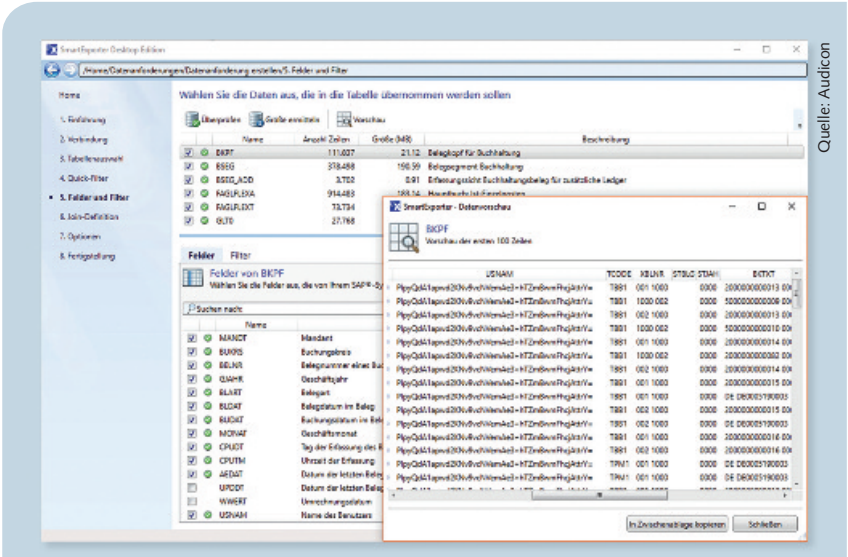
Umsetzung der DSGVO innerhalb eines SAP-Systems

Hat ein Unternehmen ein oder mehrere SAP-Systeme im Einsatz, sind die Vorgaben der DSGVO nicht nur bei der Arbeit im SAP-Umfeld zu beachten, sondern auch bei der Extraktion der Daten aus dem SAP-System, etwa für Datenanalysen. Die Unternehmen sind in der Pflicht, für eine entsprechende Einhaltung der Vorgaben zu sorgen.



Quelle: Audicon

Datenanforderungs-Belegköpfe – Vorschau der Belegköpfe mit AES-256-verschlüsselten Namen des Benutzers.

*Von Klaus van der Meulen**

Eine Wirtschaftsprüfungsgesellschaft benötigt im Rahmen der Abschlussprüfung einer Gesellschaft von diesem Mandanten die dem Prüfungsauftrag entsprechenden Daten. Doch die angeforderten Daten aus dem ERP-System enthalten regelmäßig auch personenbezogene Daten, etwa die Kennung des Erfassers einer Buchung. Die zum Schutz der Persönlichkeitsrechte vorgesehenen Prinzipien der DSGVO erfordern, dass der Mandant diese Daten jedoch nicht einfach so aus seinem SAP-System abziehen und klar lesbar zur Prüfung bereitstellen darf, sondern den Personenbezug entfernt oder unkenntlich macht.

Die Audicon-Software SmartExporter ermöglicht dem Endanwender nach der Einrichtung, Daten aus SAP ohne Hilfe der SAP-IT einfach zu extrahieren, so dass beispielsweise nachgelagerte Auditing-Tools, wie IDEA, Auswertungen auf Grundlage dieser Daten machen können. Ab der Version 2016 R1 bietet das Datenextraktions-Tool eine entsprechende Lösung an, mit der personenbezogene Daten bei der Extraktion aus SAP pseudonymisiert, verschlüsselt und anonymisiert werden können.

Der Mandant kann dementsprechend mit SmartExporter schon bei der Extraktion der Daten aus dem SAP-System ganz einfach definieren, welche Daten pseudonymisiert werden sollen. Wenn er die Daten seiner Wirtschaftsprüfungsgesellschaft zur Verfügung stellt, entspricht er damit vollumfänglich den Anforderungen der DSGVO. Darüber hinaus bietet SmartExporter auch die Möglichkeit, für statistische Zwecke Daten zu anonymisieren.

Verschlüsselung der SAP-Daten

Um sicherzustellen, dass ein Endanwender im Sinne der DSGVO keine oder so wenig personenbezogene Daten wie möglich erhält, kann in der Datenextraktionslösung SmartExporter der dafür autorisierte SAP-Administrator sogenannte Data-Privacy-Profile definieren. Mit Hilfe dieser Profile kann er granular bestimmen, welche Daten verschlüsselt

**Klaus van der Meulen ist Produktmanager für SmartExporter und Leiter der SmartExporter-Entwicklung bei Audicon.*

Pseudonymisierung nach DSGVO

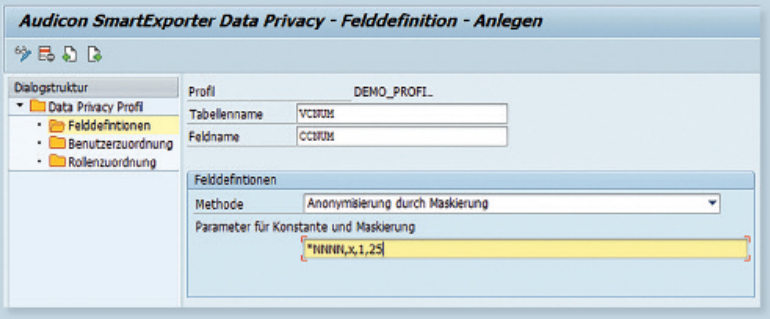
Die Autoren der DSGVO gehen in Artikel 4 auf die Begriffe Pseudonymisierung und Anonymisierung wie folgt ein:

Erwägungsgrund 26 „… Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. …

Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke."

DSGVO: Datenschutz wird Grundrecht

Mit der am 25. Mai 2018 in Kraft tretenden Datenschutzgrundverordnung – DSGVO – kommen auf Unternehmen weitreichende Änderungen zu. Denn mit der DSGVO erfährt das Datenschutzrecht in Deutschland mit dem bis dahin geltenden Bundesdatenschutzgesetz eine Weiterentwicklung. Während viele Grundsätze des BDSGs materiell und inhaltlich ihre Gültigkeit behalten, erfolgt durch die DSGVO in einigen Belangen eine Konkretisierung in anderen auch eine deutliche Verschärfung. So legt die DSGVO unter anderem fest, dass der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ein Grundrecht ist und erhöht die möglichen Strafen bei Verstößen. Die neuen Regelungen betreffen vor allem auch die automatisierte Verarbeitung der personenbezogenen Daten und sind daher für alle relevant, die datenführende IT-Systeme administrieren oder als Anwender nutzen.



Quelle: Audicon

Anlegen von Felddefinitionen zur Anonymisierung durch Maskierung in SmartExporter.

oder anonymisiert werden sollen. Verschiedene Verschlüsselungsalgorithmen wie beispielsweise AES-256 werden dabei unterstützt.

Der SAP-Administrator weist dazu einzelnen SAP-Benutzern oder -Rollen ein Profil zu, so dass automatisch bei der nächsten Extraktion durch den zugeordneten Benutzer die im Profil definierten Daten verschlüsselt oder anonymisiert werden. Profile können von den Endanwendern in den einzelnen Fachabteilungen bequem importiert und exportiert oder auch transportiert werden – der SAP-Administrator behält trotzdem die Kontrolle über die Vergabe der Berechtigungen.

Auch die Entschlüsselung ist möglich

SmartExporter bietet darüber hinaus mit der neuen Version 2018 R1 die Möglichkeit, dass autorisierte Personen verschlüsselte Daten wieder entschlüsseln können. Besteht bei einer Prüfung ein hinreichendes Interesse die Pseudonymisierung aufzuheben, zum Beispiel weil Unstimmigkeiten in den Daten einen konkreten Verdacht auf dolose oder trügerische Handlungen begründen, können die Daten in einem definierten Verfahren wieder entschlüsselt werden.

Mit der Entschlüsselungs-Transaktion ermittelt der Anwender nach Auswahl der ursprünglichen Datenanforderung den entsprechenden Schlüssel, um dann im Anschluss die Daten wieder entschlüsseln zu können. Zuletzt können dann für die weitere Bearbeitung die Daten als Datei gespeichert werden und so etwa bei einem Fraud-Verdacht eingehender geprüft werden.

Selbstverständlich sind alle SmartExporter-Data-Privacy-Transaktionen über entsprechende Zugriffsrechte geschützt. Um Missbrauch vorzubeugen, werden entsprechende Rollen zum Anzeigen und Ändern im Standard ausgeliefert – die vollständige Kontrolle über die Daten ist zu jedem Zeitpunkt gewährleistet.

Die Vorteile liegen auf der Hand:

- Der autorisierte SAP-Administrator hat die volle Kontrolle, welcher Benutzer welche Daten nur verschlüsselt sehen darf.
- Sensible Daten werden auf dem SAP-System während des Extraktionsprozesses möglichst früh verschlüsselt, so dass der Endanwender keine Möglichkeit der Manipulation hat, um sensible Daten in klar lesbarer Form zu sehen. *(cr)* @