General Data Protection Regulation in SAP

expertum
consulting excellence

What is GDPR?

What is GDPR?

- The GDPR is intended to unify the privacyregulation **in the whole of Europe**. The processing of European personal data will need to comply to the same regulations in every memberstate of the EU as of may 2018. Thus simplifying and allowing closer control on cross-border data processing.

  BUT: each country defines its own specificities at ratification.
- All companies that collect **personal data**: all information that allows to identify a person
- In force as off **25/5/2018**
- Non-compliance **Fines** 4% of annual turnover, or 20mio€ whichever is the greater -> board level concern

Key components

Right to be forgotten

Protection of sensitive data

Notification of Data breaches within 72 hours

Transparancy/approval of data subjects

Data Integrity

Rights of the Datasubject

Rights of the datasubject

- Right to review the stored data
- Right to request correction or deletion
- Right to refuse direct marketing
- Right to refuse automated decision making & profiling
- Right to move data from one service provider to another

DPIA? DPO?

DPIA:

- Data Protection Impact Assessment is required **to demonstrate** your **compliance**
- Evidence of compliance is your responsibility
- Regular updates needed

DPO:

- Data privacy Officer for companies that conduct a large amount of data processing on a daily basis – sensitive personal data or not.
- Manage relation with Privacy commission
- Point of contact internal & external

Data integrity

Lawful, Fairness and Transparency

Purpose Limitation

Data Minimization

Integrity and Confidentiality

Accuracy

Storage Limitation

GDPR in SAP

expertum
consulting excellence

8 key components

Identify

Process

Archive

Scramble

Authorize

Pseudonymize

Consent

Alert

8 key components

Identify

Process

Archive

Scramble

Authorize

Pseudonymize

Consent

Alert

Identify – Personal Data Definition

Any Information

Relating to an

identified or identifiable natural person (“data subject”)

Who is and/or can be identified

directly or indirectly

In particular by reference to

one or more identifiers (“types of subject data”)

Such as

- Personal Data (Art 4)
- Online Identifers (Rec 30)
- Special Category Personal Data (Art 9)

Identify – Identifiers for Personal Data

Identifier

(Art 4)

Name

Address

Email address

Passport number

Bank info

Date of Birth

Genetic Data

…

Online Identifier

(Rec 30)

IP Address

MAC Address

Cookies

Advertising ID

Browser fingerprint

GPS Data

Log Files

…

Special Category Identifier

(Art 9)

Biometric Data

Trade Union Membership

Race

Ethnic Origin

Political Opinion

Sexual Orientation

…

Identify - Typical SAP data fields

- Employees: SAP HCM infotypes: personal data for ethnic origin, military status, and disability (infotypes 0002 and 0077), severely challenged persons (infotype 0004), addresses (infotype 0006), bank details (infotype 0009), related person (infotype 0021), internal medical services (infotype 0028 with all the subtypes), and residence status (infotype 0094).
- Customers (KNA1, KNBK, KNVK)
- Vendors (LFA1, LFBK)
- Addresses (ADRC, ADR2, ADR3, ADR6)
- Business partners (BP000, BP030),
- Users (USR03)
- Credit cards (VCNUM)

Identify - Where used?

- Once the relevant master data fields are identified, the storage and (business) usage of these data fields needs to be mapped
- SAP data model is complex & interconnected
- For standard & custom developments (fields, tables, programs)
- For protection and for “right to insight”

What? | Why? | Where? | How long? | Who? | Source?

Identify – SAP Tools

SAP Information Steward

- Tool for personal data discovery, mapping, and management
- Holistic view on system landscape
- Allows drill down from system to tables to field level
- Categorization and tagging of personal data fields (also for GDPR)
- As not easy to identify all personal data fields - profiling (formats used for personal data)
  - xx.xx.xxxx
  - XX and 34 fields
- Classify and group data ; reporting

Other tools:
- SAP ABAP
- Custom development to identify, link & report on data elements
- UI logging

expertum
consulting excellence

8 key components

Identify

Process

Archive

Scramble

Authorize

Pseudonymize

Consent

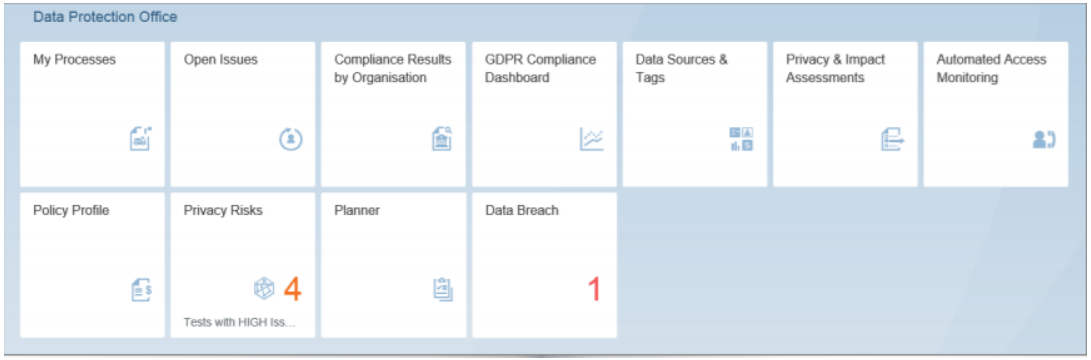
Alert

Process – "The" GDPR Tool: Process Control

SAP Process Control

- Document Policies
- Document Consent
- Document Controls
- Document DPIA's, reviews & updates

Can also be used for non-GDPR regulations

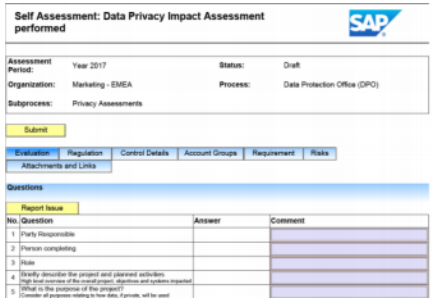


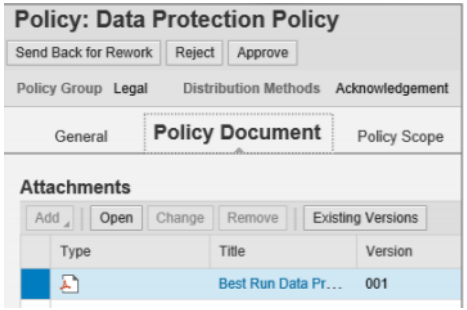
expertum
consulting excellence

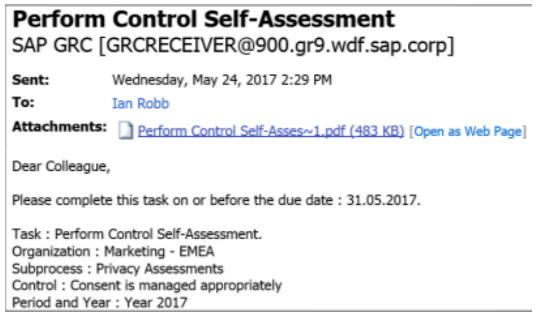
Process – SAP Tools

Process Control

- Data Privacy Impact Assessments
  - Show compliancy
  - Document controls
  - Test controls
  - Process & Policy Documentation
  - Issues & action plans
- Controls
  - Controls on user access (role based)
  - Controls on data reading
- Consent management
  - Automated for internal use
  - Documentation for external
  - Response policies Data breach







expertum
consulting excellence

8 key components

Identify

Process

Archive

Scramble

Authorize

Pseudonymize

Consent

Alert

Archive

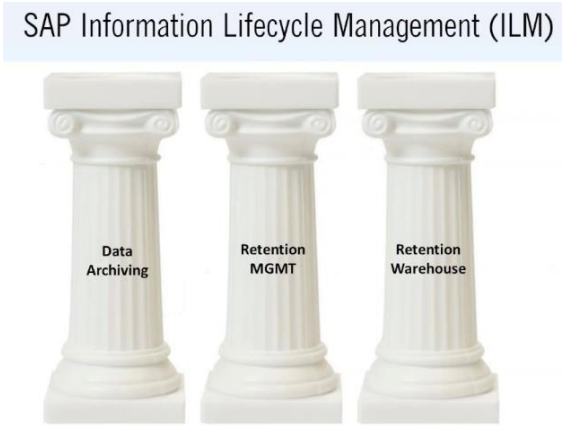
- When data is no longer active or needed for its primary purpose, the data needs to be "inactivated". Yet legal retention periods require traceability of interactions.

- Limit the available data to the required minimum
  - Total cost of ownership reduction
  - Improves performance
  - Less data to protect

Archive – SAP Tools

SAP ILM (Information Lifecycle Manager)

- Moves data out of business systems into long term archival storage
- Enforcement of "right of erasure" of SAP data
- Rules for controlling residence and retention policies
  - More than 100 built-in rules for deletion of archived data
- Rules for legal holds
- Rules for e-discovery
- Archiving and deletion reviews, auditing, and reporting
- Can be used as a solution for system shutdown



Other Tools:

- **SAP Archiving**
- **Open Text**

expertum
consulting excellence

8 key components

Identify

Process

Archive

Scramble

Authorize

Pseudonymize

Consent

Alert

Scramble

- Protect personal data in non productive systems
- Scrambling
  - Data can still be used, without link to persons
  - Availability of current data for test systems & development systems
  - Respecting syntax/configuration requirements

- Recognizable by situation/combination of data elements needs to be removed !
- Make test data a selective set/ data copy

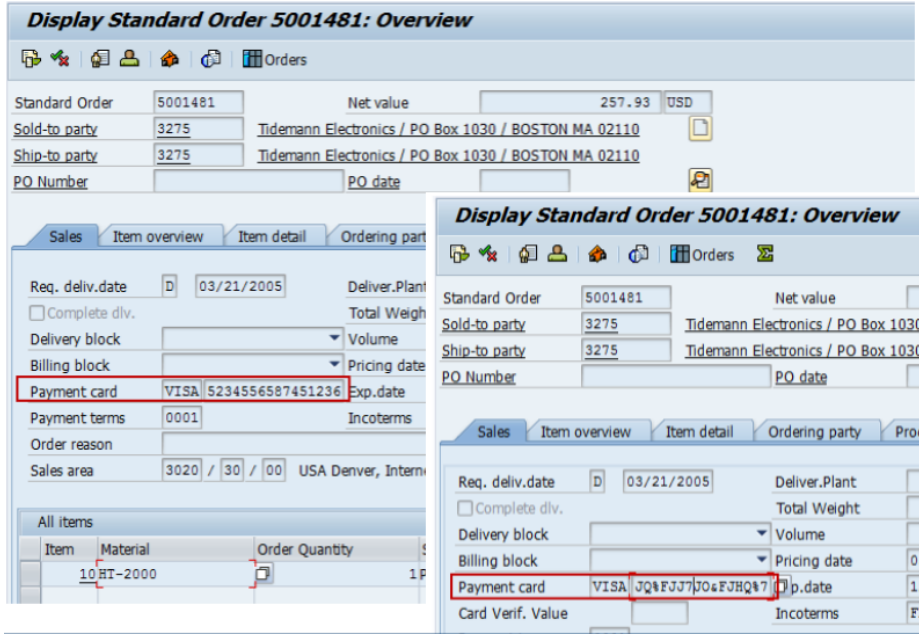
- **SAP TDMS: Test Data Migration Server**
- **EPI USE LABS**

expertum
consulting excellence

Scramble – SAP Tools

SAP TDMS (Test Data Migration Server)

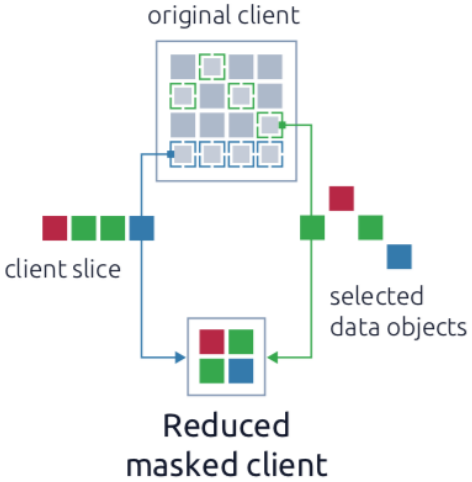
- Fast extraction of data from production system into non-production system
- Allows to take a time slice worth of data
- Or a subset of data (master/transactional)
- Scrambles the data
- Quick and efficient refresh of data in the non-production environment
- Reduce infrastructure expenditures by greatly reducing the volume of data in the test environment

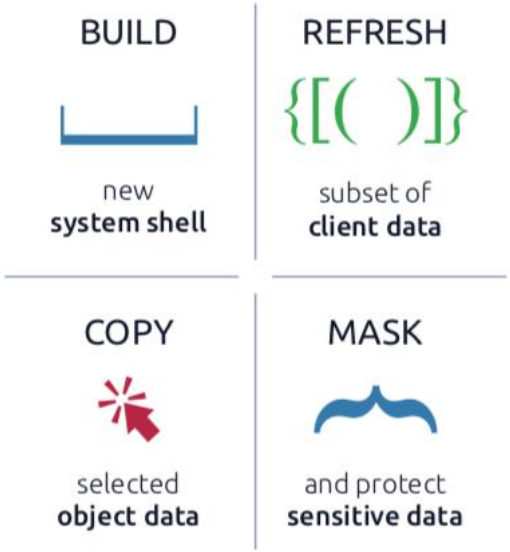


Scramble – SAP Tools

EPI USE LABS - Data Sync Manager™

- Client SyncTM for high performance client copying
- Object SyncTM for reliable test data when you need it
- Data SecureTM to protect your sensitive data
- System BuilderTM to build a new system shell quickly





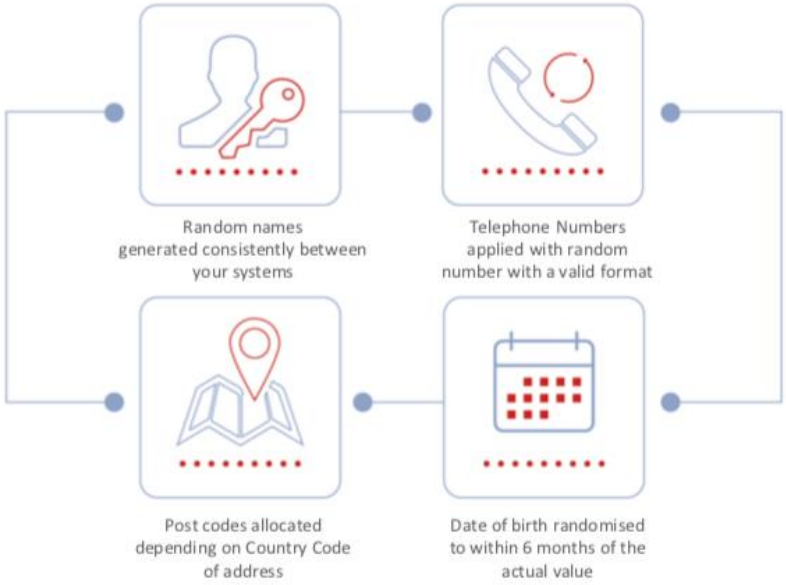
Data Secure™

- Protect sensitive data
- Safeguard across the landscape
- Comply with data protection laws

expertum
consulting excellence

Scramble – SAP Tools

EPI USE LABS



8 key components

Identify

Process

Archive

Scramble

Authorize

Pseudonymize

Consent

Alert

expertum
consulting excellence

Authorize

- Limit access to sensitive data:
  - Use a solid, flexible and clear **authorization concept**
  - Define a strict access management policy and process
  - Consistent across SAP applications & dbase layer (ECC, S/4HANA, HANA, BW, HR, FIORI, CRM,…)

- Restrict access to blocked data elements
- Restrict access to data reports
- Store data extracts at secure locations
- Implement sufficient security parameters to prevent unauthorized access

Authorize – SAP Tools

SAP GRC Access Control

- Manage lawful and block unlawful access to personal data
- Approvals and policies for users with access to personal data
- Categorization of roles and systems that store personal data
- Data access governance (user and role management, authorizations)
- User access reviews, auditing, and reporting

Access Violation Management
SAP IDM and SSO

expertum
consulting excellence

8 key components

Identify

Process

Archive

Scramble

Authorize

Pseudonymize

Consent

Alert

Pseudonymize

"Turning data Pseudonymous in such a way that the data subject is not or no longer identifiable"

- In case the subject requests so
- Selective, finetuning of authorization
- Field based
- Does not change underlying data
- Keeping historical data in reporting
- Regardless of access path
- Mass maintenance

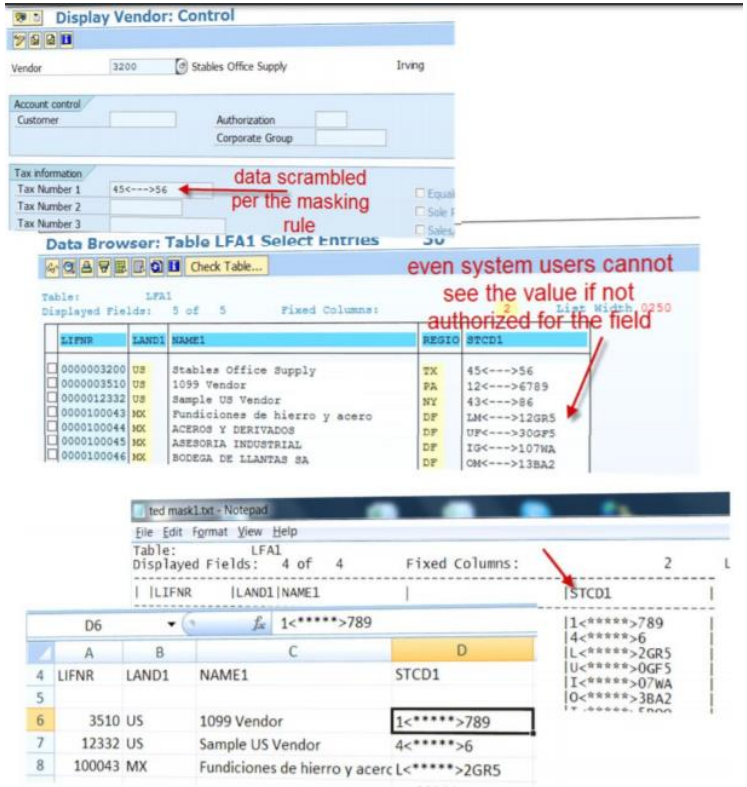
- **SAP UI Masking**
- **EPI Use Labs Masking**

expertum
consulting excellence

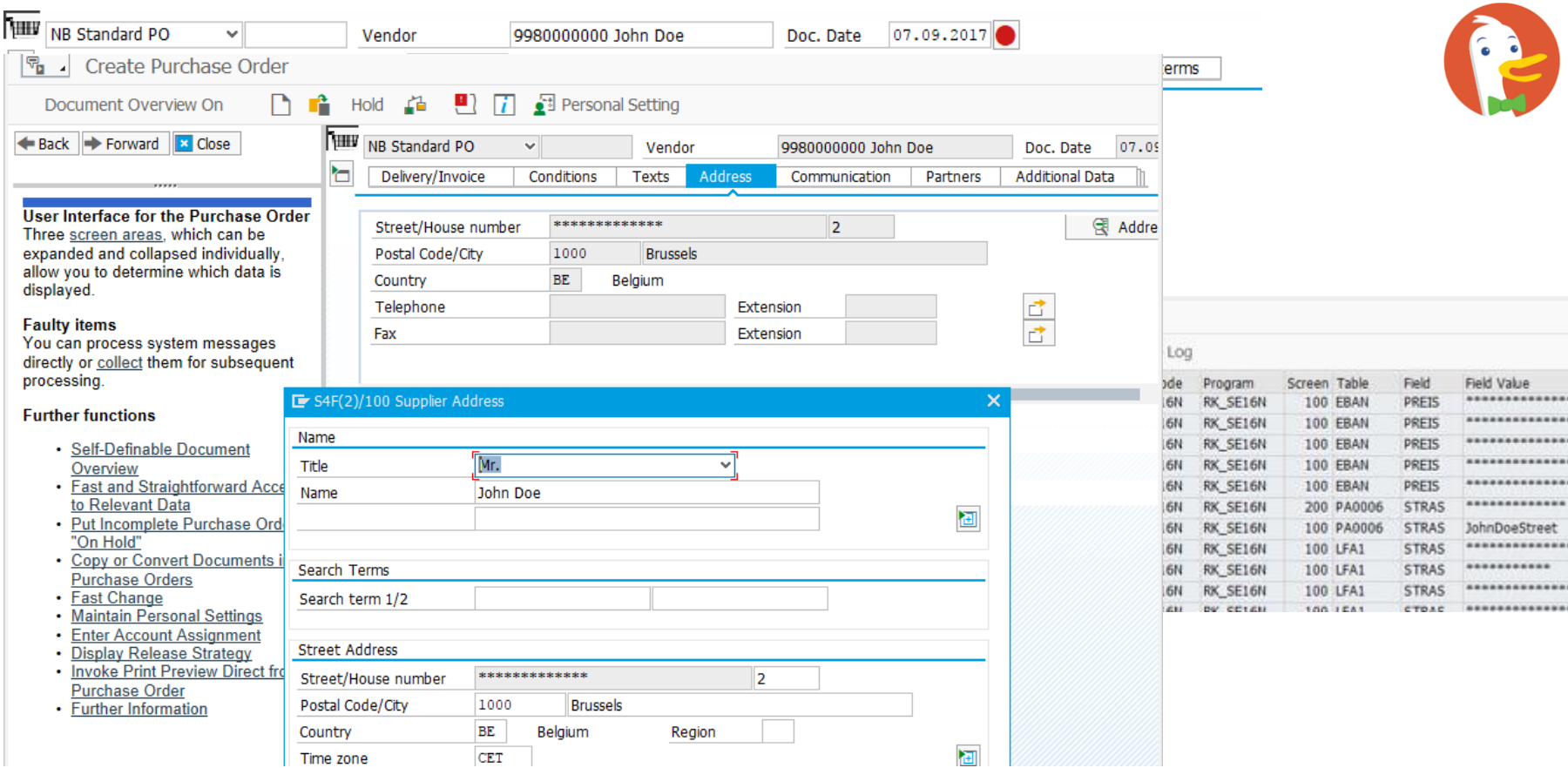
Pseudonymize – SAP Tools

UI Masking:

- To conceal sensitive data from specific users
- Active form of suppressing display of data in SAP GUI
- Does not change underlying data
- Define fields to be masked, and rules
  - configure **which (and how)** data is masked
  - configure **who (role/user) is authorized** to see unmasked data
- Automatic proposal of related tables & programs
- Also provides a BADI for complex business logic
- Also protects data during download, export, and print
- Mail alert when access is granted



expertum consulting excellence


NB Standard PO
Vendor
9980000000 John Doe
Doc. Date
07.09.2017
Create Purchase Order
Document Overview On
Hold
Personal Setting
Back
Forward
Close
User Interface for the Purchase Order
Three screen areas, which can be expanded and collapsed individually, allow you to determine which data is displayed.
Faulty items
You can process system messages directly or collect them for subsequent processing.
Further functions
Self-Definable Document Overview
Fast and Straightforward Acce to Relevant Data
Put Incomplete Purchase Ord "On Hold"
Copy or Convert Documents i Purchase Orders
Fast Change
Maintain Personal Settings
Enter Account Assignment
Display Release Strategy
Invoke Print Preview Direct fr Purchase Order
Further Information
Delivery/Invoice
Conditions
Texts
Address
Communication
Partners
Additional Data
Street/House number
Postal Code/City
1000
Brussels
Country
BE
Belgium
Telephone
Extension
Fax
Extension
S4F(2)/100 Supplier Address
Name
Title
Mr.
John Doe
Search Terms
Search term 1/2
Street Address
Region
Time zone
CET
Log
Program
Screen
Table
Field
Field Value
RK_SE16N
EBAN
PREIS
PA0006
STRAS
JohnDoeStreet
LFA1

8 key components

Identify

Process

Archive

Scramble

Authorize

Pseudonymize

Consent

Alert

expertum
consulting excellence

Consent

Any **freely given**, specific, informed and **unambiguous**

Indication of

The subject's wishes

By which he or she

by a statement or by a clear affirmative action

Signifies agreement to

The processing of personal data

relating to

him or her

Consent - Tools

SAP Process Control

- Consent management
  - Automated for internal use
  - Documentation for external
  - Response policies Data breach

Perform Control Self-Assessment
SAP GRC [GRCRECEIVER@900.gr9.wdf.sap.corp]

Sent: Wednesday, May 24, 2017 2:29 PM
To: Ian Robb
Attachments: Perform Control Self-Asses~1.pdf (483 KB) [Open as Web Page]

Dear Colleague,

Please complete this task on or before the due date : 31.05.2017.

Task : Perform Control Self-Assessment.
Organization : Marketing - EMEA
Subprocess : Privacy Assessments
Control : Consent is managed appropriately
Period and Year : Year 2017

Other:

- **SAP Hybris Cloud for Customer**
- **Custom reports**
- **EPI-Use Labs toolset**

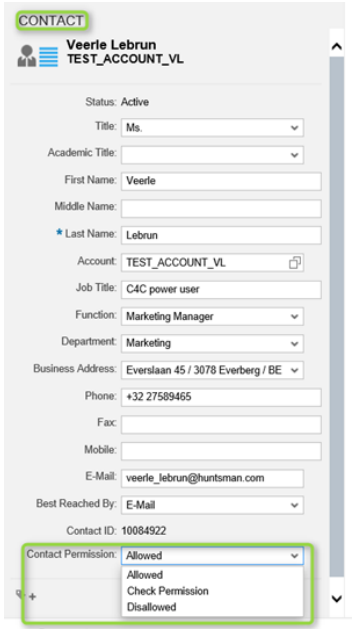
expertum
consulting excellence

Consent Management

- New SAP tools using social media integration, Hybris, HR Tools and ILM have consent documentation included

Social Media Consent Management has the following features:

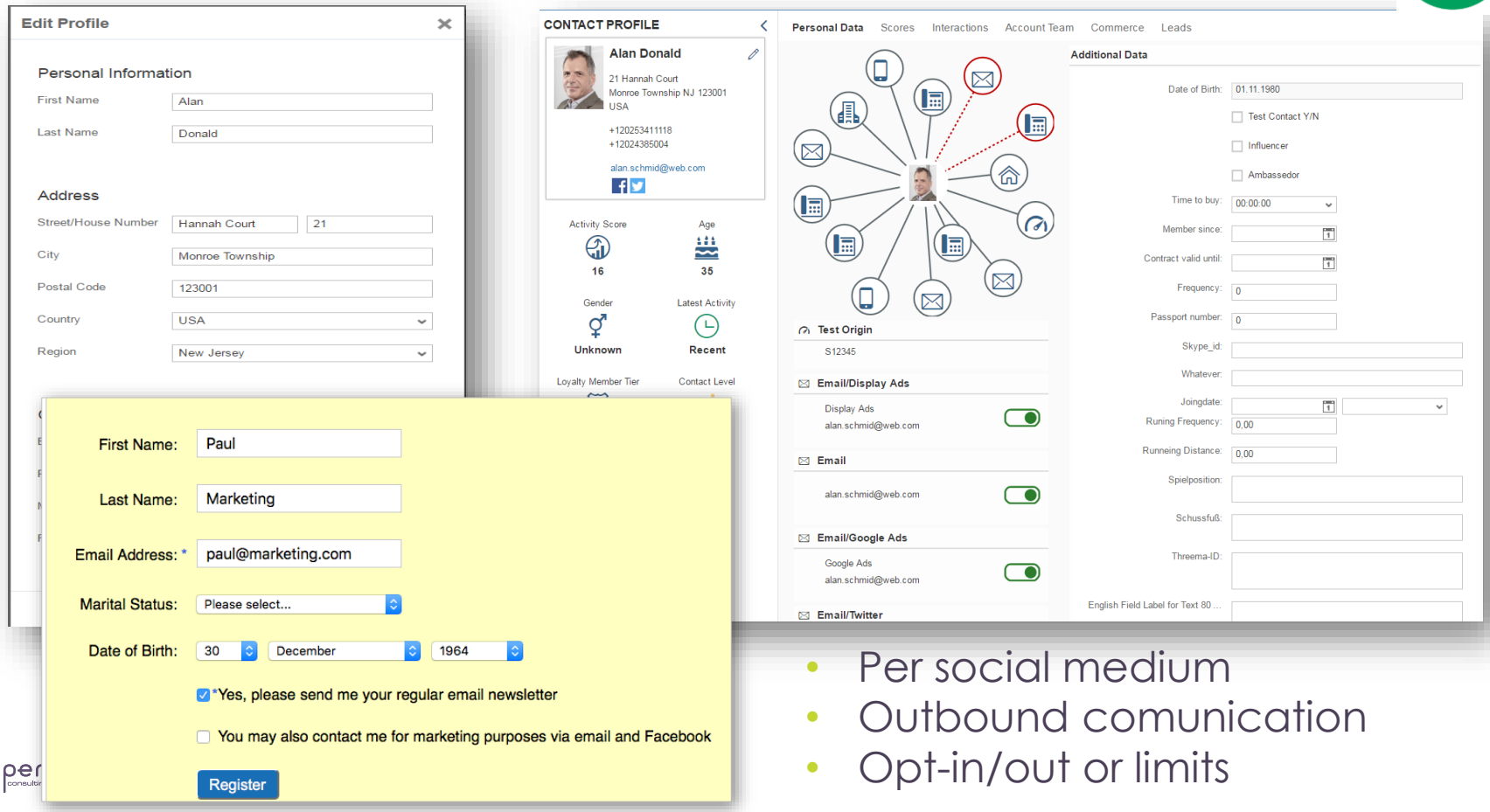
- Creating groups based on social media channels and data providers
- Defining social consent management based on the country and grouping
- Making four types of consent type available



Cloud for Marketing: marketing permissions: communication channel or channels you can use for the campaign are restricted to those for which permission has been granted

KCONS is a standard SAP Table which is used to store Consent Data: Consent data provided for legal entity information. This is available within R/3 SAP systems depending on the version and release level

expertum
consulting excellence



- Per social medium
- Outbound comunication
- Opt-in/out or limits

8 key components

Identify

Process

Archive

Scramble

Authorize

Pseudonymize

Consent

Alert

Alert

- Data Breach notification within 72 hours
- Continuous monitoring of who accesses specific data elements
- Insight to data usage – authorization finetuning
- Alert when not compliant to predefined rules
- Document data breach
- Impact analysis – cause & extent of breach
- Inform data owners

Alert – SAP Tools

Read Access Logging

- Logs and monitors user access to sensitive or classified data
- Configure which fields and elements are relevant based on the purpose
- System captures the read access in a log file
  - Who had access to what and when
- Monitors & alerts on data access
  - Direct sm30, se16,…
  - Indirect: RFCs, Web Dynpro, Web services
- Log can be analysed to determine the source of the data leakage

expertum
consulting excellence

Other:

- **UI Logging**
- **SAP Process Control (also** for response follow-up)
- **Fraud Management**

Search Result

View: Extended | Hits: 8

Created At (Local Time)	User Name	Client IP Address
06.09.2017 15:48:24,00	AIDE	10.32.196.27
06.09.2017 15:43:36,00	AIDE	10.32.196.27
06.09.2017 15:36:15,00	SDEWILDE	10.32.196.26
06.09.2017 15:33:29,00	SDEWILDE	10.32.196.26
06.09.2017 15:18:44,00	AIDE	10.32.196.27
06.09.2017 15:18:42,00	AIDE	10.32.196.27
06.09.2017 15:18:40,00	AIDE	10.32.196.27
06.09.2017 15:16:26,00	AIDE	10.32.196.27

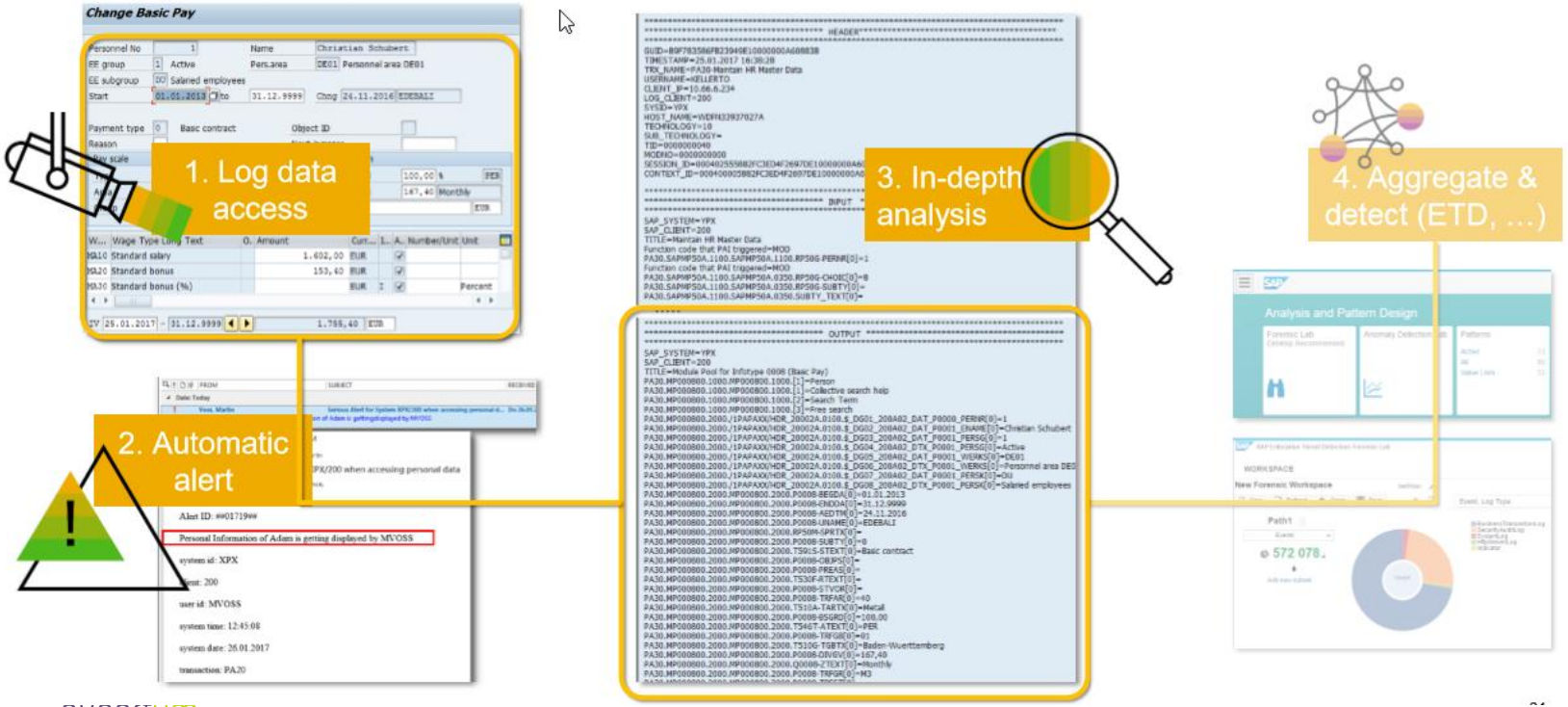
Detailed Information

Details | Access Environment

Log Domain	Log Domain Description	Field Value	Type	Field
		Stresemannstraße 12 / D-28207 Bremen	Output	:SAPLBUS_LOCATOR(3000)SCREEN_3000_

Alert – SAP Tools

UI Logging



UI Masking

- Conceal specific data (values in fields) unless required for the task

“the speed limiter”

Advantages:

- Decrease the risk of data leakage
  - Data minimization
  - Hide personal data
  - Also for downloads, printouts
- Keeps reports/aggregates accurate

UI Logging

- Keep data accessible, but log and analyze access

“the speed camera”

- Advantages:
  - Key to successful logging: not only logging, but being able to identify unauthorized , non-compliant or malicious activity – through automated warnings
  - Psychological barrier against non-task related access

8 key components – SAP Tools

Identify

- SI Steward
- SAP Reports
- UI logging

Processes

- SAP Process Control

Archive

- ILM
- SAP Archiving

Scramble

- TDMS

Authorize

- SAP Access Control
- Authorization Concept

Pseudonymize

- UI Masking

Alert

- RAL
- UI Logging
- Fraud Mgt

Consent

- SAP Process Control
- Hybris C4C
- Your CRM/dbase

Expertum

GDPR Roadmap

expertum
consulting excellence

The Expertum GDPR Roadmap for SAP (1/2)

1. Identify which data is relevant
   - Workshop to analyse data needed/ available per Process stream in SAP
   - Identify system located; server location
   - Autosearch tool for Personal datafields
   - Identify user access

2. Document your Processes, DPIAs & controls in Process Control

3. Limit your scope
   - Archive old data – Set up Archiving procedure
   - Slice system copy to test systems

The Expertum GDPR Roadmap for SAP (2/2)

4.Scramble Test Data

5. Restrict Display Access

- Analyse who has access to which fields
- Adjust authorizations
- Pseudonymize specific data fields

6. Enhance Control

- Access Control - UI Logging – Process Control
- Set-up alerts

Expertum Support

Project Management

Identify

- SI Steward
- SAP Reports
- UI logging

Processes

- SAP Process Control

Archive

- ILM
- SAP Archiving

Scramble

- TDMS

Authorize

- SAP Access Control
- Authorization Concept
- Access Violation Mgt

Pseudonymize

- UI Masking

Alert

- RAL
- UI Logging
- Fraud Mgt

Consent

- SAP Process Control
- Hybris C4C
- Your CRM/dbase

expertum
consulting excellence

Expertum network

Expertum delivers expertise. Partly because we respect our boundaries.

If you need assistance outside our expertise, we are happy to connect you to some of our tried and trusted partners.

expertum
consulting excellence

Thanks for listening! Any questions?

Heidi Cloetens
GRC Consultant

+32 479 92 79 46
Heidi.cloetens@expertum.net

www.expertum.net

Inspire by Experience.