Volker Lehnert
(volker.lehnert@sap.com) is Product Owner of Data Protection and Privacy for SAP Business Suite and SAP S/4HANA. Please note that he is not a lawyer, and he does not provide legal advice. In this article, he shares his personal opinion on data protection requirements and features based on his 11 years of experience in customer projects and his 5 years of experience in the development of data protection features.

SAPinsider
This article appeared in the Jul ▪ Aug ▪ Sep 2017 issue of *SAPinsider* (www.SAPinsiderOnline.com) and appears here with permission from the publisher, WIS Publishing.
WIS pubs

Meeting Modern Data Protection Requirements

How SAP Business Suite Helps You Comply with the Latest Data Protection Regulations

Modern business systems are a treasure trove of highly sensitive information, such as the names, contact information, and various financial and health details for an organization's current and former employees and family members, as well as valuable information about business partners, shareholders, and customers. As the volume and types of data collected continue to increase through smart devices, social media, and other technologies, so too have laws and regulations designed to protect this data from misuse.

One of these regulations is the European General Data Protection Regulation (GDPR) — a regulation intended to strengthen the protection of personal data for individuals within the European Union (EU). The GDPR goes into full effect on May 25th, 2018, replacing the existing data protection directive 95/46/EC with a wider scope and increased penalties for non-compliance. In particular, the GDPR significantly broadens the definition of personal data and it applies to any company — whether that company is physically located within or outside of the EU — that processes data, offers services or goods, or monitors the behavior of people in the EU.

The GDPR will have global implications, changing IT landscapes worldwide. So, what does this mean for those processing data with SAP Business Suite applications? This article shows you how basic technical features and security safeguards included with SAP Business Suite applications help you comply with key areas of the GDPR data protection legislation. In particular, we will look at how SAP Business Suite helps you cover legal grounds for processing personal data, ensure the rights of data subjects (those whose personal data is being processed), and establish key technical and organizational measures (see the next page for a note about terminology in this article).

Before diving into the details of the legal grounds specified by the GDPR, however, it is critical to first understand the GDPR's definition of personal data.

The GDPR Definition of Personal Data — And Why It Matters

With the GDPR, all companies within its defined material and territorial scope that deal with the personal data of EU residents must comply with its requirements.

The GDPR's definition of personal data is quite broad — "any information relating to an identified or identifiable natural person" is included within its scope.[1] Simply put, an "identifiable person" is identified by attributes such as last name, first name, telephone number, address, age, gender, and profession.

With this definition, a significant amount of data can be considered personal data. While neither the broad definition of personal data nor its scope are in themselves business critical,

[1] See Article 4, Section 1, in the GDPR (http://data.europa.eu/eli/reg/2016/679/oj).

A Note About Terminology

It is important to understand the distinction between the various types of measures discussed in this article:

- An **organizational measure** is an action or a sequence of actions that controls the behavior of people, such as management advice, procedure guidelines, and training.
- A **technical measure** is a configuration, feature, or software that controls something technical, such as authentication or encryption.
- Combined **technical and organizational measures (TOMs)** describe a holistic set of appropriate data protection safeguards. For example, a sophisticated authentication mechanism is worthless when passwords are shared, so an additional organizational measure is required with procedural guidelines that prohibit people from sharing passwords.

violations are subject to administrative fines of up to 4% of the fined company's worldwide turnover.

Now that the scope — and implications — of what constitutes personal data in the context of the GDPR is clear, let's examine the legal grounds defined in the GDPR for processing personal data, and the role SAP features and functionality can play in covering them.

Covering Legal Grounds for Processing Personal Data

According to the GDPR, the processing of personal data is lawful if at least one of the following grounds applies (see **Figure 1**):

- The data subject has given consent
- A contract requires the processing
- The controller (in most cases, the legal entity responsible) is subject to a legal obligation to do so
- If vital or public interests are involved
- If there is a legitimate interest

Here, we take a closer look at each of these conditions, and the ways in which SAP Business Suite applications can help you meet them.

Consent

Consent is an agreement between a data subject and a controller, in which the data subject formally agrees to the processing of personal data — via a signature or by actively clicking on a checkbox, for example. SAP Business Suite supports the documentation of consent with two features: the Marketing Permissions feature in the SAP Customer Relationship Management (SAP CRM) application and the Marketing Permissions feature for customer master data available with SAP NetWeaver 7.40.

Contract

A contract between the data subject and the controller defines the purpose of the processing of

Figure 1 According to the European General Data Protection Regulation (GDPR), processing personal data is lawful if at least one of these specified conditions is met

personal data — for example, a contract between an advertiser and a media company would require personal data to settle the contract and payment, and the processing would then be limited to that purpose. If the controller wants to process additional personal data or use it for purposes other than the one specified in the contract — for example, if the media company wants to sell that data to other companies — additional, specific consent from the data subject is required.

Most business activities performed using SAP Business Suite applications are based on contracts. SAP Business Suite applications enable you to prove the existence of a contract using transactional or master data — for example, you can view existing sales contracts or payment transactions.

Legal Obligation

The processing of data due to legal obligation — for example, the reporting of salary figures to tax authorities — must be proven by organizational measures, meaning any documentation that describes processes, guidelines, or directives that control people's behavior. For example, you could document processing activities using SAP governance, risk, and compliance (GRC) solutions and then link to that information from SAP Business Suite.

Vital and Public Interest

The processing of data due to vital interest is not a typical scenario for SAP Business Suite customers. This condition might apply if data processing is required to provide medical care for an unconscious person, for instance, and the GDPR also mentions "epidemics," "humanitarian emergencies," and "natural and man-made disasters" as valid grounds.[2] While the SAP for Healthcare industry solutions and the Industrial Hygiene and Safety component of SAP Environment, Health, and Safety Management partially process data based on these grounds, the existence of these grounds must be proven by organizational measures, such as documentation stored in SAP GRC solutions.

The processing of personal data based on public interest applies in cases of relevant national or EU law, such as police checking personal data during an inquiry. Similar to vital interest, public interest is a legal ground that must be documented organizationally.

Legitimate Interest

The processing of personal data based on legitimate interest requires balancing legally protected interests to determine whether the interests of processing the data are more important than the data protection rights of the data subject. By nature, this is something that cannot be solved by automated means and must be covered by organizational measures. Solid reasoning and documentation are particularly important in this case, since the merits of "legitimate interest" can often be challenged.

Ensuring the Rights of Data Subjects

The GDPR defines numerous rights for data subjects that organizations must ensure. While some of these rights can only be ensured by organizational measures, here we'll highlight some that require a technical measure — a configuration, feature, or solution that controls something technical — or at least technical support, and look at how SAP Business Suite applications can help.[3]

Blocking and Deletion of Personal Data

Based on our experience at SAP, one of the most impactful rights defined by the GDPR is the blocking and deletion of personal data that is no longer required within the purpose defined for the processing. According to the GDPR, personal data must be deleted after the primary purpose of the processing has ended. If the data must be retained to comply with retention periods required by other legislation — such as tax legislation — access to it must be blocked or restricted, and it must be kept only for the duration of the longest legal retention period, after which it must be deleted.

To help with this task, as of SAP NetWeaver 7.40, SAP Business Suite applications provide simplified blocking and deletion functionality that is based on SAP Information Lifecycle Management (SAP ILM). All SAP Business Suite applications include required SAP ILM objects that enable the transfer of data to an archive, which fulfills the blocking requirement. In addition, all SAP Business Suite applications support the "end of purpose" check,

[2] See Recital 46 in the GDPR (http://data.europa.eu/eli/reg/2016/679/oj).

[3] For a complete list of rights, see http://data.europa.eu/eli/reg/2016/679/oj.

also based on SAP ILM, that is triggered from central personal master data sets, such as central business partner, customer, and vendor master data. With this check enabled, all applications registered with a central personal master data set are triggered to check whether they still need that data — if no longer needed, the data is marked as blocked and access is restricted.

Restricting the Processing of Personal Data

Another requirement specified by the GDPR is the ability to restrict the processing of personal data based on a data subject's request while keeping the data available for the establishment, exercise, or defense of legal claims — for instance, if you want a legal clarification due to incorrect data that led to a wrong business decision.

The blocking and deletion functionality included with SAP Business Suite applications can be configured to address this requirement by leaving only data in the system that is relevant to the defined processing purpose and must be processed. SAP ILM also provides a legal hold functionality that can be used to retain relevant data as needed.

Providing Access to Personal Data in a Readable Format

The GDPR also specifies the right of data subjects to have access to any of their personal data that is undergoing processing. SAP Business Suite enables organizations to provide data subjects with this information through its reporting tools. Currently, SAP is changing from application-specific reporting to a centralized approach, which will allow for centralized reporting on data that is undergoing processing. Regardless of the reporting approach, the decision about which data to report remains with the company using the SAP software, so a detailed, customized, and specific configuration will be required.

In addition, data subjects have the right to obtain any personal data undergoing processing in machine-readable format, which is easily provided by the download functionality available with SAP Business Suite reporting tools.

Establishing Technical and Organizational Measures

In addition to meeting legal requirements for processing personal data and ensuring the specified rights of data subjects, the GDPR requires businesses to establish technical and organizational measures (TOMs) to ensure the protection of personal data. While the GDPR does not list specific required TOMs — it gives only example definitions — it clearly requires that appropriate TOMs be implemented and reviewed on a regular basis (for more on related documentation and controlling requirements, see the sidebar "Documentation and Controlling Become Key").

So how do you know which TOMs to implement to ensure GDPR compliance? Fortunately, there is existing legislation that can provide guidance — for example, the TOMs specified by Germany's current

Documentation and Controlling Become Key

With the European General Data Protection Regulation (GDPR), organizations are required to not only implement technical and organizational measures to safeguard the personal data they are processing, but also document in a record of processing activities how they have done it and why they chose certain measures.* They must also document the controls that are in place to regularly verify that the safeguards are appropriate, and for any new processing of personal data, they need to conduct impact assessments to evaluate how that processing will affect the protection of personal data.** Software such as SAP governance, risk, and compliance (GRC) solutions that bundles the requirements of regulations such as Sarbanes-Oxley, the US Food and Drug Administration, and the GDPR can help you significantly simplify and manage these tasks.

* See Article 30 in the GDPR (http://data.europa.eu/eli/reg/2016/679/oj).

** See Article 35 in the GDPR (http://data.europa.eu/eli/reg/2016/679/oj).

Technical and Organizational Measures	Content
Physical Access Control	Prevent unauthorized persons from gaining access to data processing systems with which personal data is processed or used.
Authentication	Secure procedures to enable system access based on personal authentication.
Authorization	Procedures allowing differentiation in which data can be accessed and in which mode.
Disclosure Control	Ability to document all access to personal data.
Change Control	Ability to document all changes to personal data.
Transmission Control	Procedures and safeguards for the transmission of personal data, such as encryption during transmission.
Job Control	Data controller must ensure that the data processor is following instructions and guidelines. This organizational task has some technical aspects, such as system auditing.
Availability Control	Procedures such as backup, disaster recovery, and business continuity.
Data Separation	Personal data collected for a specified purpose must be separated from personal data collected for other purposes.

Figure 2 The measures required by Germany's Federal Data Protection Act (BDSG) are a useful guideline for meeting European General Data Protection Regulation (GDPR) requirements

Federal Data Protection Act (BDSG)[4] can serve as a useful guideline for establishing basic safeguards for processing personal data (see **Figure 2**).

SAP Business Suite applications provide built-in features and functionality that support most of the TOMs listed in Figure 2 (the only area that is not supported is the physical access control, which relates to preventing unauthorized physical access to buildings or rooms where personal data is processed). To give you an idea of how SAP Business Suite provides this support, we'll take a closer look at three key TOMs that, based on our experience, are required by the GDPR.

Data Separation

Based on our experience at SAP, the purpose limitation requirement set by the GDPR is a precondition for several technical measures. It requires the ability to separate data by attributes so that data collected for one purpose remains separate from data collected for another purpose — a separation also required to support the data subject's right of access, blocking and deletion requirements, and system access for transmission of data. It also establishes the assumption that all access — including access by persons, machines, software logic, and any kind of transmission — must be controlled by authorizations defined by purpose.

For this reason, the personal data to be processed needs attributes that reflect the purpose of the processing, which can be reflected by the line organizational attributes used to define organizational structures in SAP Business Suite (see **Figure 3** on the next page). Line organizational attributes can be used to separate the data controller, which is usually a single legal entity — a company code, for example. In a group of companies, it is critical to organize the data in a way that separates a single legal entity from any other data.

To define compliant authorizations, to organize system interfaces, to block and delete personal data, and to fulfill transparency requirements, a properly maintained line organizational software setup is required that reflects the legal entity or controller that processes that data. Our experience indicates that organizations must often adapt or even rethink their master data structures to meet this requirement.

Authorization

Remember the challenges involved in avoiding or mitigating authorization and segregation-of-duties

[4] View the full text of Germany's Federal Data Protection Act (BDSG), which was enacted to implement the European data protection directive 95/46/EC, at www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html.

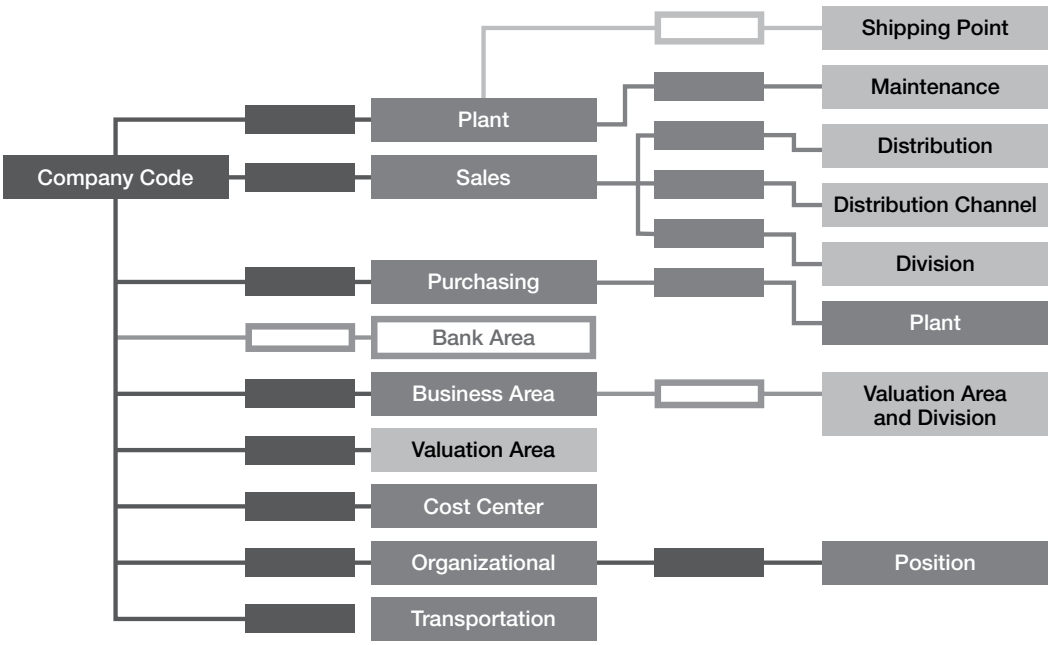

Figure 3 Some of the line organizational attributes used by SAP Business Suite to define organizational structures can be used to reflect processing purpose

(SoD) conflicts in the early days of the Sarbanes-Oxley Act? Authorizations that comply with data protection regulations such as GDPR are even harder to achieve.

To comply with GDPR, any access on personal data needs to follow a strict basic authorization concept.[5] Essentially, access to personal data should be granted only if the user has a reason to handle that data according to the predefined purpose of the data processing. In addition, any access should be at least separated by the legal entity or controller that processes that data, and also by process organizational attributes such as order type. SAP Business Suite includes a traditional technical authorization concept that allows separation by these types of attributes.

Transmission Control

To safeguard the security of personal data, proper encryption during transmission is required, but it is even more important to avoid illegal transmissions. This means that you need to identify any interface in a system dealing with personal data, document the interface, and provide authorizations ensuring that only designated personal data is accessed according to the purpose of the processing — this includes any data access that takes place over remote function call (RFC) connections.

To help make RFC communications more secure, SAP introduced the Unified Connectivity (UCON) concept, a basic functionality included with SAP NetWeaver and, in turn, SAP Business Suite.[6]

Conclusion

So what will happen after May 25th, 2018? Some discussions between lawyers and regulatory authorities have focused on how the GDPR will be enforced outside the European Economic Area, while others are centered on whether supervisory authorities will, in fact, impose fines up to 4% of the annual turnover if a company is in violation of the GDPR. Regardless of the answers to these questions, the well-known quote from US Deputy Attorney General Paul McNulty holds true: "If you think compliance is expensive, try non-compliance."

Learn more about the GDPR at **www.eugdpr.org** and **http://data.europa.eu/eli/reg/2016/679/oj**. ■

[5] For a detailed discussion of basic authorization concepts, see *Authorizations in SAP Software: Design and Configuration* by Volker Lehnert and Katharina Stelzner (SAP PRESS, 2011).

[6] For more on the Unified Connectivity (UCON) concept for RFC communication, see the article "Secure Your System Communications with Unified Connectivity" in the January-March 2014 issue of *SAPinsider* (SAPinsiderOnline.com).