asug
Americas' SAP Users' Group

Simplify Data Protection and Privacy Programs with SAP Data Privacy Governance

Dr. Sandro Lovisa, Chief Product Owner SAP Data Privacy Governance, SAP SE
Evelyne Salie, Senior Director Center of Excellence for Finance and Risk, SAP SE

Session ID: ASUG84279

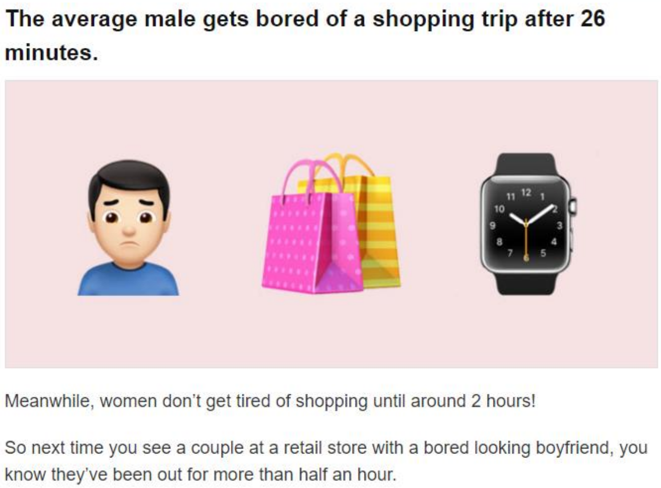
SAP SAPPHIRENOW | asug ANNUAL CONFERENCE

May 7 – 9, 2019

About the Speakers

Dr Sandro Lovisa

- Chief Product Owner of SAP Data Privacy Governance
- Leading the SAP Data Protection & Privacy Cloud solution development
- Fun fact:



The average male gets bored of a shopping trip after 26 minutes.

Meanwhile, women don't get tired of shopping until around 2 hours!

So next time you see a couple at a retail store with a bored looking boyfriend, you know they've been out for more than half an hour.

Evelyne Salie

- Senior Director, SAP Center of Excellence for Finance & Risk
- SAP Data Protection & Privacy global Business Development
- Fun fact:

In Switzerland it is illegal to own just one guinea pig.

This is because guinea pigs are social animals, and they are considered victims of abuse if they are alone.

Why isn't this a law everywhere?!

Key Outcomes/Objectives

1. Get to know SAP’s Data Privacy Governance Cloud Offering
2. Learn how to automate, create transparency and safe costs
3. Understand competitiveness of direct integration to S/4

Legal Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. This presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has 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's strategy and possible future developments, products and/or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information on this document is not a commitment, promise or legal obligation to deliver any material, code or functionality. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or noninfringement. This document is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this document, and shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of this document. This limitation shall not apply in cases of intent or gross negligence.

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, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

NOTE: The information contained in this presentation is for general guidance only and provided on the understanding that SAP is not herein engaged in rendering legal advice. As such, it should not be used as a substitute for legal consultation. SAP SE accepts no liability for any actions taken as response hereto.
It is the customer’s responsibility to adopt measures that the customer deems appropriate to achieve GDPR compliance.

Data Protection & Privacy Solutions within SAP:

Data Protection and Privacy Regulations ask for safeguard measures in data processing systems:

Privacy governance

- Record of processing activities
- Data privacy impact assessment
- Controls and related testing
- Continuous control monitoring
- Policy distribution and acceptance
- Compliance reporting

Data management

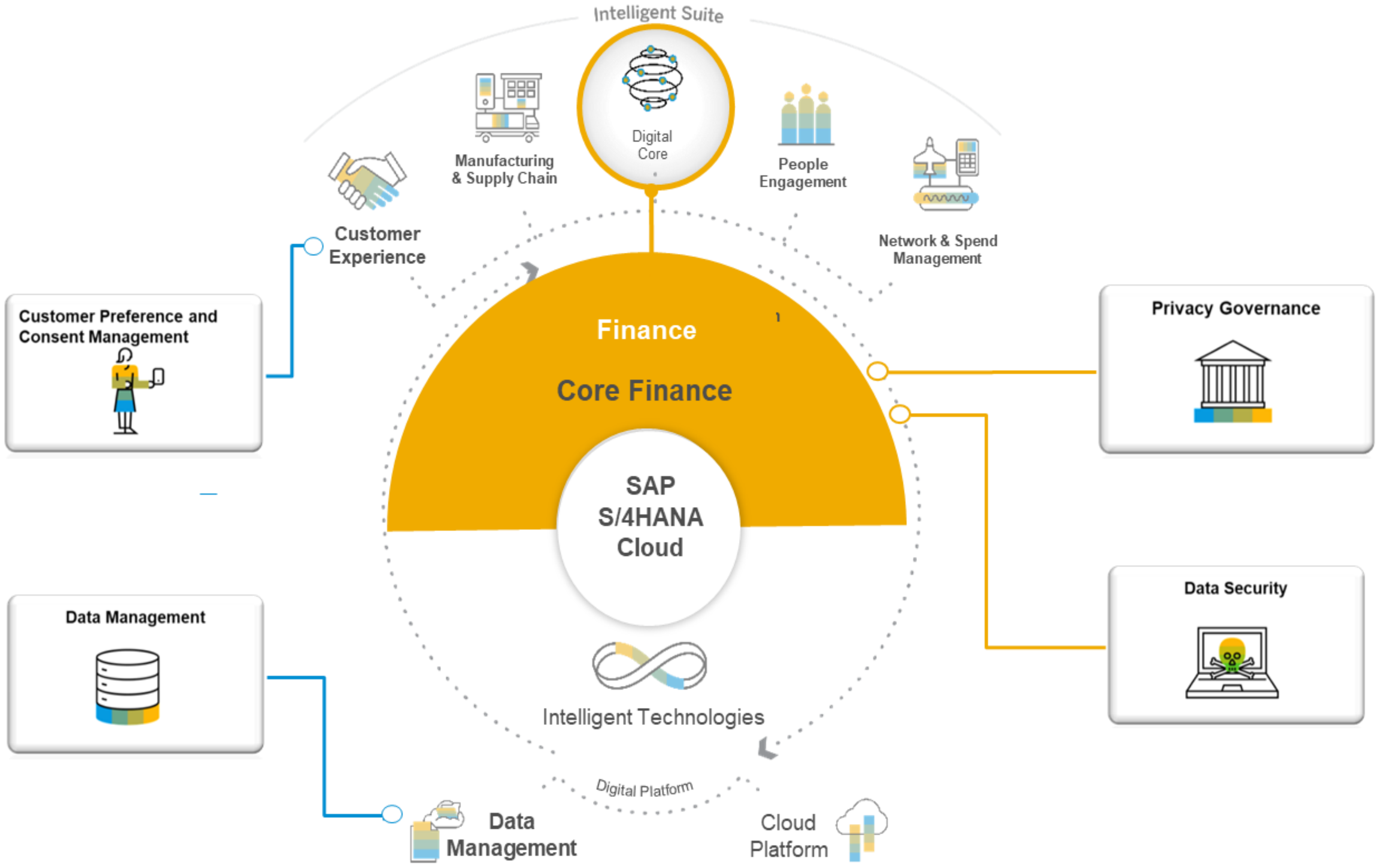
- Privacy data mapping, profiling
- Blocking and deletion
- Data flow analysis
- Data access
- Data transfer
- Data minimization
- Data storage

Data security

- Access governance
- Customer identity management
- Breach detection, notification, and management
- Data protection (for example, encryption and masking)
- Data access logging
- Data loss prevention

Customer preference and consent management

- Personal profile, preferences, and consent
- Centralized personal profile, preferences, and consent in a secure audit-ready vault
- Enforcement of personal profile, preferences, and consent to third parties
- Data handling practices



Intelligent Suite

Digital Core

Manufacturing & Supply Chain

People Engagement

Customer Experience

Network & Spend Management

Customer Preference and Consent Management

Privacy Governance

Finance

Core Finance

SAP S/4HANA Cloud

Data Management

Data Security

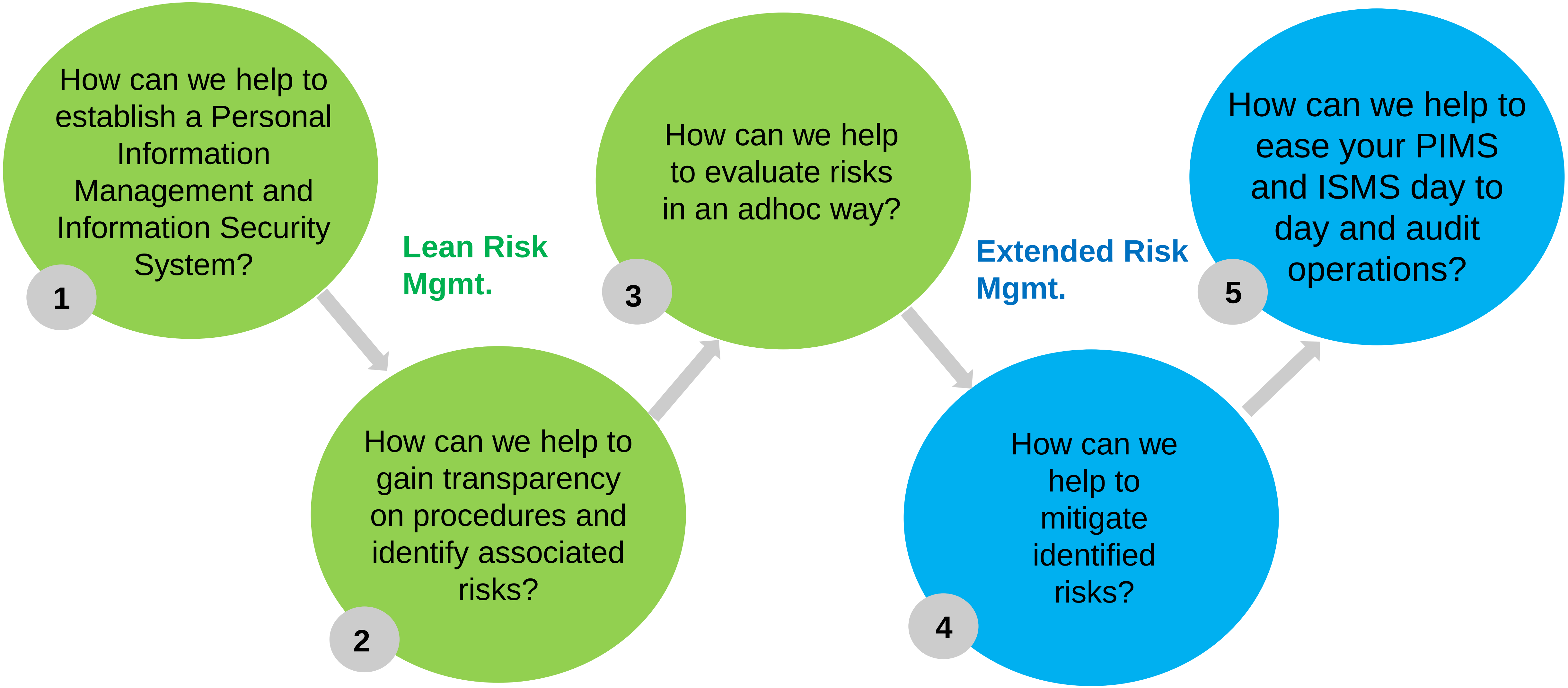
Intelligent Technologies

Digital Platform

Data Management

Cloud Platform

Agenda



1 How can we help to establish a Personal Information Management and Information Security System?

2 How can we help to gain transparency on procedures and identify associated risks?

Lean Risk Mgmt.

3 How can we help to evaluate risks in an adhoc way?

4 How can we help to mitigate identified risks?

Extended Risk Mgmt.

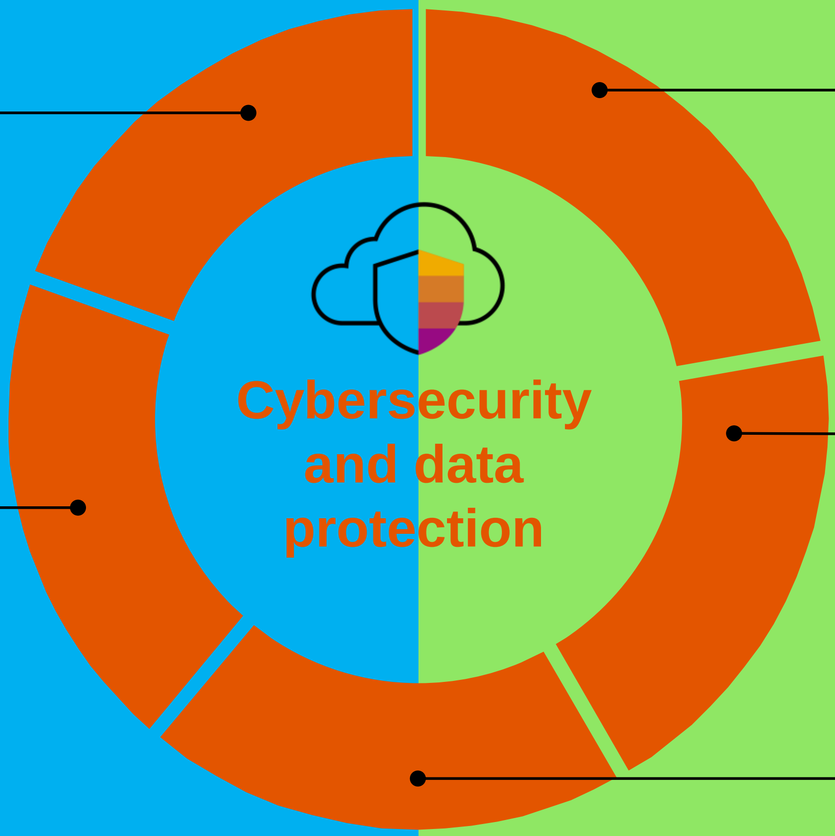
5 How can we help to ease your PIMS and ISMS day to day and audit operations?

SAP Data Privacy Governance

Data protection and privacy (DPP) governance for the extended enterprise

Extended Risk Mgmt.

Lean Risk Mgmt.



Monitor and report*
Report status and details via a unified cockpit

Manage risks and controls*
Identify and audit DPP risks and mitigating controls

Manage policies and regulations
Create, disseminate, and acknowledge DPP policies

Survey and track
Gather and report records of processing activities (ROPA)

Assess business impact
Perform data protection (DPIA) and security* business impact analysis

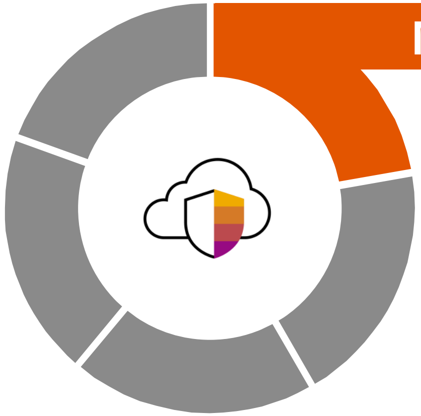
*Coming, see current roadmap

How can we help to establish a Personal Information Management and Information Security System?

Lean Risk Mgmt.
Available

SAP Data Privacy Governance

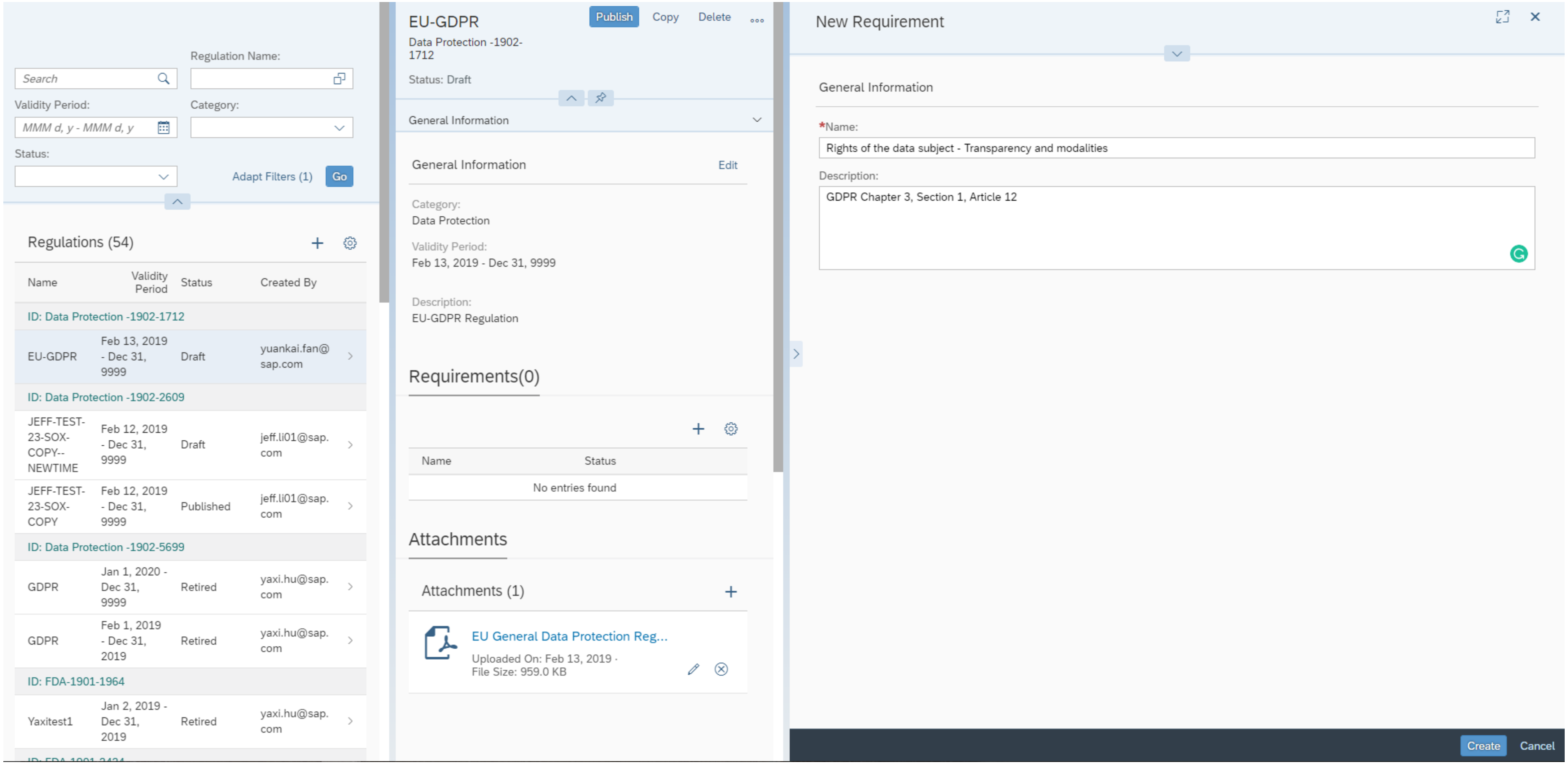
Data protection and privacy governance for the extended enterprise



Manage regulations and policies

- Maintain Regulations
- Deduct legal requirements
- Create and disseminate policies related to data protection, privacy, and security
- Streamline policy management lifecycle while establishing clear responsibilities
- Leverage email or mobile options to make policy distribution and acceptance easier and faster
- Gather policy acknowledgements by those subject to them

Maintain Regulations and Deduct Requirements



Search

Regulation Name:

Validity Period: MMM d, y - MMM d, y

Category:

Status:

Adapt Filters (1) Go

Regulations (54)

Name	Validity Period	Status	Created By
ID: Data Protection -1902-1712			
EU-GDPR	Feb 13, 2019 - Dec 31, 9999	Draft	yuankai.fan@sap.com
ID: Data Protection -1902-2609			
JEFF-TEST-23-SOX-COPY--NEWTIME	Feb 12, 2019 - Dec 31, 9999	Draft	jeff.li01@sap.com
JEFF-TEST-23-SOX-COPY	Feb 12, 2019 - Dec 31, 9999	Published	jeff.li01@sap.com
ID: Data Protection -1902-5699			
GDPR	Jan 1, 2020 - Dec 31, 9999	Retired	yaxi.hu@sap.com
GDPR	Feb 1, 2019 - Dec 31, 2019	Retired	yaxi.hu@sap.com
ID: FDA-1901-1964			
Yaxitest1	Jan 2, 2019 - Dec 31, 2019	Retired	yaxi.hu@sap.com
ID: FDA-1901-2424			

EU-GDPR

Data Protection -1902-1712

Status: Draft

General Information

General Information Edit

Category:
Data Protection

Validity Period:
Feb 13, 2019 - Dec 31, 9999

Description:
EU-GDPR Regulation

Requirements(0)

Name	Status
No entries found	

Attachments

Attachments (1)

EU General Data Protection Reg...
Uploaded On: Feb 13, 2019 ·
File Size: 959.0 KB

New Requirement

General Information

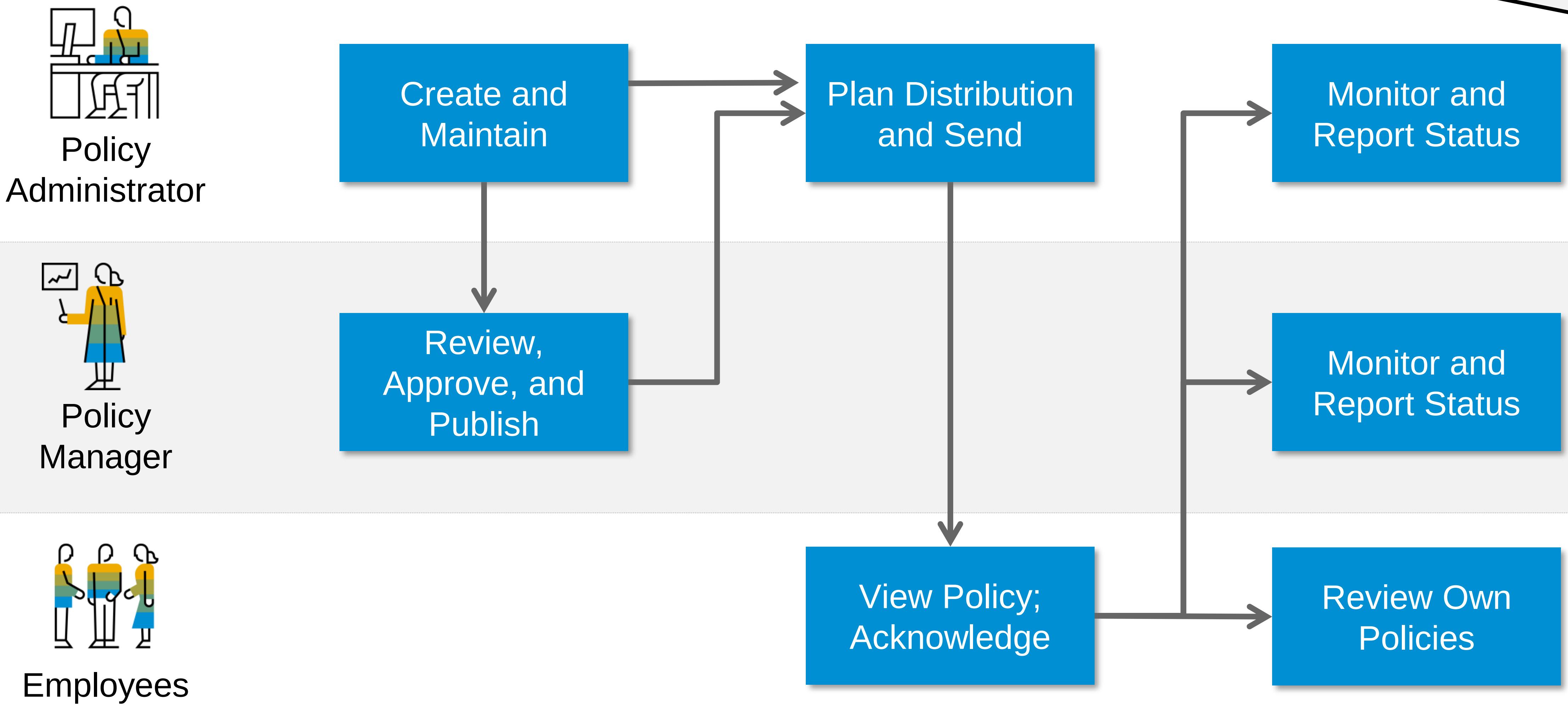
*Name:
Rights of the data subject - Transparency and modalities

Description:
GDPR Chapter 3, Section 1, Article 12

Define and Distribute Policies

Chapter IV GDPR
Data Controller and processor obligations

Relates to
Art. 40 GDPR
Codes of Conduct



Policy Administrator

Create and Maintain

Plan Distribution and Send

Monitor and Report Status

Policy Manager

Review, Approve, and Publish

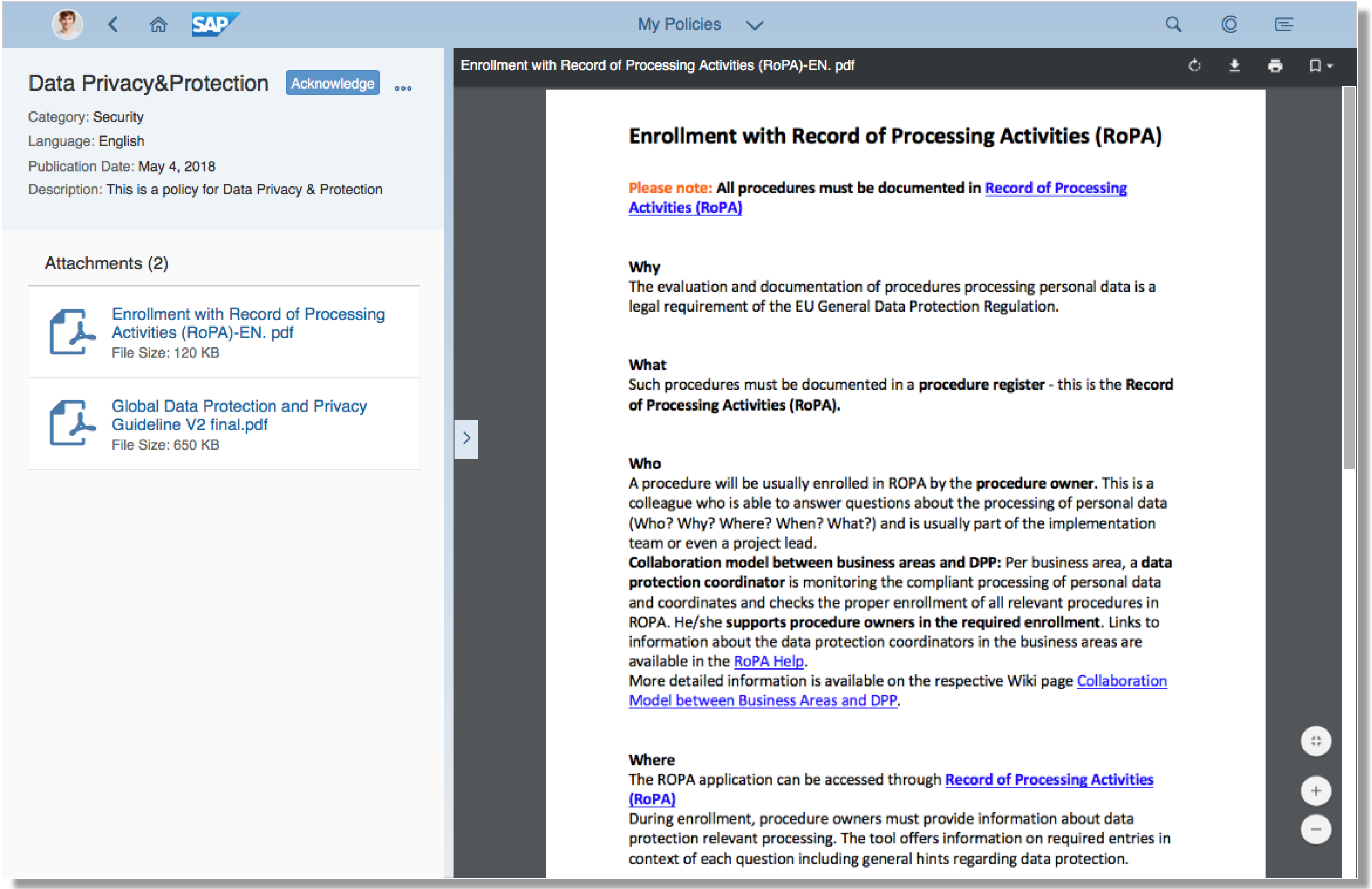
Monitor and Report Status

Employees

View Policy; Acknowledge

Review Own Policies

"Rinse and repeat" to keep policies updated



Data Privacy&Protection Acknowledge ...

Category: Security

Language: English

Publication Date: May 4, 2018

Description: This is a policy for Data Privacy & Protection

Attachments (2)

Enrollment with Record of Processing Activities (RoPA)-EN. pdf
File Size: 120 KB

Global Data Protection and Privacy Guideline V2 final.pdf
File Size: 650 KB

Enrollment with Record of Processing Activities (RoPA)-EN. pdf

Enrollment with Record of Processing Activities (RoPA)

Please note: **All procedures must be documented in Record of Processing Activities (RoPA)**

Why
The evaluation and documentation of procedures processing personal data is a legal requirement of the EU General Data Protection Regulation.

What
Such procedures must be documented in a **procedure register** - this is the **Record of Processing Activities (RoPA).**

Who
A procedure will be usually enrolled in ROPA by the **procedure owner**. This is a colleague who is able to answer questions about the processing of personal data (Who? Why? Where? When? What?) and is usually part of the implementation team or even a project lead.
Collaboration model between business areas and DPP: Per business area, a **data protection coordinator** is monitoring the compliant processing of personal data and coordinates and checks the proper enrollment of all relevant procedures in ROPA. He/she **supports procedure owners in the required enrollment.** Links to information about the data protection coordinators in the business areas are available in the RoPA Help.
More detailed information is available on the respective Wiki page Collaboration Model between Business Areas and DPP.

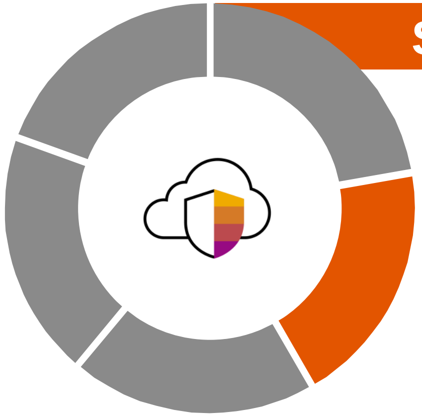
Where
The ROPA application can be accessed through Record of Processing Activities (RoPA)
During enrollment, procedure owners must provide information about data protection relevant processing. The tool offers information on required entries in context of each question including general hints regarding data protection.

How can we help to gain transparency on procedures and identify associated risks?

Lean Risk Mgmt.
Available

SAP Data Privacy Governance

Data protection and privacy governance for the extended enterprise

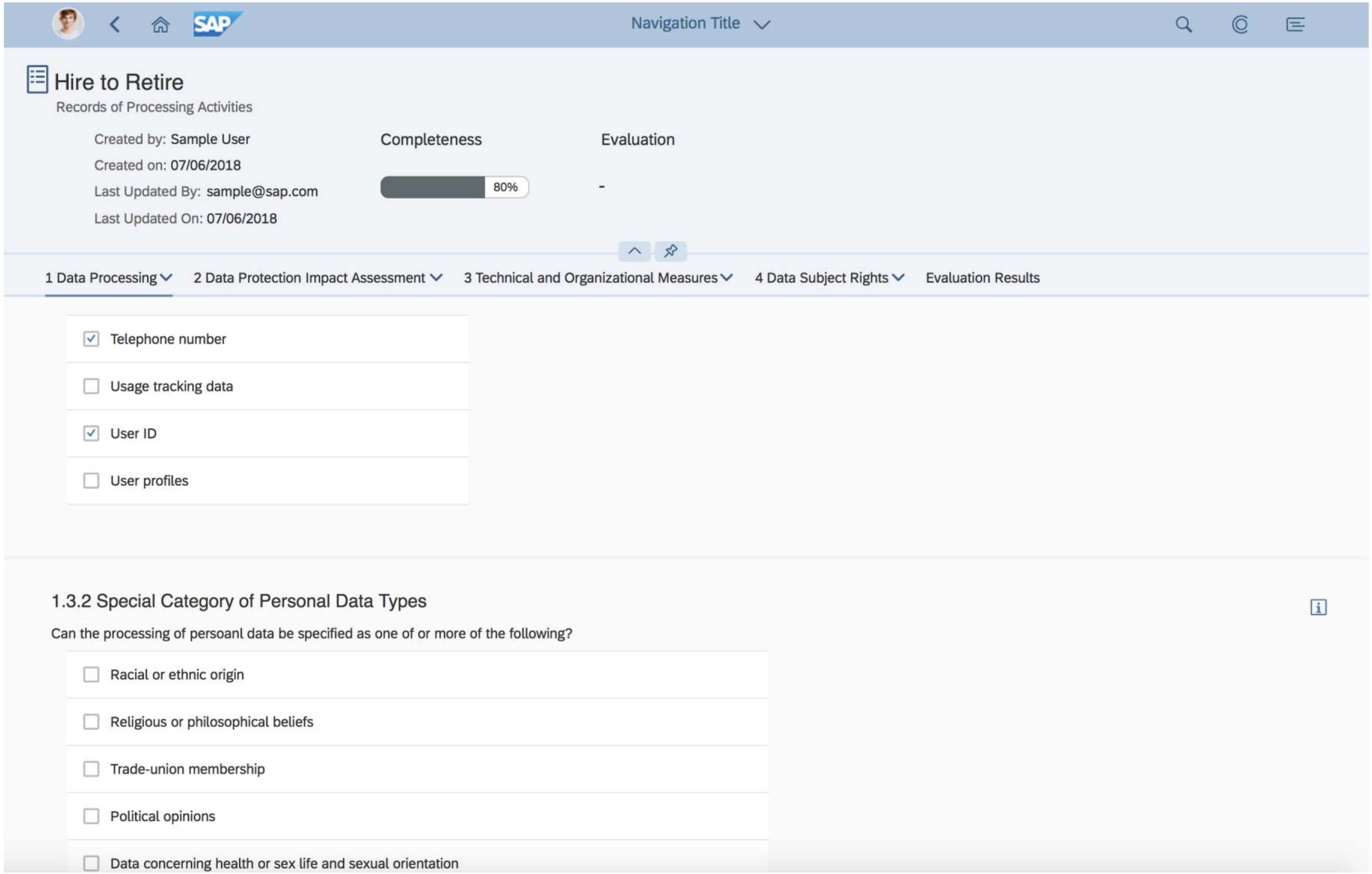


Survey and track

- Create records of processing activities (ROPA) surveys, optionally leveraging existing templates
- Publish surveys to gather ROPA information
- Use survey results to populate a repository to report ROPA information
- Evaluate whether a data protection impact assessment (DPIA) is required

*Coming, see current roadmap

Records of Processing Transparancy: Contributor View



Hire to Retire

Records of Processing Activities

Created by: Sample User

Created on: 07/06/2018

Last Updated By: sample@sap.com

Last Updated On: 07/06/2018

Completeness

80%

Evaluation

-

1 Data Processing
2 Data Protection Impact Assessment
3 Technical and Organizational Measures
4 Data Subject Rights
Evaluation Results

☑ Telephone number

□ Usage tracking data

☑ User ID

□ User profiles

1.3.2 Special Category of Personal Data Types

Can the processing of persoanl data be specified as one of or more of the following?

□ Racial or ethnic origin

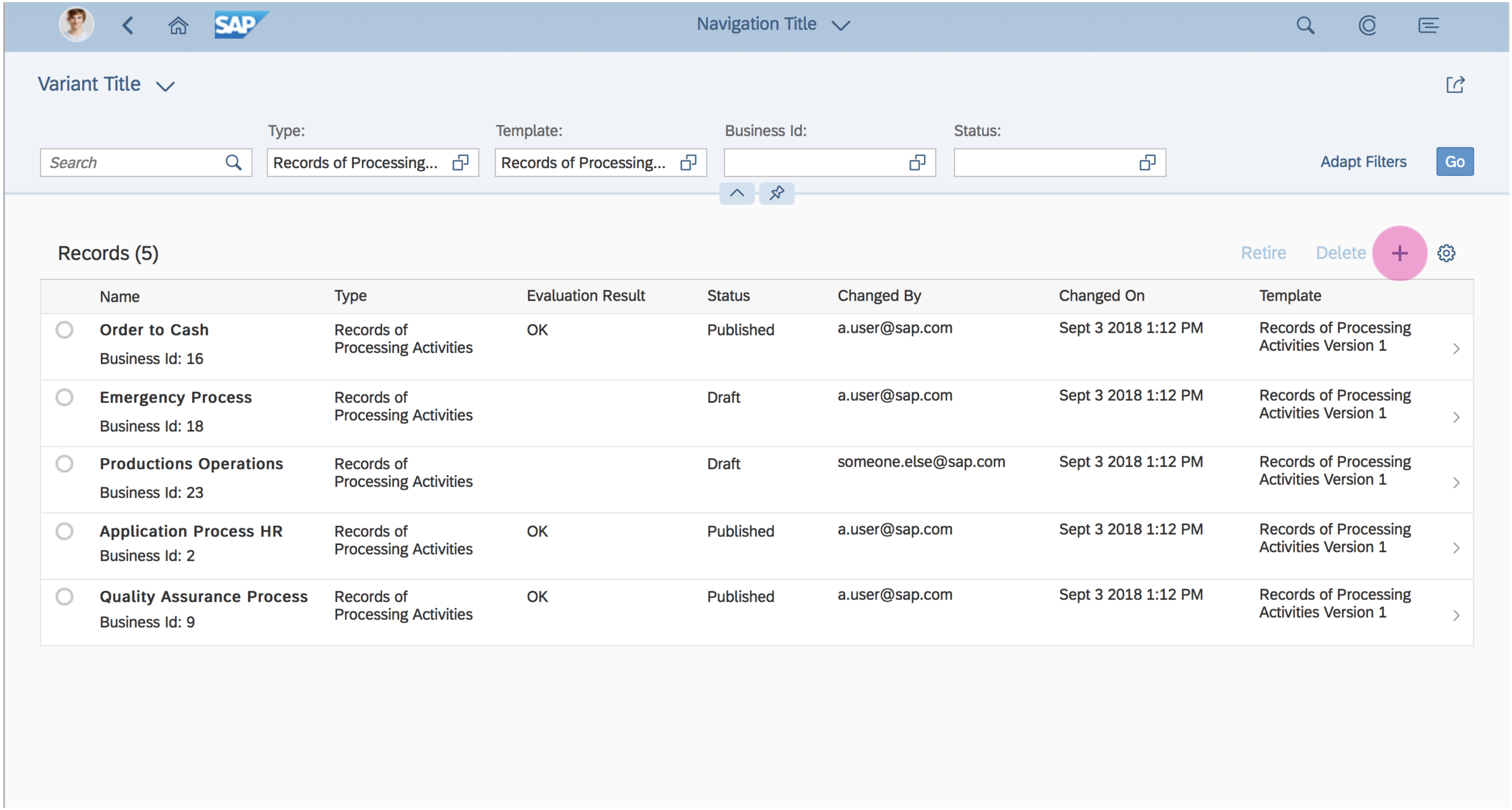
□ Religious or philosophical beliefs

□ Trade-union membership

□ Political opinions

□ Data concerning health or sex life and sexual orientation

Records of Processing Transparancy: Manager View



Search

Type: Records of Processing...

Template: Records of Processing...

Business Id:

Status:

Records (5)

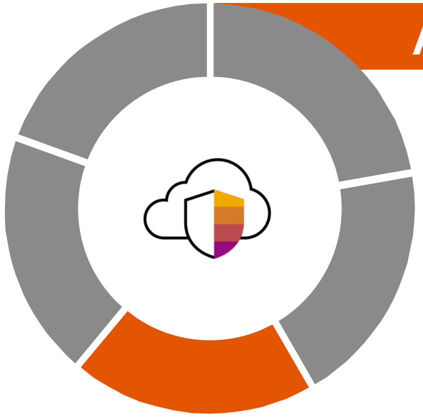
	Name	Type	Evaluation Result	Status	Changed By	Changed On	Template
○	**Order to Cash** Business Id: 16	Records of Processing Activities	OK	Published	a.user@sap.com	Sept 3 2018 1:12 PM	Records of Processing Activities Version 1
○	**Emergency Process** Business Id: 18	Records of Processing Activities		Draft	a.user@sap.com	Sept 3 2018 1:12 PM	Records of Processing Activities Version 1
○	**Productions Operations** Business Id: 23	Records of Processing Activities		Draft	someone.else@sap.com	Sept 3 2018 1:12 PM	Records of Processing Activities Version 1
○	**Application Process HR** Business Id: 2	Records of Processing Activities	OK	Published	a.user@sap.com	Sept 3 2018 1:12 PM	Records of Processing Activities Version 1
○	**Quality Assurance Process** Business Id: 9	Records of Processing Activities	OK	Published	a.user@sap.com	Sept 3 2018 1:12 PM	Records of Processing Activities Version 1

How can we help to evaluate risks in an adhoc way?

Lean Risk Mgmt.
Available

SAP Data Privacy Governance

Data protection and privacy governance for the extended enterprise



Assess business impact

Data protection impact assessment

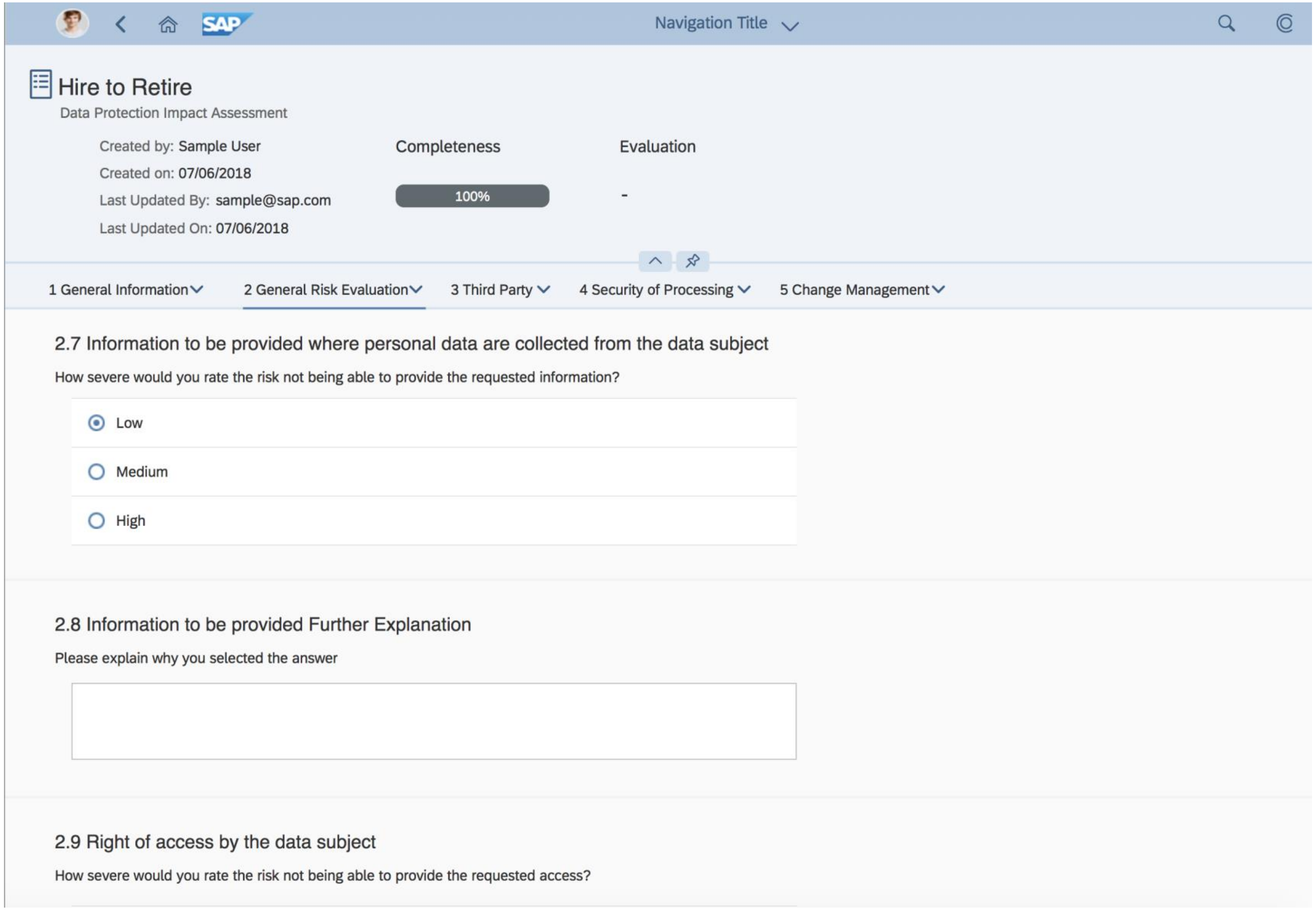
- Assess criticality of DPP-relevant processes with data privacy impact assessments
- Enable a lean risk evaluation to assess and monitor risks associated with DPP-relevant processes

Security business impact analysis

Planned 2019Q2

- Deploy survey-based security threat modeling and issue mitigation for appropriate defense strategies

Data Protection Impact Assessment: Contributor View



Hire to Retire

Data Protection Impact Assessment

Created by: Sample User

Created on: 07/06/2018

Last Updated By: sample@sap.com

Last Updated On: 07/06/2018

Completeness

100%

Evaluation

-

2.7 Information to be provided where personal data are collected from the data subject

How severe would you rate the risk not being able to provide the requested information?

- ● Low
- ○ Medium
- ○ High

2.8 Information to be provided Further Explanation

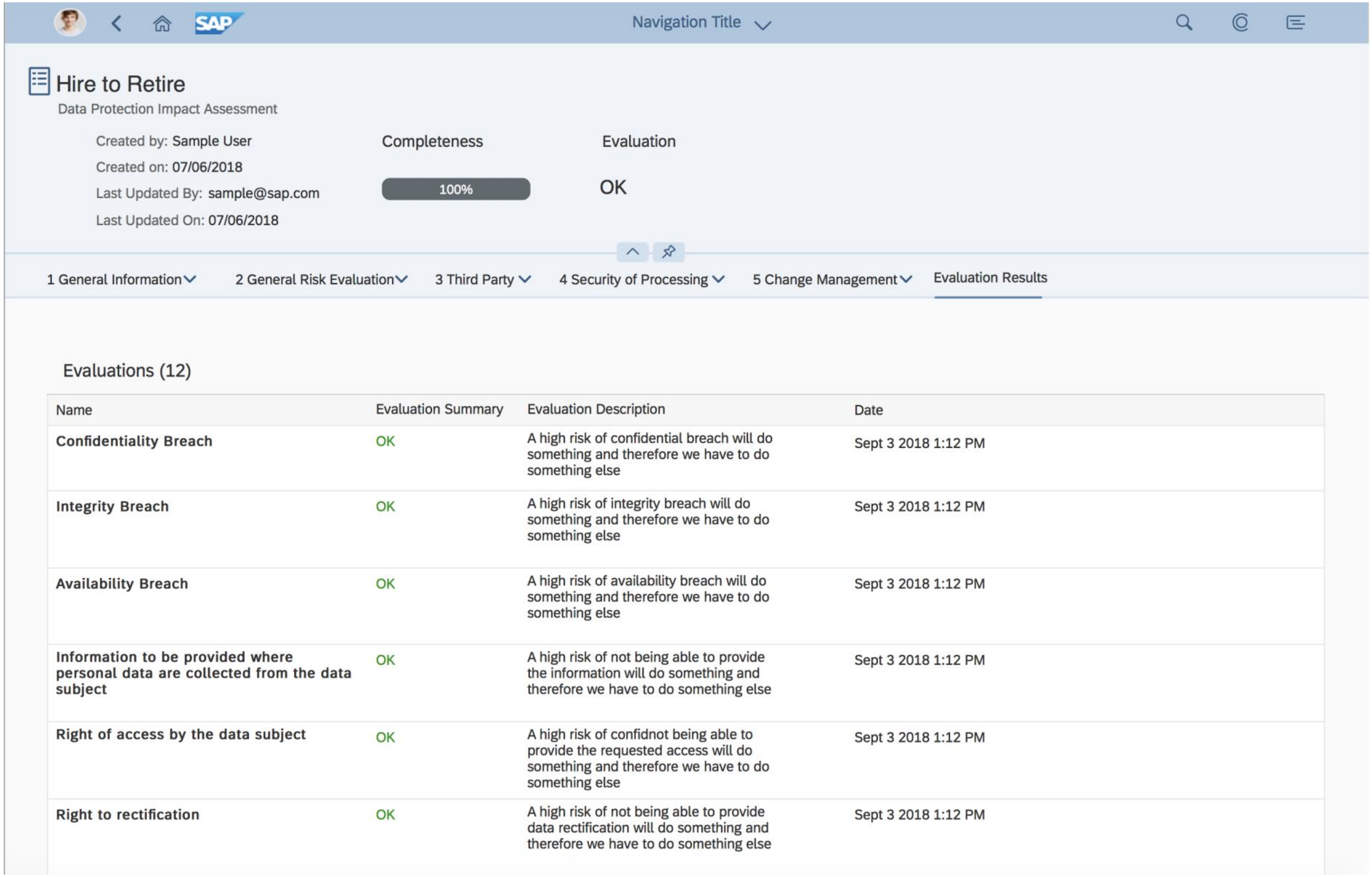
Please explain why you selected the answer

2.9 Right of access by the data subject

How severe would you rate the risk not being able to provide the requested access?

Detail Risk View with Explanations

Planned 2019Q1



Hire to Retire

Data Protection Impact Assessment

Created by: Sample User

Created on: 07/06/2018

Last Updated By: sample@sap.com

Last Updated On: 07/06/2018

Completeness

100%

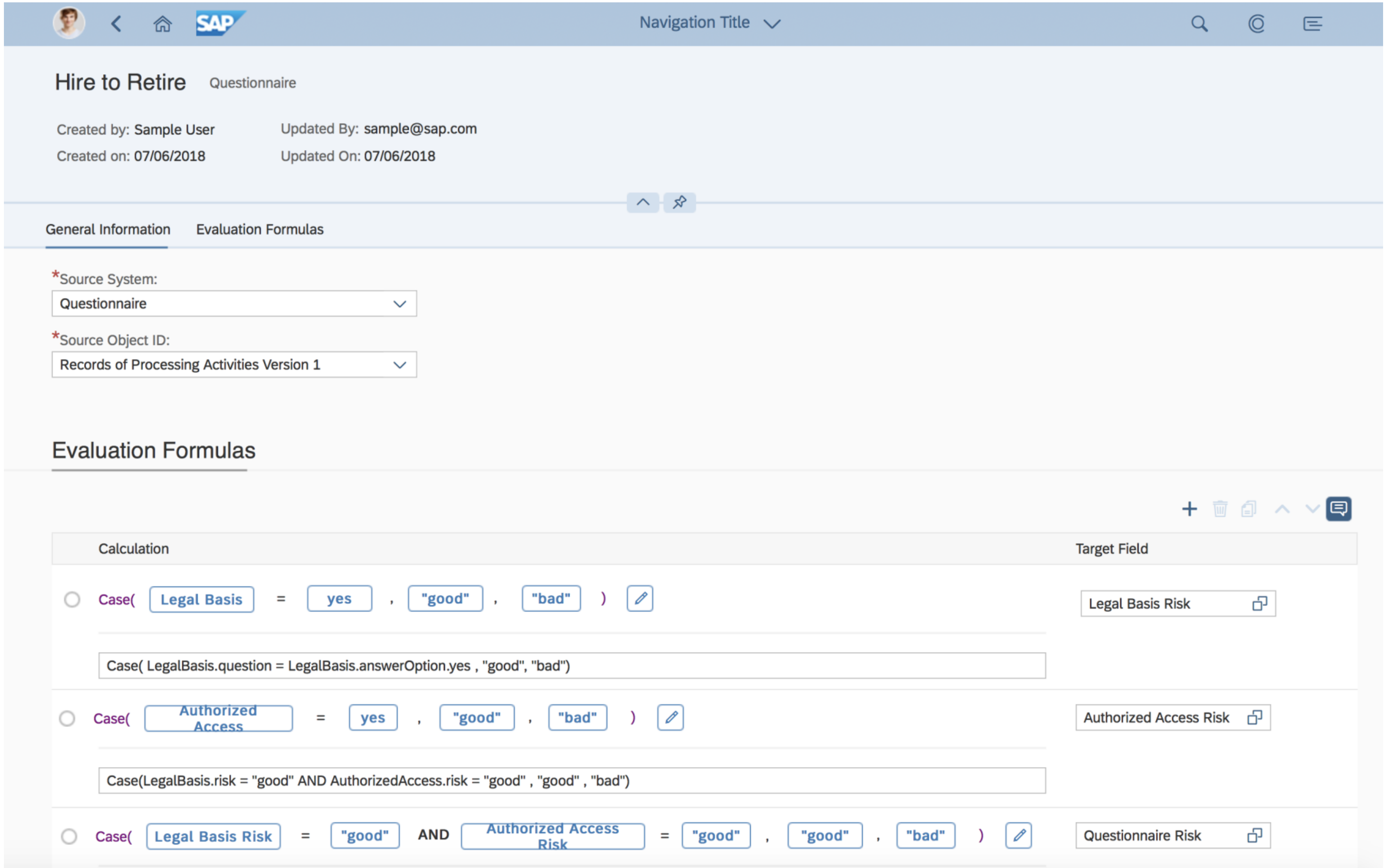
Evaluation

OK

Evaluations (12)

Name	Evaluation Summary	Evaluation Description	Date
Confidentiality Breach	OK	A high risk of confidential breach will do something and therefore we have to do something else	Sept 3 2018 1:12 PM
Integrity Breach	OK	A high risk of integrity breach will do something and therefore we have to do something else	Sept 3 2018 1:12 PM
Availability Breach	OK	A high risk of availability breach will do something and therefore we have to do something else	Sept 3 2018 1:12 PM
Information to be provided where personal data are collected from the data subject	OK	A high risk of not being able to provide the information will do something and therefore we have to do something else	Sept 3 2018 1:12 PM
Right of access by the data subject	OK	A high risk of confidnot being able to provide the requested access will do something and therefore we have to do something else	Sept 3 2018 1:12 PM
Right to rectification	OK	A high risk of not being able to provide data rectification will do something and therefore we have to do something else	Sept 3 2018 1:12 PM

Evaluation Engine: Flexible Formulas



Hire to Retire Questionnaire

Created by: Sample User

Created on: 07/06/2018

Updated By: sample@sap.com

Updated On: 07/06/2018

*Source System: Questionnaire

*Source Object ID: Records of Processing Activities Version 1

Evaluation Formulas

Calculation	Target Field
○ Case(Legal Basis = yes , "good" , "bad") Case(LegalBasis.question = LegalBasis.answerOption.yes , "good", "bad")	Legal Basis Risk
○ Case(Authorized Access = yes , "good" , "bad") Case(LegalBasis.risk = "good" AND AuthorizedAccess.risk = "good" , "good" , "bad")	Authorized Access Risk
○ Case(Legal Basis Risk = "good" AND Authorized Access Risk = "good" , "good" , "bad")	Questionnaire Risk

Security Business Impact Analysis

Chapter IV GDPR
Data Controller and processor obligations

Relates to
Art. 32 GDPR
Security of Processing

Relates to
ISO 27001 or other IT Security Standards

Planned
2019Q2

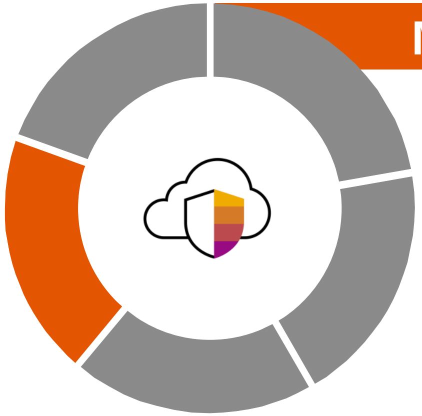
- Technically: full reuse of survey-based RoPA infrastructure
- Functionally: IT Security specific
  - vocabulary,
  - master data,
  - status management and
  - work flow definition
- Pre-defined content
- Support of linking with RoPA and DPIA records

How can we help to mitigate identified risks?

Extended Risk Mgmt.
Planned for 2H2019

SAP Data Privacy Governance

Data protection and privacy governance for the extended enterprise



Mitigate risks via risk assessment and controls

- Maintain a risk catalog*
- Assess risks*
- Document manual and automated controls related to DPP requirements and risks*
- Detect compliance breaches via operational DPP checks (automated controls)*
- Support DPP-related audit process*

*Coming, see current roadmap

DPP Risk Framework

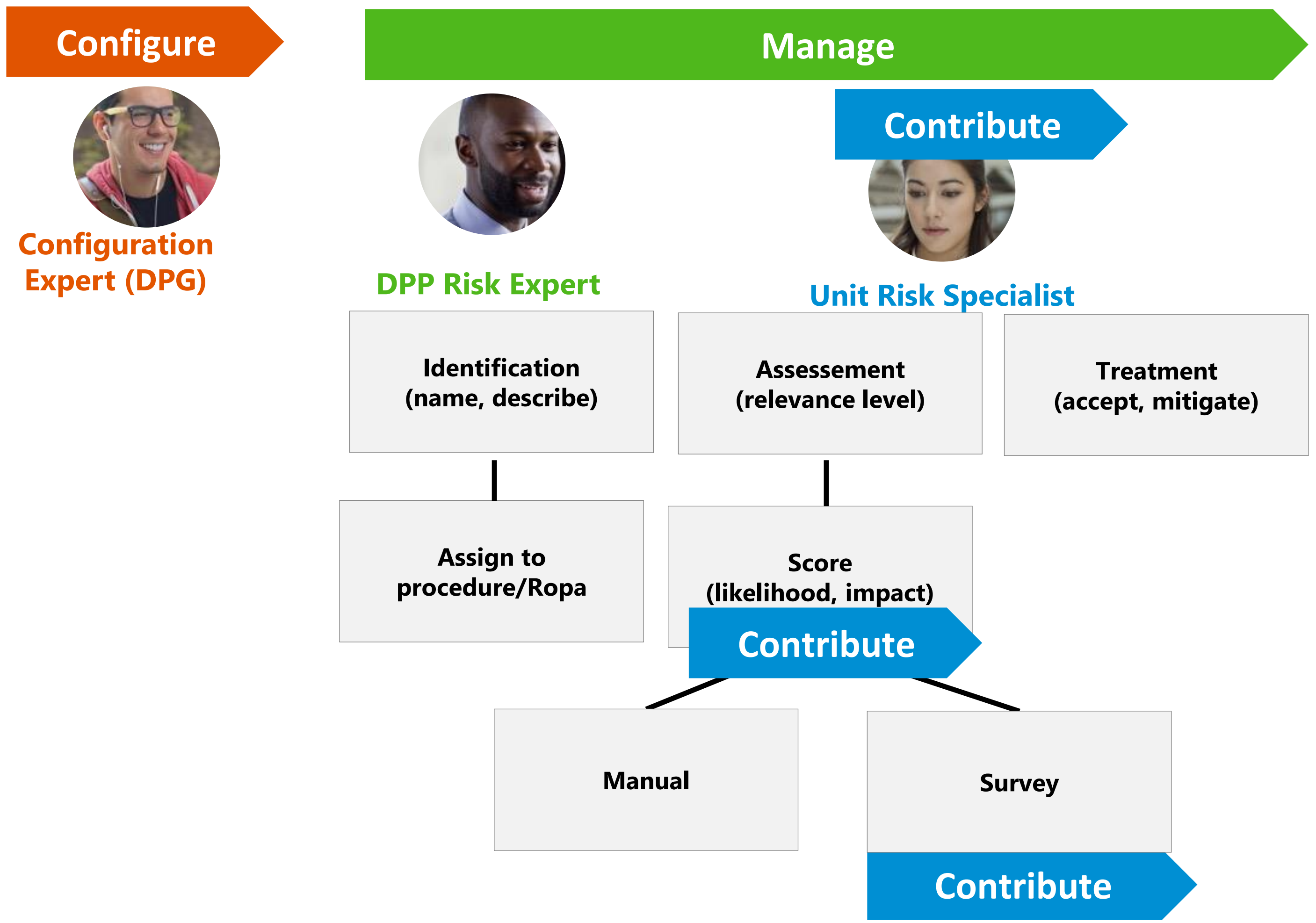
Chapter IV GDPR
Data Controller and processor obligations

Relates to
Art. 32 GDPR
Security of Processing

Future
2H2019

- Risk assessment
  - Performed by assessing Probability (optional) and Impact, resulting into calculated Risk Level
  - Different assessment methods would be available (Qualitative, Quantitative, Scoring)
  - Assessment can be entered either manually or calculated based on the survey answers (reusing Survey-based infrastructure)
  - Multiple risk impacts can be evaluated for single risk
- Risk Mitigation
  - Responses and its mitigations of the risks can be entered either manually or controls from the „Control Framework“ can be used as responses and mitigate the risks
  - Risk mitigations can be influenced automatically by the result of the control evaluation in the Control Framework
- Further Integration scenarios
  - Support of linking with RoPA and DPIA records resulting into aggregated risk level of the linked record (e.g. DPIA Risk Level)
  - Risk KRI can be defined to evaluate the risks by executing a procedures in the connected systems
- Reporting
  - Multiple standard reports and dashboards would be available (Top risks, Risk Heatmap, Marci Chart)

DPP Risk Framework: Business Flow



Configure

Manage

Contribute

Configuration Expert (DPG)

DPP Risk Expert

Unit Risk Specialist

Identification (name, describe)

Assessement (relevance level)

Treatment (accept, mitigate)

Assign to procedure/Ropa

Score (likelihood, impact)

Contribute

Manual

Survey

Contribute

Future 2H2019

Planned App

Config for DPG Risk

Risk Identificatio n

Risk Analysis

Fill Form

Treatment Definition

(Remediatior)

DPP Control Framework

Chapter IV GDPR
Data Controller and processor obligations

Relates to
Art. 32 GDPR
Security of Processing

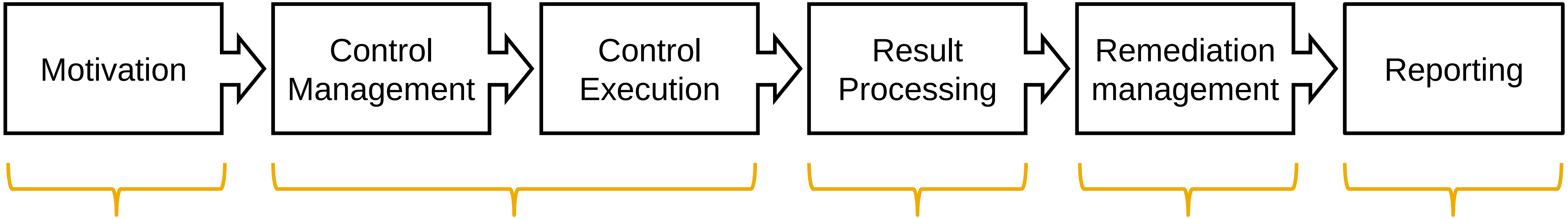
Future
2H2019

- Main features of Control Framework
  - Master Data creation/upload
  - Control Library
  - Manual Control
  - Automated Control
  - Connector to SAP and non-SAP systems
  - Issue and Remediation
  - Content Management

DPP Risk Framework: Business Flow

Detect compliance breaches and high risks via automated procedures

Future
2H2019



Motivation → Control Management → Control Execution → Result Processing → Remediation management → Reporting

Use Case

- DPG
- IT Controls

Detection

Identify deviations from given patterns, policies, etc.

Investigation

Clarify identified issues

Remediation

Decide and trigger mitigation activities

Reporting

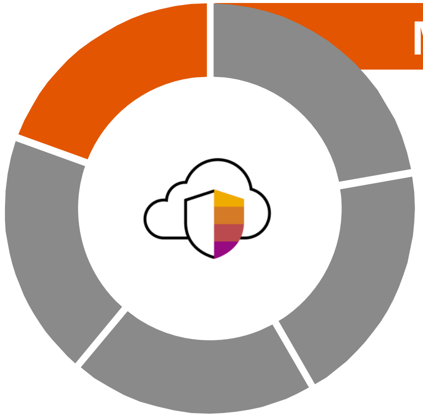
Analyze and optimization and reporting

How can we help to ease your PIMS and ISMS day to day and audit operations?

Extended Risk Mgmt.
Planned for 2H2019

SAP Data Privacy Governance

Data protection and privacy governance for the extended enterprise



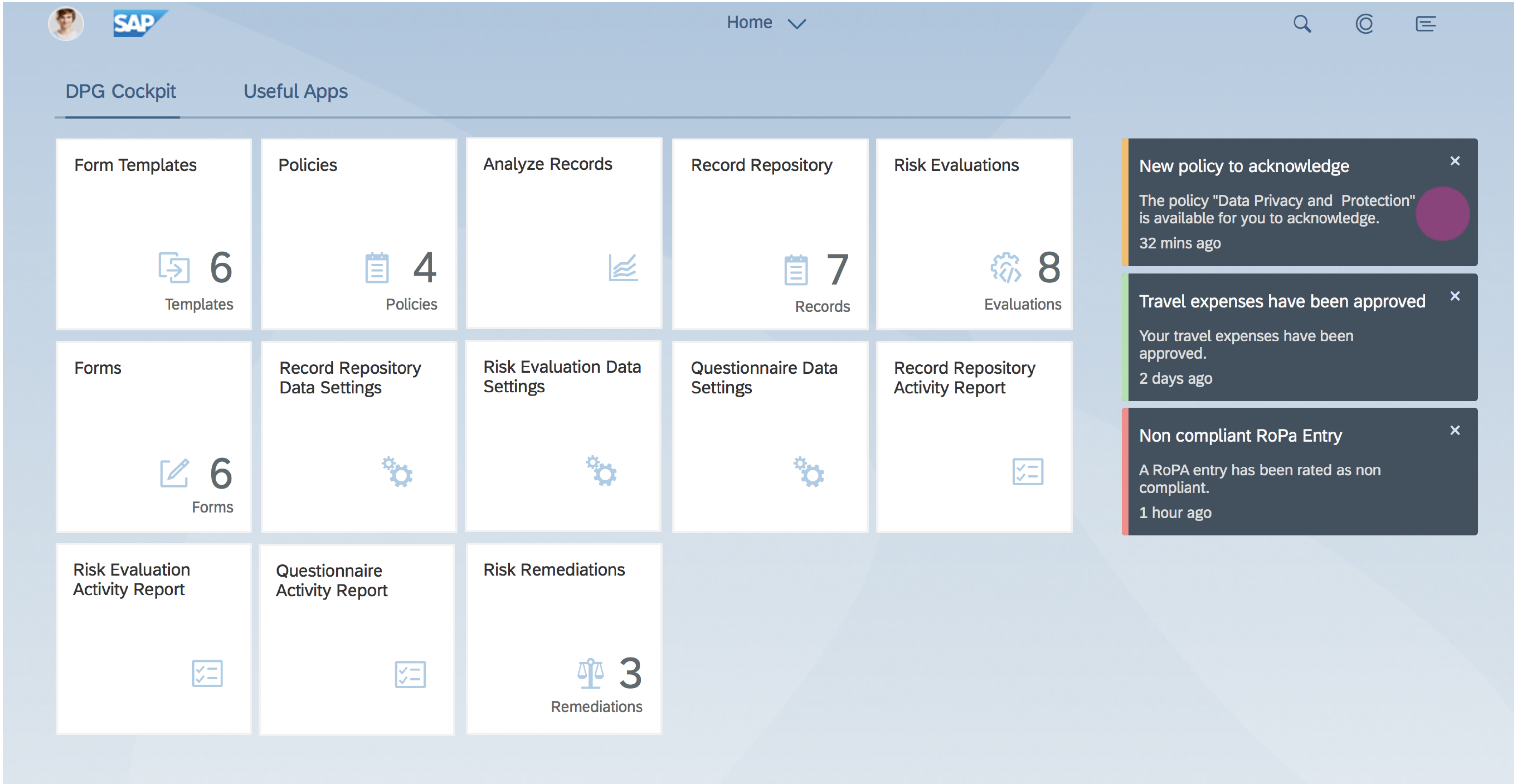
Monitor and report

Monitoring

- Provide insights into status and information for regulatory reporting
- Integrate with SAP Analytics Cloud for flexible reporting capabilities*
- Create a cockpit for a single point of entry for DPP tasks such as connectivity to SAP Information Lifecycle Management*
- Create ROPA entries based on data analysis of SAP S4/HANA Cloud and third-party systems*

*Coming, see current roadmap

Single Point of Entry via the SAP Fiori launchpad



Home

DPG Cockpit

Useful Apps

Form Templates 6 Templates	Policies 4 Policies	Analyze Records	Record Repository 7 Records	Risk Evaluations 8 Evaluations
Forms 6 Forms	Record Repository Data Settings	Risk Evaluation Data Settings	Questionnaire Data Settings	Record Repository Activity Report
Risk Evaluation Activity Report	Questionnaire Activity Report	Risk Remediations 3 Remediations		

New policy to acknowledge

The policy "Data Privacy and Protection" is available for you to acknowledge.

32 mins ago

Travel expenses have been approved

Your travel expenses have been approved.

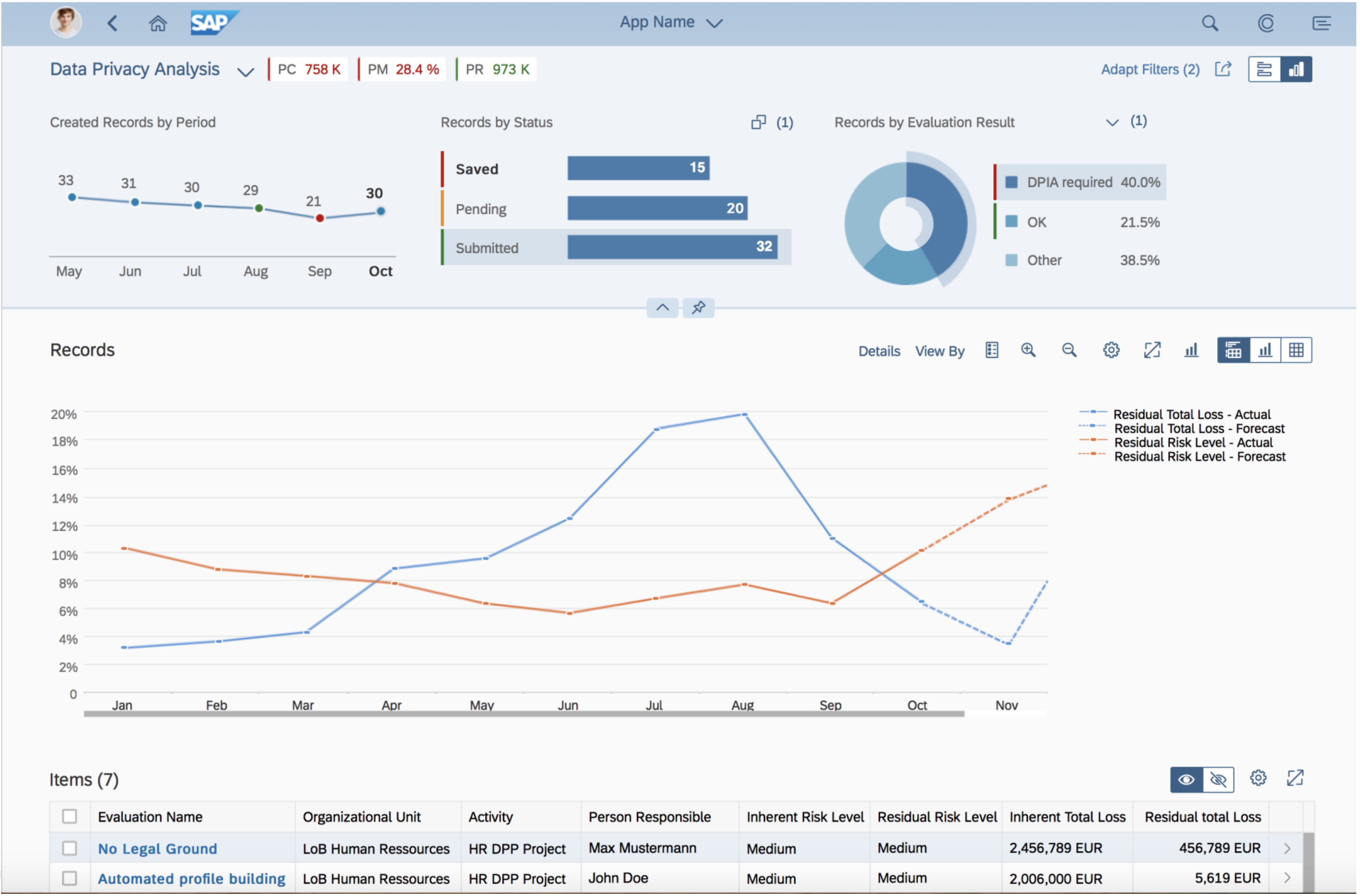
2 days ago

Non compliant RoPa Entry

A RoPA entry has been rated as non compliant.

1 hour ago

Customized Analytics via SAP Analytics Cloud Platform



Items (7)

□	Evaluation Name	Organizational Unit	Activity	Person Responsible	Inherent Risk Level	Residual Risk Level	Inherent Total Loss	Residual total Loss	
□	No Legal Ground	LoB Human Ressources	HR DPP Project	Max Mustermann	Medium	Medium	2,456,789 EUR	456,789 EUR	>
□	Automated profile building	LoB Human Ressources	HR DPP Project	John Doe	Medium	Medium	2,006,000 EUR	5,619 EUR	>

SAP Data Privacy Governance

Automated Record of processing activities

Chapter IV GDPR
Data Controller and processor obligations

Relates to
Art. 30 GDPR
Records of Processing Activities

Future
1H2020

Description

Generate an automated records of processing Art. 30 GDPR

- Generate data statistics to support and validate manual created records of processing
- Fully automated, data-driven evaluation of personal data related processes in live systems
- Generate ROPA entries automatically

Value Drivers

- Validate manual ROPA input with real data and detect inconsistencies in manual ROPA records
- Provide data-based insights into personal data processing
- Linking of auto and manually created records allows auditability

Innovations

Immediate DPP data evaluation based on real data and within distributed landscapes

Scope

- Use S/4HC data statistics to improve documentation quality
- Connect to multiple backends to centralize efforts and improve tracking accuracy

Key Benefits

- Ease DPP compliance and accuracy by establishing a DPP governance hub based on real data evaluation

Summary

2 Step Approach

Lean Risk Mgmt.

Extended Risk Mgmt.

Manage policies

- Create and disseminate policies related to data protection, privacy, and security
- Gather policy acknowledgements by those subject to them
- Gather training attendance status as further evidence that appropriate policies are understood*

Survey and track

- Create records of processing activities surveys, optionally leveraging existing templates
- Publish surveys to gather ROPA information
- Use survey results to populate a repository to report ROPA information and determine whether a data protection impact assessment is required
- Create ROPA entries based on data analysis of SAP S4/HANA Cloud and third-party systems*

Assess business impact

- Assess criticality of DPP-relevant processes with data privacy impact assessments
- Deploy survey-based IT security threat modeling and issue mitigation for appropriate defense strategies*

Manage risk and controls

- Enable a risk framework to assess and monitor risks associated with DPP-relevant processes*
- Document manual and automated controls related to DPP requirements and risks*
- Detect compliance breaches via operational DPP checks (automated controls)*
- Support DPP-related audit process*

Monitor and report

- Provide insights into status and information for regulatory reporting
- Create a cockpit for a single point of entry for DPP tasks such as connectivity to SAP Information Lifecycle Management*
- Integrate with SAP Identity Management for DPP access risks, risk assessments, and access optimization*

*Coming, see current roadmap

Take the Session Survey.

We want to hear from you! Be sure to complete the session evaluation on the SAPPHIRE NOW and ASUG Annual Conference mobile app.

Presentation Materials

Access the slides from 2019 ASUG Annual Conference here:

http://info.asug.com/2019-ac-slides

Q&A

For questions after this session, contact us at [email] and [email].

Let’s Be Social.

Stay connected. Share your SAP experiences anytime, anywhere.

Join the ASUG conversation on social media: **@ASUG365 #ASUG**

Thank you

Dr Sandro Lovisa

Chief Product Owner of SAP Data Privacy Governance

Leading the SAP Data Protection & Privacy Cloud solution development

Sandro.Lovisa@sap.com

Join us at:

SAP GRC

SAP CLOUD TRUST CENTER
sap.com/cloud-trust-center

Evelyne Salie

Senior Director, SAP Center of Excellence for Finance & Risk

SAP Data Protection and Privacy Knowledge Hub

Global Head of oCFO GTM Strategy

Evelyne.salie@sap.com

Join me online: Twitter LinkedIn

THE BEST RUN SAP

Follow all of SAP

www.sap.com/contactsap

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 platforms, 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.

THE BEST RUN SAP