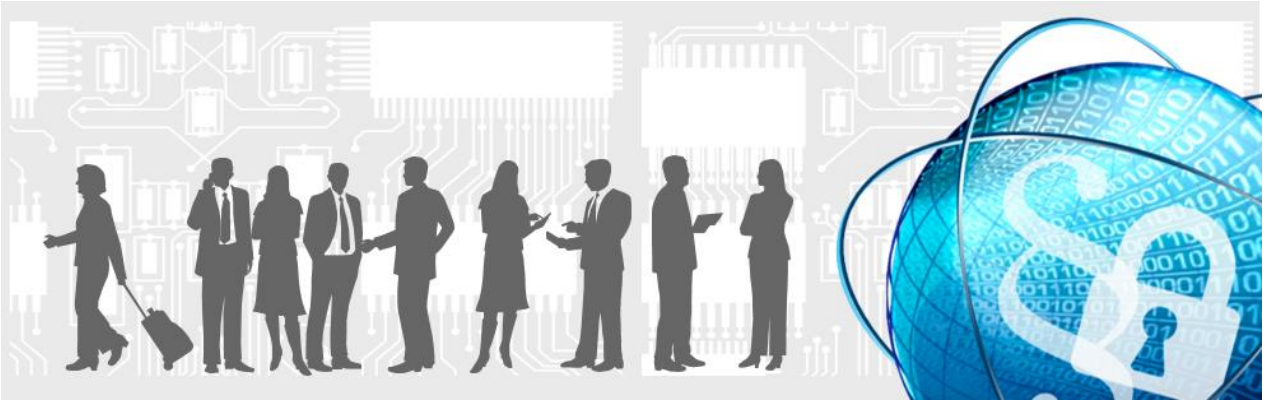
Data Protection and Privacy at SAP



Getting Ready for May 25, 2018

Part 2: Product and Services Compliance

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

- **PUBLIC** -

Background

In May 2016, the European Union (EU) adopted a newly harmonized data protection law called the General Data Protection Regulation (GDPR). As of May 25, 2018, the GDPR will be a directly applicable law in all member states within the EU and the European Economic Area (EEA). While the GDPR does not introduce many substantially new concepts, it increases the compliance requirements of data controllers and personal data processors.

This is the second in a series of papers entitled, 'Getting ready for May 25, 2018' providing an overview of SAP's approach to implement the GDPR to best support its customers.

This paper, '*Part 2: Product and Services Compliance'*, deals with two important topics: Firstly, it provides an overview of the changes that SAP is making to its products and how their features can help SAP's customers implement GDPR requirements. The second topic summarises SAP's approach to services compliance as it is vital for SAP to ensure that its services are provided in a GDPR compliant way.

How can SAP Products and their features help implement GDPR requirements?

What changes under the GDPR?

In summary, the GDPR aims to harmonize data protection requirements across Europe. Customers ("controllers" as defined by Art. 4 (7) of the GDPR) and service providers ("processors" as defined by Art. 4 (8) of the GDPR) must implement a number of new legal requirements, which will substantially affect their businesses. Controllers and processors each need to verify which obligations under the GDPR apply to them and how to implement them accordingly.

To what extent are SAP Products GDPR compliant?

SAP has been consistent in its approach to data protection as part of SAP's general product standards. This is now being extended in order to reflect the new requirements of the GDPR.

With the above in mind, **SAP is committed to ensure compliance with the GDPR as a company by May 2018**, as well as to develop our products to support our customers in applying applicable GDPR requirements to the fullest extent possible.

Development measures include the ongoing enhancement of already existing product features as well as the implementation of new requirements. For example, certain legal requirements under the GDPR which are aimed at controllers primarily deal with how a controller processes personal data within a company. If configured in the correct way, the use of SAP software products can assist controllers comply with certain obligations under the GDPR.

Which features or other aspects of SAP products already support GDPR compliance?

If configured accordingly, many features within SAP's existing products already support GDPR compliance. The features vary depending on the product, but our guiding principles are:

- Support Data Subject Rights. Products may include functionalities to identify and report data, including personal data, and product documentation provided by SAP to assist in fulfilling obligations to data subjects, and system inherent consent management to assist in fulfilling the updated consent obligations under the GDPR. Moreover, available data retention and deletion functionalities assist in the goals of data minimization, blocking, and deletion of personal data.

- Enhance Technical and Organizational Measures. In addition to the technical and organisational measures we commit to in a contract, many SAP products contain additional product specific functionalities such as logging, specific role- and rights-logic, encryption or data masking which assist you in maintaining appropriate security to protect personal data.

- Provide Options for International Data Transfer. As we mentioned in *Part 1*, SAP supports international data transfers through EU Standard Contractual Clauses (aka 'Model Clauses'). In addition, for those customers that require their personal data to be stored and processed solely within the EU/EEA, SAP's '*EU Access*' service enables customers to achieve this. SAP's EU Access customers have their personal data processed and accessed only from within the EU, EEA and Switzerland where even remote access outside these regions is excluded. This offering is available for on-premise support as well as a number of SAP cloud solutions.

Services Compliance at SAP

How does SAP handle data protection internally to provide a GDPR compliant approach in providing services to customers?

To demonstrate our compliance obligations with data protection and privacy laws, SAP has implemented a wide range of internal measures to protect data controlled by us and our customers from unauthorized access and processing, accidental loss, or destruction. What follows is an overview of each measure relevant to GDPR compliance.

1. ***Maintaining Consistency with SAP third party subprocessors****: mandatory recruitment requirements.*

SAP utilizes third party subprocessors for product development and service delivery which is a vital and integral part of SAP's core services solution offerings.

When SAP uses subprocessors to handle customer personal data as part of a service it ensures that each subprocessor passes a rigorous three-step recruitment control management process before it is actively permitted to manage customer personal data on SAP's behalf.

- Establish Contracts for Proper Handling. Firstly, prior to being engaged by SAP, each third party subprocessor must enter into a comprehensive Master Data Protection Agreement (MDPA) with SAP. Part of the MDPA sets out a contractual commitment for the subprocessor to adhere to TOMs (as referred to above). The MDPA also imposes the same data protection obligations on the subprocessor as those that are set out in the various data processing agreements between SAP and its customers. Based on this approach, SAP enables an adequate level of data protection and privacy throughout the whole range of its global service offerings as required by the GDPR.

- Check Technical and Organizational Measures. Secondly SAP requires the third party subprocessor to complete and sign what is known as a "Data Protection Questionnaire" (DPQ). The detailed DPQ is based on SAP's standard technical and organizational measures (TOMs) which are a set of minimum standards for security and data protection measures to be implemented by the third party subprocessors. The DPQ is then evaluated by SAP's central data protection team. If a subprocessor fails to meet these requirements under the DPQ (i.e., it does not have the necessary TOMs in place) then the subprocessor fails the recruitment process and will not be engaged by SAP for the purposes of handling customer personal data on SAP's behalf.

- Failing to agree to the terms of the MDPA or the requirements of the DPQ or providing insufficient information in relation to it will result in SAP not engaging with prospective vendors as subprocessors.

- Monitor Third Party Subprocessor Compliance. The third stage concerns continual monitoring of the subprocessor which is also another vital element of SAP's vendor control management process. Within the MDPA, the subprocessor must contractually commit to its terms and the requirements of the DPQ on an on-going basis. This includes allowing SAP to execute data protection audits of its processes, systems and premises. All onsite audits include several interviews with management, employees and staff responsible for data protection. They also include an intense documented procedure and an onsite inspection of work spaces, data centers and server rooms.

  All audits are documented and reported to SAP's data protection officer.

2. ***Our Commitment to the Customer:*** *Customer facing data processing agreements.*

When SAP enters into an agreement for services with its customers, if commissioned personal data processing takes place, SAP ensures that a data processing agreement is in place between the parties in order to assist its customers in meeting their obligations as a data controller.

As a processor, SAP uses these data processing agreements to lay out our commitments to proper data handling, working on customers' instructions, international data transfer and appropriate technical and organizational measures for the relevant product or service.

Because our controller-processor agreements with our customers have been based on relevant legal and regulatory requirements in Germany, now generally considered new Europe-wide standard under the GDPR, our existing data processing agreements already comply with the future requirements of the GDPR.

As market leader in enterprise application software, SAP is at the center of today's business and technology revolution. SAP is fully committed to compliance with the EU GDPR, as well as continued compliance with data protection rules around the globe.