Towards *General Data Protection Regulation* Compliance with SAP Business One.

Peter Dominik & Shula Ben Dosa, SAP Business One Product Management, SAP
27th March 2018

EXTERNAL

SAP Run Simple

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.

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

Agenda

1. GDPR – Regulation & Key Terms

§ Scope, relevancy, due 25th May 2018

2. What is available with SAP Business One

§ Authorizations, Data Ownership, Change Logs, Access Log

3. What is to come 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 (Germany only)

§ Live demo

4. Summary + Q&A’s

§ GDPR/DPP Sessions at SMB Innovation Summits in Barcelona and Orlando

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR), EU Regulation 2016/679, effective 25th May 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

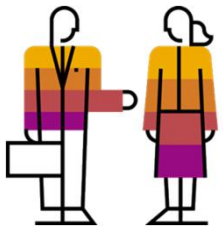
© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

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.

Data Subjects



Natural persons e.g. retail customers, internal employees, contact persons etc.

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
- …

?

Data Controller

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

Data Processor

Your business software

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

Acquisition → Opportunity → Order/ Contract → Execution → Invoicing

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

GDPR at a Glance

Demonstration of compliance

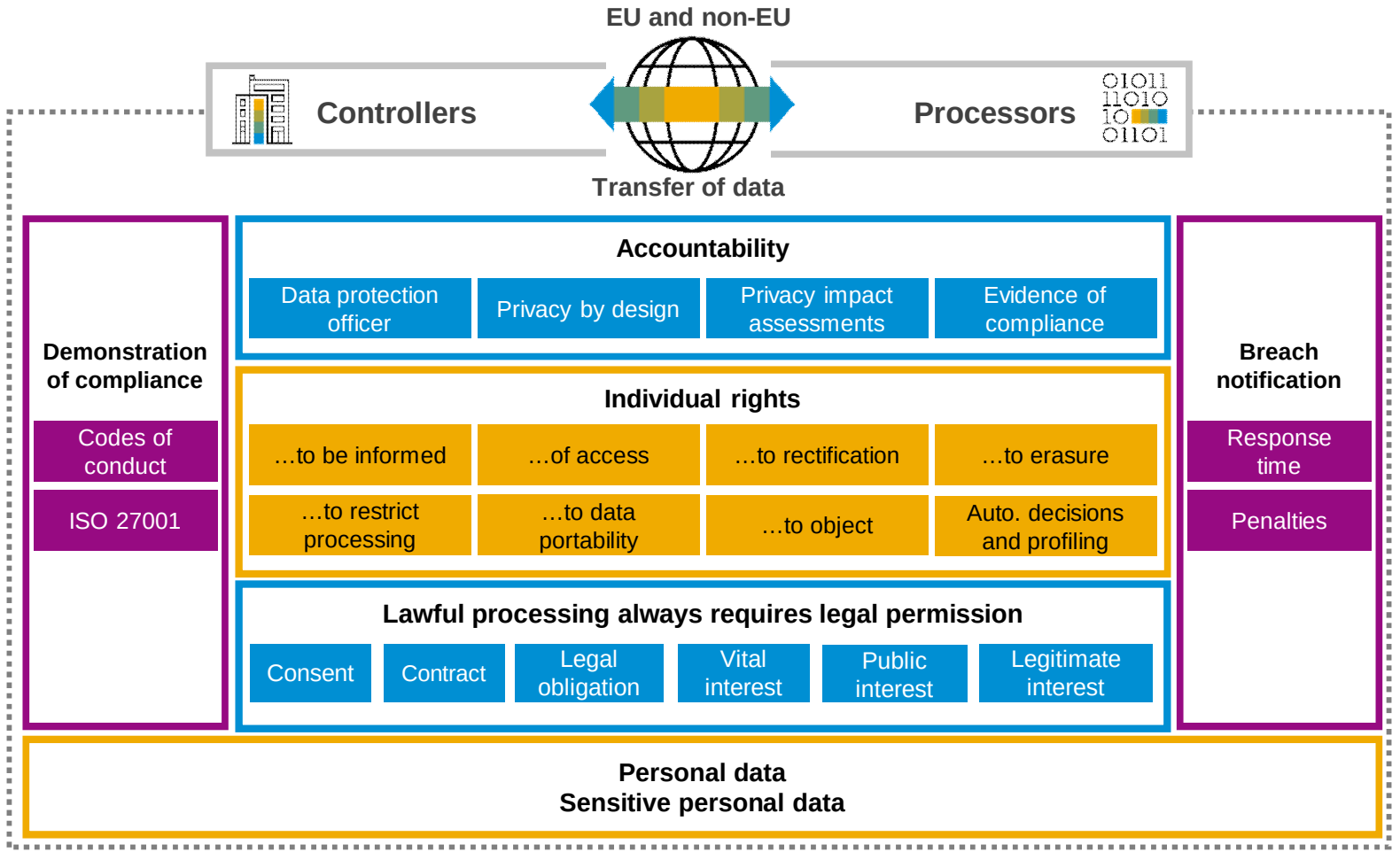
- Compliance and accountability are integral to a data protection program.
- Codes of conduct and policies can help ensure accountability.

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

- 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

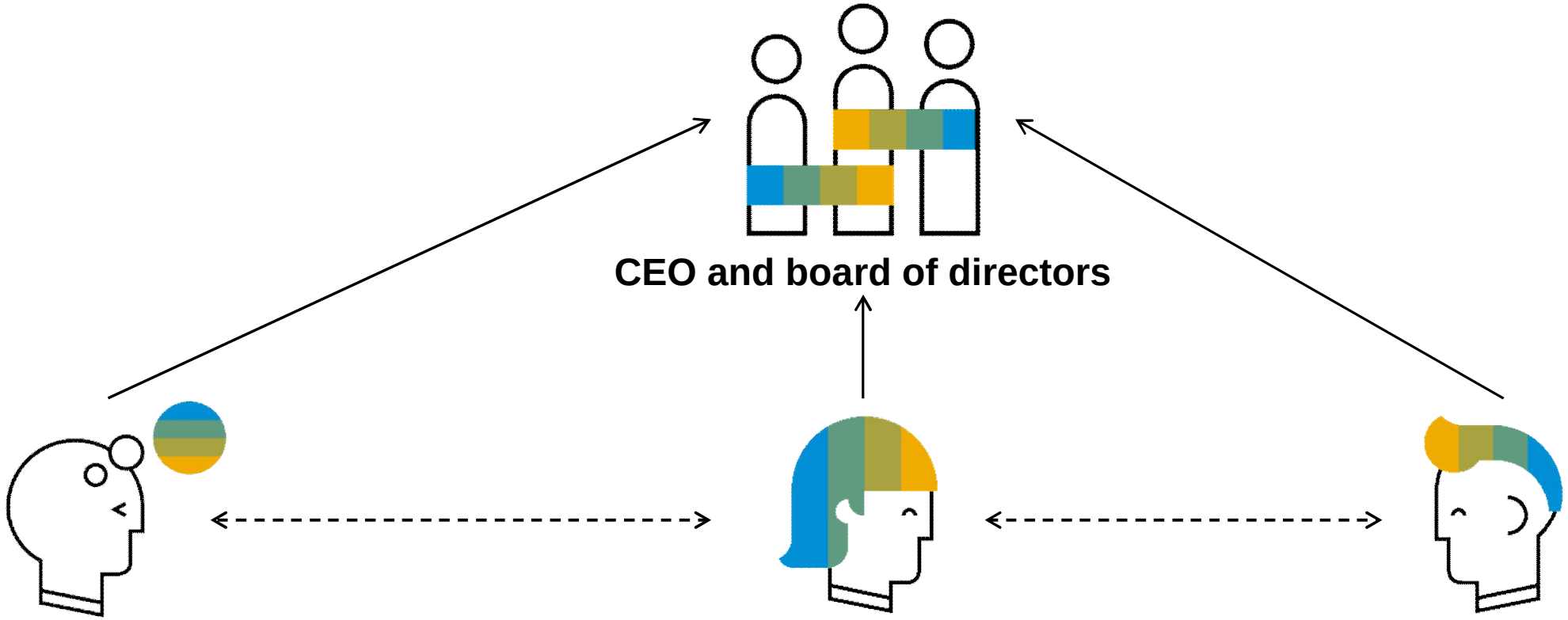
- Mandatory notification to authority within 72 hours of becoming aware of breach
- Communication to affected individuals without undue delay
- Maximum fine can apply

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.

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

Who is involved?



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

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

GDPR and SAP Business One

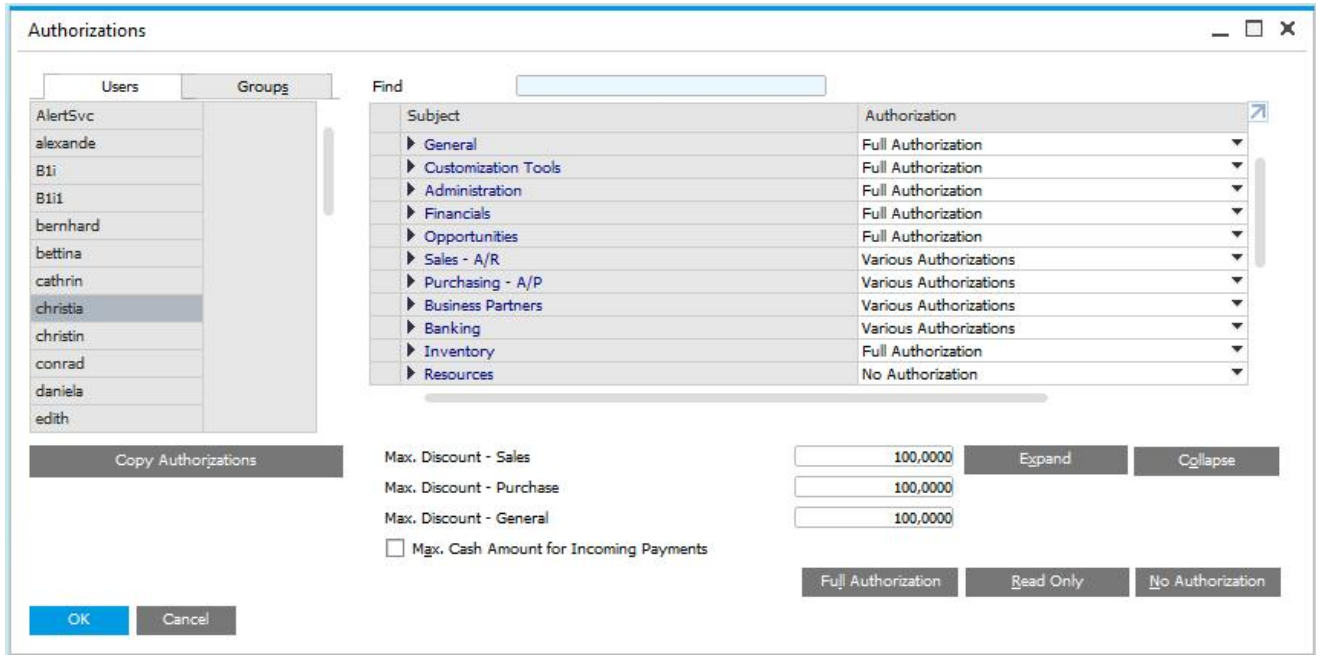
Glossary – Good to Know Key Terms

- **GDPR** – General Data Protection Regulation adopted by the European Union due on May 25th, 2018.
- **Natural Person** – A real human being (as distinguished from a corporation, machine or robot).
- **Personal Data** – Any data that can identify a natural person (name, date of birth, address, car license plate).
- **Sensitive Personal Data** – Special category of data with stronger protection and special rules required (religion/confession, social security number, blood type).
- **Data Subject** – A natural person for whom the system stores personal data.
- **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.

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

Available GDPR / DPP Functions in SAP Business One

Authorizations



Feature

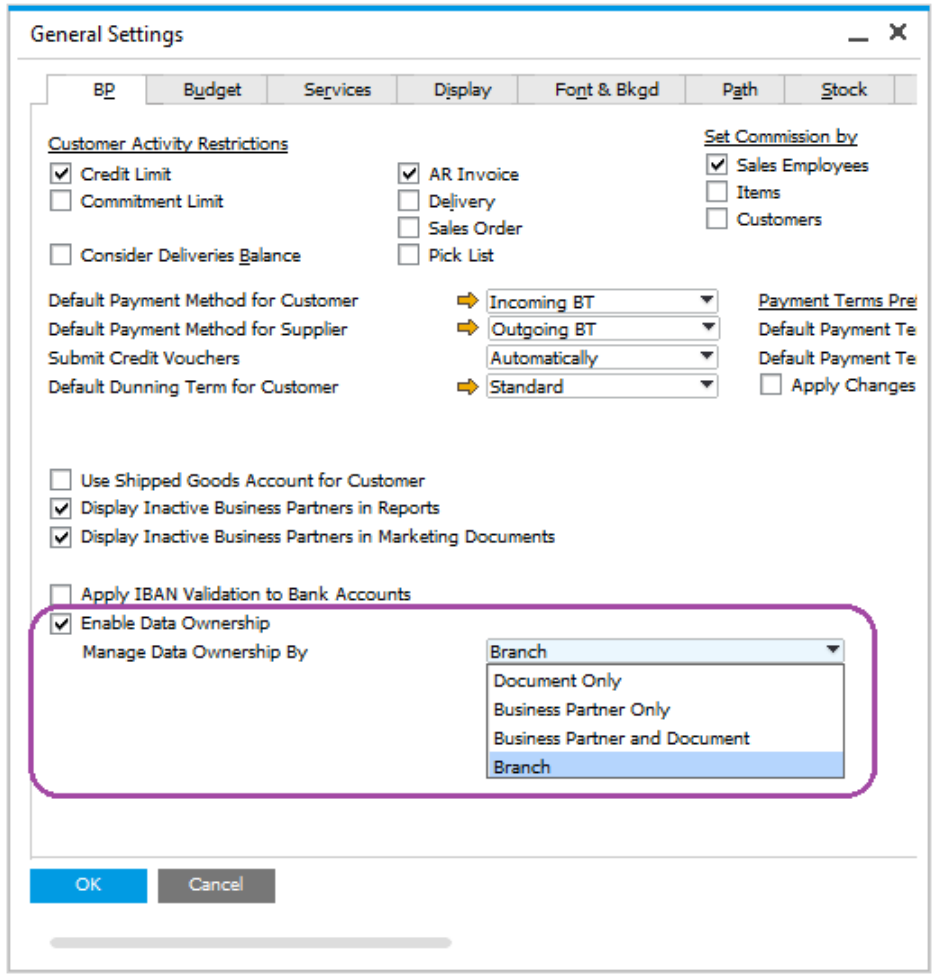
- Authorizations allow users to view, create, and update documents that you assign to them, according to data ownership definitions.
- By default, a new user has no authorizations. Each user can have only one manager who assigns permissions. You can define users as either regular users or superusers.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

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

Data Ownership (1/3)



Feature

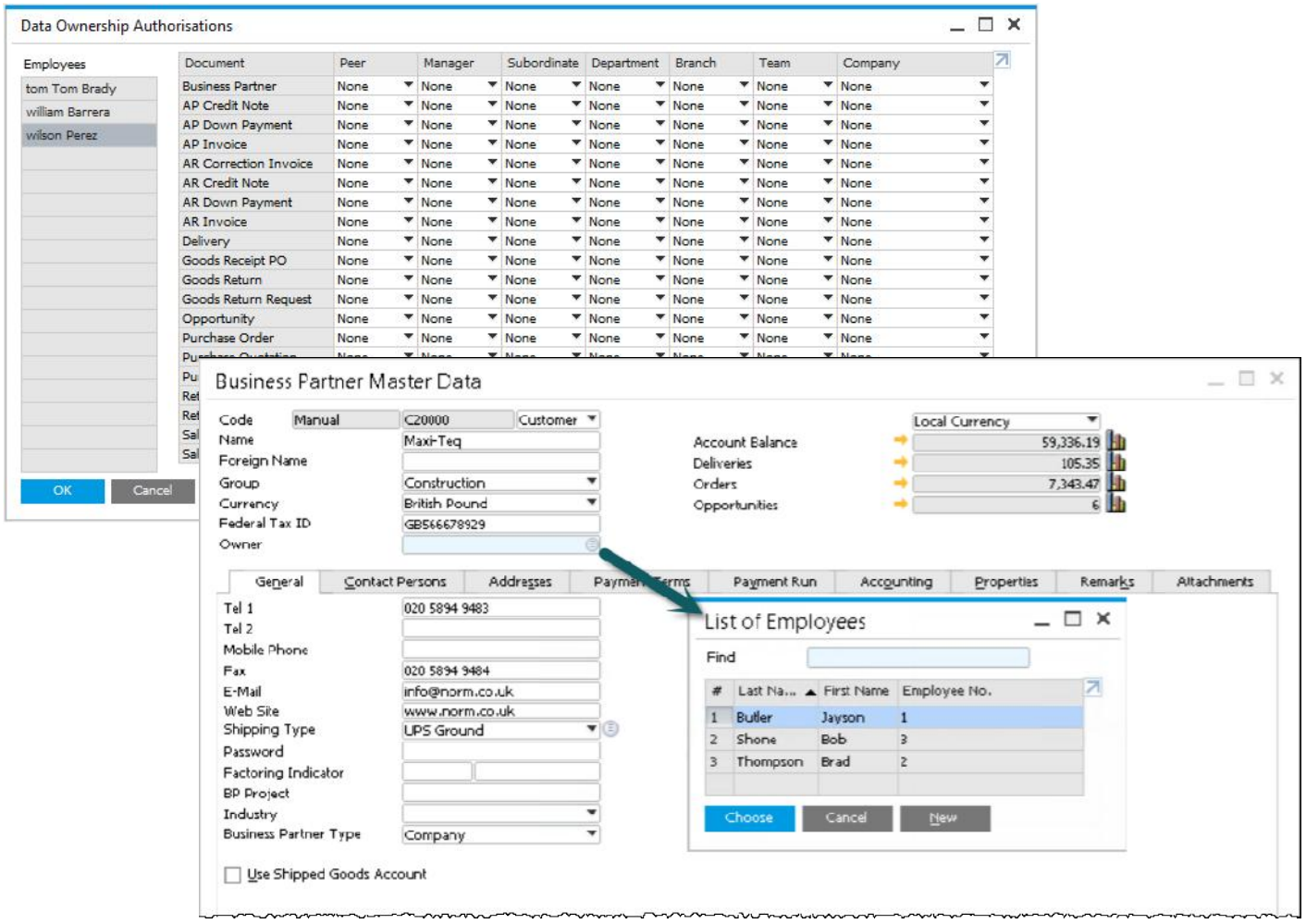
- Data ownership allows the company to have control over data elements. With the data owner function, you can define the rightful owner of data and information.
- Therefore, your company's data can be secured and protected by the predefined authorization. Information and data can be accessed by permitted 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.

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

Data Ownership (2/3)

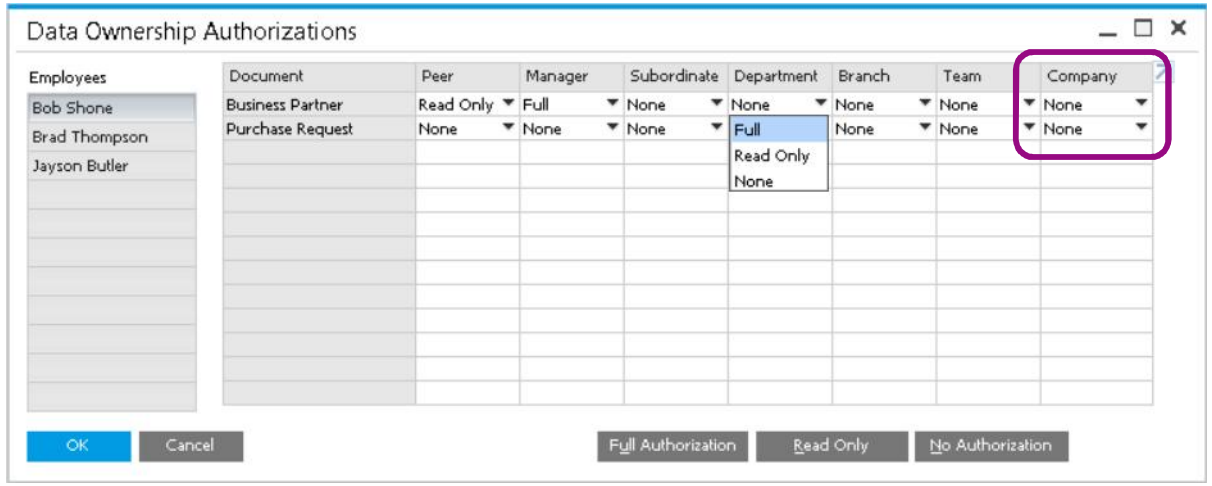


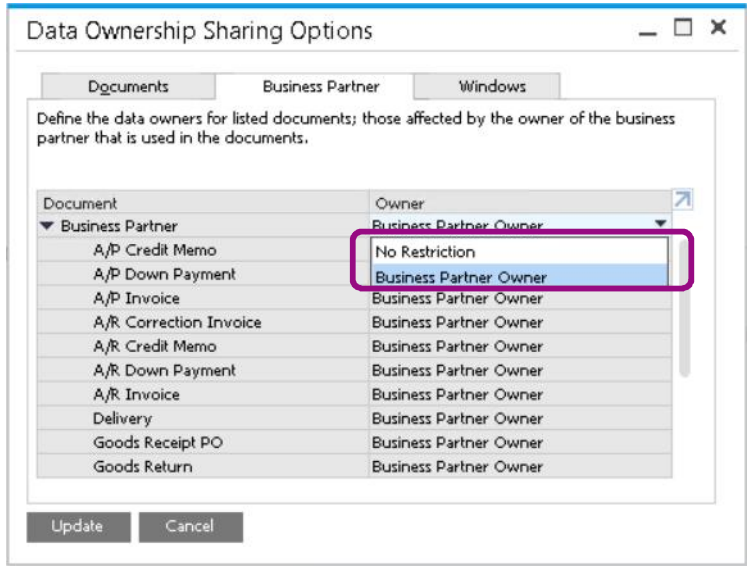
Feature

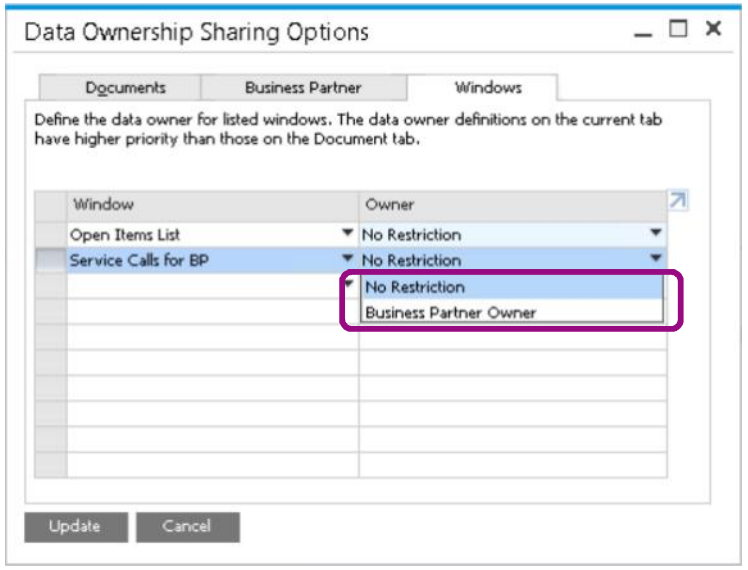
- Data ownership management extended to business partners with SAP Business One 9.2.
- Restrict access and visibility of:
  - Business Partner Master Data
  - Documents using Business partner with owners
- Manage data ownership by:
  - Documents Only:
    - Permissions are defined per document.
  - Business 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.

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

Data Ownership (3/3)







Feature

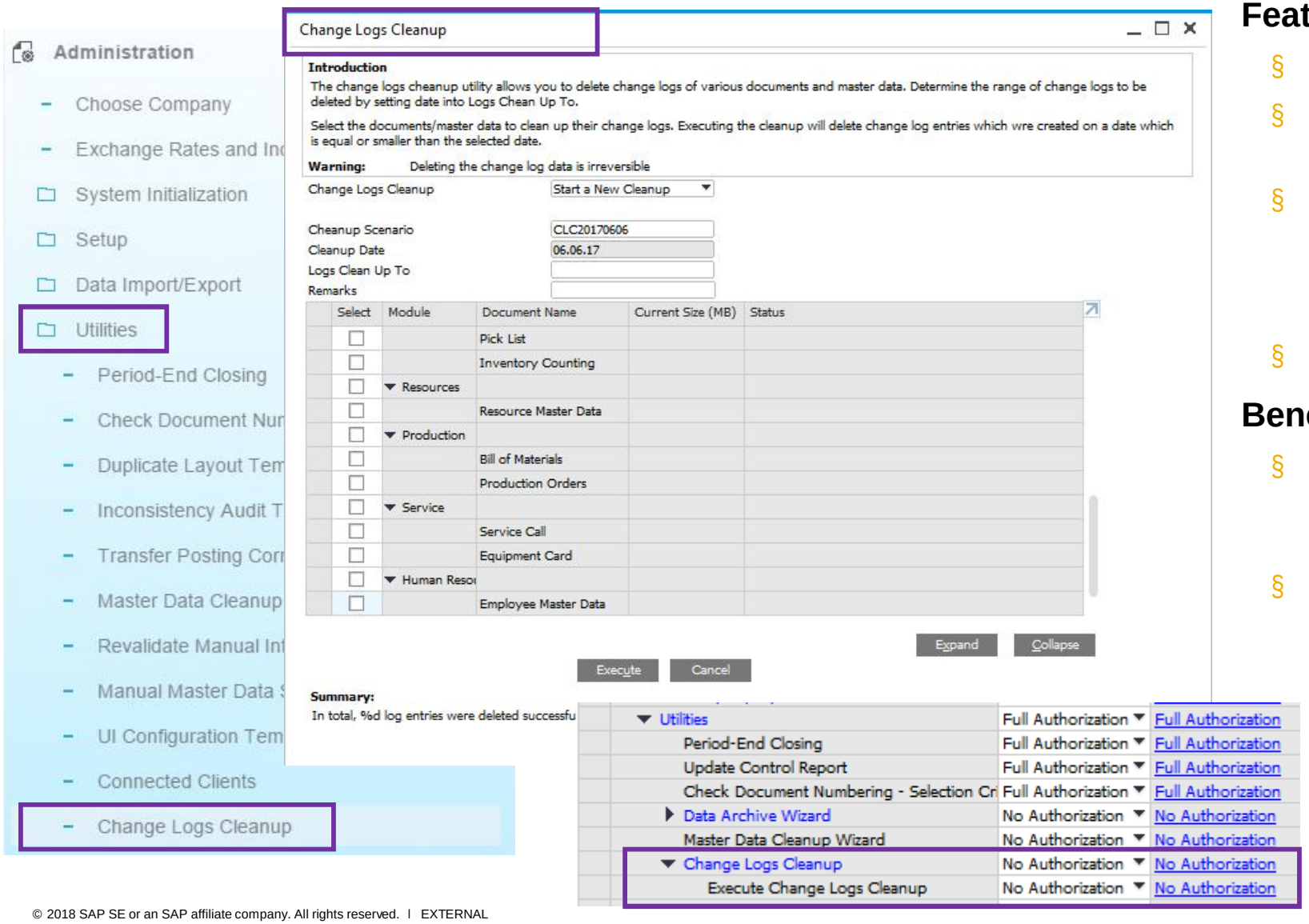
- Bypass Data Ownership by granting access at Company level.
- Restrict system reports like Open Items List to reflect only results against specific Business Partners for specific users.
- Exclude specific restrictions and enable read access.

Benefits

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

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

Change Log Cleanup Utility



Feature

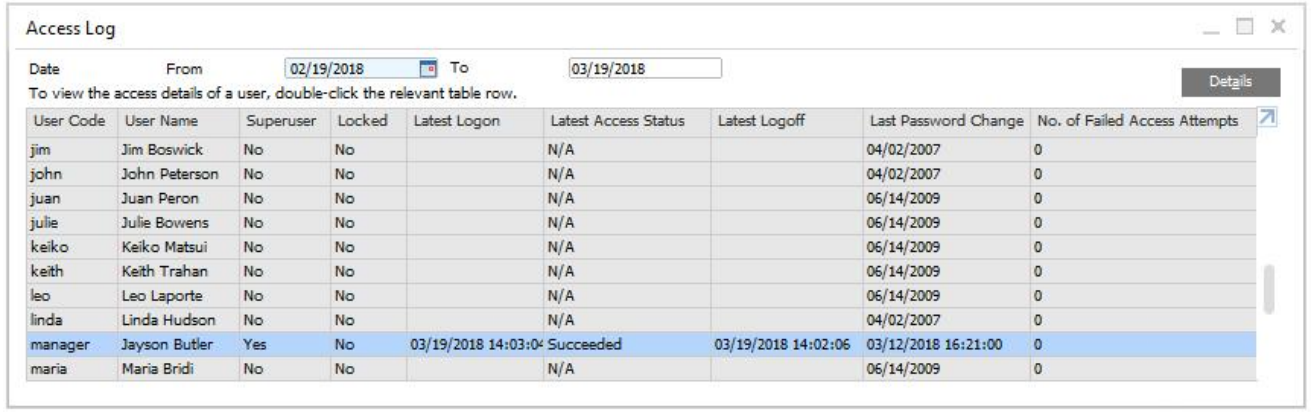
- New Change Log Cleanup Utility available.
- Enables users to cleanup the change log to reduce the size of a company database.
- Users have the ability to determine which objects from the change log entries should be deleted and restrict the deletion to a specific date range.
- Utility subject to appropriate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

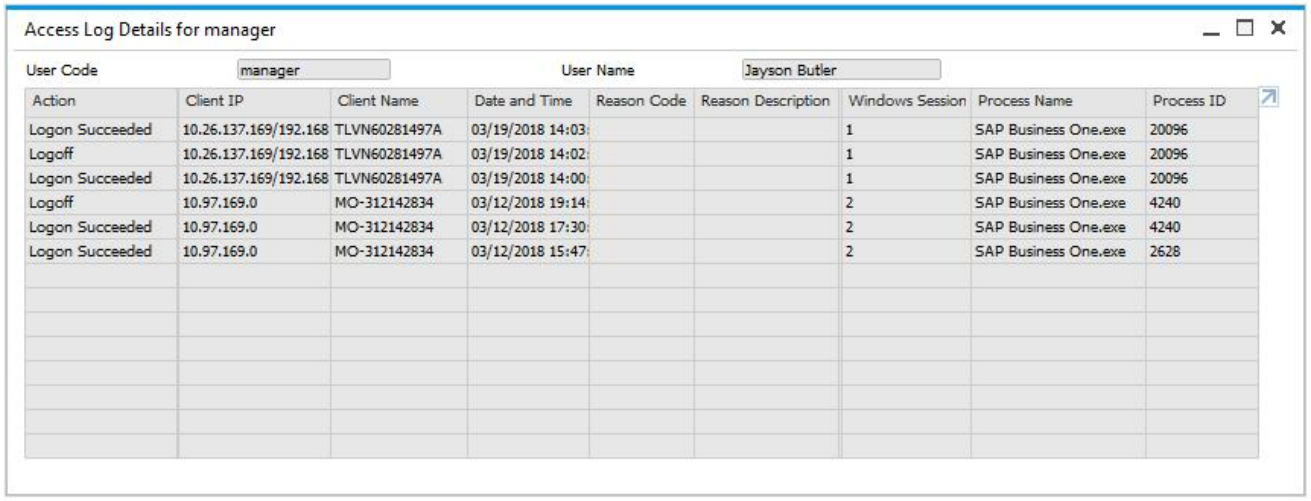
Benefits

- 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.

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

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

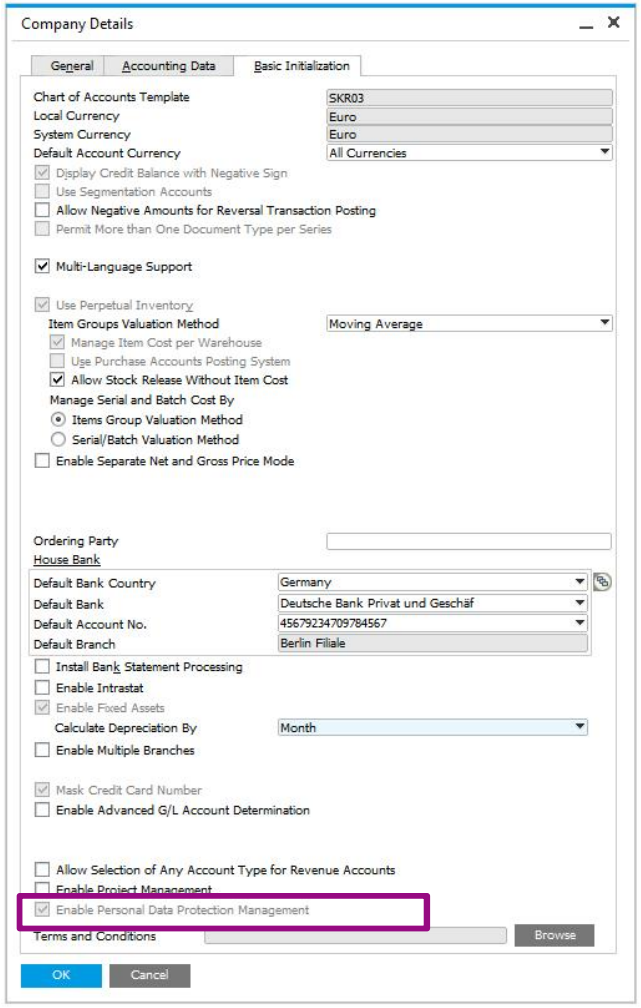
Benefits

- 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.

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

GDPR / DPP Enhancements for
SAP Business One – Demo

DPP Initialization Function – New with SAP Business One 9.3 PL04



Feature

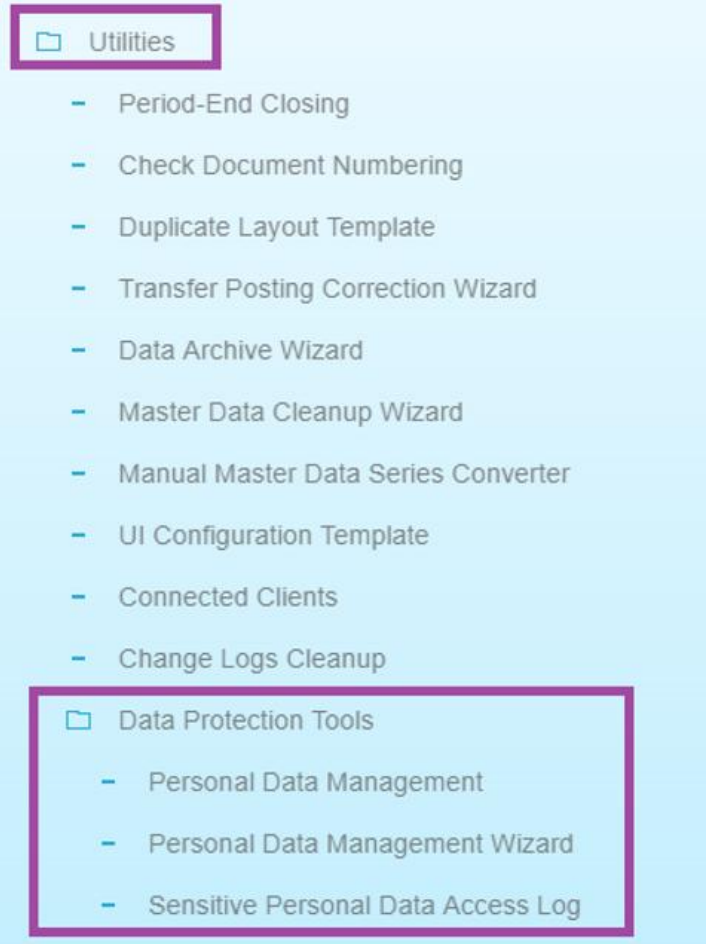
- Initialization setting on Company Details form to activate all new Data Privacy and Protection enhancements in SAP Business one.
- Automatically activated for all localizations for EU countries, Norway and Switzerland after upgrade to 9.3 PL04. It can be turned off (not recommended) before any natural 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.

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

Data Protection Tools – Main Menu Entry



Feature

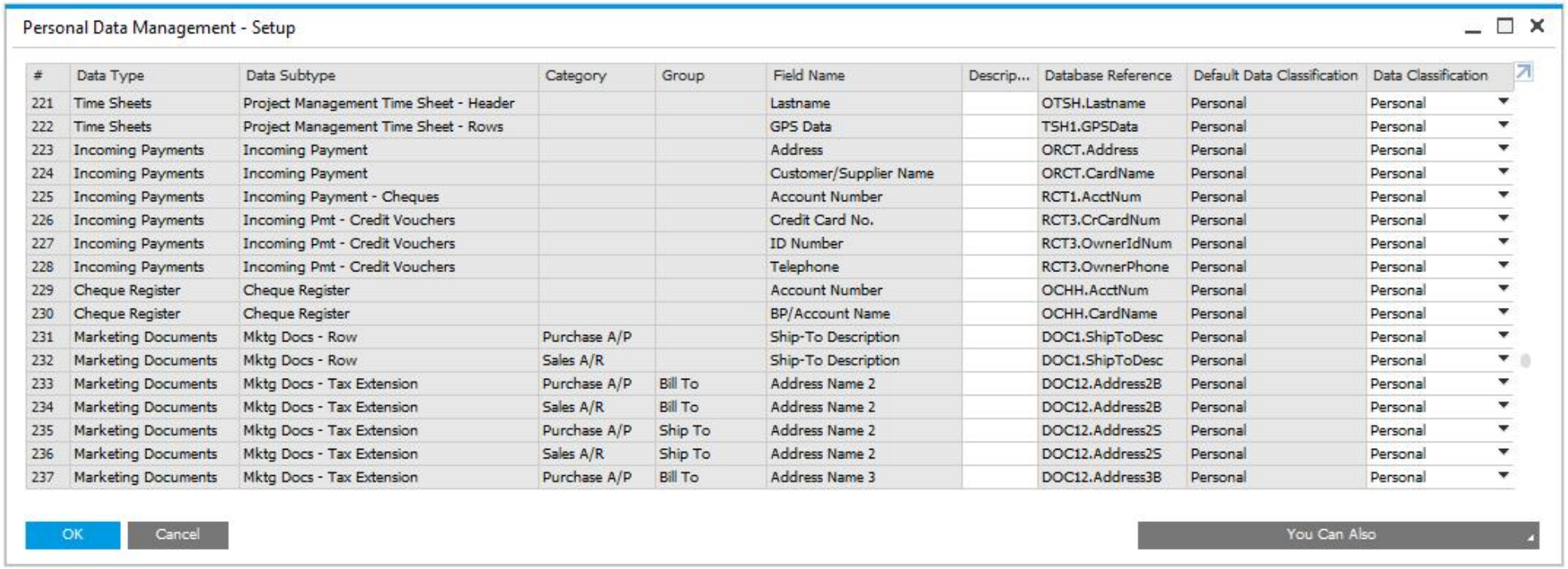
- Data Protection Tools are managed under Administration/Utilities.

Benefit

- Centralized location for managing personal data protection.

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

Personal Data Management Setup



#	Data Type	Data Subtype	Category	Group	Field Name	Descrip...	Database Reference	Default Data Classification	Data Classification
221	Time Sheets	Project Management Time Sheet - Header			Lastname		OTSH.Lastname	Personal	Personal
222	Time Sheets	Project Management Time Sheet - Rows			GPS Data		TSH1.GPSData	Personal	Personal
223	Incoming Payments	Incoming Payment			Address		ORCT.Address	Personal	Personal
224	Incoming Payments	Incoming Payment			Customer/Supplier Name		ORCT.CardName	Personal	Personal
225	Incoming Payments	Incoming Payment - Cheques			Account Number		RCT1.AcctNum	Personal	Personal
226	Incoming Payments	Incoming Pmt - Credit Vouchers			Credit Card No.		RCT3.CrCardNum	Personal	Personal
227	Incoming Payments	Incoming Pmt - Credit Vouchers			ID Number		RCT3.OwnerIdNum	Personal	Personal
228	Incoming Payments	Incoming Pmt - Credit Vouchers			Telephone		RCT3.OwnerPhone	Personal	Personal
229	Cheque Register	Cheque Register			Account Number		OCHH.AcctNum	Personal	Personal
230	Cheque Register	Cheque Register			BP/Account Name		OCHH.CardName	Personal	Personal
231	Marketing Documents	Mktg Docs - Row	Purchase A/P		Ship-To Description		DOC1.ShipToDesc	Personal	Personal
232	Marketing Documents	Mktg Docs - Row	Sales A/R		Ship-To Description		DOC1.ShipToDesc	Personal	Personal
233	Marketing Documents	Mktg Docs - Tax Extension	Purchase A/P	Bill To	Address Name 2		DOC12.Address2B	Personal	Personal
234	Marketing Documents	Mktg Docs - Tax Extension	Sales A/R	Bill To	Address Name 2		DOC12.Address2B	Personal	Personal
235	Marketing Documents	Mktg Docs - Tax Extension	Purchase A/P	Ship To	Address Name 2		DOC12.Address2S	Personal	Personal
236	Marketing Documents	Mktg Docs - Tax Extension	Sales A/R	Ship To	Address Name 2		DOC12.Address2S	Personal	Personal
237	Marketing Documents	Mktg Docs - Tax Extension	Purchase A/P	Bill To	Address Name 3		DOC12.Address3B	Personal	Personal

Feature

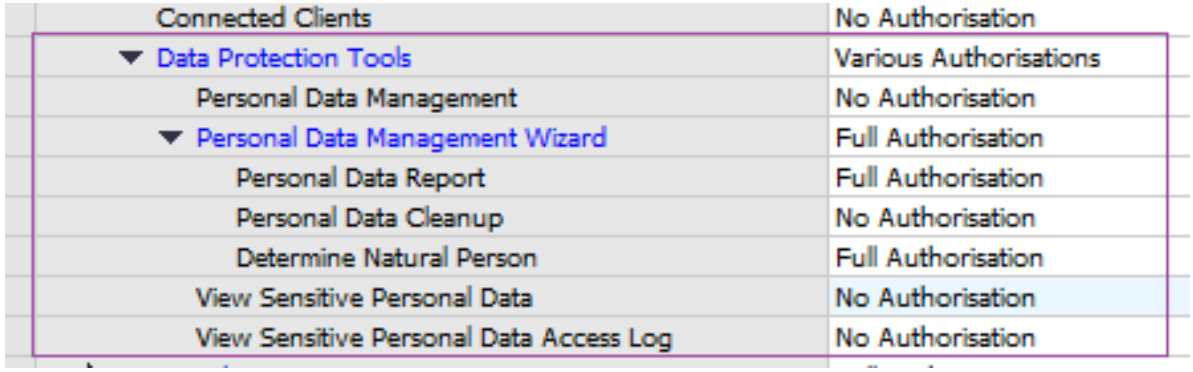
- New control to define and categorize personal Data.
- User Defined Fields in GDPR objects can be determined as personal data.
- New entry under Data Protection Tools.

Benefits

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

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

Personal Data Management Authorizations



Connected Clients	No Authorisation
Data Protection Tools	Various Authorisations
Personal Data Management	No Authorisation
Personal Data Management Wizard	Full Authorisation
Personal Data Report	Full Authorisation
Personal Data Cleanup	No Authorisation
Determine Natural Person	Full Authorisation
View Sensitive Personal Data	No Authorisation
View Sensitive Personal Data Access Log	No Authorisation

Feature

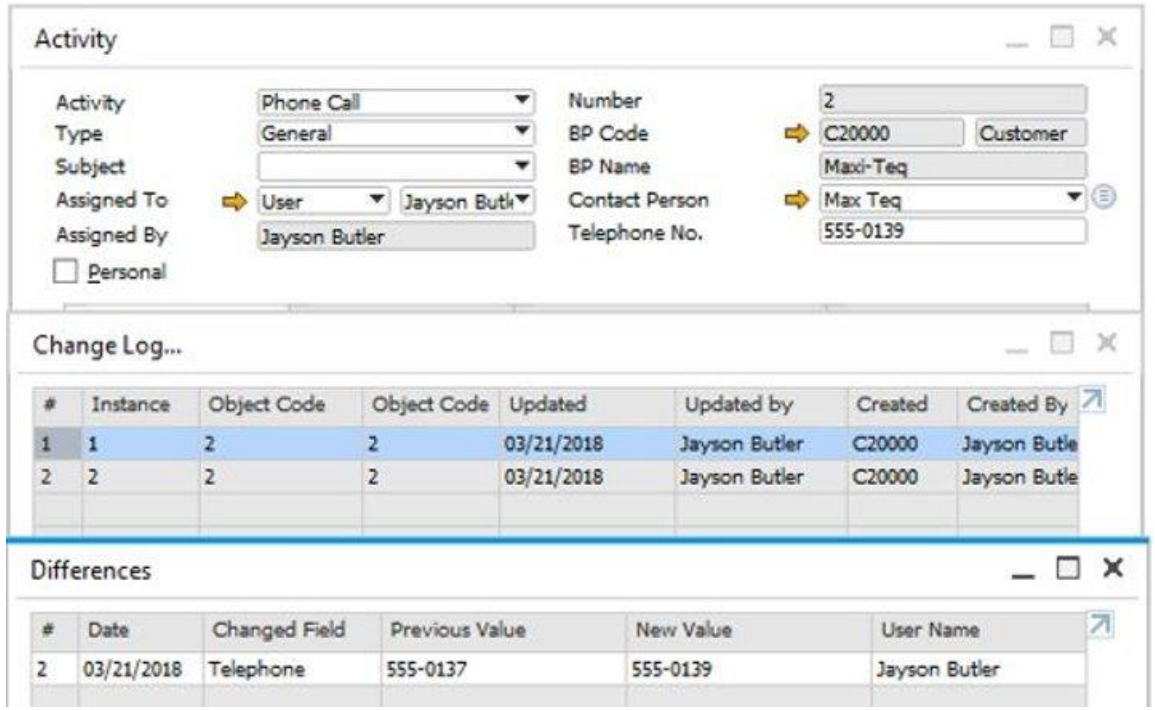
- Extension of General Authorizations form to support authorizations for new Data Protection Tools.

Benefits

- Ability to restrict access and set authorizations to sensitive data.
- Ability to restrict access to the various functions under Data Protection Tools.

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

Personal Data – Change Log Enhancements



Feature

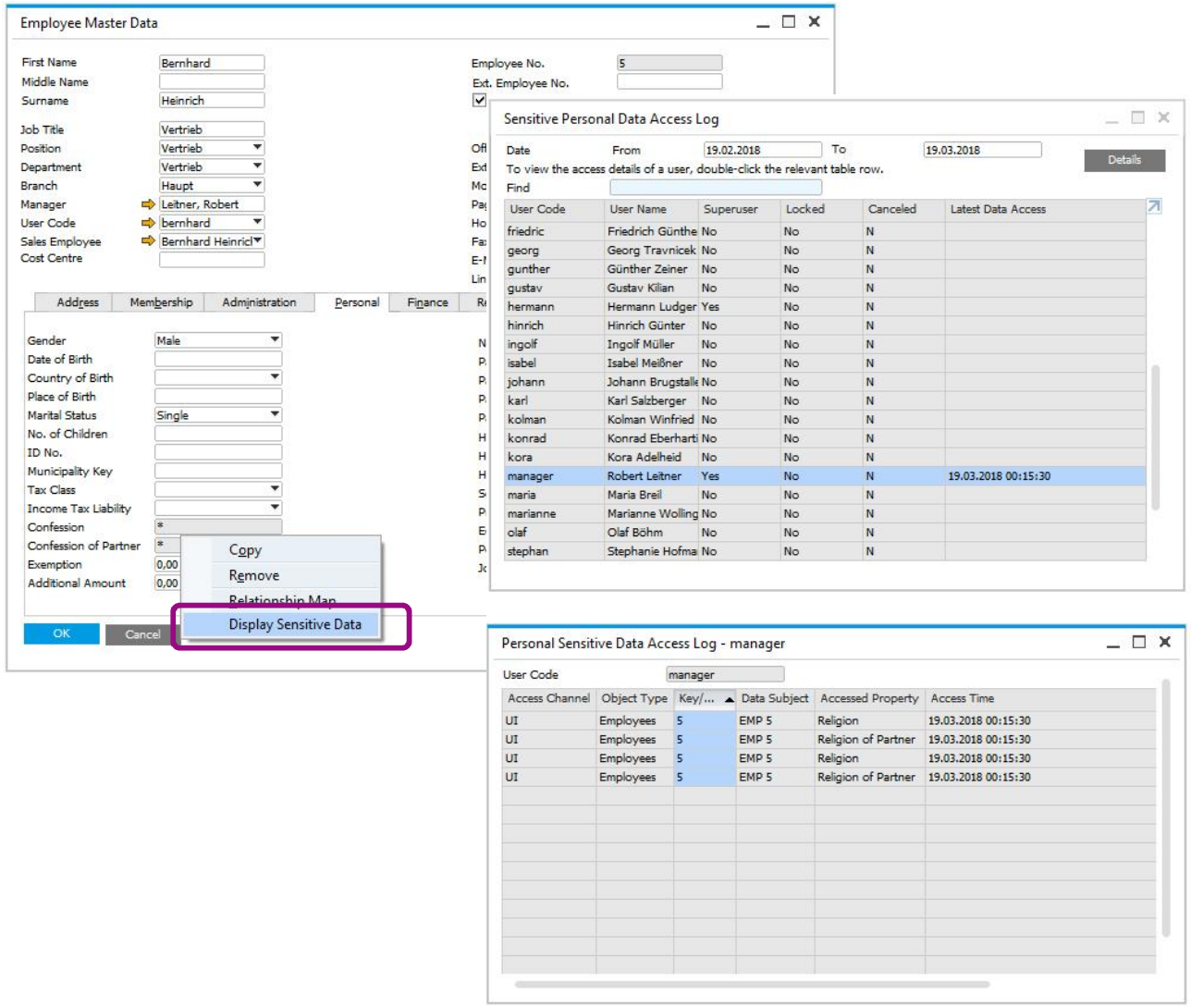
- New objects supported in the Change Log: **Activities, Checks for Payments, Service Contacts**.

Benefit

- Logging changes (date, time, owner) to personal data is a critical requirement of GDPR.

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

Sensitive Personal Data – Access Log (Germany only)



Feature

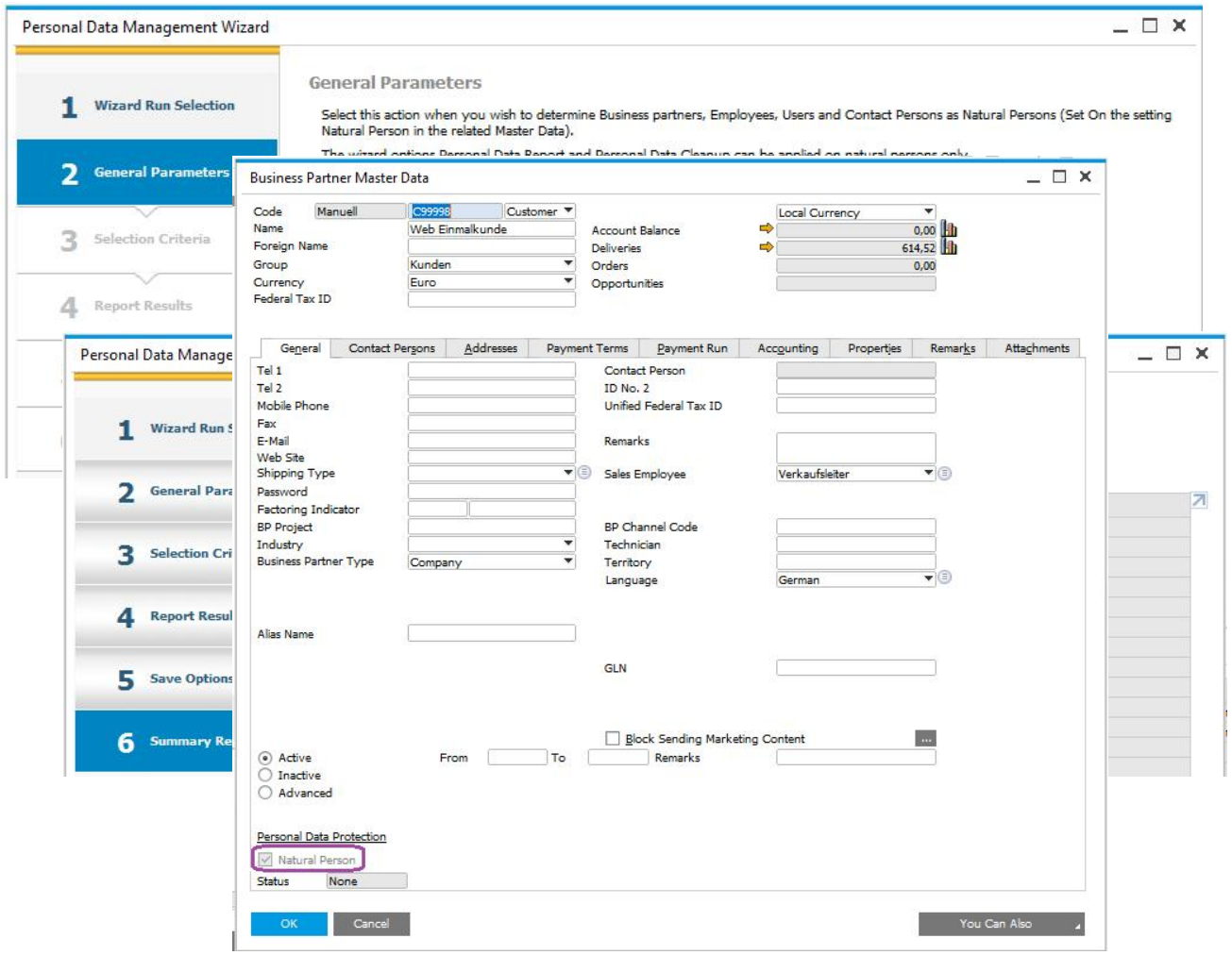
- Control by log/record of any access to a special category of personal data – sensitive personal data.
- In the core SAP Business One application it affects the Germany localization only.
- Values are encrypted in the database.
- Values are hidden by default on User Interface – special authorization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

Benefit

- Selected authorized users can view hidden sensitive personal data values.

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

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

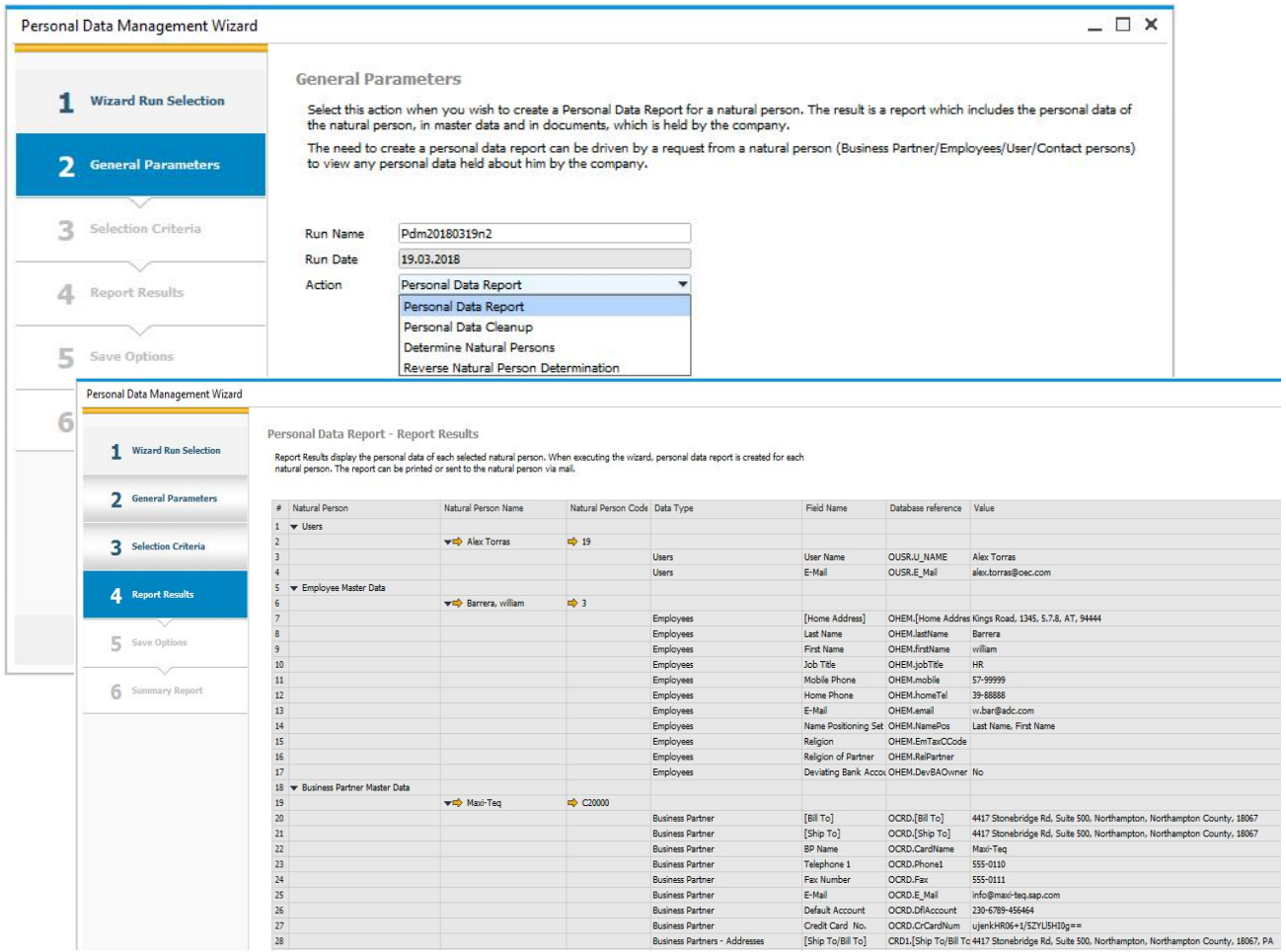
- Helps to apply the natural person determination setting on a range of different data subjects.
- Natural Person setting is essential to use certain functions of Personal Data Tools for GDPR.

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

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

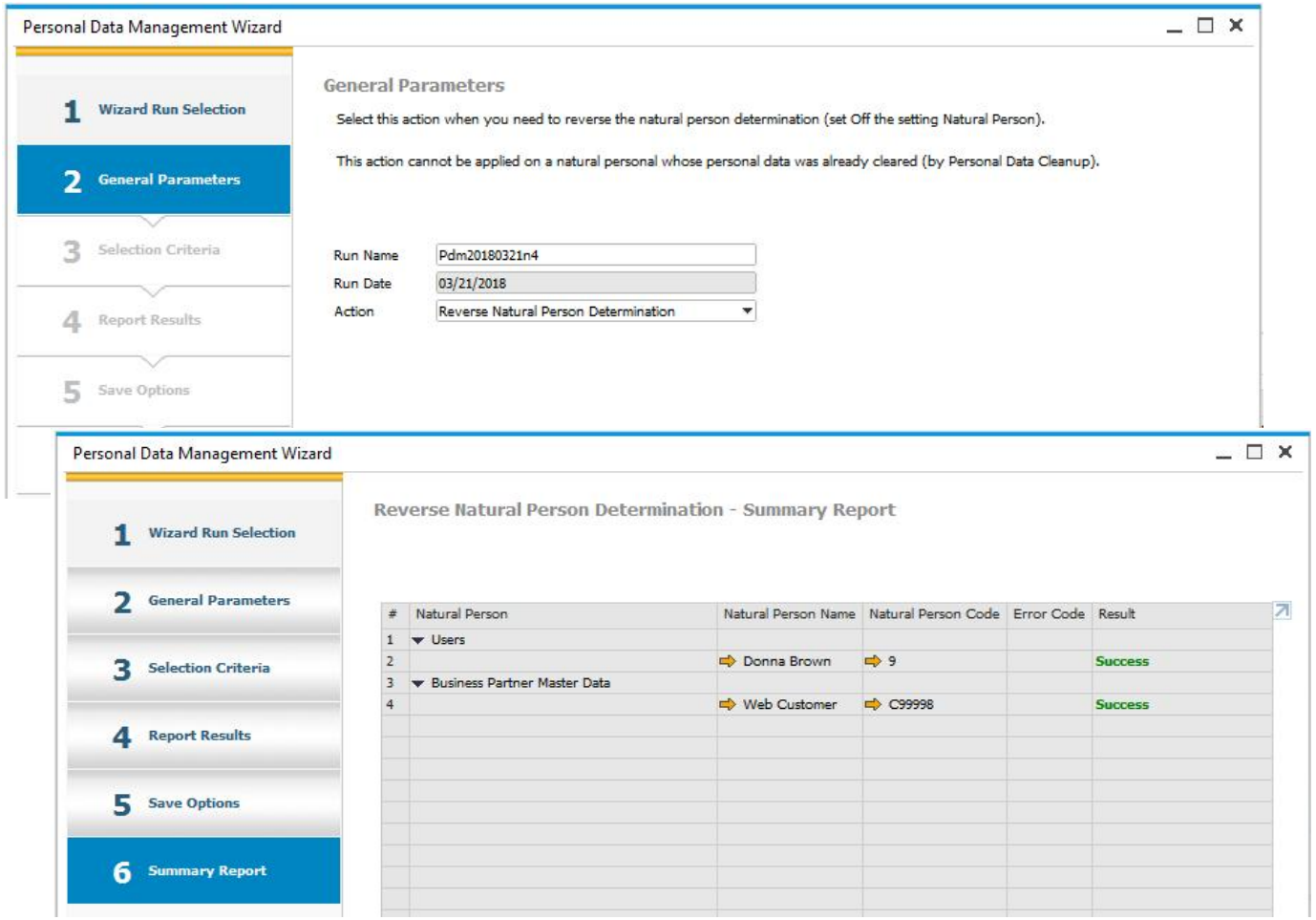
- New option to generate Personal Data Reports for selected natural persons.
- The report gathers personal data from master data and transactions.

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.

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

Reverse Natural Person Determination



Feature

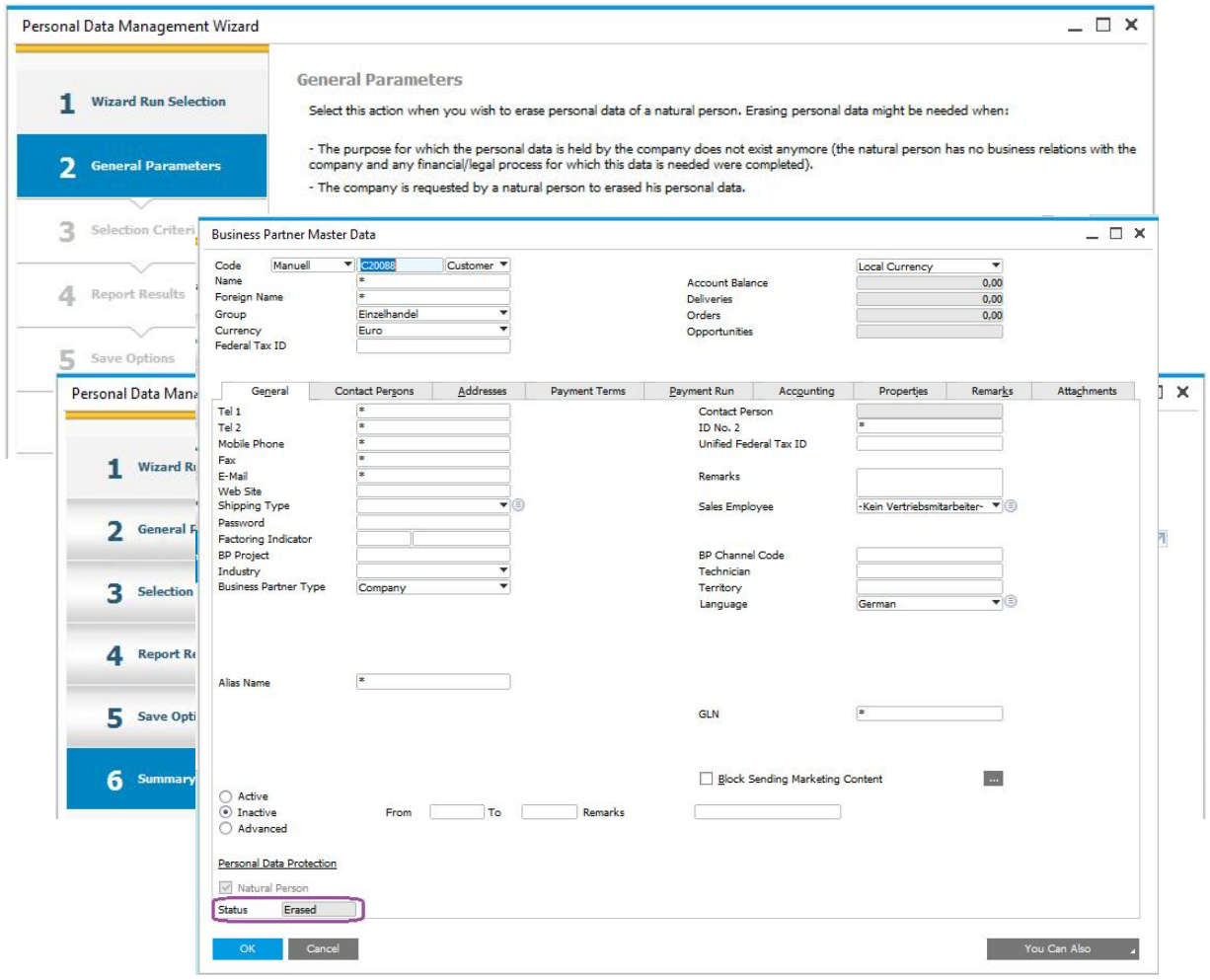
- New function under Personal Data Management Wizard to reverse a natural person determination in case of user mistakes

Benefit

- Helps to reverse the natural person determination on a range of data subjects

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

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.

© 2018 SAP SE or an SAP affiliate company. All rights reserved. I EXTERNAL

Summary + Q&A’s

GDPR at SAP Business One 9.3 PL04

Thank you.

Contact information:

Peter Dominik and Shula Ben Dosa
SAP Business One Product Management, SAP

peter.dominik@sap.com
shula.ben.dosa@sap.com

Run Simple