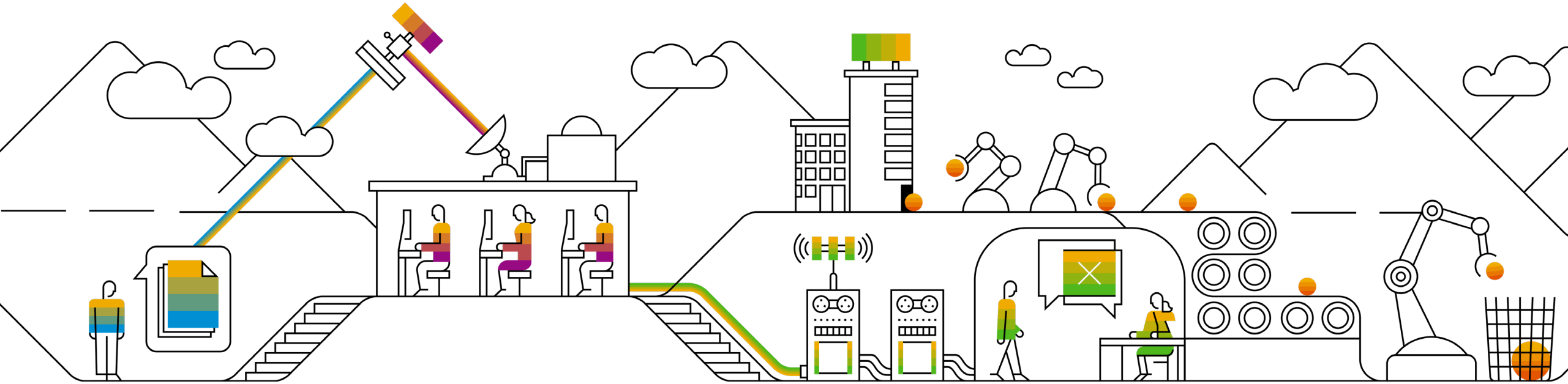


Data Protection in SAP S/4HANA and SAP Business Suite Software: Processing and Safeguards

Volker Lehnert, SAP
Sabine Rau, SAP
March 12, 2019

PUBLIC

THE BEST RUN SAP

Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, 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 presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document 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 in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation 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 non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP’s intentional 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.

Personal disclaimer

SAP does not provide legal advice, nor does the presenter.

The implementation of data protection requirements by any data controller is a complex challenge with interdependent legal and technical aspects. The responsibility to identify and implement adequate technical features, regarding the organizational aspects, remains with the controller.

The following presentation is only about technical features which might help a controller in achieving compliance with data protection regulations.

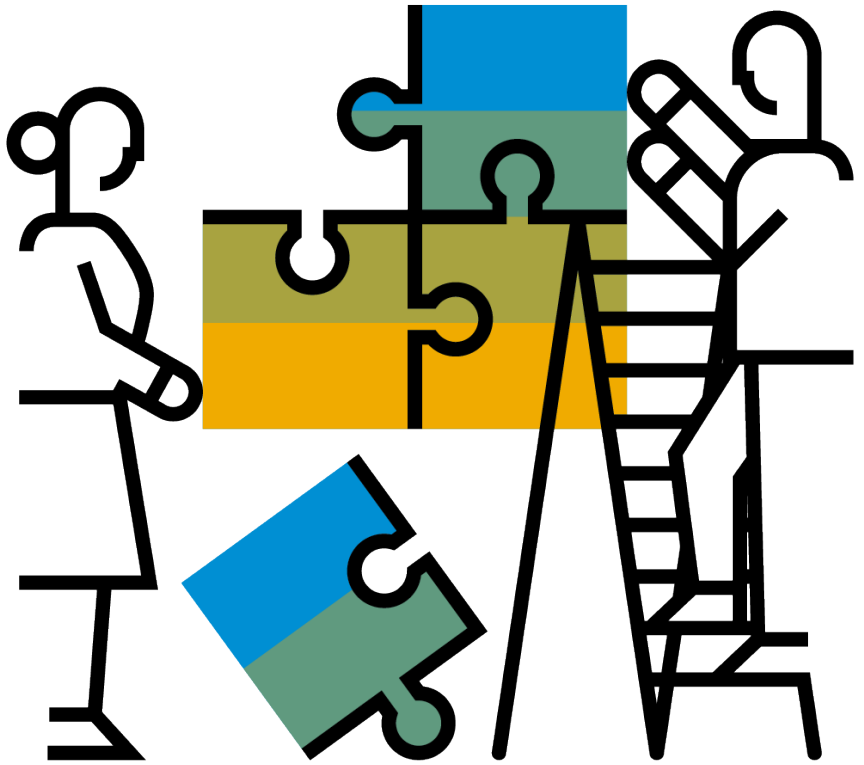
To help the audience understanding the shown approach, in-context information is given without claiming completeness or correctness.

The goal of this presentation is that you will no longer receive this particular look when talking about GDPR compliance in the future.

General Data Protection Regulation (GDPR) has become an **alarming buzzword**. This presentation will help you to figure out what GDPR means for your business and how SAP S/4HANA on Premise and Cloud help you to run your business in compliance with GDPR.

In the first chapter, we will share a few fundamentals and provide a holistic picture.

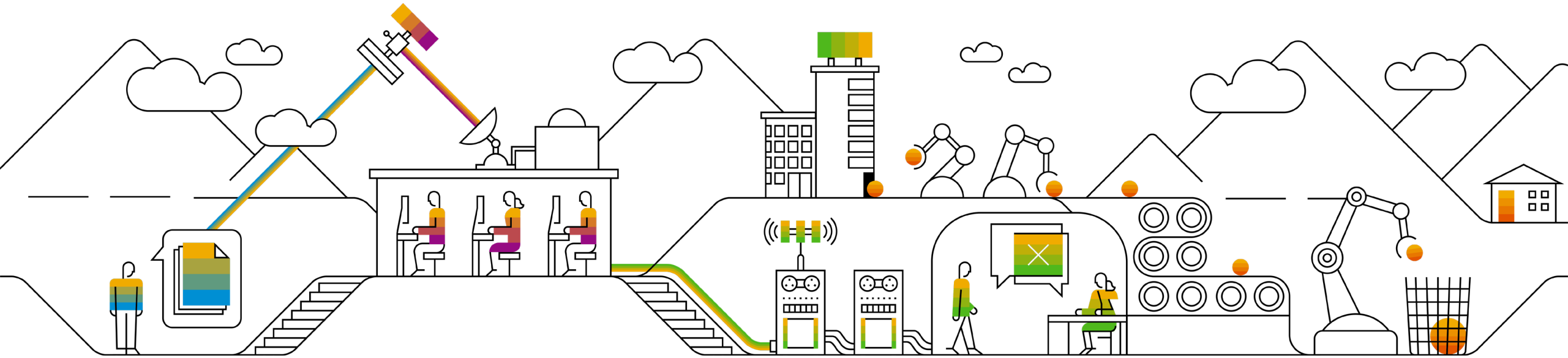
Please keep in mind that all information we share will only help you to employing our data protection features.



Agenda

1. An Introduction to EU General Data Protection Regulation
2. Basic GDPR Definitions and Examples
3. Processing of Personal Data
4. Rights of the Data Subject
5. Security Safeguards

An Introduction to EU General Data Protection Regulation



1. An introduction to EU General Data Protection Regulation

Do you need to care about GDPR?

The **General Data Protection Regulation** (GDPR) entered into **force** on May 25, 2018.

It addresses various obligations for **controllers** (organizations deciding on the processing of personal data for their purposes) and for **processors** (processing on behalf of the controller).

GDPR is **applicable** for controllers and processors where the processing is related to:

- The **offering of goods or services** to data subjects* in the EU
- The **monitoring of behavior** of data subjects in the EU

Penalties can range up to 4% of annual global revenue or **€20 million,** whichever is higher.

* A data subject is an identifiable person, that is, one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (GDPR Art. 4.1).

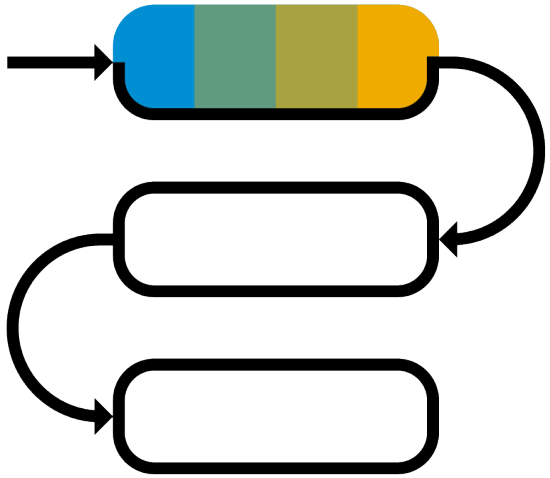
1. An introduction to EU General Data Protection Regulation

It’s all about justification

The processing of personal data is forbidden

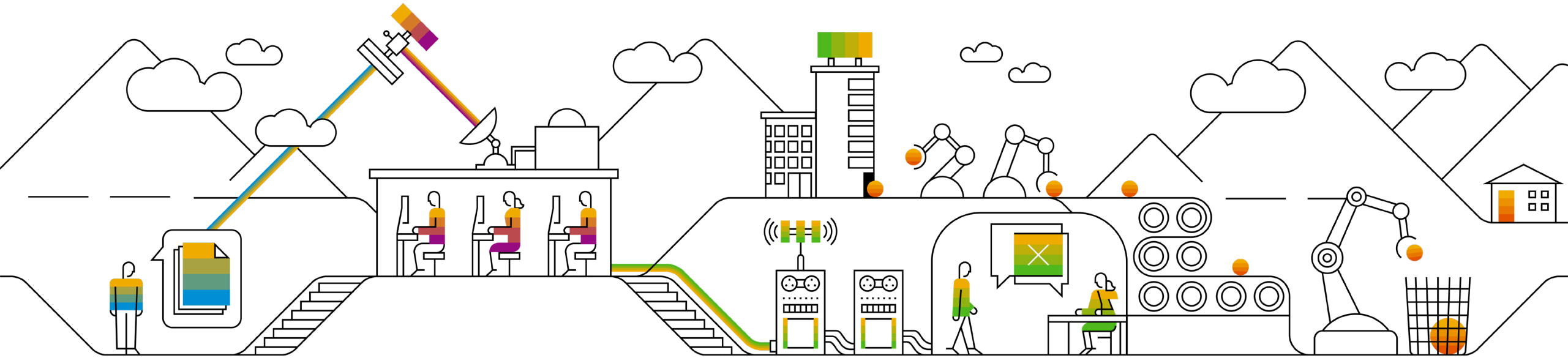
As long as no justifiable reason is given, such as:

- Contracts
- Other legal reasons (allowing or enforcing the processing)
- Effective declaration of consent for the data subject



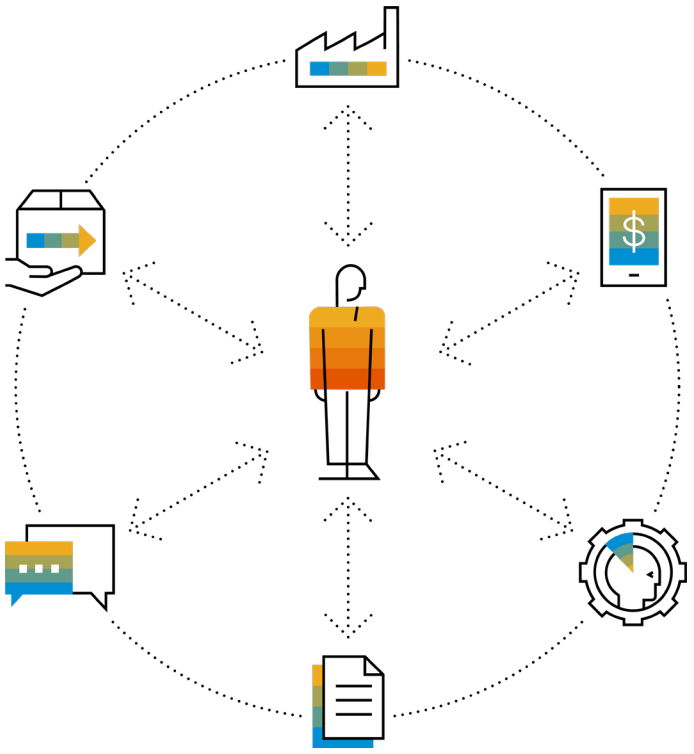
Justification must be verifiable for and in every processing step.

Basic GDPR Definitions and Examples



2. Basic GDPR definitions and examples

Definition of personal data and data subject



“ ‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;”

Article 4, No. 1 GDPR

In effect:

- Information that identifies individuals
- Information that contains identifiers
- Information that contains distinguishing characteristics

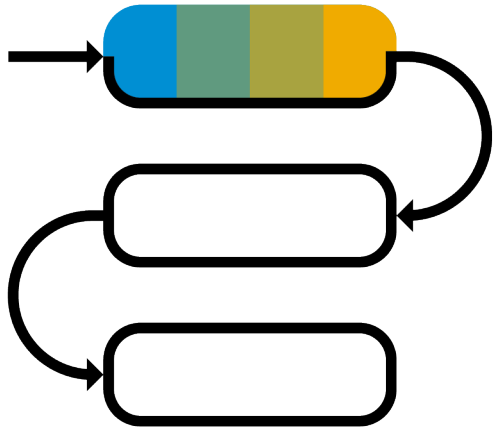
Any set of attributes allowing the identification of a data subject

2. Basic GDPR definitions and examples

Processing

“ ‘Processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”

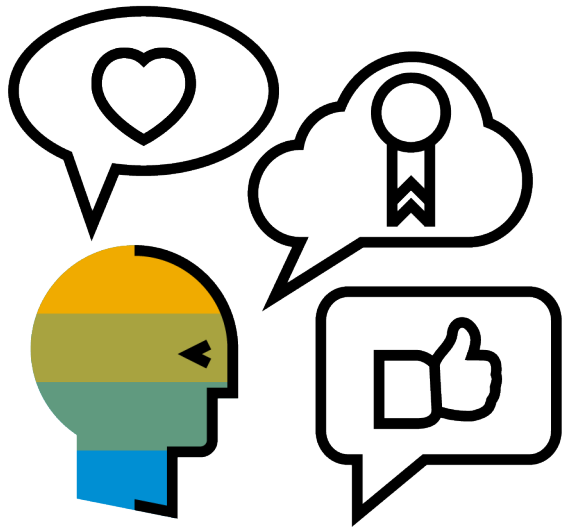
Article 4 No. 2 GDPR



Processing is simply **any operation** on personal data.

2. Basic GDPR definitions and examples

Controller

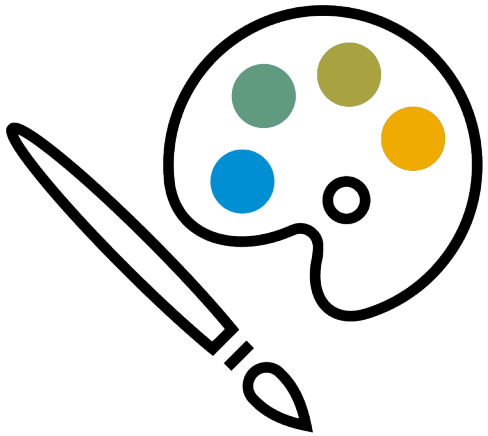


Data controller decides:

- To collect the personal data in the first place and the legal basis for doing so
- Which items of personal data to collect, i.e., the content of the data
- The purpose or purposes the data are to be used for
- Which individuals to collect data about
- Whether to disclose the data, and if so, to whom
- How to handle data subject access and other individuals' rights
- How long to retain the data

2. Basic GDPR definitions and examples

Purpose



Any processing of personal data is based on "*specified, explicit and **legitimate purposes** and not further processed in a manner that is incompatible with those purposes.*"

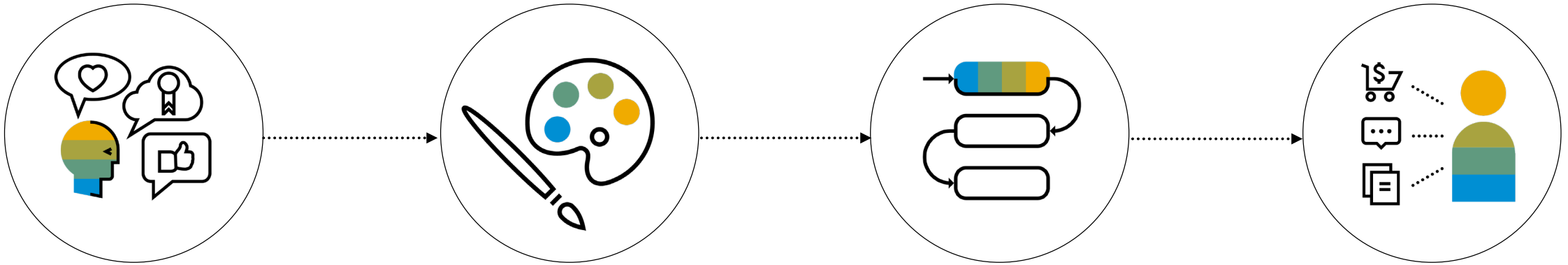
(Article 5 (1) Lit. b EU GDPR)

Purpose, in GDPR terms:

- Is not your **ideas about what you could do** with personal data
- Is not about **generic marketing slogans,** even if they are part of a company's mission
- Is nothing that you are not able to **specify explicitly** when the processing starts
- Is based on the **legal reasons** to process personal data defined in **Article 6 (1) GDPR** in every case

2. Basic GDPR definitions and examples

… so far?



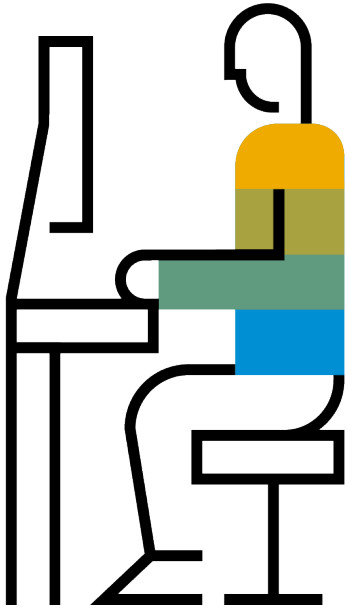
Controller determines the **purposes** and means of the **processing** of **personal data**

2. Basic GDPR definitions and examples

Data processor

A **data processor** is a natural or legal person, public authority, agency, or any other body that processes personal data “on behalf” of the controller.

- Controller determines the purpose and the means of the processing of personal data.
- Controller is fully responsible.
- Controller must be in “control” of processing activities.
- Processor cannot decide on processing activities independently.
- Processor cannot use personal data for its own purpose.

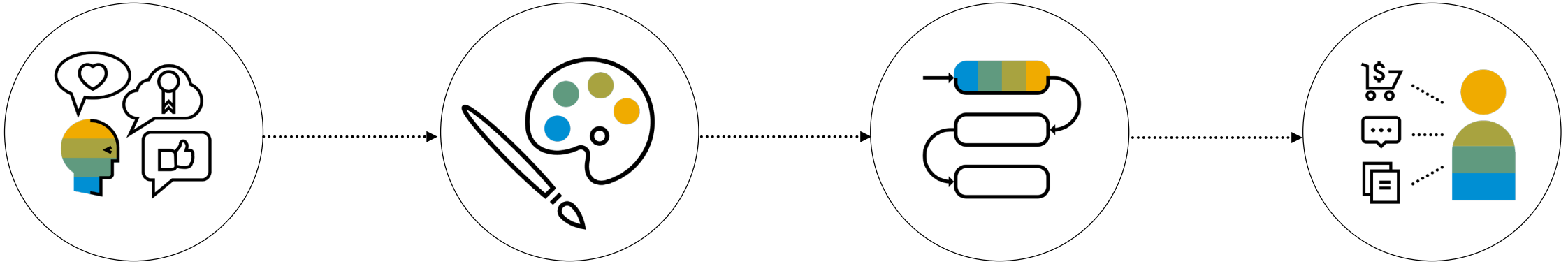


In SAP S/4HANA Cloud

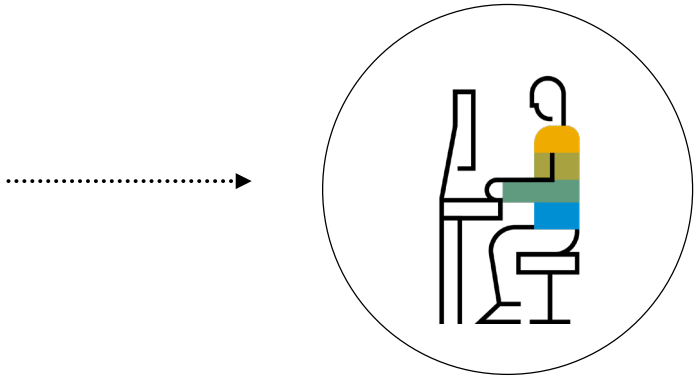
- The customer using our service remains the data controller.
- SAP becomes the customer’s data processor.

2. Basic GDPR definitions and examples

… so far?



Controller determines the **purposes** and means of **processing** **personal data**



performed by **processor**

Processing of personal data

Legal basis

Processing of personal data

Considerations I – 1

	Content	Possible technical feature?
Consent 	“Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation.” (GDPR, rec. 42, sentence 1)	Proof of consent is basically an organizational measure. However, the impact on data processing in an ERP system needs to be considered. ▪ A consent solution for SAP S/4HANA and SAP Business Suite software is available. ▪ An integration of the SAP Customer Consent solution is planned.
Contract 	Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract. (GDPR, rec. 44). More specific legislation might need to be considered. (Example: as provided based on art. 88, GDPR)	The proof of a contract is basically an organizational measure. However, an ERP system handles data documenting contracts. ▪ The existence of a contract itself is documented by corresponding documents and postings. ▪ As a supporting solution, documentation in SAP governance, risk, and compliance solutions might be considered (cloud and on premise).
Legal obligation 	ERP-based examples: tax reporting, income tax reporting, reporting for social insurance	The proof of a legal obligation is an organizational measure and not a technical feature. ▪ As a supporting solution, documentation in SAP governance, risk, and compliance solutions might be considered (cloud and on premise).

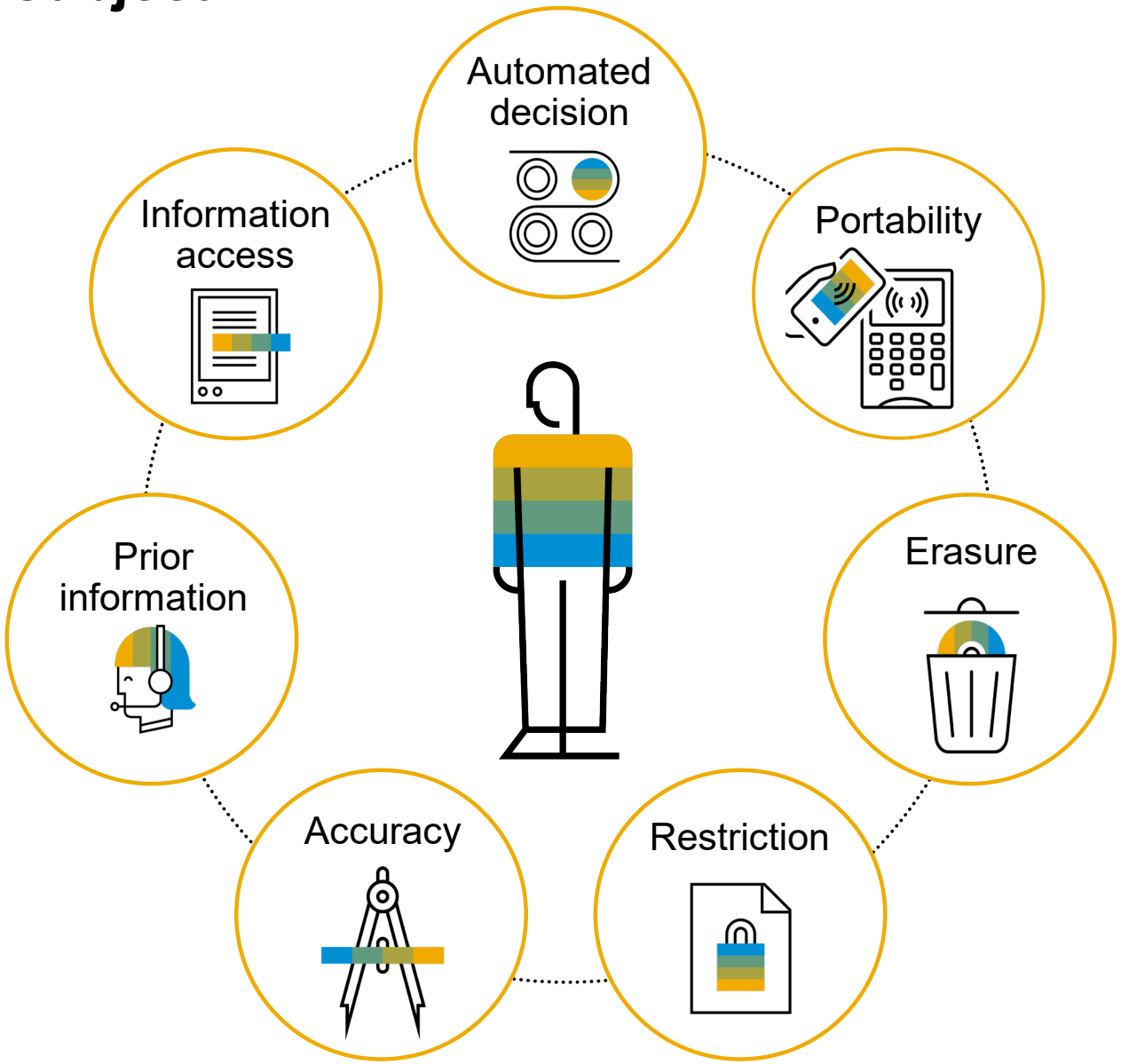
Processing of personal data

Considerations I – 2

	Content	Possible technical feature?
Protect vital interest 	“The processing of personal data should be regarded to be lawful where it is necessary to protect an interest that is essential for the life of the data subject or that of another natural person.” (GDPR, rec. 46, sentence 1)	The proof of a vital interest is an organizational measure and not a technical feature. ▪ As a supporting solution, documentation in SAP governance, risk, and compliance solutions might be considered (cloud and on premise).
Public interest 	“Where processing is … necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law.” (GDPR, rec. 45, sentence 1)	The proof of a public interest is an organizational measure and not a technical feature. ▪ As a supporting solution, documentation in SAP governance, risk, and compliance solutions might be considered (cloud and on premise).
Legitimate interest 	Proofing a legitimate interest is subject to a careful legal consideration whether “fundamental rights and freedoms of the data subject” are not overriding such an interest. (GDPR, rec. 47)	The proof of a legitimate interest is an organizational measure and not a technical feature. ▪ As a supporting solution, documentation in SAP governance, risk, and compliance solutions might be considered (cloud and on premise).

Rights of the data subject

Legal basis



Rights of the data subject

Considerations II – 1

	Content	Possible technical feature?
Prior information 	Information about which data will be processed; the purposes of processing for which the personal data are intended; the data controller; and the retention policies	This information is an organizational measure and not a technical feature. ▪ For SAP S/4HANA, SAP S/4HANA Cloud, and SAP Business Suite, an “information retrieval framework” (IRF) is being implemented that will logically support the rights of the data subject.
Information access 	The data subject’s right to get information as to whether or not personal data concerning him or her is being processed, and if so, the data subject’s right to access of this data	All personal data in SAP Business Suite is available for reporting in application-specific reports. ▪ For SAP S/4HANA, SAP S/4HANA Cloud, and SAP Business Suite, an “information retrieval framework” (IRF) is being implemented.
Accuracy 	Assurance that personal data is accurate, kept up to date, and able to be corrected (upon request)	Correction is a simple standard functionality. ▪ Accuracy in terms of avoiding doublets and keeping the data up to date is supported from the SAP Master Data Governance application.

Rights of the data subject

Considerations II – 2

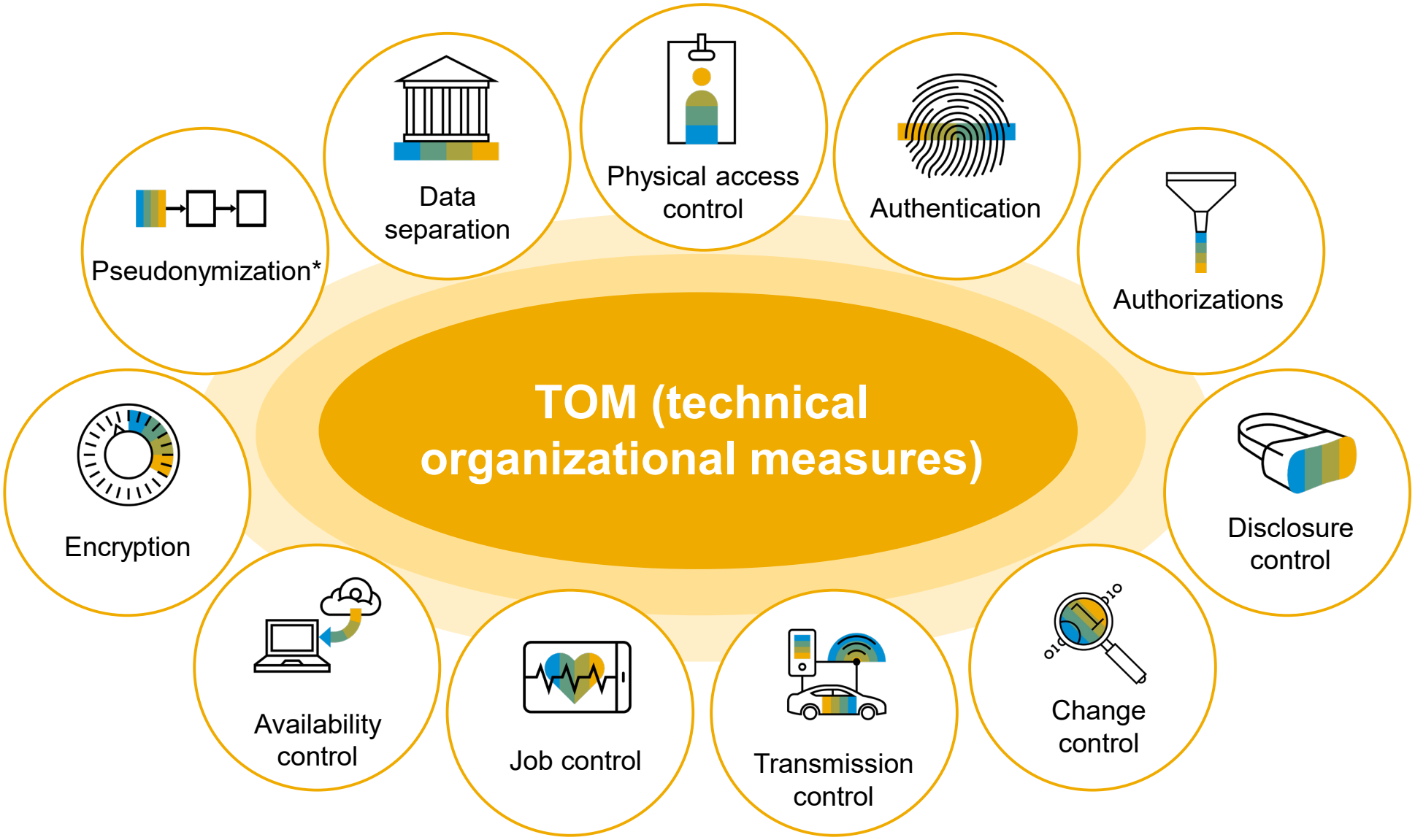
	Content	Possible technical feature?
Erasure 	The ability to delete personal data when all retention periods have passed and to block personal data as soon as the primary purpose has passed and the residence time has elapsed	Functionality for simplified blocking and deletion exists in SAP S/4HANA and SAP Business Suite. ▪ End-of-purpose checks and blocking indicators ▪ SAP Information Lifecycle Management, for use in retention management
Restriction 	The right of the data subject, in certain cases, to obtain a restriction of processing from the controller	Exercising data subject's right to restricting processing data is handled by the blocking and deletion functionality.
Automated decision 	The right of the data subject that any automated decision can become subject to manual interference	Any features providing such capabilities ensure that such decisions can get overruled manually.

Rights of the data subject

Considerations II – 3

	Content	Possible technical feature?
	The right of the data subject to receive his or her personal data in a structured, commonly used, and machine-readable format	Most information access features provide download functionality. The challenges here are missing international standards and the complexity of personal data in business. For SAP S/4HANA Cloud, an “information retrieval framework” (IRF) is implemented, allowing the download.

Security safeguards



* See slide 37

Security safeguards

Considerations 1

	Content	Possible technical feature?
	Prevention of unauthorized persons from gaining access to data processing systems with which personal data is processed or used	SAP functionality does not usually provide access control, such as badges or other physical controls.
	Secure procedures to enable system access based on personal authentication	This entails standard authentication features.
	Procedures allowing the differentiation of which data can be accessed and in which mode	Standard authorization concepts and identity and access management (IAM) apply here.

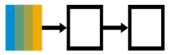
Security safeguards

Considerations 2

	Content	Possible technical feature?
	Ability to document all access to personal data	Logging features apply.
	Ability to document all changes to personal data	Standard change logging features apply.
	Procedures and safeguards for the transmission of personal data, such as encryption during transmission	Standard features, such as encrypted communication, apply.

Security safeguards

Considerations 3

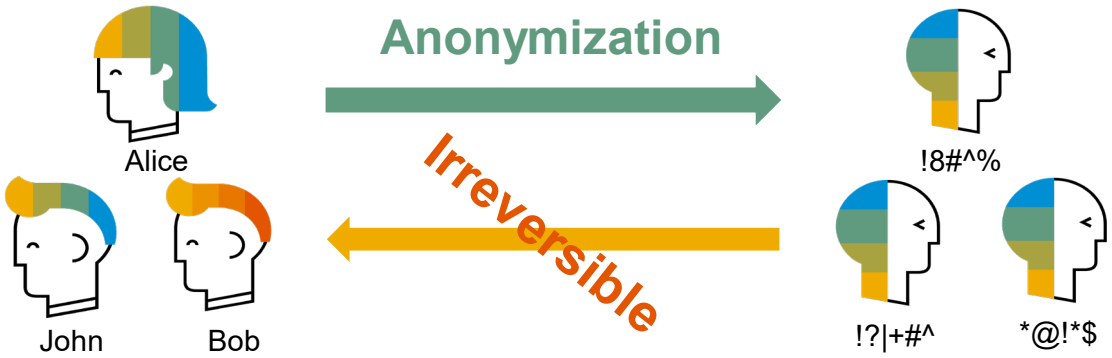
	Content	Possible technical feature?
Job control 	Ensuring that the data processor is following data controller's instructions and guidelines – an organizational task that has some technical aspects of a system audit	Standard system audit is applicable.
Availability control 	Procedures such as backup, disaster recovery, and business continuity	Standard and third-party features apply.
Pseudo-nymization 	Pseudonymization: changing the data in a way that the data subject is not identifiable without using additional information that is kept separately; pseudonymization and anonymization (irreversible) difficult to achieve	Not applicable (details on following slide), **Practical consequence** We will not deliver features claiming pseudonymization or anonymization. We are researching procedures that offer opportunities to reduce the identification potential in terms of de-personalizing personal data

Security safeguards

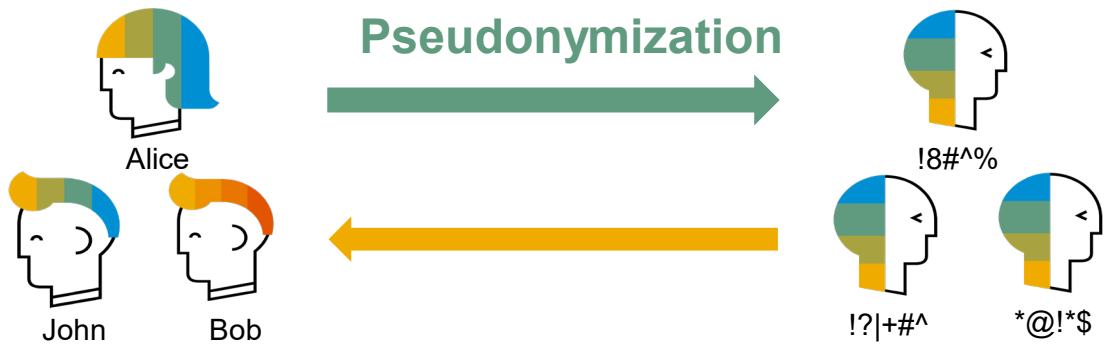
Considerations 4

	Content	Possible technical feature?
	Encoding a message or information in such a way that only authorized parties can access it	Encryption of communication and information is supported by encryption functionality in SAP S/4HANA and SAP Business Suite.
	Personal data collected for a specified purpose that must be separated from personal data collected for other purposes	Compliant master data structures apply. ▪ Data separation supported by line-organizational attributes and process-organizational attributes

Appendix: De-personalization and pseudonymizing



Anonymization is a procedure that **deletes all attributes** that allow the identification of a data subject. If a single data set in a pool of billions of data sets still identifies the data subject, then anonymization has not been attained. Effectively anonymized data is no longer subject to data protection requirements.



"Pseudonymization" is a procedure that **associates pseudonyms to all attributes** that allow the identification of a data subject, separating the key information technically. If a single data set in a pool of billions of data sets still identifies the data subject, then pseudonymization has not been attained.

Practical consequence

We will not deliver features claiming pseudonymization or anonymization. We are researching procedures that offer opportunities to reduce the identification potential in terms of de-personalizing personal data.

Further information sources about data protection and privacy

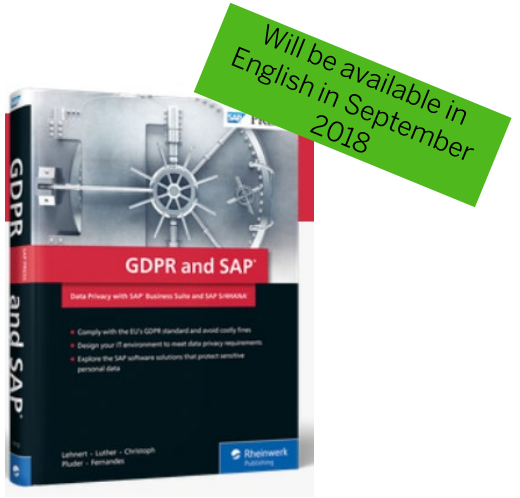
How SAP is implementing the requirements of the General Data Protection Regulation (GDPR) to best support its customers

Source: Cloud Trust Center

Getting ready for General Data Protection Regulation with product and services compliance (parts 1 and 2)

Source:

Part 1: Getting Ready
Part 2: Product and Services Compliance



GDPR and SAP
Data Privacy with SAP Business Suite and SAP S/4HANA

Source:
https://www.rheinwerk-verlag.de/gdpr-and-sap_4652/

Meeting Modern Data Protection Requirements

Source:
SAP Insider

SAP Integrated Report 2016 (Governance)

Security, privacy, and data protection

Source:
Integrated Report

Thank you.

Contact information:

Volker Lehnert
Senior Director Data Protection, SAP S/4HANA
volker.lehnert@sap.com

Sabine Rau
SAP S/4HANA Solution Management
sabine.rau@sap.com