

Get ready for the new General Data Protection!

The new General Data Protection Regulation (GDPR) 2016/679 will come into force in Spring 2018.

Companies of all sizes that store and process the personal data of EU citizens have only very little time left in which to implement the data security guidelines and the extensive accountability obligations. Failing this, any breaches will be subject to massive fines of up to 20 million euros or up to four percent of annual sales.

What does this mean for companies?

The tier system of the new General Data Protection Regulation already provides for penalties of up to two percent of globally generated annual sales for processing procedures that are not correctly documented (Article 28). Upon a breach of data security, companies are obligated to inform the responsible authorities within 72 hours (Article 31).

According to the definition of the new regulation, it is already considered a breach of data protection where an employee gains access to data that he/she does not necessarily need to carry out his/her work. Further, companies must ensure that employees are able to recognise when their handling of personal data is in breach of any laws.

What actions must be taken by 2018?

First and foremost, all companies must examine in detail in which systems data affected by the legislation is stored.

As a second step, an in-house audit should clarify to what extent the company is able to reliably track and provide evidence of how this data is used if, for example, it leaves the system.

As a result of the ever-increasing complexity of IT environments, it is a great challenge for compa-

The new EU General Data Protection Regulation (GDPR) was released on 25 May 2016. Companies that process the personal data of EU citizens have two years from this date in which to adapt their processes, services and products to meet the requirements of the new data protection regulations. This also entails a duty to inform in the event of a breach of data protection, which is why the use of personal data must be reliably tracked and monitored. A breach of data protection is subject to heavy fines of up to 20 million euros or 4% of annual sales.

nies to track what data is stored in which systems and through which channels it could potentially be shared. ERP systems such as SAP contain and process copious amounts of personal data. Within this controlled IT environments the specifications of the new data protection guidelines can be implemented as part of the standard process if the applications are equipped with authorisation structures and audit logs.

Does this protect you?

No. For example, the SAP authorisation structures no longer apply as soon as data leaves the SAP environment.

As a result, there is no way to trace how the data is subsequently used and to what extent it may be misused. Within most companies, such data exports are performed on a daily basis without the employees being aware of the consequences. This concerns all commercial sectors.

A prerequisite is the introduction of an audit or logging solution that records who exports and forwards what kind of data and when. If available, an integration into a Governance Risk Compliance solution (GRC) is recommended so that notifications can be sent to the responsible parties in the event of a breach of the rules. Ideally the datasets have already been classified before being exported. Hence that mandatory regulations can be added to the personal data for its entire lifecycle, and downloads can be evaluated and handled in real time. The export of sensitive data is entirely prohibited, where necessary.

In addition, this increases the awareness of employees to the subject of data protection and alerts them to potential breaches. The additional introduction of a Rights Management System (RMS) helps to prevent breaches of data protection (Article 31) and to provide evidence of and monitor how the data is used outside the ERP system.

Moreover, the new regulation obligates companies to appoint a data protection officer, in individual cases even where they have less than 250 employees (Article 35ff).

The time has now come for the responsible parties to examine their security concept to ensure that it complies with the regulations that will apply in the future.

Get ready for GDPR with HALOCORE®

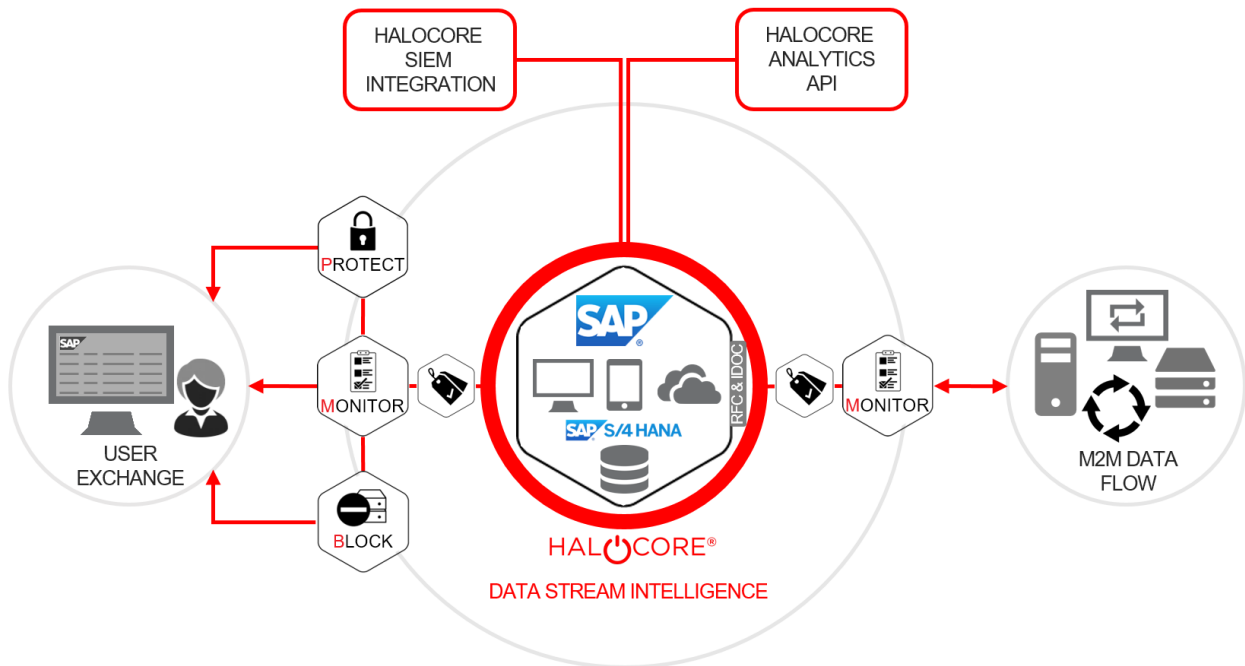
HALOCORE® is a unique solution for the protection of intellectual property and sensitive and personal data that is exported from SAP. HALOCORE® has a modular structure in order to guarantee effective protection within just a few days:

MONITOR: Complete transparency over SAP exports and “firefighter activities”. Automated implementation of compliance guidelines for SAP data exports with context-based classification. Alerting of compliance breaches and closing detection gaps in SAP Access Control (GRC).

HALOCORE® Data Stream Intelligence (HDSI) provides monitoring and classification of different types of data streams (RFC, IDOC etc.) between SAP systems and the connected satellite systems. Enterprises gain insights into the „invisible“ SAP application activities and significantly reduce their IT security risk.

BLOCK: Recognising and preventing sensitive SAP data from being leaked and used in a manner that is in breach of the rules. Control of unlawful data use with a context-based classification.

PROTECT: Encrypting SAP data exports with Microsoft Azure Information Protection (AIP / RMS) and sharing these across the company. Integration of completely customizable and safety-related classification features.



About SECUDE
 SECUDE is an international provider of innovative IT data protection solutions for SAP customers.
 The focus is on data confidentiality and protecting applications and access controls for IT resources, without impacting business processes and user friendliness. SECUDE solutions are trusted by many Fortune 500 and DAX companies.
 With locations in Europe, North America and Asia, SECUDE supports customers all over the world with the implementation of their IT security strategies.

GERMANY
 SECUDE GmbH
 Altrottstrasse 31
 69190 Walldorf
 T.: +49 6227 733 910
 F.: +49 6227 733 930

USA
 SECUDE Americas
 380 Sundown Drive
 Dawsonville, GA 30534
 T.: +1 (706) 215-3854

SWITZERLAND
 SECUDE International AG
 Werftstrasse 4A
 6005 Luzern
 T.: +41 61 366 30 00
 F.: +41 61 366 30 26

INDIA
 SECUDE Solutions India
 No. T2/6, Dr. V S I Estate
 Chennai - 600 041
 T.: +91 44 4297 5600