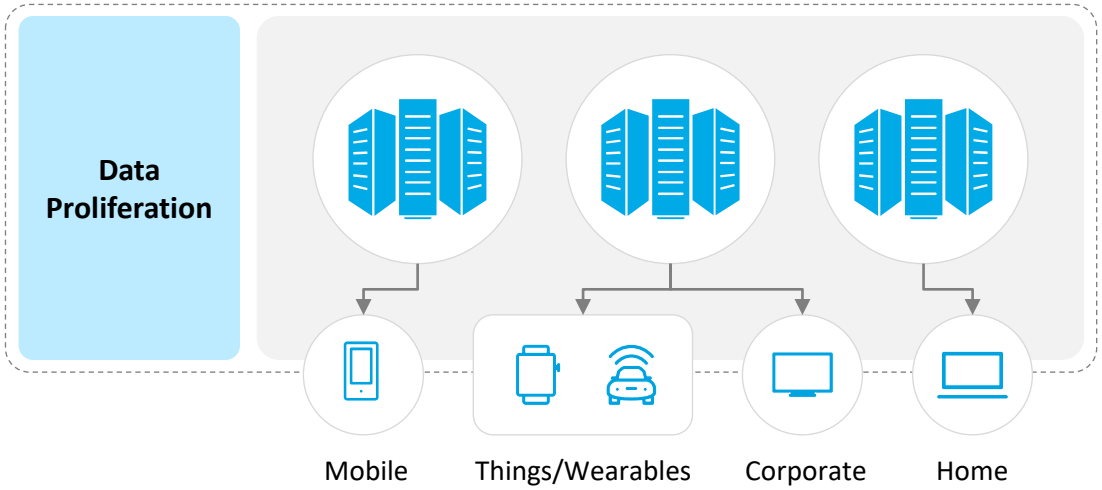
The purpose of this Webinar is to give some thoughts on how (personal) DATA PROTECTION BY DESIGN CAN be met efficiently in large IT SAP implementations without depriving the business from the VALUE of the data under protection

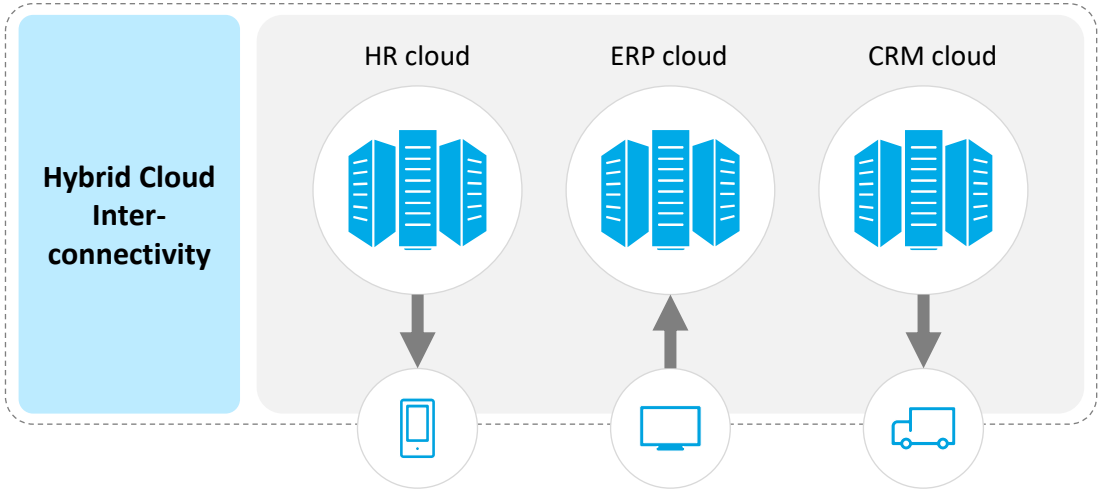
SAP & Data Protection

What does it mean for my business

Data Privacy and Protection on ERP: why now?

Need for a comprehensive Data-centric Security Strategy across corporate entities & business operations





Data crosses traditional boundaries as organizations **transform** their **ERP processes** with the **cloud, and hybrid networks**.

Organizations need a **data-centric security strategy** to **mitigate business risks** triggered by data privacy and protection **laws**, **proliferation** of data and **cyber threats**.

Benefits of Data-centric Security Strategy

- Data asset protection
- Compliance with privacy regulations
- Extended enterprise security
- Brand protection
- Data breach resiliency
- Maintain customer privacy
- Data protection for cloud
- Data risk protection throughout the data lifecycle

Bring privacy into the picture: why now?

Sensitive data is not only personal data, but rather data deemed sensitive by the organization

	DESCRIPTION	IMPLICATION FOR ERPs	CLOUD CONSIDERATIONS
Enterprise data	• Intellectual property • Trade secrets	• Customer information • Supplier information	• Product/material master data • Customer master data • Vendor master data • Bill of materials master data • Production order/recipe data
Financial information	• Bank account information • Financial statements	• Consolidated financial statements • Credit card/bank information	• Employee master data • Vendor/customer master data • Financial data/reports
Personally Identifiable Information (PII)	• Salary • Home address • Home phone number • Personal email address • National identifier (e.g., SSN) • Driver license number • Race/ethnic origin • Political or philosophical views • Gender or gender identity • Religious beliefs or affiliations • Trade union membership • Veteran status	• Provide overall program management for technical systems and analytics workstreams • Measure value and return on use cases • Develop and implement training and knowledge transfer	• Provide overall program management for technical systems and analytics workstreams • Measure value and return on use cases • Develop and operationalize intake model for new use cases
Regulatory	• Environmental Protection (EPA) related data	• Details on contracts with the government agencies	• Sourcing/procurement data • Quality assurance data

***Note:** This list of data types is not all inclusive, but rather a set of examples

SAP Capabilities

Helicopter view of “privacy enhancing” capabilities

-

Data protection Strategies

Data Protection Strategies

	OS Layer	Database Layer	Network Layer	Application Layer
Foundational	• Access controls for **OS command execution** from the application layer	• **Role-Based Access Control (RBAC)** • **HANA Transparent Data Encryption** • **Analytical Privileges** for access controls	• **Secure Socket Layer (SSL) and Transport Layer Security (TLS)**—Security communication traffic over internet protocols • **Secure Network Communication (SNC)**	• **Role-Based Access Control (RBAC)** • Functional and organizational restrictions • authorization groups, • enablement of (custom) authorization checks
Intermediate		• **SAP Test Data Migration Server:** Scrambles the data from production before it is copied to the non-production systems • **HANA Dynamic Data Masking** • **HANA Data Anonymization**		• **SAP UI Masking and Logging** • **SAP Read Access Logging (RAL):** Monitor and log visibility of sensitive data • Development of **custom security solutions** by using customer exits
Mature		• **SAP Information Lifecycle Management (ILM):** Automates data retention through policies to govern the data lifecycle in the SAP system • HANA **Client-Side Encryption** • **SAP Data Custodian** • **SAP Information Steward**		• **3rd party Encryption, DLP Solutions**

Foundational and intermediate solutions are also required for advanced data privacy and protection

SAP tools in correlation with privacy

SAP GRC Process Control and Risk Management

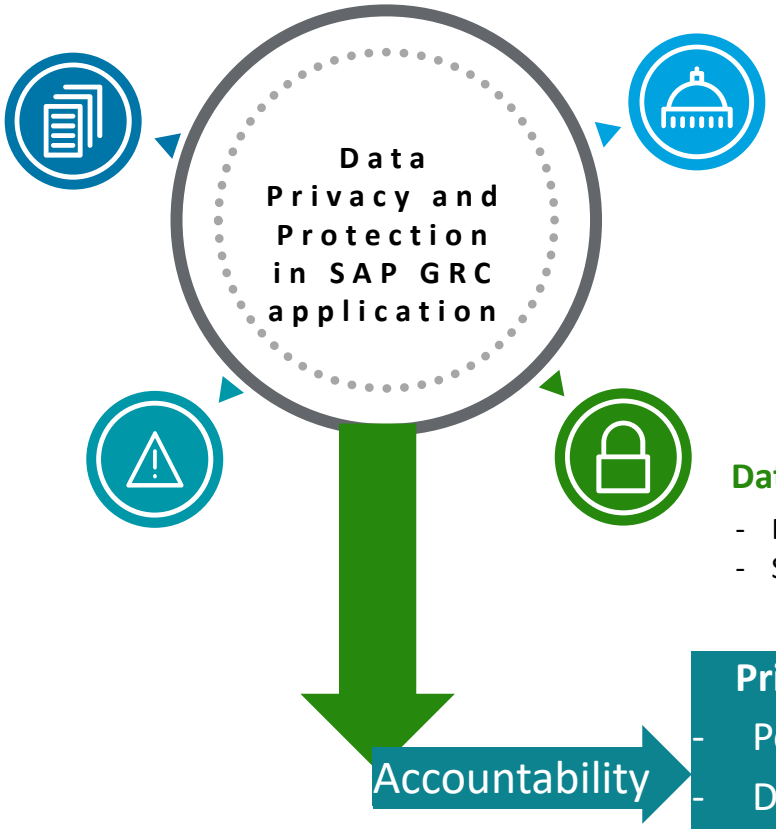
✓ Do you know the types of data you have?

Records of Data Processing Activities

- Treatment Description
- Added data fields
- Warnings for sensitive data

Risk analysis & assessment

- Assessing inherent / residual risks
- Mapped to data processing activities
- Triggering mitigation plans



DPO Operating Model

- DPO granted “owner” of tasks & their follow-up
- Launchpad
- Notifications for tasks for own tasks and of others

Data Breach Management

- Incident description form
- Email communication
- DPO active intervention (validation, etc.)
- Maintenance of risk Log

Data Protection by design

- Data Protection Impact Assessment
- Standard questions & types of risks

Privacy-Enhancing settings in SAP GCR

- Policy management functionality
- DPO work box
- Email communications...

SAP tools in correlation with Privacy

SAP UI Data Protection Masking

Data Protection Masking
Field-level authorization; otherwise, data masked/cleared/hidden or disabled

Attribute-based authorization
Creation of policies on how to protect sensitive data

Authorization trace
Used for verification of authorization configuration

Reveal on demand
Masks field value by default; optional reveal by giving reason for viewing the data (authorized users only)

Data-element-based-masking

Recording tool

Field access trace
Writes a trace entry whenever a user accesses fields

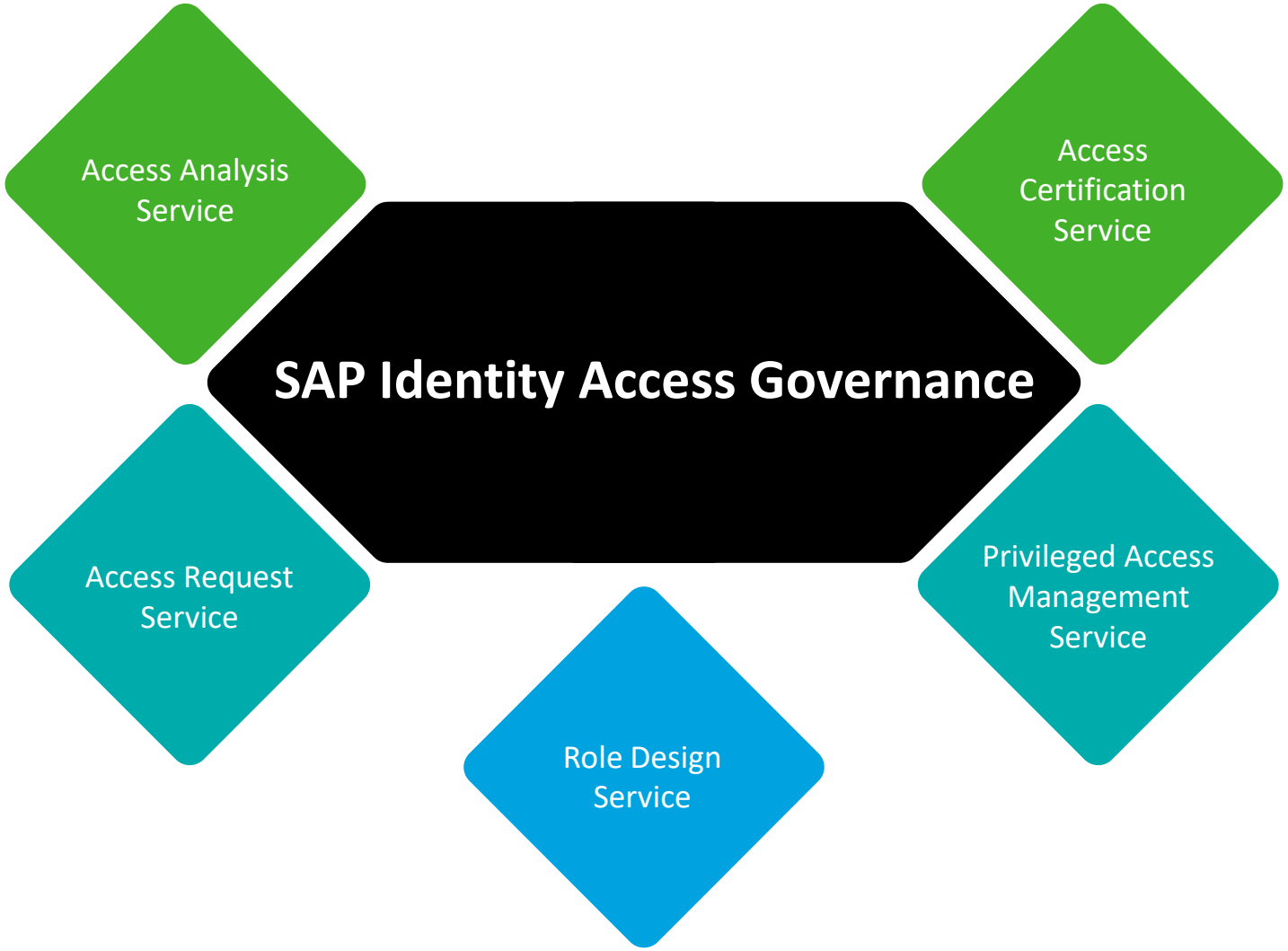
Data Protection based on sensitive & context attributes
Masking & blocking applied to core entity, being sensitive attribute; context attributes encompass information related to sensitive attribute

Data blocking
Block access to entire sensitive records by suppressing lines in table-style UI elements

SAP Fiori Applications

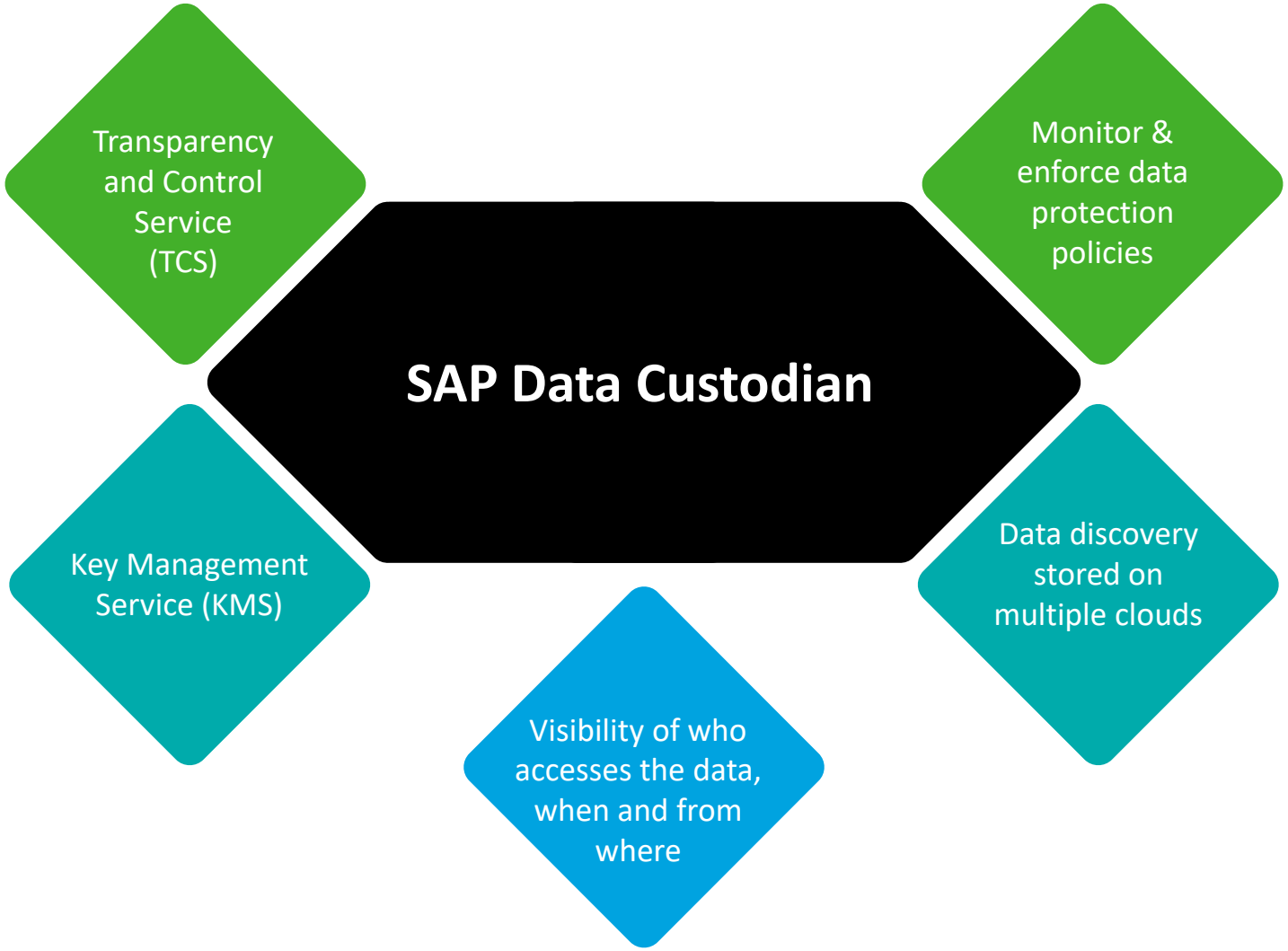
SAP tools in correlation with Privacy

SAP Identity Access Governance



SAP tools in correlation with Privacy

SAP Data Custodian



SAP Privacy Add-ons can improve data governance as per examples below:

SAP Privacy Governance
- Security & privacy governance
- Data-driven assessments
- Data subject's rights requests

SAP UI Data Protection Masking
- Reveal on demand
- Authorization trace
- Data protection masking

SAP Data Mapping & Protection by BigID (SAP branded)
- Data discovery & catalogue
- View on sensitive data across data stores
- Identify data usage
- Map data with ML, data classification, correlation and cataloguing
- View on data localization

SAP Data Custodian
- Transparency and Control Service
- Key Management Service
- Monitor & enforce data protection policies
- Customer controlled encryption keys
- Key lifecycle management
- Secure storage of keys in cloud

Information Lifecycle Management
- Data archiving & management
- Retention management
- System decommissioning

SAP Data Retention Manager
- Manage business purpose
- Delete data subject information
- Retention and residence rules handling
- Archiving and destruction

SAP Privacy Modules

1

SAP Privacy Governance

- Security and privacy governance
- Data-driven assessments
- Data subjects' rights requests

2

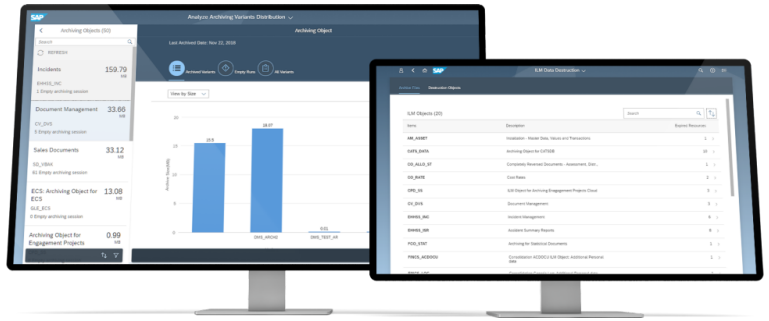
SAP Data Mapping & Protection by BigID

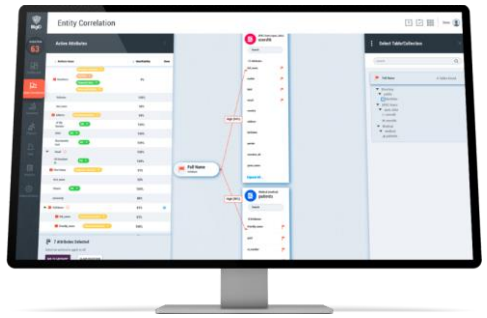
- Data discovery & catalogue
- View on sensitive data across data stores
- Identify data usage
- Map data with machine learning data classification, correlation and cataloguing
- Visualize data location

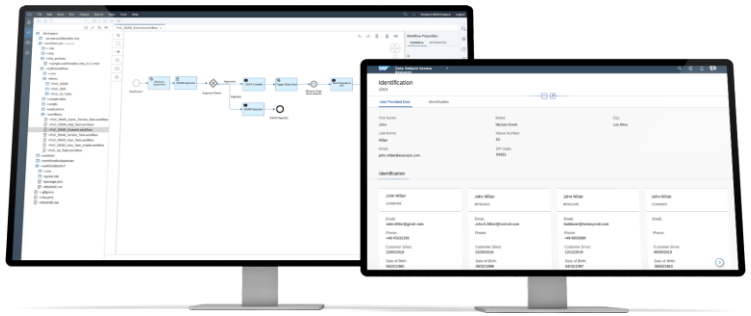
3

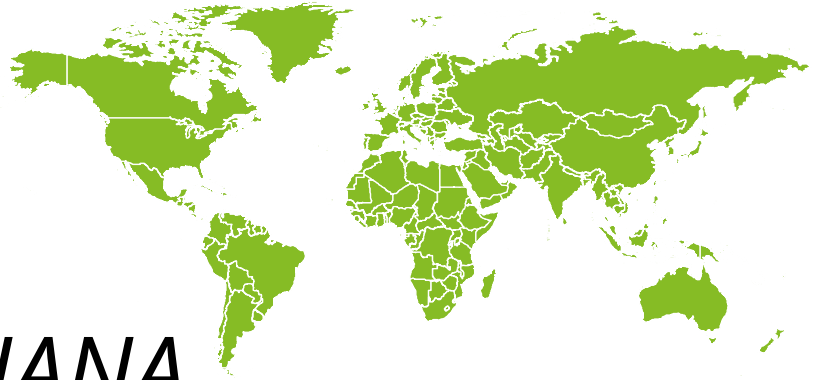
Information Lifecycle Management

- Data archiving and management
- Retention management
- System decommissioning









Privacy in SAP/S4HANA

Implementation in a global organization

- Malene Fagerberg
Deloitte DK

Holistic privacy compliance in ERP solutions

Law, Technology and business processes

The interactions of privacy

Compliance for SAP/S4HANA cannot be obtained within the solution itself, but requires interplay between the law, technology and your organisation

Law

Implementing SAP/S4HANA in a global organization requires compliance with several different laws and regulations depending on in which legal jurisdictions the solution is implemented, e.g., the GDPR in EU, the Russian data localization law, the Chinese cyber security law and PIPL, the American CCPA or other national local privacy or security laws.

Technology

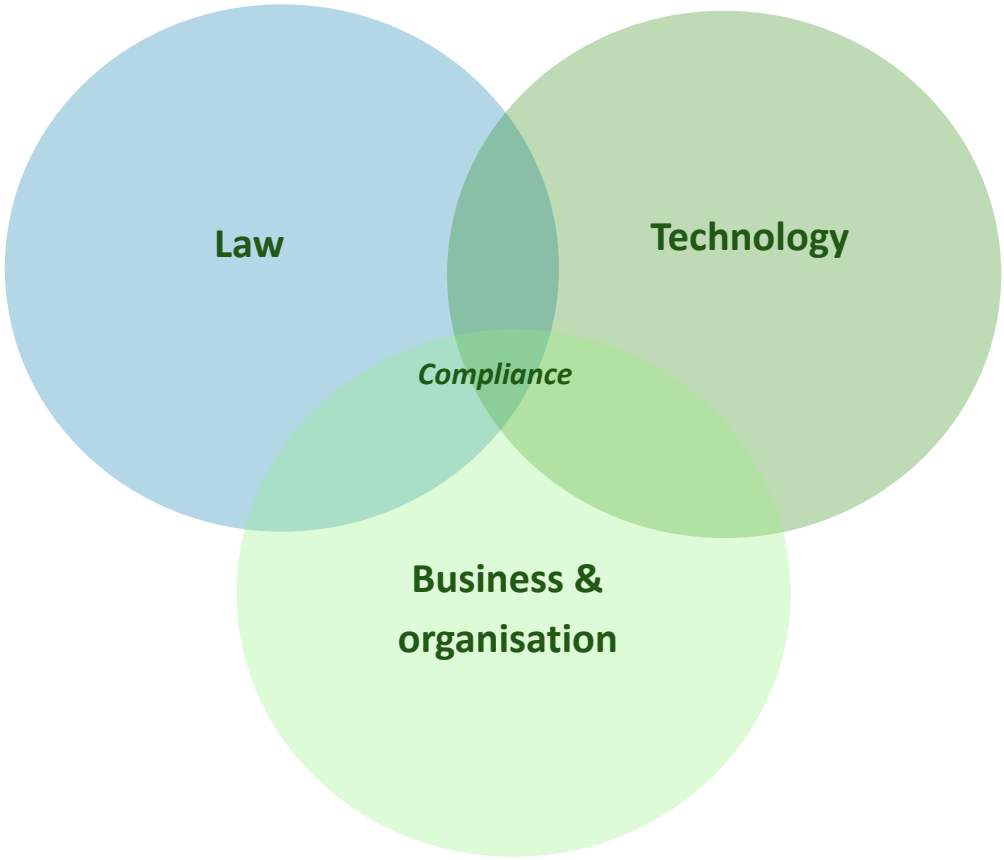
Technology supporting privacy is important for compliance, since privacy regulations require organisations to:

- protect personal data through IT-security measures
- implement privacy-by-design where the protection of personal data is considered already when designing and implementing solutions

Furthermore: Technology may support the data protection compliance through the use of tools, such as data tagging, data loss prevention solutions or automated risk assessments.

Business and Organisation

The organisation's strategy and business objectives are determining factors in data protection compliance. Risk management is necessary to obtain business objectives. Risk management should be based on a structured approach to risk assessments within privacy and security in both processes and IT solutions in order to assess, manage and mitigate risks in accordance with the organisation's risk appetite.



Data Protection broader than the implementation of SAP S/4 HANA

Compliance of data processing goes beyond the data processing activity taking place in the solution and must be supported by general compliance in the organisation

Personal data breach management / Incidence response

Management of the 72 hour deadline, assessment of the risk to the data subjects and requirements of documentation require fast coordination and aligned processes between the relevant functions

- Set-up process for management and logging of data breach incidents
- Collect information of security breaches
- Investigate incidents (forensics)
- Notify the Data Protection Agency of a security breach within 72 hours
- Notify the data subjects of the security breach

Vendor management

A large part of the processing of personal data for which an organisation is data controller of is done by third parties

- Procurement process must ensure that data protection and security is considered before implementation of SAP S/4 HANA
- The SAP data processing agreement must be reviewed and approved by the organisation as well as entering into data processing agreements and/or agreements on joint controllership with other vendors in relation to the S/4 HANA implementation, e.g. data migration tool vendors.
- Auditing of vendors (data processors) and sub-suppliers (sub-processors) must be conducted continuously.

Training and awareness

Data protection starts at the bottom. Processing of personal data is done and managed by the employees of the organisation every day

- Implement and monitor learning program for employees , e.g. a LMS e-learning portal
- Launch awareness campaigns about personal data protection and GDPR
- Test the awareness level e.g. periodic phishing tests

Governance

A governance model must be in place to ensure accountability

- Produce a governance model between legal entities (global and local) in the organisation to ensure all legal requirements are handled by the right legal entity
- Ensure that data processing agreements are in place between the different legal entities within the organisation
- Set up Binding Corporate Rules (BCR) in the global organisation if needed
- Ensure implementation of SAP S/4 HANA meets the organisations internal policies, standards and guidelines
- Set up risk metrices and reporting in line with the organisation's ERM processes

Information security

Data protection must be incorporated into the general work with information security as an aspect hereof

- SAP S/4 HANA should be incorporated seamlessly into the organisation's IT architecture, including the SIEM and data loss prevention systems
- Access to SAP S/4 HANA should be provided from the organisations IAM solution, preferable using SSO
- SAP S/4 HANA should be incorporated into the organisation's ISMS and controls maintained here
- SAP S/4 HANA should be hardened according to SAP hardening guides and best practice

Data Subject Rights Management

The organisation must be able to handle data subject rights and request in either a manual or technically supported way in accordance with the GDPR

- Provide notification to the data subjects on the organisations processing of their personal data in a general privacy notice, not per solution
- Respond to data subject requests
- Consent management
- Support data portability and erasure of personal data
- SAP does provide extraction tools to extract personal data from SAP solutions in case of a DSAR request, however, this data should be incorporated into the overall process for access requests since personal data might be processes in and outside of SAP S/4 HANA.

Data Lifecycle Management

How to manage your data throughout its lifecycle

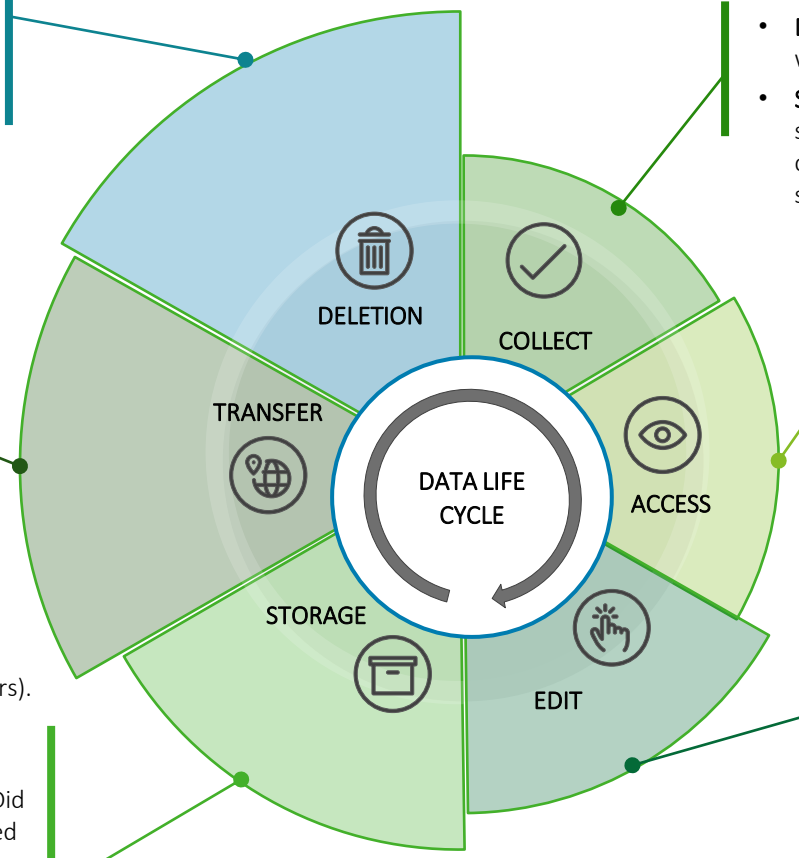
Data life cycle management

To ensure data protection is adequately integrated into SAP S/4 HANA, risk assessments of the implementation solution and the processes it supports, should be performed as soon as a design draft is in place and must take into account all aspects of the data life cycle. Based on these assessments – the design is finalised and mitigative controls are set up completing the privacy-by-design.

- **Deletion**. Do you delete data automatically when the maximum retention period has been reached?
- SAP offers data blocking which makes data unavailable based on roles and deletion where data is completely and irrevocably deleted from the cloud.

- **Transfers**. Do you transfer personal data to third countries? (geo-location for storage, external consultants, external tools)
- Did you perform a TIA and implement security measures to mitigate the risks associated with the transfers?
- Do you operate globally? Did you consider third country national data localization laws?

- **Storage**. Where do you store data? (SaaS, on premise, location of servers).
- Is the data encrypted or masked?
- **Retention**. Have you defined the maximum data retention periods? Did you consider retention periods based on global baseline and local legal requirements? Do you differentiate on data types?



- **Data mapping**. Did you map your data? Do you know where to find sensitive data types?
- **Single source of truth**. Create and maintain a single source of master data. Do you unnecessarily keep duplicate data e.g., in integrations with other solutions?

- **Access control**. Who can access your environments? (prod, test, dev, pre-prod)
- Did you set up single sign-on (SSO), password policies and multi-factor-auhtification (MFA)?
- Did you set up role-based-access control (RBAC) and define roles?

- **Data quality**. Have you implemented quality rules that guarantee the consistency of the data collected?
- What is the source solution? Is the modification of the data included in all the solutions in which they are contained?
- Do you use external data quality tools in ensure continuously data quality?
- **Logs**. Do you keep track of changes and the history of data changes?

Assessments

✓ Privacy Impact Assessment (PIA)

Is to be triggered when a solution or high-level business process contain personal data. A PIA is a risk assessment, which may be incorporated into the enterprise risk management program (ERM) of the organisation, and which may be carried out alongside any Information Security Risk Assessments. The purpose is to establish an overview of the processing activity, the privacy risks it entails, and set up mitigative actions and controls to reduce the risk to an acceptable level.

✓ Data Protection Impact Assessment (DPIA)

Is a more extensive risk assessment, which must comply to the requirements hereto set out in the GDPR and general practice of data protection supervisory authorities. A DPIA must be performed, when the PIA done prior to this assessment reveals the processing may involve a high risk to the rights and freedoms of the individuals.

✓ Transfer Impact Assessment (TIA)

Is to be triggered when the PIA reveals that personal data is transferred to a third country. This assessment is to ensure a legal basis for transfers to third countries along with ensuring that relevant and appropriate safeguards are implemented in order to reduce the risk to an acceptable level.

✓ Information Security Risk Assessment

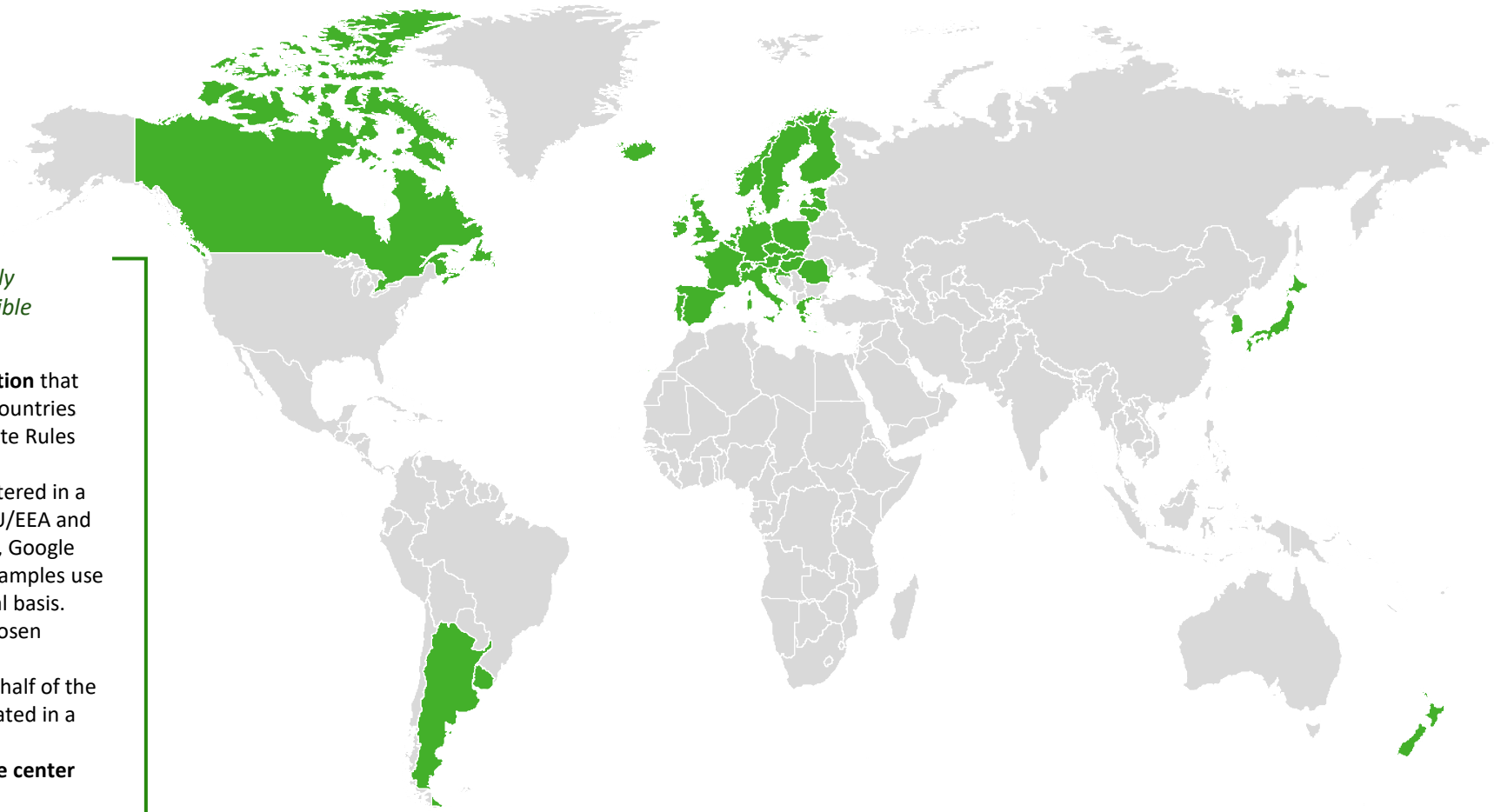
Is to be triggered when an IT solution is assessed. The Information Security Risk Assessment will identify the threats and vulnerabilities of the solution and implementation thereof and assess the likelihood and impact of the risk. It will determine which security measures need to be in place to mitigate the risk down to an acceptable level based on the risk tolerance, this will trigger system hardening and configurations.

Third country data transfers

Global companies and global solutions data transfers

Deep dive on third country transfers

How third country transfers become relevant in SAP S/4 HANA implementation

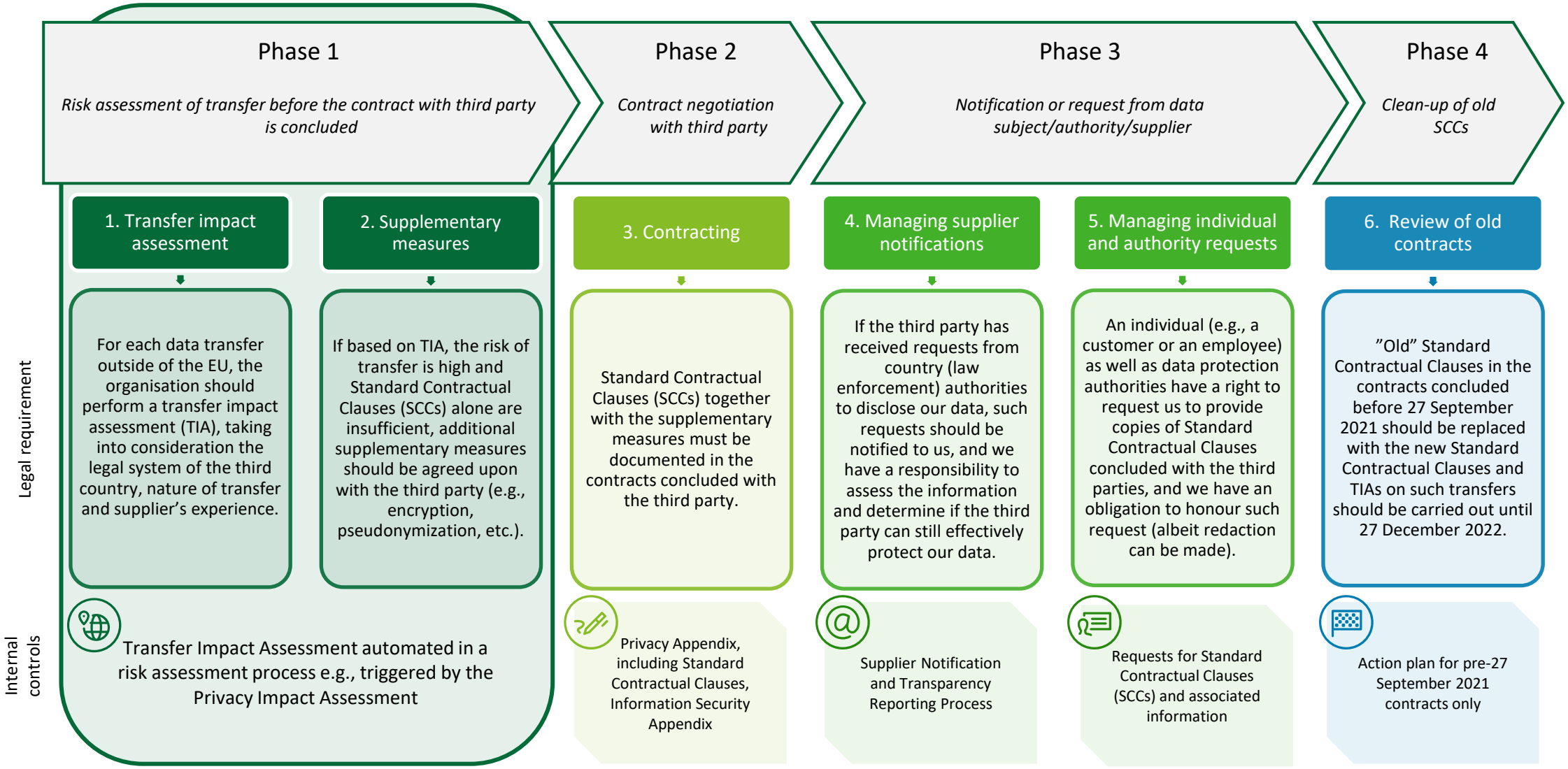


Third country transfers of personal data are usually relevant in a SAP S/4 HANA implementation. Possible scenarios in the following:

- S/4 HANA is implemented in a **global organisation** that operates beyond EU/EEA and adequate third countries (see green countries on map). Binding Corporate Rules (BCR) could be considered.
- S/4 HANA is hosted in a **public cloud** headquartered in a third country or geo-settings chosen beyond EU/EEA and adequate third countries, e.g., Microsoft Azure, Google Cloud Platform or Amazon Web Services. All examples use Standard Contractual Clauses (SCCs) as the legal basis.
- S/4 HANA is hosted in SAP, but **geo-settings** chosen beyond EU/EEA and adequate third countries.
- **External consultants** are processing data on behalf of the company working out of a third country, or located in a third country.
- Company is using an internal or external **service center** located in a third country.
- Company using **external tools** for e.g., migration of data into HANA, that operate from or are located in a third country.

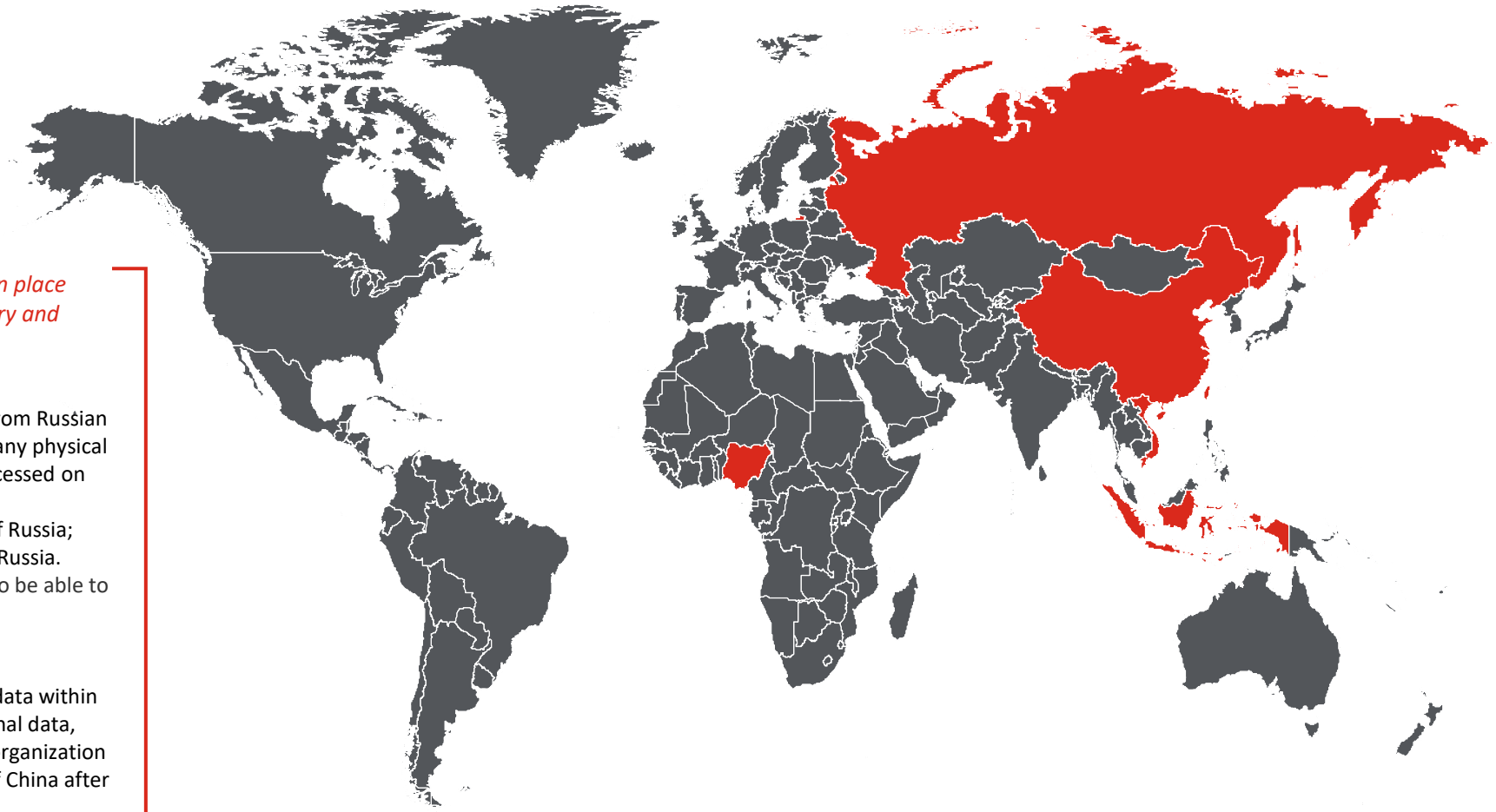
Deep dive on third country transfers

Compliance steps when transferring personal data to a third country



Deep dive on third country transfers

Third country transfers – the other way around



Some third countries have data localization laws in place e.g., requiring data to be stored in the third country and limiting transfers to the EU/EEA. Examples:

Russian data localization law:

- Companies that collect personal information from Russian citizens, even if those companies do not have any physical presence within Russia, must be stored or processed on servers located in Russia.
- Data can be transferred to countries outside of Russia; however, the original database must reside in Russia.
- SAP does have a Russian data center in order to be able to comply with the Russian national privacy laws.

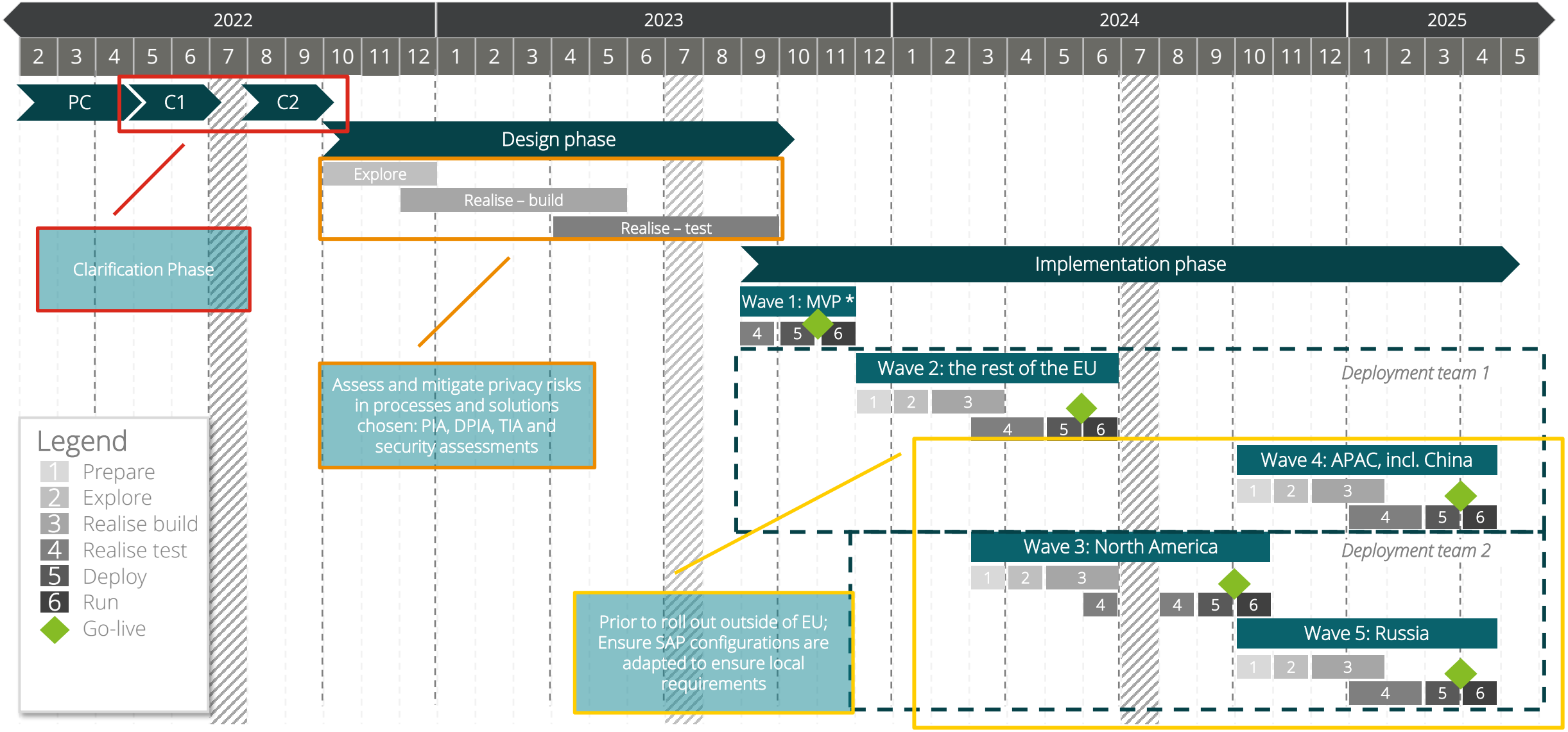
Chinese data localization law:

- Operators must store personal and important data within China. The data stored in China should be original data, however, if there are any business needs, the organization can provide copied data to countries outside of China after they pass a risk assessment.
- SAP does have a Chinese data center in order to be able to comply with Chinese cyber security and privacy laws.

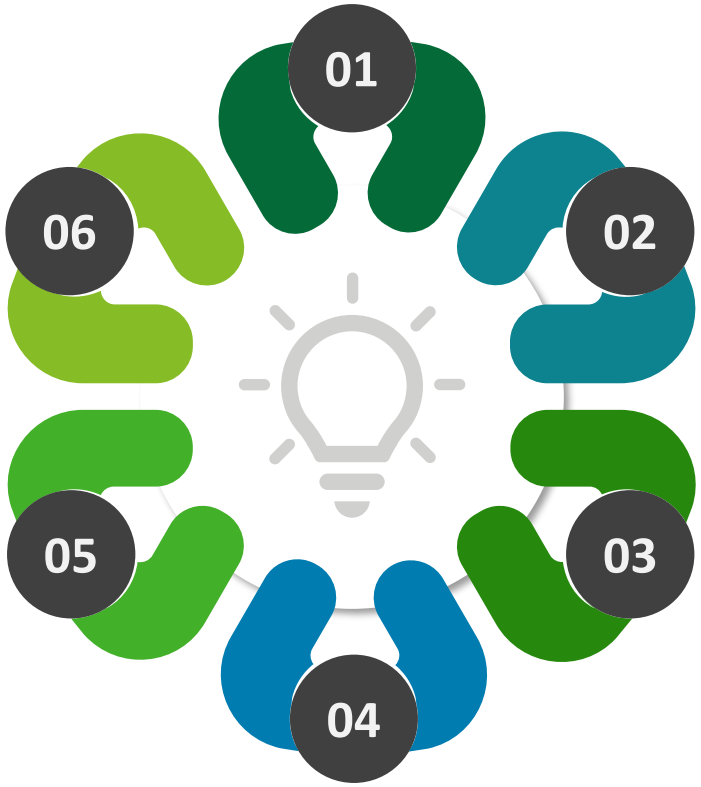
Key take-aways

towards ***Your*** risk-based design of data strategy within SAP

Timeline



Involved stakeholders



CEO

CRO

CISO

Head of Data (Governance)

Head of Compliance

CPO & DPO & Legal

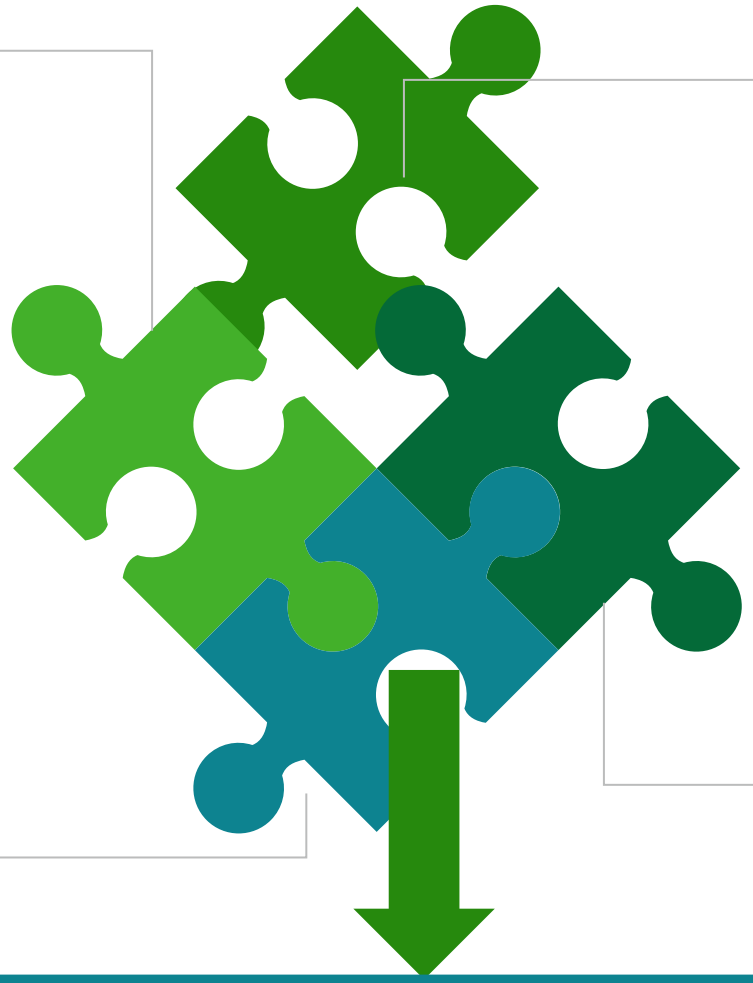
Your SAP Data Protection Roadmap

Can never be 1 solution fits ALL

Embedding “privacy by design” in the SAP roll-out program….

Step 1
Define which business modules are in scope

Step 2
Create data lineage and inventory



Step 3
Define guidance on internal SAP privacy measures

Step 4
Define guidance on external privacy software

Integrate in your holistic data protection program

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, tax and legal, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of 225,000 professionals, all committed to becoming the standard of excellence.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.