Introduction to EU GDPR Compliance
with SAP Business One

SAP Business One Product Management
May 2018
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.
Table of Contents

1. GDPR – Regulation & Key Terms
   ▪ Scope, relevancy, important to consider, due May 25, 2018

2. GDPR relevant functionality delivered prior to SAP Business One 9.3 PL04
   ▪ Authorizations, Data Ownership, Change Logs, System Access Log

3. GDPR relevant functionality delivered with SAP Business One 9.3 PL04
   ▪ Personal Data Tools - Setup and Personal Data Management Wizard (Report, Natural Person, Cleanup)
   ▪ Access log for sensitive personal data and encryption/masking of these data (Germany only)
What is GDPR?
The General Data Protection Regulation (GDPR), EU Regulation 2016/679, effective May 25, 2018, gives individuals control and protection of their personal data. Data controllers, who determine the purpose and means of processing personal data, and processors, who process for controllers, are affected.

Penalties up to 4% of annual global revenue or €20 million – whichever is greater.

Who must comply?
Organizations that offer goods or services to, or monitor the behavior of, EU data subjects and those that process or hold the personal data of EU residents.

Applies to:
Natural persons, whatever their nationality or place of residence in the EU, in relation to the processing of their personal data.
What should be considered to comply with data privacy regulation?

**KEY MESSAGE**
- In general, **no personal data** must be stored **without purpose and explicit consent** to it.
- All **companies doing business in the EU** need rules which define **which personal data is needed**, how consent must be captured, what retention periods are needed for data, how data can be accessed, deleted and more.
- **Start with analysis** of organization and its business processes.

**Which data do you have?**
- Master & transactional data
- Basic & sensitive personal data
- …

**Who has access to my data?**
- Where is data stored?
- Access authorization
- Access log
- …

**What is purpose of the data?**
- Explicit consent for data usage and storage
- Deletion by request
- Retention periods for data
- …

**Your organizational rules**
- Which data is needed for which process?
- How do business partners **give their consent** for data processing (e.g. contracts, marketing permissions…)?
- How and how often is **compliance being audited**?
- What happens in case of **data privacy requests** or violations?
- …more

**Your business software**
- **Private customer** master & transactional data
- **Service Agent** master & transactional data
- **Employee** master & transactional data e.g. address, religion, time sheet
- **User** authorization & access control logging
- …more

---

© 2018 SAP SE or an SAP affiliate company. All rights reserved. | CUSTOMER
GDPR at a Glance

### Lawful processing
- Requires a legal basis, e.g. a contract, consent, or legitimate interest for the processing of personal data
- Must keep such data accurate and stored only as long as needed

### Personal data
- Includes online identifiers, mobile device IDs, IP addresses, and more; may include de-personalized data
- Requires parental consent for children under 16 years

### Controllers and processors
- Non-EU data controllers and processors must also comply when processing data of EU individuals.
- Controller is accountable for failures of the data processor; both controller and processor are liable for breaches.

### Breach notification
- Mandatory notification to authority within 72 hours of becoming aware of breach
- Communication to affected individuals without undue delay
- Maximum fine can apply

### Individual rights
- The GDPR suggests self-service apps for personal data-related information requests
- Rights apply across all systems, including those of third parties.
- Businesses generally cannot charge and must respond in <1 month.

### Demonstration of compliance
- Compliance and accountability are integral to a data protection program.
- Codes of conduct and policies can help ensure accountability.

### Accountability
- Produce and maintain evidence of compliance-supporting actions
- Build data protection into product design and development
- Appoint a data protection officer (DPO) if your company has large-scale processing requirements

### Lawful processing always requires legal permission
- ▪ Requires a legal basis, e.g. a contract, consent, or legitimate interest for the processing of personal data
- ▪ Must keep such data accurate and stored only as long as needed

### Personal data
- Sensitive personal data
- ▪ Includes online identifiers, mobile device IDs, IP addresses, and more; may include de-personalized data
- ▪ Requires parental consent for children under 16 years

### Controllers
- Non-EU data controllers and processors must also comply when processing data of EU individuals.
- Controller is accountable for failures of the data processor; both controller and processor are liable for breaches.

### Breach notification
- Mandatory notification to authority within 72 hours of becoming aware of breach
- Communication to affected individuals without undue delay
- Maximum fine can apply

### Individual rights
- The GDPR suggests self-service apps for personal data-related information requests
- Rights apply across all systems, including those of third parties.
- Businesses generally cannot charge and must respond in <1 month.
GDPR at a Glance

Protects fundamental rights related to the processing personal data

Controllers and processors

- Non-EU data controllers and processors must also comply when processing data of EU individuals.
- Controllers determine the purpose and means of processing personal data and bear primary responsibility for compliance.
- Processors are those who process personal data on behalf of a controller.
- Controller is accountable for failures of the data processor, and both controller and processor are liable for breaches.
Personal Data

- Personal data relates to an identified or identifiable person and includes online identifiers such as name, phone, e-mail address, mobile device IDs, IP address…
- Sensitive personal data includes data such as ethnic origin, biometric or genetic data, or health, and can be subject to more stringent requirements.
- De-personalized data is in scope
- Special categories of personal data may require stronger reasons to process and tougher protections
Lawful processing

- In general, there must be a legal basis, like a contract, **explicitly expressed consent**, or legitimate interest for the processing of personal data.
- Personal data must only be used for specific purposes, kept accurate, and not be stored longer than needed.
- Parental consent is generally required for those under 16 years.
GDPR at a Glance

Protects fundamental rights related to the processing personal data

Individual rights
- GDPR recommends support of individual data requests through a self-service system where possible.
- Rights generally apply across all systems, including those of third parties.
- Businesses generally cannot charge and must respond in <1 month.

Lawful processing always requires legal permission
- Consent
- Contract
- Legal obligation
- Vital interest
- Public interest
- Legitimate interest

Personal data
- Sensitive personal data

Controllers  Processors

Transfer of data

EU and non-EU
GDPR at a Glance
Protects fundamental rights related to the processing personal data

Accountability
- Involves a comprehensive framework and set of principles which allows (just as examples):
  - to produce and maintain evidence of actions to achieve and evaluate compliance
  - to assess data privacy risks and consider data protection in the early stages of product and project design
- Assign a DPO - Data Protection Officer – (companies with large-scale processing of personal data)
GDPR at a Glance
Protects fundamental rights related to the processing personal data

Individual rights
- to be informed
- of access
- to rectification
- to erasure
- to restrict processing
- to data portability
- to object
- Auto. decisions and profiling

Accountability
- Data protection officer
- Privacy by design
- Privacy impact assessments
- Evidence of compliance

Lawful processing always requires legal permission
- Consent
- Contract
- Legal obligation
- Vital interest
- Public interest
- Legitimate interest

Breach notification
- Mandatory notification to supervisory authority within 72 hours of becoming aware of a personal data breach
- Communication to affected individuals without undue delay if breach is likely to result in high risk to rights and freedoms of individuals
GDPR at a Glance
Protects fundamental rights related to the processing personal data

- **Controllers**: EU and non-EU
- **Processors**: EU and non-EU
- **Data protection officer**: Accountability
- **Privacy by design**: Accountability
- **Privacy impact assessments**: Accountability
- **Evidence of compliance**: Accountability
- **Data transfer**: Lawful processing always requires legal permission
- **Lawful processing**: Consent, Contract, Legal obligation, Vital interest, Public interest, Legitimate interest
- **Sensitive personal data**
- **Individual rights**:
  - ...to be informed
  - ...of access
  - ...to rectification
  - ...to erasure
  - ...to restrict processing
  - ...to data portability
  - ...to object
  - Auto. decisions and profiling
- **Breach notification**:
  - Response time
  - Penalties

Demonstration of compliance
- Compliance and accountability need to be an integral part of an overall data protection program.
- Communication of the codes of conduct, as well as privacy policies and procedures, help support compliance, with good understanding of data protection processes.
- Certifications will be a means to demonstrate compliance, but are not yet officially required or recognized.
- Other standards can also help show compliance, eg ISO 27001 (best-practice standard for information security, broader than GDPR).
Who is involved – Basic scheme

- **Governance**
  - Chief compliance officer
  - Chief risk officer
  - Head of legal
  - Chief audit executive

- **Data protection officer**
  - Other data protection experts (chief data officer…)

- **Operations**
  - Chief information officer
  - Chief information security officer
  - Business process owners
GDPR and SAP Business One
Glossary – Good to Know Key Terms

- **DPP** – Data Protection and Privacy.
- **Natural Person** – A real human being (as distinguished from a corporation, machine or robot); new property in SAP Business One to identify records of personal data.
- **Data Subject** – A natural person for whom the system stores personal data.
- **Personal Data** – Any data that can identify a natural person (name, date of birth, address, telephone number, e-mail address, car license plate, IP address, etc.).
- **Sensitive Personal Data** – Special category of data with stronger protection and special rules required (religion/confession, ethnic origic, blood type, etc.).
- **Data Controller** – Who determines the purpose and means of processing personal data and bears primary responsibility for compliance.
- **Data Processor** – Who processes personal data on behalf of a controller.
- **GDPR Objects** – SAP Business One objects which store personal data.
GDPR / DPP relevant functionality available
Prior to SAP Business One 9.3 PL04
Authorizations

Feature

- Authorizations allow users to view, create, and update documents that you assign to them, according to data ownership definitions.
- By default, a new user has no authorizations. Each user can have only one manager who assigns permissions. You can define users as either regular users or superusers.
- You can define approval processes for the purchasing and sales transactions in the system that override the standard permissions.

Benefits

- Control and set which natural person (user) has access to which form, object or a single field in selected cases.
- You can restrict user access to documents and/or personal data.
Authorization Simplification with v9.3

Feature
- Authorization Groups renamed to User Groups and relocated under Setup - General.
- 3 Categories:
  - Authorization: User authorizations with validity dates; individual users within the User Group can have further refined validity dates.
  - Form Settings: User form settings.
  - Cross All Types: Applies to all types.
- Cockpit template can be set up as default for the group (see New Cockpit Templates for more info).
- Copy Form Settings now has a Groups tab; all users in the chosen group inherit the form settings.

Benefits
- Manage temporary authorizations.
- Quickly apply form setting defaults to a group of users.
Data Ownership (1/3)

Feature

- Data ownership allows the company to have control over data elements. With the data owner function, you can define the rightful owner of data and information.
- Therefore, your company's data can be secured and protected by the predefined authorization. Information and data can be accessed by permitted roles and users only.
- From 9.3 release, when managing multiple branches the user's branch assignment will automatically determine access to BPs and Documents when the BPs'/Documents' branch assignment matches the user's branch assignment.

Benefits

- Decide on activation of new functions to better control and contribute to GDPR compliance.
- Restrict user access to documents which are relevant to their role/daily work.
Data Ownership (2/3) – with Business Partners

Feature

- Data ownership management extended to business partners with SAP Business One 9.2.
- Restrict access and visibility of:
  - Business Partner Master Data
  - Documents using Business partner with owners
- Manage data ownership by:
  - Documents Only:
    - Permissions are defined per document.
  - Business Partners Only:
    - Permissions for documents are defined by whether users have permission to the business partner used in documents.
  - Business Partners and Documents:
    - When Business Partners have owners, permissions for documents are decided by whether users have permission for the business partner used in documents.
    - When Business Partners have no owner, permissions are decided per document.
Data Ownership (3/3)

Feature

- Bypass Data Ownership by granting access at Company level.
- Restrict system reports like Open Items List to reflect only results against specific Business Partners for specific users.
- Exclude specific restrictions and enable read access.

Benefits

- Additional layer of authorization and security.
- Enhanced usability as only relevant data is considered.
- Safe guard company information against data theft.
Feature

- Use the change log to gain an overview of changes in most windows of SAP Business One.
- Each time you update, for example, tax groups, withholding tax, house banks, freight, credit card, authorizations, employee master data, sales, purchasing documents, production orders, or charts of accounts, the application records the change and can show it as required in the Change Log window.

Benefit

- By tracking the change log, your auditors can more easily verify and audit G/L entries.
- Original and new values are stored and logically grouped.
Feature

- New Change Log Cleanup Utility available with B1 9.3 PL00.
- Enables users to clean up the change log to reduce the size of a company database.
- Users have the ability to determine which objects from the change log entries should be deleted and restrict the deletion to a specific date range.
- Utility subject to appropriate user authorisation.

Benefits

- Improved performance when running upgrades due to a reduced amount of data to be upgraded.
- Companies running SAP Business One for a long time with a large change log are able to delete old changes that were registered.
System Access Log

Feature

- The Access Log window displays the access details of SAP Business One users who have logged on and logged off with one of the following:
  - SAP Business One client
  - DI API

Benefits

- Tracking and recording date, time and users logging into the system.
- This is a very important prerequisite when fraudulent operations need to be analyzed and is a prerequisite for corporate governance.
GDPR / DPP relevant functionality delivered with SAP Business One 9.3 PL04
DPP Initialization Function

**Feature**

- Initialization setting on Company Details form to activate all new Data Privacy and Protection enhancements in SAP Business One.
- Automatically activated for all localizations for EU countries, Norway and Switzerland after upgrade to 9.3 PL04. It can be turned off (not recommended) before any natural person is determined and/or any personal data erasure or personal data block is executed.

**Benefit**

- Decide on activation of new functions to better control and contribute to GDPR and Data Privacy Protection compliance.
Data Protection Tools – Main Menu Entry

Feature
- Data Protection Tools are managed under Administration/Utilities.

Benefit
- Centralized location for managing personal data protection.
# Personal Data Management Setup

## Feature
- New control to define and categorize personal Data.
- User Defined Fields (UDF) in GDPR objects can be determined as personal data.
- New entry under Data Protection Tools.

## Benefits
- Centralized location for management and maintenance of Personal Data.
- Structured and categorized location.

---

### Table: Personal Data Management - Setup

<table>
<thead>
<tr>
<th>#</th>
<th>Data Type</th>
<th>Data Subtype</th>
<th>Category</th>
<th>Group</th>
<th>Field Name</th>
<th>Description</th>
<th>Database Reference</th>
<th>Default Data Classification</th>
<th>Data Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>221</td>
<td>Time Sheets</td>
<td>Project Management Time Sheet - Header</td>
<td>Lastname</td>
<td>OTSH-Lastname</td>
<td>OTSH-Lastname</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
</tr>
<tr>
<td>222</td>
<td>Time Sheets</td>
<td>Project Management Time Sheet - Rows</td>
<td>GPS Date</td>
<td>TSHP-GPSSDate</td>
<td>TSHP-GPSSDate</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
</tr>
<tr>
<td>223</td>
<td>Incoming Payments</td>
<td>Invoicing Payment</td>
<td>Address</td>
<td>ORCH-Address</td>
<td>ORCH-Address</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
</tr>
<tr>
<td>224</td>
<td>Incoming Payments</td>
<td>Invoicing Payment</td>
<td>Customer/Seller Name</td>
<td>ORCH-CustomerName</td>
<td>ORCH-CustomerName</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
</tr>
<tr>
<td>225</td>
<td>Incoming Payments</td>
<td>Invoicing Payment - Cheques</td>
<td>Account Number</td>
<td>RCTA-ActNum</td>
<td>RCTA-ActNum</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
</tr>
<tr>
<td>226</td>
<td>Incoming Payments</td>
<td>Invoicing Payment - Credit Vouchers</td>
<td>Credit Card No.</td>
<td>RCTA-CreditCard</td>
<td>RCTA-CreditCard</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
</tr>
<tr>
<td>227</td>
<td>Incoming Payments</td>
<td>Invoicing Payment - Credit Vouchers</td>
<td>ID Number</td>
<td>RCTA-IdentNo</td>
<td>RCTA-IdentNo</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
</tr>
<tr>
<td>228</td>
<td>Incoming Payments</td>
<td>Invoicing Payment - Credit Vouchers</td>
<td>Telephone</td>
<td>RCTA-Telephone</td>
<td>RCTA-Telephone</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
</tr>
<tr>
<td>229</td>
<td>Cheque Register</td>
<td>Cheque Register</td>
<td>Account Number</td>
<td>GCH-ActNum</td>
<td>GCH-ActNum</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
</tr>
<tr>
<td>230</td>
<td>Cheque Register</td>
<td>Cheque Register</td>
<td>BP Account Name</td>
<td>OCH-CardName</td>
<td>OCH-CardName</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
</tr>
<tr>
<td>231</td>
<td>Marketing Documents</td>
<td>Mktg Docs - Row</td>
<td>Purchase A/P</td>
<td>DOCI-ShtToDesc</td>
<td>DOCI-ShtToDesc</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
</tr>
<tr>
<td>232</td>
<td>Marketing Documents</td>
<td>Mktg Docs - Row</td>
<td>Sales A/R</td>
<td>DOCI-ShtToDesc</td>
<td>DOCI-ShtToDesc</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
</tr>
<tr>
<td>233</td>
<td>Marketing Documents</td>
<td>Mktg Docs - Tax Extension</td>
<td>Purchase A/P</td>
<td>DOCI-ShtToDesc</td>
<td>DOCI-ShtToDesc</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
</tr>
<tr>
<td>234</td>
<td>Marketing Documents</td>
<td>Mktg Docs - Tax Extension</td>
<td>Sales A/R</td>
<td>DOCI-ShtToDesc</td>
<td>DOCI-ShtToDesc</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
</tr>
<tr>
<td>235</td>
<td>Marketing Documents</td>
<td>Mktg Docs - Tax Extension</td>
<td>Purchase A/P</td>
<td>DOCI-ShtToDesc</td>
<td>DOCI-ShtToDesc</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
</tr>
<tr>
<td>236</td>
<td>Marketing Documents</td>
<td>Mktg Docs - Tax Extension</td>
<td>Sales A/R</td>
<td>DOCI-ShtToDesc</td>
<td>DOCI-ShtToDesc</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
</tr>
<tr>
<td>237</td>
<td>Marketing Documents</td>
<td>Mktg Docs - Tax Extension</td>
<td>Purchase A/P</td>
<td>DOCI-ShtToDesc</td>
<td>DOCI-ShtToDesc</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
<td>Personal</td>
</tr>
</tbody>
</table>

© 2018 SAP SE or an SAP affiliate company. All rights reserved. | CUSTOMER
Personal Data Management Authorizations

Feature

- Extension of General Authorizations form to support authorizations for new Data Protection Tools.

Benefits

- Ability to restrict access and set authorizations to sensitive data.
- Ability to restrict access to the various functions under Data Protection Tools.
Personal Data – Change Log Enhancements

Feature
- New GDPR objects supported in the Change Log: Activities, Checks for Payments, Service Contracts.

Benefit
- Logging changes (date, time, owner) to personal data is a critical requirement of GDPR.
- Change log needs to be available everywhere personal data are stored and maintained.
Sensitive Personal Data – Access Log (Germany only)

Feature
- Control by log/record of any access to a special category of personal data – sensitive personal data.
- In the core SAP Business One application it affects the German localization only.
- Values are encrypted in the database.
- Values are hidden by default on User Interface – special authorization and control needed to unhide and display the value.

Benefit
- Selected authorized users can view hidden sensitive personal data values.
Determine Natural Person

Feature
- New function under Personal Data Management Wizard which enables determining users, employees, business partners and contact persons as natural persons.

Benefit
- Helps to apply the natural person determination setting on a range of different data subjects.
- Natural Person setting is essential to use certain functions of Personal Data Tools for GDPR.
Personal Data Report (Driven by a person’s request)

KEY SCENARIO / GDPR REQUIREMENT
- Natural persons are allowed to contact any organization to request details of which personal data the organization stores and processes about them.
- The organization needs to provide a report on this.

Feature
- New option to generate Personal Data Reports for selected natural persons.
- The report gathers personal data from master data and transactions.

Benefits
- Helps to follow up and execute natural person requests to retrieve any personal data which is held by the company.
- Helps the company verify personal data correctness following natural person feedback on personal data reports.
Reverse Natural Person Determination

Feature
- New function under Personal Data Management Wizard to reverse a natural person determination in case of user mistakes

Benefit
- Helps to reverse the natural person determination on a range of data subjects
Personal Data Cleanup – Irreversible Erasure of Personal Data

Feature
- New and very important Personal Data function under Personal Data Management Wizard to erase all personal data (by setup in Personal Data Management) of selected natural persons from master data and transactions.
- Erased data on all affected master data and transactions will be replaced with asterisks.
- Status of natural person whose personal data was erased will change to Erased.
- This action is irreversible and must be taken after proper consideration and checking that all data retention periods are over and there is no legal obligation to hold the data of natural person.

Benefit
- Helps to follow up and execute natural person requests to remove and erase personal data after legal periods to hold data have finished and there is no reason to block the data.
Other Important Rules in SAP Business One

**Drafts:** AR or AP documents and AR or AP document drafts share the same setup. Data stored in drafts can be reported but cannot be automatically / massively erased. The company needs to drop the drafts.

**Credit Card Number:** From 9.3 PL02, full credit card number storage and display is no longer allowed.

**Personal Data Report:** System groups the personal data in transactions by the content of personal data. When ship to address is the same in all the transactions, the personal data will be displayed only once and not separately for each transaction.

**Personal Data Cleanup:** In SAP Business One, documents need to be closed to execute cleanup.

After deleting personal data of data subject, the master data of the data subject cannot be used anymore for creating new transactions.

Assuming the company finalizes the financial/accounting processes within e.g. 2 years, it is recommended running personal data cleanup for business partners which are determined as natural persons, using the selection criteria “No transactions Since”. By this selection criteria non active natural BPs can be identified and the company can decide whether to have a cleanup process or not.

**Target Group in Campaign:** Lines need to be dropped manually. It is strongly recommended to drop on regular basis the campaign lines which refer to external BPs when there is no explicit consent from the data subject.

**Sales Opportunities:** Can go through personal data cleanup or can be dropped instead.

**Attachments:** In 9.3 PL04 not supported under Personal Protection Tools.
Executive Summary
Delivers functionality that helps customers to comply with GDPR Data Privacy regulations (effective May 25, 2018)

Available by design
- General Authorizations
- Data Ownership tools
- System Access log
- Change logs to various forms/screens
- Manual and selective erasure of certain personal data
- HANA Enterprise Search function to report all occurrences of natural person data (supported for SAP HANA version only)
- Data Archiving (not supported for SAP HANA version)

GDPR Relevant Data
- Any object storing personal data is relevant for the EU GDPR
- Business Partners:
  - Contact persons
  - Sales Employees and Buyers
  - End consumer customers (natural persons)
- Employees and Users
- Business Documents:
  - Activities, services, opportunities
  - Marketing documents
  - Blanket agreements / Project management

How to Manage Personal Data in SAP Business One*
- Data Privacy Tools
  - Personal Data Setup
  - Personal Data Management Wizard (Report, Data Erasure and Data Encryption / Decryption for sensitive personal data)
  - Sensitive Personal Data Access Log**
- Enhanced Change log to personal data related fields and objects

* Enhancements released with SAP Business One 9.3 PL04.
** Supported for Germany only
GDPR at SAP Business One (1/2)

**General Authorizations:** Authorizations allow users to view, create, and update documents and master data of business partners that you assign to them, according to data ownership definitions. By default, a new user has no authorizations. Each user can have only one manager who assigns permissions.

**Data Ownership:** Data ownership allows the company to have control over certain data elements. With the data owner function, user can define the rightful owner of data and information. Therefore, selected company's data can be secured and protected by the pre defined authorization. Information and data can be accessed by permitted roles and users only.

**Data Archiving:** Companies who have worked with SAP Business One for over two years can use the data archive wizard to archive closed transactional data relating to previous financial periods that have been closed. Closed transactional data can be closed sales and purchasing documents, reconciled journal entries, etc. Remark: this option is not supported for SAP HANA version.

**System Access Log:** SAP Business One allow users with special authorization to scan and review details about logs to the application such as which users logged into the system and when this action happened.

**Change Log:** Allowing users with assigned authorizations to check details about changes in certain fields i.e. when the change was made, storing original and updated values.

**Manual erasure of personal data:** Users are allowed to manually erase certain personal data unless these serve as primary keys and are used and interconnected with other objects. It is the user’s responsibility to ensure that erasure of certain personal data is not in conflict with any regulations.

**HANA Enterprise Search:** Enterprise search enables the user to search certain fields and their values of the business objects in SAP Business One, version for SAP HANA that have been stored in the SAP HANA database server.
**Personal Data Setup:** Centralized place to categorize which data is personal. There are certain predefined objects which are by their nature related to natural persons. Users may perform certain customizations and extend this setting. Customized user-defined fields in the predefined objects can also be marked by users as personal.

Sensitive personal data stored in core application fields are predefined without possibility to extend to additional fields. Sensitive personal data is accessible by authorized users only.**

**Access Log to Sensitive Personal Data:** Tracking and logging controls to record read-access by a user to specific predefined sensitive personal data.

**Personal Data Management Wizard:** Includes a report which lists all records of personal related fields in a structured form. Possibility to query certain natural person and all occurrences and data stored about this natural person.

To support “right to be forgotten”, authorized users, based on their judgement, are able to erase selected personal data, provided this action is not in conflict with other legislation.

**Extending Change Log to additional forms:** Extending functions allowing users with assigned authorizations to check details about changes in fields stored in various objects/forms.

** Supported for Germany only**