

General Data Protection Regulation in SAP



What is GDPR?

What is GDPR?

- The GDPR is intended to unify the privacy regulation **in the whole of Europe**. The processing of European personal data will need to comply to the same regulations in every member state 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 of **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

Transparency/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



8 key components

Identify



Process



Archive



Scramble



Authorize



Pseudonymize



Consent



Alert



8 key components

Identify



Process



Archive



Scramble



Authorize



Pseudonymize



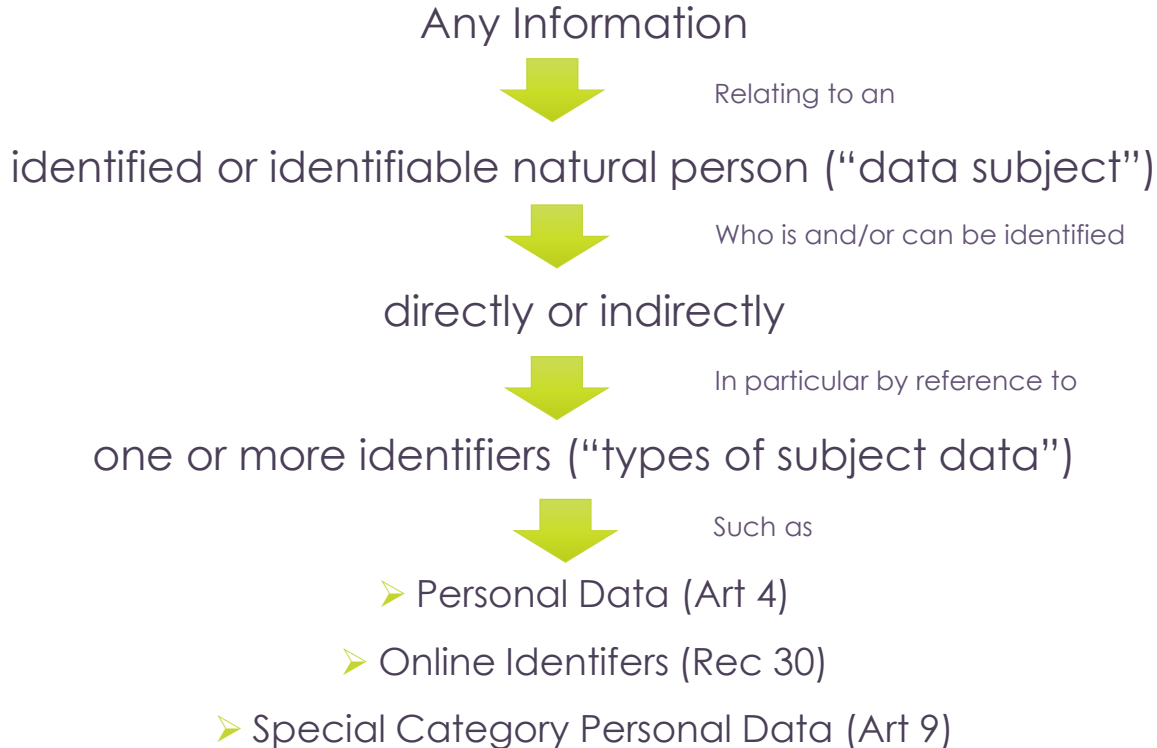
Consent



Alert



Identify – Personal Data Definition



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

8 key components

Identify



Process



Archive



Scramble



Authorize



Pseudonymize



Consent



Alert



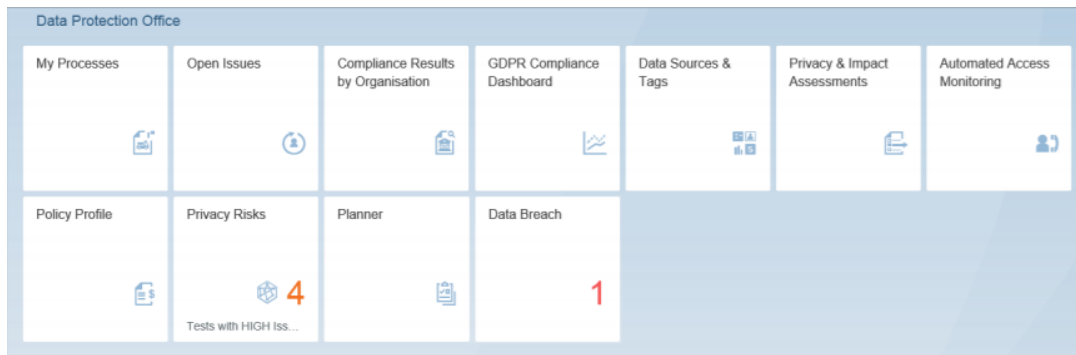
Process – “The” GDPR Tool: Process Control



SAP Process Control

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

Can also be used for non-GDPR regulations



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

Self Assessment: Data Privacy Impact Assessment performed

Assessment Period: Year 2017 Status: Draft
Organization: Marketing - EMEA Process: Data Protection Office (DPO)
Subprocess: Privacy Assessments

Submit

Attachments and Links

Questions

No.	Question	Answer	Comment
1	Party Responsible		
2	Person completing		
3	Role		
4	Identify duration the project and planned activities		
5	Identify sources of the personal data, retention and access request		
6	Identify the purpose of the project		
7	Consent of persons relating to how this purpose will be used		

Policy: Data Protection Policy

Send Back for Rework **Reject** **Approve**

Policy Group **Legal** Distribution Methods Acknowledgement

General **Policy Document** Policy Scope

Attachments

Add **Open** **Change** **Remove** **Existing Versions**

Type	Title	Version
	Best Run Data Pr...	001

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

8 key components

Identify



Process



Archive



Scramble



Authorize



Pseudonymize



Consent



Alert

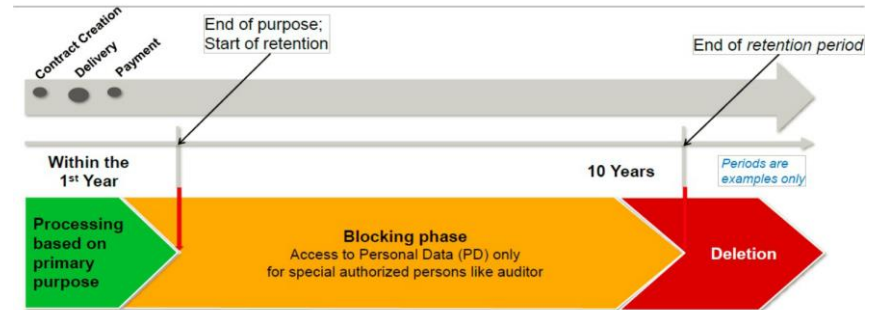


Archive



- 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

Lifecycle of personal data handled



Requirement:

Personal Data that are no longer needed for the primary processing purpose must be deleted, unless there are other retention periods defined by law or contract, in that case it has to be blocked.

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

SAP Information Lifecycle Management (ILM)



Other Tools:

- ⌚ SAP Archiving
- ⌚ Open Text

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**

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

Display Standard Order 5001481: Overview

Standard Order: 5001481 Net value: 257.93 USD

Sold-to party: 3275 Tidemann Electronics / PO Box 1030 / BOSTON MA 02110

Ship-to party: 3275 Tidemann Electronics / PO Box 1030 / BOSTON MA 02110

PO Number: PO date:

Sales Item overview Item detail Ordering party

Req. deliv.date: D 03/21/2005 Deliver.Plant: Total Weight: Volume: Pricing date: 0

☐ Complete div.

Delivery block: Billing block: Payment card: VISA 5234556587451236 Exp.date: Payment terms: 0001 Incoterms: Order reason: Sales area: 3020 / 30 / 00 USA Denver, Intern

All items

Item	Material	Order Quantity
10	RT-2000	1

Display Standard Order 5001481: Overview

Standard Order: 5001481 Net value:

Sold-to party: 3275 Tidemann Electronics / PO Box 1030

Ship-to party: 3275 Tidemann Electronics / PO Box 1030

PO Number: PO date:

Sales Item overview Item detail Ordering party Pro

Req. deliv.date: D 03/21/2005 Deliver.Plant: Total Weight: Volume: Pricing date: 0

☐ Complete div.

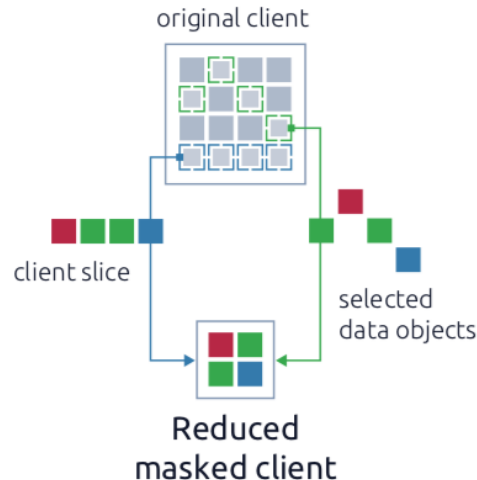
Delivery block: Billing block: Payment card: VISA JQ%FJJ7J0%FJHQ%7J Exp.date: 1 Card Verif. Value: Incoterms: F

Scramble – SAP Tools



EPI USE LABS - Data Sync Manager™

- ✓ Client Sync™ for high performance client copying
- ✓ Object Sync™ for reliable test data when you need it
- ✓ Data Secure™ to protect your sensitive data
- ✓ System Builder™ to build a new system shell quickly



BUILD



new
system shell

REFRESH



subset of
client data

COPY



selected
object data

MASK



and protect
sensitive data

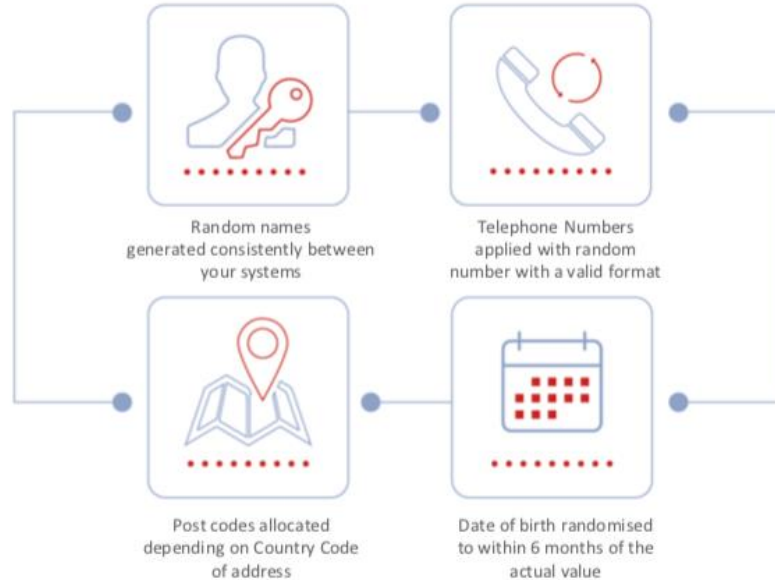
Data Secure™

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

Scramble – SAP Tools



EPI USE LABS



8 key components

Identify



Process



Archive



Scramble



Authorize



Pseudonymize



Consent



Alert



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**

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



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

Display Vendor: Control

Vendor: 3200 Stables Office Supply Irving

Account control: Customer Authorization: Corporate Group

Tax information:

Tax Number	Value
Tax Number 1	45<--->56
Tax Number 2	
Tax Number 3	

Data Browser: Table LFA1 Select Entries

LIFNR	LAND1	NAME1	REGIO	STCD1
0000003200	US	Stables Office Supply	TX	45<--->56
0000003510	US	1099 Vendor	PA	12<--->6789
0000012332	US	Sample US Vendor	NY	43<--->86
0000100043	MX	Fundiciones de hierro y acero	DF	1M<--->12GR5
0000100044	MX	ACEROS Y DERIVADOS	DF	UP<--->30GF5
0000100045	MX	ASERORIA INDUSTRIAL	DF	IG<--->107WA
0000100046	MX	BOCEGA DE LLANTAS SA	DF	OM<--->13BA2

Annotations: "data scrambled per the masking rule" points to the tax number field. "even system users cannot see the value if not authorized for the field" points to the STCD1 column header.

masked.txt - Notepad

Table: LFA1

Displayed Fields: 4 of 4 Fixed Columns: 2

LIFNR	LAND1	NAME1	STCD1
6	3510	US	1099 Vendor
7	12332	US	Sample US Vendor
8	100043	MX	Fundiciones de hierro y acero

Annotations: A red arrow points to the masked value '1<*****>789' in the STCD1 column for row 6.



Create Purchase Order

Document Overview On



Hold



Personal Setting

Back Forward Close



NB Standard PO

Vendor

9980000000 John Doe

Doc. Date 07.09



Delivery/Invoice

Conditions

Texts

Address

Communication

Partners

Additional Data

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 Access to Relevant Data](#)
- [Put Incomplete Purchase Order "On Hold"](#)
- [Copy or Convert Documents in Purchase Orders](#)
- [Fast Change](#)
- [Maintain Personal Settings](#)
- [Enter Account Assignment](#)
- [Display Release Strategy](#)
- [Invoke Print Preview Direct from Purchase Order](#)
- [Further Information](#)

Street/House number ***** 2

Postal Code/City 1000 Brussels

Country BE Belgium

Telephone Extension

Fax Extension

Address

S4F(2)/100 Supplier Address

Name

Title **Mr.**

Name John Doe

Search Terms

Search term 1/2

Street Address

Street/House number ***** 2

Postal Code/City 1000 Brussels

Country BE Belgium Region

Time zone CET

Log

Code	Program	Screen	Table	Field	Field Value
6N	RK_SE16N	100	EBAN	PREIS	*****
6N	RK_SE16N	100	EBAN	PREIS	*****
6N	RK_SE16N	100	EBAN	PREIS	*****
6N	RK_SE16N	100	EBAN	PREIS	*****
6N	RK_SE16N	200	PA0006	STRAS	*****
6N	RK_SE16N	100	PA0006	STRAS	JohnDoeStreet
6N	RK_SE16N	100	LFA1	STRAS	*****
6N	RK_SE16N	100	LFA1	STRAS	*****
6N	RK_SE16N	100	LFA1	STRAS	*****

8 key components

Identify



Process



Archive



Scramble



Authorize



Pseudonymize



Consent



Alert



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

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

CONTACT

Veerle Lebrun
TEST_ACCOUNT_VL

Status: Active

Title: Ms. ▼

Academic Title: ▼

First Name: Veerle

Middle Name:

* Last Name: Lebrun

Account: TEST_ACCOUNT_VL

Job Title: C4C power user

Function: Marketing Manager ▼

Department: Marketing ▼

Business Address: Everslaan 45 / 3078 Everberg / BE ▼

Phone: +32 27589465

Fax:

Mobile:

E-Mail: veerle_lebrun@huntsman.com

Best Reached By: E-Mail ▼

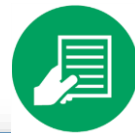
Contact ID: 10084922

Contact Permission: Allowed ▼

- Allowed
- Check Permission
- Disallowed

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



Edit Profile

Personal Information

First Name:

Last Name:

Address

Street/House Number:

City:

Postal Code:

Country:

Region:

CONTACT PROFILE

Alan Donald

21 Hannah Court
Monroe Township NJ 123001
USA

+120253411118
+12024385004

alan.schmid@web.com

Activity Score: 16

Age: 35

Gender: Unknown

Latest Activity: Recent

Loyalty Member Tier:

Contact Level:

Personal Data

Scores Interactions Account Team Commerce Leads

Additional Data

Date of Birth:

☐ Test Contact Y/N

☐ Influencer

☐ Ambassador

Time to buy:

Member since:

Contract valid until:

Frequency:

Passport number:

Skype_id:

Whatever:

Joiningdate:

Running Frequency:

Running Distance:

Spielposition:

Schussfuß:

Threema-ID:

English Field Label for Text 80 ...

Test Origin

S12345

Email/Display Ads

Display Ads: ☐ alan.schmid@web.com

Email

alan.schmid@web.com ☐

Email/Google Ads

Google Ads: ☐ alan.schmid@web.com

Email/Twitter

First Name:

Last Name:

Email Address: *

Marital Status:

Date of Birth:

☒ *Yes, please send me your regular email newsletter

☐ You may also contact me for marketing purposes via email and Facebook

- Per social medium
- Outbound communication
- 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_

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

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 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.



Thanks for listening! Any questions?

Heidi Cloetens
GRC Consultant

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

www.expertum.net

Inspire by Experience.