# European Union's General Data Protection Regulation (EU GDPR) and SAP Business One
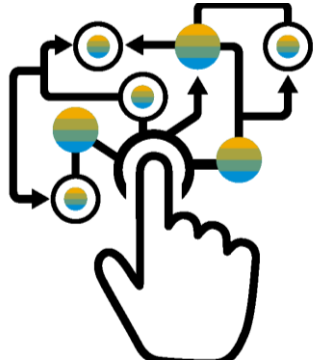## Executive Summary

May 2018

THE BEST RUN **SAP**

# 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.**

# 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
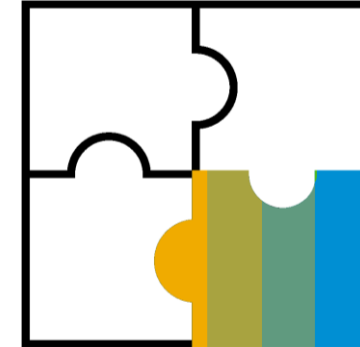
## How to Manage Personal Data in SAP Business One*

- 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 predefined 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.

# GDPR at SAP Business One (2/2)

**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*

Follow all of SAP

THE BEST RUN SAP