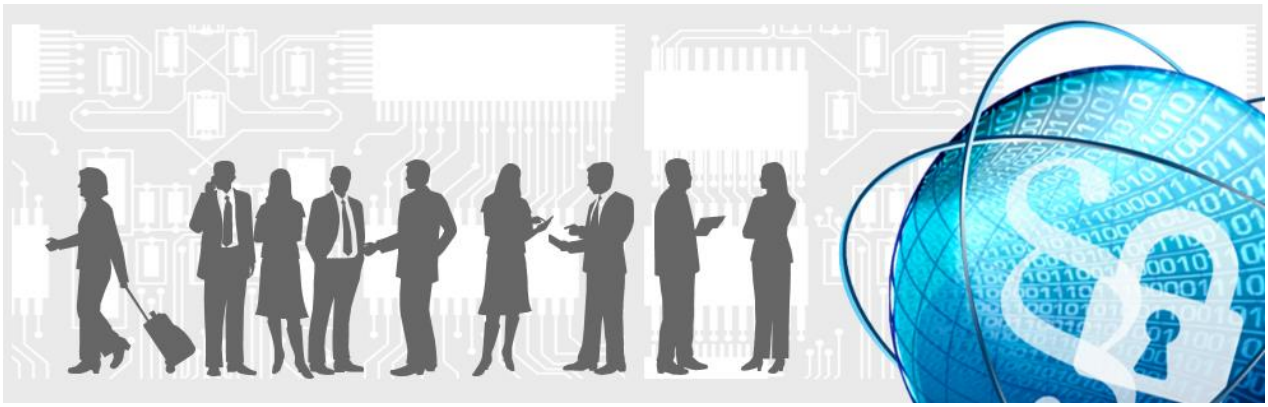
SAP Data Protection and Privacy



Getting ready for May 25, 2018

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

Background

In May 2016, the 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 EU and EEA Member States. While the GDPR does not introduce many substantially new concepts, it increases the compliance requirements on controllers and on processors of personal data.

This paper provides an overview about the changes introduced by the GDPR that pertain mainly to processors and how SAP is implementing them to best support its customers.

The role of the Data Protection Officer (DPO)

Under the GDPR, it will become mandatory for certain controllers and processors to designate a Data Protection Officer (DPO). This will be the case for all public authorities and bodies that process personal data, and for other organisations that - as a core activity - monitor individuals systematically and on a large scale, or that process special categories of personal data on a large scale.

At SAP, we have always seen the designation of a DPO as a central part of our data protection strategy. SAP has established an entire Data Protection and Privacy (DPP) team consisting of attorneys, auditors and technical experts. The team's core responsibilities include the shaping of SAP's data protection policies and standards, providing advice, recommending key compliance measures, monitoring compliance, conducting audits, training of staff and incident response. The DPO and his team are also the designated point of contact for inquiries by individuals and supervisory authorities.

To provide truly global services, DPP maintains a worldwide network of data protection and privacy coordinators, one in each line of business and/or legal entity. The data protection and privacy coordinators provide input from other jurisdictions and help DPP implement data protection and privacy requirements across SAP.

Good to know for customers: The DPP team works together with development and operational units across SAP to provide training and advice, and thus help them maintain the data protection compliance of SAP's products and services.

Data Protection Management System (DPMS)

An important task of all companies operating in the EU is to ensure a high level of data protection awareness and data protection adherence across the company. Our 300.000+ customers expect that all SAP employees follow the data protection regulations at all times.

In order to address such a complex issue to a global organization in more than 120 countries, SAP has developed and implemented a Data Protection Management System (DPMS).

The DPMS is SAP's approach for managing compound requirements of data protection in a structured way. The SAP DPMS is based on SAP's policy for security and data protection, covers the technical and organizational measures and strictly follows an annual Plan-Do-Check-Act cycle. The core elements of management system are specific guidelines for all units, various data protection trainings and regular controls with the help of more than 150 audits every year.

In order to meet highest demands on the quality of our data protection adherence, SAP has decided to certify the DPMS with the British Standard BS10012. The BS 10012 describes the fundamentals for setting up and driving a data protection management system. Since the DPMS is designed as a highly adaptive system, it can easily be integrated into existing other management systems like ISO 9001 or ISO 27001. Initially implemented at SAP's global support organizations in 2010, the DPMS has been successively expanded every year and is now implemented in almost all areas and countries at SAP.

SAP's DPMS is annually certified by the British Standards Institute (BSI). The certificate and an annual comprehensive audit report can be downloaded and provided to our customers.

Records of Processing Activities – Procedure Enrolment Tool (PET)

All SAP areas which process personal data are responsible for a data protection compliant setup of their processes, services and products. For each procedure they also have to document data protection relevant aspects like:

- Processed data and special categories
- Purpose of data processing
- International data flows
- Lists of subprocessors
- Deletion concepts

In order to fulfil the requirements of documentation and regular control of processing activities, specifically trained employees in each business unit act as data protection champions and ensure the proper enrolment and maintenance of their procedures.

In order to increase transparency of the procedure inventory and to streamline this comprehensive task, a tool for the enrolment, documentation and reporting of procedures has been developed and implemented: the Procedure Enrolment Tool (PET).

The PET is an up-to-date application, guiding the process owners through all questions, providing general information on data protection basics or detailed information on the root cause for specific questions. It also provides a risk assessment, on-the-fly feedback to the compliance status of the procedure or status information on the completeness level for each data entry.

The PET enrolment is supported by a set of general data protection guidelines, PET-specific trainings and will be accompanied by a record with contacts at the DPP team. Regular checks with the business unit responsible will help the organization to get a complete and reliable overview on the completeness of all listed procedures and their individual compliance with data protection requirements.

The PET is being rolled out in 2017 to all board areas, which have already started to complete their PET entries. We anticipate having all existing data protection relevant procedures inventoried by the end of 2017.

Local Data Processing and International Transfers

Already today, European data protection law permits data transfers to countries outside the EU and the EEA only if an adequate level of protection is ensured. Only very few countries fulfill this requirement by law. However, European data protection law permits international data transfers based on bilateral arrangements, such as the former Safe Harbor regime and now the EU-U.S.Privacy Shield, and other legal instruments, such as the Standard Contractual Clauses (in this document referred to as 'EU SCCs').

Under the GDPR, existing transfer restrictions applying to transfers of personal data out of the European Union will be preserved but enforced in a much stronger fashion. For any business or organization with multinational operations, this is an important topic.

While the EU-U.S. Privacy Shield is an important vehicle for transferring personal data between the EU and the U.S. and has substantially improved levels of protection compared to Safe Harbor, SAP has and will continue to rely on the EU SCCs due to their global nature.

SAP approaches the mechanism by which it utilizes the EU SCCs in the following two ways:

For those data transfers to our global SAP affiliates SAP has the benefit of an Intra-Group Agreement on Data Protection and Privacy (which we refer to as an "IGA"). This reflects SAP's structures when transferring and processing personal data for internal purposes but also when processing data on behalf of customers. It provides for a lawful mechanism of transferring personal data outside the EEA based on the EU SCCs and forms a legally binding agreement between the SAP global entities establishing requirements for a baseline protection of personal data.

In order to provide a premium global approach to providing services, SAP has a strong supplier ecosystem, which is critical to the ongoing success of our solutions. SAP's Global Procurement Organization enforces procedures whereby each SAP supplier handling personal data (our sub processors) must satisfy strict internal verifications based on our data protection and privacy requirements. Due diligence checks are also undertaken through a detailed Data Protection Questionnaire and contractual assurances set down in a Master Data Protection Agreement.

Where a supplier provides services to our customers involving a transfer of data outside of the EEA, the Master Data Protection Agreement employs the EU SCCs as the method of transfer.

Our approach to international data transfer mirrors the way SAP works internally, consistent with SAP's move into the Cloud and towards the Internet of Things and other new technologies. Teams are spread across SAP locations, and shared services are no longer provided only by central SAP entities. In short, SAP has adopted collaborative structures, which effectively reflect the needs of providing services to our customer base in the most effective way. Therefore, SAP's data processing capabilities are growing in Europe, the U.S. and various other countries. As a company that is headquartered in Europe but operates globally, we have an advantage due to our large cloud capacities in Europe, North America, Asia and other regions. That gives us the possibility to offer local services, and we always strive to offer services to customers based on local laws and regulations.

Listening to our customers, at SAP we have realized that there is more and more demand to verify where, how and by whom data – in particular personal data – is accessed and processed. We see more and more customers require that personal data is not transferred to or accessed from outside the EU. In light of this demand, SAP has extended many of its service, support, development and maintenance offerings and offers its European customers the choice to have their data processed within the EU, the European Economic Area (EEA), and Switzerland. This includes selected Cloud services where data is hosted in those countries but also on premise installations, remote access to which is performed out of EU locations only.

Data Security measures and breach notification

The GDPR introduces a general data breach-reporting obligation. Any business that suffers a data breach will be subject to the new reporting requirements under the GDPR. While controllers take the primary burden of reporting data breaches to authorities and individuals, processors also need to inform controllers of the occurrence of a data breach. The GDPR also introduces a direct obligation on the processor to implement appropriate security measures.

The security standards provided by SAP for both on-premise and cloud software are among the most stringent in the industry. SAP's security strategy follows a holistic approach that focuses on processes, technology, and people. Security recommendations, regular security checks, and continuous monitoring constitute the pillars of this strategy. All of SAP's activities are based on an efficient and effective information security system, and routine measures are carried out to raise employees' awareness of related topics.

Our technologies and processes are designed to protect computers, networks and data from general cyber threats (such as unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals). SAP, in addition, needs to focus on security of business applications as these provide the fundamentals for our customers' core business processes.

Security remains a neck-and-neck race between hackers and software vendors and cloud service providers. SAP has a long tradition of clearly understanding its customers' expectations in the context of confidentiality, integrity, and availability when customers entrust their business to SAP software systems and services. Customers can rely on the fact that SAP constantly monitors the evolution of the threat landscape, adjusting countermeasures to mitigate evolving threats. At the core of these countermeasures, SAP has defined and implemented a company-wide strategy to systematically counter risks to information security our customers' might be facing which is based on three pillars: "Prevent– Detect – React":

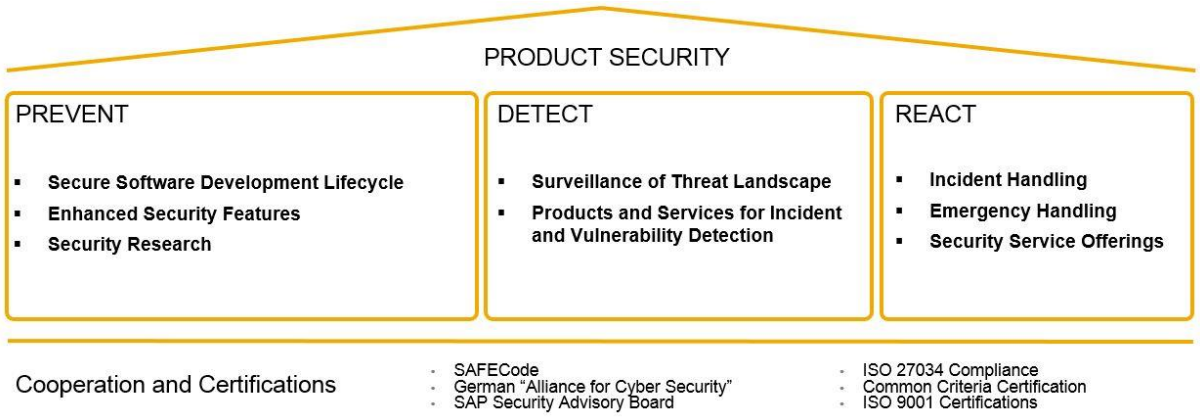


Figure: SAP Product Security Strategy

The "Prevent" pillar encompasses all measures that are put in place from the very beginning of product's lifecycle. Baking security in from the first thought about a product has been proven to be the most effective way to ensure a high security level.

Within the "Detect" part of the security strategy, SAP focuses on an early detection of deviations from what has been defined within the security framework laid out in the "Prevent" section. This includes, but is not limited to, an ongoing analysis of the threat landscape outside of SAP to prepare for adequate countermeasures. It also comprises technical measures such as a dedicated application to continuously monitor an entire system landscape for harmful events.

At the core of the "React" pillar, SAP has set-up a mature organization to immediately react upon and professionally manage security incidents. It includes all relevant measures to inform and protect SAP's customers. Security is a joint effort. And with regard for personal data related incidents, Security works closely together with the relevant governance teams including DPP to ensure fast mitigations and also inform a customer without undue delay if an incident in the customer's system is recognized. This enables the customer to check on his own notification requirements as early as possible.

SAP joins forces with computer emergency response teams of governments and other global players to be able to exchange information on attacks as quickly as possible.

Employee data protection awareness and education

Making employees aware of what is expected of them in this domain helps build a culture that value protecting of personal data. Ongoing privacy education and awareness training gives all employees access to the information needed to recognize and properly handle personal information, on a day-to-day basis. The entire SAP workforce worldwide receives a data protection and information security-focused training covering all business and staff units. Our efforts go a long way to help raising raise awareness of and sensitivity to privacy and data protection throughout the company. We provide educational papers, internal websites, easy to digest presentations to our employees. In addition, SAP is focused on raising security awareness in the company and we have introduced a set of target group-specific mandatory security training for all employees.

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

Revision Table:

Version 1.0 2017-2-14	DPP