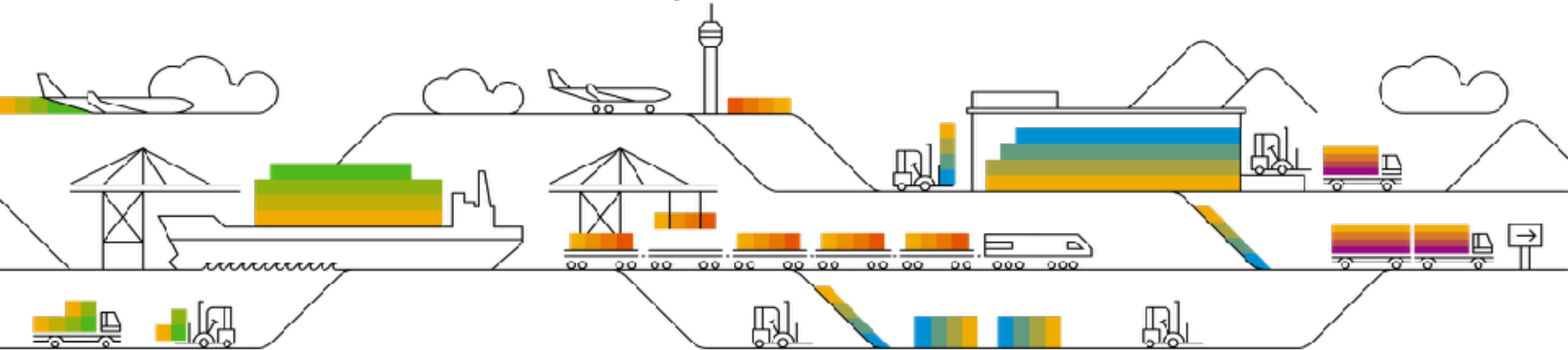


# Executive Summary

## European Union's General Data Protection Regulation (EU GDPR)

In Deutschland: Datenschutz-Grundverordnung (DSGVO).



# 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.**

Im April 2016 verabschiedete die Europäische Union (EU) ein neu harmonisiertes Datenschutzgesetz, die European Union's General Data Protection Regulation.

Ab dem 25. Mai 2018 soll die GDPR in allen Mitgliedstaaten der EU und des Europäischen Wirtschaftsraums (EWR) als unmittelbar anwendbares Recht gelten. Die GDPR führt zwar nicht viele wesentliche neue Konzepte ein, erhöht jedoch die Anforderungen an die Verarbeitung personenbezogener Daten in Bereichen wie:

1. Unterstützung der Löschung personenbezogener Daten (sog. "Recht auf Vergessenwerden")
2. Änderungen an persönlichen Daten protokollieren
3. Lesezugriff auf vertrauliche persönliche Daten protokollieren
4. Bereitstellung von Berichten oder Anzeigefunktionen zur Information von Personen über die über sie gespeicherten personenbezogenen Daten

## Für wen gilt die European Union's General Data Protection Regulation (GDPR) (gültig ab 25. Mai 2018)

### Wer muss es befolgen?

Organisationen, die Waren oder Dienstleistungen anbieten und dazu die personenbezogenen Daten von EU-Bürgern verarbeiten oder speichern oder Unternehmen, die das Verhalten von Personen überwachen.

### Gilt für:

Natürliche Personen, unabhängig von ihrer Staatsangehörigkeit oder ihrem Wohnsitz in der EU, in Bezug auf die Verarbeitung ihrer personenbezogenen Daten

## Unterstützt Kunden bei der Einhaltung der European Union's General Data Protection Regulation (GDPR).



### Bereits verfügbar

- Allgemeine Berechtigungen
- Werkzeuge zum Dateneigentum
- Datenarchivierung
- Zugriffsprotokoll
- Änderungsprotokoll für eine Vielzahl von Formularen/Masken
- Manuelle selektive Löschung bestimmter persönlicher Daten
- HANA Enterprise Search-Funktion für das Auswerten des Vorkommens von personenbezogenen Daten (verfügbar für SAP Business One, Version for SAP HANA only)



### GDPR relevante Daten

- Jedes Objekt, das persönliche Daten speichert ist EU GDPR relevant
- Geschäftspartner:
  - Ansprechpartner
  - Vertriebsmitarbeiter und Einkäufer
  - Endkunde (natürliche Person)
- Mitarbeiter und Systemanwender
- Geschäftsbelege:
  - Aktivitäten, Services, Opportunities
  - Marketing Belege
  - Rahmenverträge / Projektmanagement



### Wie können persönliche Daten in SAP Business One verwaltet werden\*

- Data Privacy Werkzeuge
  - Einrichtung Persönlicher Daten
  - Personal Data Management Wizard (Report, Daten-verschlüsselung/-entschlüsselung, Maskierung, Löschung)
  - Protokoll für Zugriff auf vertrauliche Daten
- Erweitertes Änderungsprotokoll für Felder und Objekte mit persönlichen Daten

*\*Erweiterungen geplant für Release 9.3 PL03 und PL04 – Termine unter Bestätigungs- und Änderungsvorbehalt.*

# GDPR in SAP Business One – Was ist bereits heute verfügbar?

**Allgemeine Berechtigungen:** Berechtigungen ermöglichen dem Benutzer, Marketing-Belege, die ihm zugewiesen sind anzuzeigen, zu erstellen und zu aktualisieren entsprechend der Dateneigentum-Einstellungen. Per Standard hat ein neuer Benutzer keine Berechtigungen. Jedem Benutzer ist nur ein Manager zugeordnet, der die Berechtigungen zuweist.

**Dateneigentum:** Dateneigentum ermöglicht dem Unternehmen, die Kontrolle über bestimmte Datenelemente auszuführen. Mit der Funktion Dateneigentum kann der Benutzer den rechtmäßigen Eigentümer der Daten und der Informationen definieren. Dadurch können ausgewählte Unternehmensdaten durch vordefinierte Berechtigungen gesichert und geschützt werden. Auf diese Daten und Informationen können dann nur eine berechtigte Rolle und ein berechtigter Anwender zugreifen.

**Datenarchivierung:** Unternehmen, die länger als zwei Jahre mit SAP Business One arbeiten, können den Archivierungsassistenten nutzen, um abgeschlossene Transaktionen aus bereits vergangenen und geschlossenen Perioden zu archivieren. Geschlossene Transaktionen können z.B. geschlossene Verkaufs- und Einkaufsbelege oder abgestimmte Journaleinträge sein.

**Zugriffsprotokoll:** SAP Business One erlaubt Benutzern mit speziellen Berechtigungen die Zugriffsprotokolle, welche Zugriffszeiten- und -arten protokollieren, einzusehen.

**Änderungsprotokoll:** Erlaubt es den Benutzern mit speziellen Berechtigungen, die Änderungen an bestimmten Feldern, wie z.B. den Zeitpunkt und den alten sowie neuen Feldwert, zu verfolgen.

**Manuelles Löschen von persönlichen Daten:** Benutzer sind berechtigt, manuell bestimmte persönliche Daten zu löschen, selbst wenn diese als Primärschlüssel dienen und mit anderen Objekten verbunden sind. Es liegt in der Verantwortung des Benutzers sicherzustellen, dass das Löschen solcher Daten nicht im Konflikt mit anderen Bestimmungen steht.

**HANA Enterprise Search:** Enterprise Search ermöglicht dem Benutzer Felder (wie Beschreibung, Betrag, Bemerkung, etc...) von Geschäftsobjekten in SAP Business One, Version für SAP HANA, zu durchsuchen, die zuvor in der SAP HANA Datenbank gespeichert worden sind.

# GDPR in SAP Business One – Was kommt?

## Einrichtung persönlicher Daten:

Zentraler Ort, um die persönliche Daten als solche zu kategorisieren. Es werden bestimmte vordefinierte Objekte ausgeliefert, die naturgemäß personenbezogen sind. Benutzer können hier Anpassungen und Erweiterungen vornehmen können.

Vertrauliche Daten, die in Feldern der Kernapplikation gespeichert sind, werden als solche vordefiniert sein, ohne Erweiterungsmöglichkeit auf weitere Felder. Kundenindividuelle benutzerdefinierte Felder können ebenfalls vom Benutzer als vertraulich gekennzeichnet werden.

**Zugriffsprotokoll auf vertrauliche persönliche Daten:** Verfolgungs- und Protokollierungs-Steuer-elementen, um den Lesezugriff eines Benutzers auf bestimmte vordefinierte vertrauliche persönliche Daten aufzuzeichnen.

**Personal Data Management Wizard:** Enthält einen Bericht, in dem alle Datensätze zu personenbezogenen Feldern in strukturierter Form aufgeführt werden. Möglichkeit, bestimmte natürliche Personen und alle Vorkommen und Daten, die über diese natürliche Person gespeichert sind, abzufragen.

Flexible Steuerungswerkzeuge für autorisierte Benutzer zum Verschlüsseln und Entschlüsseln von Werten, die in ausgewählten Feldern gespeichert sind. Um das "Recht auf Vergessenwerden" zu unterstützen, können autorisierte Nutzer auf der Grundlage ihres Urteils ausgewählte personenbezogene Daten löschen, sofern diese Maßnahme nicht im Widerspruch zu anderen Rechtsvorschriften steht.

**Erweiterung Änderungsprotokoll um weitere Formulare:** Erweiterungsfunktionen, mit denen Benutzer mit zugewiesenen Berechtigungen Details zu Änderungen in Feldern überprüfen können, die in verschiedenen Objekten / Formularen gespeichert sind

## GDPR in SAP Business One – Ein Hinweis

Es ist wichtig zu betonen, dass SAP hier keine rechtliche Beratung anbietet. Es liegt in der Verantwortung des Kunden, Maßnahmen zu ergreifen, die der Kunde für angemessen hält, um die Einhaltung der GDPR zu erreichen. Wir ermutigen jeden Partner in Zusammenarbeit mit Ihren Kunden, sich die erforderliche Zeit zu nehmen, um die Gesetzgebung zu verstehen und wie sich bestehende Verfahren und Prozesse ändern müssen.

Die Bereitstellung von Lösungen für die GDPR-Compliance in SAP-Business-One-Add-ons und -Erweiterungen, die nicht von der SAP SE bereitgestellt und gepflegt werden, liegt in der Verantwortung der SAP Business One-Partner.