Business News

DOAG Zeitschrift für die Anwender von Oracle Business- und BI-Lösungen

BS

EU-Datenschutz-Grundverordnung

Sommer 2018 | ISSN 09 36-0360 | http://bs.doag.org


Early Bird
bis zum
28. Sep.
2018
DOAG
Konferenz + Ausstellung
20. - 23. November
in Nürnberg
2018.doag.org
Eventpartner:
AOUG
SOUG
swiss oracle user group
iJUG
Verbund
ORACLE

Dirk Blaurock
DOAG Themenverantwortung
Oracle Applications Management

Liebe Leserinnen und Leser,
die neue EU-Datenschutz-Grundverordnung „General Data Protection Regulation" (GDPR) ist in aller Munde. Sie gilt für alle Unternehmen in der EU sowie für Unternehmen im Ausland, die für Unternehmen in der EU Personendaten bearbeiten oder für sich selbst Daten von Personen in der EU nutzen. Umzusetzen ist diese Verordnung bis zum 25. Mai 2018.

Auch wenn in dieser Verordnung nicht alles neu ist – sie ersetzt eine EU-Verordnung von 1995 –, so sind einige Punkte in dieser Verordnung extrem verschärft, etwa das „right to be forgotten" bezogen auf das Löschen/Anonymisieren von personengebunden Daten, oder der Grundsatz „data protection by default", der die datenschutzkonforme Nutzung im Anwendungsdesign verankert. Die Verordnung selbst ist sehr generisch und lässt einen großen Interpretationsspielraum zu, was die eigentliche Herausforderung der Umsetzung ist.

Bei Business Software wie aus dem Hause Oracle ist eine Unterstützung des Herstellers notwendig – seien es Installationen in eigenen Rechenzentren oder Cloud-Lösungen – die Verordnung muss durch die Software unterstützt werden. Europäische Anbieter wie SAP sind hier weiter als amerikanische Anbieter wie Oracle. Von SAP gibt es Praxispapiere für die Sicherstellung der Konformität, von Oracle Technologie-Whitepaper, wie mit dem Oracle-Toolset eine Datenbank konform gemacht werden kann. Es fehlen jedoch bei Oracle Anweisungen/Best Practices zu den eigenen Business-Software-Lösungen, etwa dazu, wie das „right to be forgotten" für eine Oracle E-Business Suite oder JD-Edwards-Installation umgesetzt werden kann. An einem von mir erstellten Enhancement Request bei Oracle kann man gut sehen, dass ein Interesse der Kunden da ist. Innerhalb von einem Monat wurde dieser von vielen Community-Teilnehmern positiv bewertet.

In diesem Heft haben wir Beitrage zum Thema „GDPR" zusammengestellt, um Ihnen und Ihrem Unternehmen einen zusammenfassenden Eindruck der Konsequenzen darzustellen.

Ich wünsche Ihnen viel Spaß beim Lesen und viel Erfolg bei der Umsetzung,

Ihr

Dirk Blaurock

Impressum

DOAG Business News wird von der DOAG Deutsche ORACLE-Anwendergruppe e.V. (Tempelhofer Weg 64, 12347 Berlin, www.doag.org), herausgegeben. Es ist das User-Magazin rund um die Applikations-Produkte der Oracle Corp., USA, im Raum Deutschland, Österreich und Schweiz. Es ist unabhängig von Oracle und vertritt weder direkt noch indirekt deren wirtschaftliche Interessen. Vielmehr vertritt es die Interessen der Anwender an den Themen rund um die ORACLE-Produkte, fördert den Wissensaustausch zwischen den Lesern und informiert über neue Produkte und Technologien.

DOAG Business News wird verlegt von der DOAG Dienstleistungen GmbH, Tempelhofer Weg 64, 12347 Berlin, Deutschland, gesetzlich vertreten durch den Geschäftsführer Fried Saacke, deren Unternehmensgegenstand Vereinsmanagement, Veranstaltungsorganisation und Publishing ist.

Die DOAG Deutsche Oracle-Anwendergruppe e.V. hält 100 Prozent der Stammeinlage der DOAG Dienstleistungen GmbH. Die DOAG Deutsche Oracle-Anwendergruppe e.V. wird gesetzlich durch den Vorstand vertreten; Vorsitzender: Stefan Kinnen. Die DOAG Deutsche Oracle-Anwendergruppe e.V. informiert kompetent über alle Oracle-Themen, setzt sich für die Interessen der Mitglieder ein und führen einen konstruktiv-kritischen Dialog mit Oracle.

Redaktion:
Sitz: DOAG Dienstleistungen GmbH
(Anschrift s.o.)
Chefredakteur (ViSdP): Wolfgang Taschner
Kontakt: redaktion@doag.org
Weitere Redakteure: Lisa Damerow, Mylène Diacquenod, Marina Fischer, Andreas Schmidt, Fried Saacke, Rolf Scheuch, Dr. Frank Schönthaler

Druck:
adame Advertising and Media GmbH, Berlin, www.adame.de

Fotonachweis:
Titel: © tanaonte/123RF
S. 5: © limbi007/123RF
S. 8+9 Grafiken: freepik.com
S. 14: © everythingpossible/123RF
S. 17: © Bakhtiar Zein/123RF
S. 22: © Sergei Polivanov/123RF
S. 25: © Sebastien Decoret/123RF

Titel, Gestaltung und Satz:
Alexander Kermas,
DOAG Dienstleistungen GmbH
(Anschrift s.o.)

Anzeigen:
Simone Fischer, DOAG Dienstleistungen GmbH
(verantwortlich, Anschrift s.o.)
Kontakt: anzeigen@doag.org

Mediadaten und Preise unter: www.doag.org/go/mediadaten

Zehn-Punkte-Plan für die neuen Regelungen der DSGVO

Die EU-Datenschutz-Verordnung aus Oracle-Sicht

Der Datenbank-Administrator kann mit seinem Know-how bei der Umsetzung der DSGVO unterstützen

Unsere Inserenten

Anforderungen und Umsetzung der EU-Datenschutz-Grundverordnung

Rechtsanwalt Dr. Carsten Ulbricht, Bartsch Rechtsanwälte

Ab 25. Mai 2018 gilt europaweit die europäische Datenschutz-Grundverordnung (DSGVO) und löst damit das bisher in Deutschland für den Datenschutz geltende Bundesdatenschutz-Gesetz (BDSG) ab. Im Zusammenwirken mit den Änderungen im nationalen Gesetz durch das BDSG-neu sorgt die Umsetzung der DSGVO wegen der erheblich erhöhten Bußgelder bei zahlreichen Unternehmen derzeit für viel Verunsicherung. Der Artikel erläutert die neuen Anforderungen in möglichst kompakter Form und fasst die wesentlichen Maßnahmen in einem Zehn-Punkte-Plan zusammen.

Mit der Datenschutz-Grundverordnung will die Europäische Union (EU) ein gleich hohes Datenschutz-Niveau innerhalb der EU-Staaten schaffen, die Kontrolle und Transparenz der Verarbeitung personenbezogener Daten stärken und den bisherigen Datenschutz- und Vollzugs-Defiziten durch erheblich erhöhte Bußgelder entgegenwirken. Soweit noch nicht geschehen, sollten die eigenen Datenverarbeitungsvorgänge unmittelbar analysiert und die neuen Anforderungen der DSGVO im Hinblick auf den verbindlichen Stichtag des 25. Mai 2018 unverzüglich umgesetzt werden. Unternehmen, die dies versäumen, riskieren sonst tatsächlich eine Verhängung empfindlicher Bußgelder.

Mit Umsetzung und Dokumentation der nachfolgend erläuterten Maßnahmen lassen sich die wesentlichen Anforderungen jedoch gut erfüllen. Zur leichteren Umsetzung hat die Kanzlei des Autors eine Vielzahl konkreter Hinweise, Checklisten und Musterdokumente zusammengestellt, die dabei helfen sollen, noch rechtzeitig DSGVO-compliant zu werden.

Was die EU-Datenschutz-Grundverordnung regelt

Die DSGVO regelt den Schutz personenbezogener Daten im Sinne von Artikel 4, Absatz 1 DSGVO. Nach dessen Definition sind personenbezogene Daten sämtliche Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung – wie einem Namen, einer Kennnummer, Standort-Daten, einer Online-Kennung oder einem oder mehreren besonderen Merkmalen – identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Nach dieser Definition sind also all die Informationen als personenbezogen anzusehen, die sich über die dem Unternehmen oder Dritten vorliegende Kenntnisse einer natürlichen Person zuordnen lassen. Typische personenbezogene Daten sind daher:

- Name
- Wohnadresse
- Geburtsdatum
- E-Mail-Adresse (auch geschäftliche E-Mail-Adressen wie „vorname.nachname@firma.de")
- Telefonnummer
- Eigenschaften einer Person
- Kundennummer
- Vollständige IP-Adresse
- Online-Kennungen, die eine Zuordnung zu einer Person ermöglichen

Der Anwendungsbereich der DSGVO ist sehr weit gefasst. Sobald ein Unternehmen solche personenbezogenen Daten erhebt, speichert oder verarbeitet, sind die Vorgaben der DSGVO für diese Verarbeitungsvorgänge zu beachten. Ansonsten kann die Verletzung der DSGVO empfindliche Bußgelder nach sich ziehen. Je nach Schwere des Verstoßes können die Aufsichtsbehörden bis zu zwanzig Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes als Bußgeld verhängen. Für leichtere Verstöße ist ein

Bußgeld von maximal zehn Millionen Euro oder von zwei Prozent des weltweiten Jahresumsatzes vorgesehen.

Rechtmäßigkeit

Die DSGVO sieht für die Verarbeitung personenbezogener Daten das sogenannte „Verbotsprinzip" vor. Das bedeutet, dass eine Datenverarbeitung grundsätzlich verboten ist, wenn die konkrete Verarbeitung nicht ausdrücklich von der DSGVO gesetzlich erlaubt wird oder auf der informierten Einwilligung der betroffenen Person beruht.

Soweit im Unternehmen nicht bereits ein Verfahrensverzeichnis als Übersicht über die eigenen Verarbeitungsvorgänge vorliegt, sollten im Rahmen einer Bestandsaufnahme die Vorgänge und Prozesse im Unternehmen zusammengestellt werden, bei denen personenbezogene Daten erhoben, gespeichert und verarbeitet werden. Personenbezogene Daten dürfen im Rahmen dieser Vorgänge und Prozesse zukünftig nur verarbeitet werden, wenn eine der Voraussetzungen des Artikels 6 DSGVO die jeweilige Verarbeitung ausdrücklich legitimiert. Gemäß diesem dürfen Unternehmen in folgenden Fällen Daten verarbeiten:

- Die Daten sind zur Erfüllung eines Vertrags oder einer vorvertraglichen Maßnahme erforderlich
- Der Betroffene willigt auf Grundlage einer informierten Aufklärung ein
- Die Daten werden zur Erfüllung einer rechtlichen Verpflichtung benötigt
- Die Datenverarbeitung ist zur Wahrung berechtigter Interessen des Unternehmens oder eines Dritten erforderlich und die Interessen der betroffenen Person überwiegen nicht

Nach der Bestandsaufnahme sollten Unternehmen für die eigenen Datenverarbeitungsvorgänge (wie E-Mail-Marketing) also prüfen, unter welchem der Legitimations-Tatbestände die jeweilige Verarbeitung (etwa beim E-Mail-Marketing über eine Einwilligung) legitimiert werden kann. Dabei genügt es, wenn die jeweilige Datenverarbeitung unter einen der Legitimations-Tatbestände fällt.

Informationspflicht

Die EU-DGSVO sieht im Interesse der Transparenz der eigenen Datenverarbeitung sehr weitreichende Informationspflichten der Unternehmen vor. Je nachdem, ob die personenbezogenen Daten beim Betroffenen (Artikel 13 DSGVO) oder anderweitig (Artikel 14 DSGVO) erhoben werden, ist der Betroffene gemäß den gesetzlichen Vorgaben zu informieren. Deshalb ist die betroffene Person – in der Regel schon bei der Erhebung – darüber zu informieren, welche Daten das Unternehmen für welchen Zweck verarbeitet, an welche Stellen es die Daten weitergibt oder ob eine Weitergabe beabsichtigt ist. Zudem gibt es umfangreiche Betroffenenrechte (wie Informationspflichten, Auskunftsrechte, Recht auf Berichtigung der Daten, Widerspruchsrecht), über die die Person ebenfalls zu informieren ist. So ist zum Beispiel für die eigene Webseite beziehungsweise dort stattfindende Erhebungsvorgänge (wie Vertragsschluss, Kontaktformular, Drittanbieter-Werkzeuge) in jedem Fall sicherzustellen, dass die eigene Datenschutzerklärung den differenzierten Anforderungen des Artikels 13 DSGVO genügt.

Technischer Datenschutz

Die DSGVO verknüpft den Datenschutz sehr stark mit der Technik. Deshalb sind bei der Verarbeitung personenbezogener Daten auch konkrete Anforderungen an die Datensicherheit zu erfüllen. IT-Verfahren müssen zudem schon von Anfang an darauf ausgerichtet sein, möglichst wenig personenbezogene Daten verarbeiten zu können (Privacy by Design/Privacy by Default).

Weitergabe von Daten an Dritte

Zur Anpassung der Datenschutz-Organisation an die neuen Anforderungen der DSGVO gehört es dann auch, bestehende Vertragsverhältnisse auf etwaige Änderungen, die durch die DSGVO erforderlich werden, zu prüfen. Dies gilt allem voran für Verträge zur Auftragsdatenverarbeitung nach § 11 BDSG. Diese dient nach aktueller Rechtslage als Konstruktion, um die Weitergabe personenbezogener Daten seitens eines Verantwortlichen (nachfolgend Auftraggeber) an Dienstleister (nachfolgend Auftragnehmer) innerhalb des europäischen Wirtschaftsraumes datenschutzrechtlich zulässig zu gestalten.

Typische Konstellationen, bei der die Weitergabe an einen Dienstleister über eine Auftragsverarbeitung legitimiert wird, sind die Speicherung von personenbezogenen Daten bei einem Dritten (etwa Kundendaten in der Oracle Marketing Cloud) oder aber auch die Weitergabe an einen E-Mail-Dienstleister (wie MailChimp).

Soweit das Unternehmen also einen Teil der (eigenen) Datenverarbeitung an Dritte ausgelagert hat, sind die mit dem jeweiligen Dienstleister nach § 11 BDSG geschlossenen Verträge zur Auftragsdatenverarbeitung an die neue Rechtslage anzupassen. Diese findet sich in den Artikeln 28 und 29 DSGVO, die den § 11 BDSG ablösen werden. Die DSGVO spricht dann auch nicht mehr von Auftragsdatenverarbeitung, sondern von Auftragsverarbeitung.

Fortan wird also ein entsprechender Auftragsverarbeitungsvertrag nach Artikel 28 Absatz 3 Seite 1 DSGVO die Weitergabe von personenbezogenen Daten legitimieren, ohne dass ein Erlaubnis-Tatbestand nach Artikel 6 Absatz 1 DSGVO vorliegen müsste oder die Einwilligung der betroffenen Person eingeholt worden ist. Auch an dieser Stelle zeigt sich also, dass mit der DSGVO keine komplette Neuregelung verbunden ist, sondern lediglich die auch bisher schon nach dem BDSG geltende Rechtslage an die DSGVO anzupassen ist. Unternehmen können daher ihren bisherigen Vertrag zur Auftragsdatenverarbeitung nach § 11 BDSG weiter nutzen, haben diesen aber sowohl inhaltlich als auch an die teils geänderten Begrifflichkeiten anzupassen.

Mitverantwortung des Auftragsverarbeiters

Eine wesentliche Änderung ergibt sich aus der Entscheidung des europäischen Gesetzgebers, auch den Auftragsverarbeiter, den Auftragnehmer, stärker in die Pflicht zu nehmen und ebenfalls zur Einhaltung des Datenschutzes – mit entsprechender Haftungsfolge (siehe unten) – zu verpflichten. Während nach dem BDSG noch ausschließlich der Auftraggeber als „Herr der Daten" alleine für die Datenverarbeitung und damit für die Einhaltung eines ausreichenden Datenschutzstandards verantwortlich war, finden sich in der DSGVO zahlreiche Verpflichtungen, die sich auch an den Auftragsverarbeiter richten. Diese Verpflichtungen sind in die bisherigen Verträge zur Auftragsdatenverarbeitung zu integrieren, um diese DSGVO-konform zu gestalten. So ist nach Artikel 30 Absatz 2 DSGVO auch der Auftragsverarbeiter, der Auftragnehmer, zur Führung von Verfahrensverzeichnissen verpflichtet.

Nach Artikel 32 Absatz 1 DSGVO trifft die Pflicht zu technischen und organisatorischen Maßnahmen der Datensicherheit nicht nur den Auftraggeber, sondern auch den Auftragsverarbeiter. Nach Artikel 37 Absatz 1 DSGVO hat auch der Auftragsver-

arbeiter – sofern die weiteren gesetzlichen Voraussetzungen vorliegen – einen Datenschutzbeauftragten zu bestellen. In Konsequenz ergibt sich aus Artikel 82, dass jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, Schadensersatzansprüche sowohl gegen den Auftraggeber als auch gegen den Auftragsverarbeiter, den Auftragnehmer, geltend machen kann.

Allerdings bestehen zugunsten des Auftragsverarbeiters, der auf Weisung des Auftraggebers handelt und für den nur einige Verpflichtungen nach der DSGVO greifen, Entlastungs-Tatbestände, die sich in Artikel 82 Absatz 2 DSGVO wiederfinden. So haftet ein Auftragsverarbeiter für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er einer speziell den Auftragsverarbeitern auferlegte Pflicht aus der DSGVO nicht nachgekommen ist oder wenn er ihm rechtmäßig erteilte Weisungen des Auftraggebers missachtet hat. Nach Artikel 82 Absatz 3 DSGVO ist ihm ebenfalls der Nachweis gestattet, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Begleitet wird dieser Schadensersatzanspruch der betroffenen Person auch durch Bußgelder, die wiederrum die Datenschutzbehörden nach den Artikeln 83 Absatz 3 und Absatz 4 a) DSGVO gegen den Auftragsverarbeiter verhängen können.

Rechenschaftspflicht

Das datenverarbeitende Unternehmen ist schließlich für die Einhaltung der Vorgaben der DSGVO verantwortlich und muss die Einhaltung aller zuvor genannten Datenschutz-Prinzipien nachweisen können. Dazu ist eine entsprechende Dokumentation notwendig, deren Umfang aber von der Größe des Unternehmens beziehungsweise der Menge und der Qualität der personenbezogenen Daten abhängig gemacht werden kann.

Um sich einen Überblick über die eigenen Datenverarbeitungstätigkeiten zu verschaffen, sollten Unternehmen zunächst eine Bestandsaufnahme über die Vorgänge und Prozesse machen, bei denen personenbezogene Daten erhoben, gespeichert und verarbeitet werden (nachfolgend Verarbeitungstätigkeiten). Diese Bestandsaufnahme dient im weiteren Verlauf als wichtiger Schritt, um den Umsetzungsbedarf zu analysieren. Zunächst sollte also ermittelt und festgehalten werden, im Rahmen welcher Vorgänge und Prozesse solche personenbezogenen Daten erhoben, gespeichert und verarbeitet werden. Typische Verarbeitungstätigkeiten sind etwa:

- Webseite
- Onlineshop
- Kunden-Datenverarbeitung
- Personal-Management
- Bewerber-Management
- Video-Überwachung

Im Rahmen der Bestandsaufnahme sollte jeder Verarbeitungsvorgang zunächst mit einer allgemeinen Beschreibung, Informationen über Art und Zweck der Verarbeitung, Informationen über die verarbeiteten Daten-Kategorien (wie Beschäftigtendaten) und einer Übersicht der betroffenen Personen (etwa die Mitarbeiter) schriftlich zusammengefasst werden.

In der Regel werden die wesentlichen Datenverarbeitungsvorgänge mit einem Verarbeitungsverzeichnis erfasst, in dem auch die Erfüllung der weiteren datenschutzrechtlichen Anforderungen (etwa Legitimations-Tatbestand, Erfüllung der Informationspflichten) abgeprüft und dokumentiert werden können.

Zehn Punkte zur Umsetzung der EU-DSGVO

Mit dem nachfolgenden Maßnahmenplan werden die wesentlichen Neuregelungen der Datenschutz-Grundverordnung umgesetzt.

01 „Organisatorische Maßnahmen“

Unternehmen sollten prüfen, ob sie organisatorisch hinreichend für die DSGVO aufgestellt sind. Soweit nicht bereits ein Datenschutzbeauftragter bestellt ist, sollte geprüft werden, ob eine Bestellung nicht zwingend ist. Eine Pflicht zur Bestellung eines Datenschutzbeauftragten besteht in folgenden Fällen:

- Wenn zumindest zehn Mitarbeiter regelmäßig mit automatisierter Datenverarbeitung (Erhebung und Nutzung) zu tun haben
- Wenn personenbezogene Daten verarbeitet werden, die über Rasse, ethnische Herkunft, politische Meinung, religiöse Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben einer Person informieren
- Wenn personenbezogene Daten geschäftsmäßig übermittelt, erhoben, verarbeitet oder genutzt werden

Zudem sollten Geschäftsleitung und Mitarbeiter rechtzeitig über die konkreten Folgen der DSGVO und die konkreten Maßnahmen zur Umstellung informiert werden.

02 „Bestandsaufnahme durchführen“

Unternehmen sollten zunächst die beschriebene Bestandsaufnahme bezüglich aller Vorgänge und Prozesse (nachfolgende Verarbeitungstätigkeiten) durchführen, bei denen personenbezogene Daten erhoben, verarbeitet oder weitergegeben werden. Auf Grundlage der Bestandsaufnahme sollte der konkrete Änderungsbedarf identifiziert werden.

03 „Rechtsgrundlagen prüfen“

Es ist zu prüfen, ob die identifizierten Datenverarbeitungsprozesse den Anforderungen der DSGVO, insbesondere den Rechtmäßigkeitsanforderungen des Artikels 6 DSGVO, entsprechen. Ansonsten sind die Prozesse den neuen Anforderungen anzupassen.

04 „Informationspflichten erfüllen“

Die weitreichenden Informationspflichten (Artikel 13 und 14 DSGVO), die teilweise neue Anforderungen enthalten (wie Nennung der Legitimations-Grundlage, Information über Beschwerde-Recht bei Aufsichtsbehörde), sind in den internen Dokumenten (wie Kundenverträgen) und Prozessen umzusetzen.

05 „Datenschutz- und Einwilligungserklärungen umstellen“

Etwaige Datenschutz-Erklärungen (etwa auf der Webseite) oder Einwilligungserklärungen (wie für die Zusendung von E-Mail-Werbung) sind mit Hinblick auf die neuen Anforderungen (insbesondere die Informationspflichten aus Artikel 13 DSGVO) anzupassen.

06 „(Verträge über) Datenweitergabe checken“

Unternehmen sollten bei der Weitergabe von personenbezogenen Daten prüfen, auf welcher Rechtsgrundlage diese Weitergabe erfolgt. In Fällen einer Weitergabe oder Offenlegung personenbezogener Daten an Dritte zur Verarbeitung im Auftrag des Unternehmens sollten Vereinbarungen über eine Auftragsverarbeitung im Sinne des Artikels 28 DGSVO geschlossen beziehungsweise bestehende Verträge zur Auftrags(-daten-)verarbeitung überprüft und nötigenfalls überarbeitet werden.

07 „Datensicherheit umsetzen“

Die Anforderungen, die die DSGVO (etwa bezüglich Software) schon bei der Technikgestaltung und zu den Voreinstellungen (Artikel 25 DSGVO) stellt, sind umzusetzen.

08 „Datenschutzfolgen-Abschätzung durchführen“

Unternehmen haben im Rahmen einer Datenschutzfolgen-Abschätzung (Artikel 35 DSGVO) zu prüfen, ob die eigenen Datenverarbeitungsvorgänge aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge haben. Das Ergebnis und etwaige Maßnahmen zur Reduzierung eines möglichen Risikos sind zu dokumentieren.

09 „Betroffenenrechte umsetzen“

Die in der DSGVO geregelten Betroffenenrechte (wie Recht auf Auskunft oder Recht auf Löschung) müssen in den unternehmensinternen Abläufen so abgebildet sein, dass diese gegenüber den Betroffenen umgesetzt werden können.

10 „Dokumentation organisieren“

Aufgrund der vermehrten Dokumentationspflichten der DSGVO (wie Artikel 30, 33 Absatz 5, 28 Absatz 3 lit. a) DSGVO) sollte das Unternehmen die notwendige Dokumentation (etwa in Form eines Verarbeitungsverzeichnisses) organisieren.

Die weiteren Anforderungen der e-Privacy-Verordnung

Die e-Privacy-Verordnung, deren Auswirkungen bereits intensiv diskutiert werden, liegt derzeit nur im Entwurf vor. Dieser sieht einige weitreichende Änderungen bezüglich der Verarbeitung elektronischer Kommunikationsdaten, der Speicherung von Informationen in Endeinrichtungen (wie Cookies), aber auch im Bereich des Direkt-Marketings vor.

Derzeit ist noch unklar, inwieweit an dem Verordnungstext noch Änderungen vorgenommen werden beziehungsweise wann die e-Privacy-Verordnung wirksam werden soll. Aufgrund politischer Diskussionen und der Notwendigkeit weiterer Abstimmungen im Rahmen des Gesetzgebungsverfahrens ist nach den aktuellen Informationen davon auszugehen, dass die e-Privacy-Verordnung nicht vor dem Jahr 2019 Wirkung entfalten wird.

Dr. Carsten Ulbricht
carsten.ulbricht@bartsch.law

Critical Patch Update April 2018

Oracles neuestes Critical Patch Update schließt 251 Sicherheitslücken bei Hunderten von Oracle-Lösungen. Einige der angesprochenen Sicherheitslücken betreffen mehrere Produkte. Die meisten Sicherheitslücken liegen bei Fusion Middleware (40), Oracle Financial Services Applications (36), MySQL (33) und Retail Applications (31). Aufgrund der Bedrohung durch einen erfolgreichen Angriff empfiehlt Oracle seinen Kunden dringend, die Critical Patch Update Fixes so schnell wie möglich anzuwenden. Eine komplette Liste der betroffenen Produkte ist auf der Website *„http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html“* abrufbar. Oracle veröffentlicht alle drei Monate ein Critical Patch Update. Die nächsten Termine sind 17. Juli 2018, 16. Oktober 2018 und 15. Januar 2019.

DSGVO – fünf Buchstaben, die Arbeit machen

Carsten J. Diercks, Rechtsanwalt, Politikberater und langjähriger rechtlicher Berater der DOAG

Vom 25. Mai 2018 und seiner Bedeutung für den Datenschutz haben alle bereits gehört. Der Artikel zeigt die gravierenden Änderungen im gewohnten Umgang mit Datenschutz und Datensicherheit auf, die sich durch die neuen Regelungen der Datenschutzgrundverordnung DSGVO ergeben.

Diesmal kann man kaum behaupten, von einer europäischen Regelung überrascht worden zu sein. Die Regierungen der Mitgliedsstaaten im Rat der EU und das Europäische Parlament waren großzügig bei der Bemessung einer Übergangszeit. Bereits seit dem 24. Mai 2016 ist die „Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG" (DSGVO, englisch GDPR) in Kraft. Am 25. Mai 2018 kommen die Regelungen nun zur Anwendung. Auf Grundlage der in den 1980er-Jahren entstandenen datenschutzrechtlichen Bestimmungen wurde im Jahr 1995 eine erste Generation europäischer Regelungen geschaffen. Nach zwanzig Jahren und angesichts eines gravierend veränderten Umfelds in Technik und Gesellschaft sowie durch Globalisierung war eine Neuregelung notwendig. Zwar ist mit der DSGVO nicht der große Wurf einer wirklichen Reform gelungen, es ergeben sich aber erhebliche Änderungen in der Grundkonstruktion.

DSGVO: europaweit für alle Akteure geltend

Die DSGVO gilt als Verordnung unmittelbar in allen Mitgliedsstaaten der Europäischen Union für datenverarbeitende Behörden und Unternehmen. Eine Umsetzung in den nationalen Rechtsordnungen ist nicht erforderlich. Sie bildet die neue Basis für den Datenschutz und weist starke Bezüge auch zur Datensicherheit auf. Allerdings sind die 99 Artikel und 173 Erwägungsgründe nicht gänzlich abschließend – sie lassen Raum für die Mitgliedsstaaten, diesen auszufüllen und teils auch eigene Regelungen zu treffen. Das Bundesdatenschutzgesetz wird daher daneben als „BDSG-neu" mit reduziertem Anwendungsbereich fortbestehen; ebenso die Landesdatenschutzgesetze und einige spezialgesetzliche Regelungen – so ist etwa der Beschäftigtendatenschutz weiterhin in nationaler Kompetenz.

Am Horizont ist bereits die nächste Regelung erkennbar, die nicht nur zu erheblichen politischen Diskussionen führen, sondern auch für die Wirtschaftswelt Herausforderungen bringen wird: die e-Privacy-Richtlinie, die die EU-Datenschutzrichtlinie für die elektronische Kommunikation 2002/58/EG ablösen soll und sich beispielsweise auf Cookie-Anwendungen bezieht.

Dies vorausgeschickt, ergibt sich eine im Wesentlichen einheitliche Rechtsordnung in den 28 – und ab 30. März 2019 voraussichtlich 27 – Mitgliedsstaaten. Zwar bleibt es bei nationalen Behörden, komplexe Kooperations- und Kohärenz-Mechanismen sorgen jedoch für eine einheitliche Rechtsanwendung insbesondere bei grenzüberschreitender Datenverarbeitung.

Hat ein Unternehmen mehrere Sitze in der Europäischen Union, ist die Aufsichtsbehörde am Hauptsitz des Unternehmens zuständig, die die Aufsichtsbehörden der anderen Mitgliedsstaaten erforderlichenfalls einbindet. Damit gibt es einen „one stop shop"-Mechanismus, der nicht nur für in der EU ansässigen Unternehmen gilt, sondern auch für nicht ansässige. Es herrscht fortan das Marktort-Prinzip. Die DSGVO gilt also nicht nur für Unternehmen mit einer Niederlassung in der EU, die auch aus einem Briefkasten bestehen kann, sie gilt ebenso für Unternehmen ohne Niederlassung, die Daten von Personen, die sich in der Europäischen Union aufhalten, zum Vertrieb von Waren und Dienstleistungen oder Beobachtung von Verhalten verarbeiten. Anders gesagt, jedes Unternehmen, das in der EU künftig Daten verarbeitet, unterliegt der DSGVO.

Dabei ist zu bemerken, dass sich die DSGVO weiterhin nur auf personenbezogene Daten bezieht; Unternehmens- oder Maschinendaten sind nicht betroffen. Personenbezogen sind alle Daten, die einer lebenden natürlichen Person zugeordnet werden können, sie also identifizierbar machen. Im Zweifel ist also eher von der Personenbezogenheit auszugehen. Im Zentrum aktueller Diskussionen dazu steht die Frage der Identifizierbarkeit bei Big-Data-Anwendungen. Generelle Aussagen sind dazu jedoch kaum möglich und jede Big-Data-Anwendung ist im Einzelnen zu betrachten.

Der risikobasierte Ansatz

Hinsichtlich der personenbezogenen Daten bleibt es bei dem aus dem deutschen BDSG bekannten Verbot der Verarbeitung personenbezogener Daten mit Erlaubnisvorbehalt. Eine Verarbeitung ist also nur möglich, wenn eine Einwilligung des Betroffenen vorliegt oder eine gesetzliche Regelung die Verarbeitung erlaubt. Die Änderungen ergeben sich hier im Detail: Die DSGVO setzt hier wesentlich mehr auf den sogenannten „risikobasierten Ansatz". An diversen Stellen der Verordnung wird eine Datenverarbeitung im Interesse des Verarbeiters erlaubt, wenn nicht Interessen des Betroffenen überwiegen. Dies führt zu einigen Änderungen, so entfallen das sogenannte „Listenprivileg" des BDSG oder die Regelungen zum Scoring. Letzteres wird in der DSGVO durch die De-

tail-Regelungen zum Profiling ersetzt, die jedoch nur anzuwenden sind, wenn eine Entscheidung mit rechtlicher Wirkung Ergebnis der Verarbeitung sein soll.

Von der DSGVO erfasst wird jede automatisierte Verarbeitung oder die Verarbeitung zur elektronischen Speicherung von personenbezogenen Daten. Ausgenommen sind nur die Verarbeitung zu persönlichen oder familiären Zwecken sowie der strafrechtliche Bereich der öffentlichen Verwaltung. Für den elektronischen Geschäftsverkehr gehen die Regelungen der Richtlinien RL 2000/31/EG und 2011/83/EG für Dienste-Anbieter bei der Durchleitung von Informationen, Zwischenspeicherung und Host-Provider vor. Es werden nicht mehr einzelne Verarbeitungsschritte differenziert, sondern einheitlich der Begriff der Verarbeitung benutzt. Zu den weiteren Begrifflichkeiten sei auf Artikel 4 der DSGVO verwiesen sowie bei den besonders zu schützenden sensiblen, personenbezogenen Daten auf Artikel 9 DSGVO, etwa bei biometrischen Daten, Gesundheitsdaten oder Daten zu politischen Meinungen.

Die DSGVO beschreibt darüber hinaus eine Reihe von Grundsätzen für die Datenverarbeitung. Daten müssen danach auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Rechtmäßigkeit, Treu und Glauben, Transparenz); für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (Zweckbindung); dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Datenminimierung); sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden (Richtigkeit). Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (Speicherbegrenzung); in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (Integrität und Vertraulichkeit).

Neu und eine erhebliche Arbeitslast auf den für die Datenverarbeitung Verantwortlichen ist der Grundsatz der Rechenschaftspflicht. Die DSGVO spricht hier davon, dass sie verantwortlich sind und die Einhaltung der Grundsätze nachweisen können müssen. War es bisher Aufgabe der Aufsichtsbehörden, bei Beschwerden den Verstoß zu belegen, ist es nun weit im Vorfeld die Aufgabe des Verantwortlichen, die Einhaltung der Grundsätze im Einzelnen zu dokumentieren. Dies ist eine Umkehr der Beweislast, die eine der großen Veränderungen durch die DSGVO bedingt.

Der Verantwortliche muss daher seit dem Inkrafttreten die gesamte Datenverarbeitung prüfen, durchdenken und dokumentieren, um möglichen Sanktionen zu entgehen. Die hier in Rede stehenden Summen bis zu zwanzig Millionen oder bis zu vier Prozent des weltweiten Jahresumsatzes sind hinreichend berichtet. Weniger berichtet wird, dass selbst die Datenschutzbeauftragten zugeben, diese Bußen nur in wenigen Fällen verhängen zu können. Eine flächendeckende Aufsicht ist schlichtweg nicht möglich. So wird es zu Maßnahmen gegen Leuchttürme von Branchen kommen, in der Hoffnung, dass dies zu einer breiten Anwendung der DSGVO beiträgt. Wer allerdings mit seinem Geschäftsmodell in dem Risiko steht, dass Betroffene sich sehr schnell an die Datenschutzbeauftragten wenden, wird größere Anstrengungen in Compliance investieren müssen. Angesichts der Herausforderungen bei der Implementierung der DSGVO gehen weite Kreise von Datenschutzrechtlern davon aus, dass es kaum ein Unternehmen schaffen wird, zum Stichtag noch beziehungsweise schon wieder compliant zu sein.

Zulässigkeit der Datenverarbeitung

Zurück zur Erlaubnis für die Datenverarbeitung, also der Einwilligung des Betroffenen oder einer gesetzlichen Grundlage. Die Einwilligung wird wie bisher vom Betroffenen erteilt. Sie ist jedoch zum einen widerruflich für die Zukunft ausgestaltet, zum anderen zu ihrer Wirksamkeit an Voraussetzungen geknüpft. Zwar ist keine Schriftform mehr erforderlich, die Einwilligung ist jedoch freiwillig und informiert abzugeben. Einwilligen können Kinder ab 16 Jahren, darunter ist eine Einwilligung oder die Zustimmung der Erziehungsberechtigten erforderlich.

Vor einer Einwilligung muss umfangreich informiert werden. Nach Artikel 13 DSGVO betrifft dies Identität und die Kontaktdaten des Verantwortlichen, die Kontaktdaten des Datenschutzbeauftragten, die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung, gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und gegebenenfalls zusätzliche Informationen. Dazu hat der Verantwortliche zu informieren über die Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, über die Kriterien für die Festlegung dieser Dauer; das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit; über das Recht, die Einwilligung jederzeit zu widerrufen; das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde; ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen und welche mögliche Folgen die Nichtbereitstellung hätte und das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person. Diese Informationspflichten bestehen auch, wenn die Daten von einem Dritten erhoben werden. Ausnahmen von den Informationspflichten bestehen nur, wenn die Informationen bereits dem Betroffenen bekannt sind.

Eine Menge von Angaben rund um die Einwilligung, deren Übermittlung, aktuelle Fassung etc. neben der eigentlichen Einwilligung ist sorgsam zu dokumentieren, denn gerade in diesem Feld wird die Aufsicht ansetzen. Dies gilt in besonderem Maße für die Fälle, in denen keine Einwilligung vorliegt, sondern die Verarbeitung auf einer gesetzlichen Erlaubnis besteht. Hier macht sich der risikobasierte Ansatz bemerkbar, was insbesondere die Dokumentationspflichten vor der Erhebung angeht. Artikel 6 DSGVO sieht neben der Einwilligung beispielsweise vor, dass eine Verarbeitung rechtmäßig ist, wenn

WIN VERLAG **Kiosk**

30 Tage gratis lesen

Jetzt auch als digitale Ausgabe

Auf 5 Geräten gleichzeitig lesen:
- im Web & per App

Shoppen wie man möchte:
- von Artikel bis Abo

united-kiosk.de/kiosk-win

die Verarbeitung für die Erfüllung eines Vertrags erforderlich ist, dessen Vertragspartei der Betroffene ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage des Betroffenen erfolgen; die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt; die Verarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen oder die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

Von besonderer Wichtigkeit ist jedoch die Regelung in Artikel 6 I f), nach dem die Verarbeitung zulässig ist, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten des Betroffenen, die den Schutz personenbezogener Daten erfordern, überwiegen; insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Was sich anhört wie ein Sonderfall, wird absehbar neben der Einwilligung der wichtigste Fall werden. Auf diesen werden sich zukünftig weitere Bereiche der Werbung und des Marketings stützen können. Als berechtigtes Interesse des Verarbeiters wird durchaus auch ein eigenwirtschaftliches Interesse verstanden. Die Gründe für die Abwägung mit den Betroffenenrechten müssen aber tragen und dokumentiert sein. Hier wird erheblicher Aufwand erforderlich sein und letztlich die Aufsichts- und Rechtsprechungspraxis die Grenzen definieren.

Der risikobasierte Ansatz ist auch bei den Regelungen zur Zweckänderung erkennbar: Soll eine Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, ohne Einwilligung des Betroffenen oder eine rechtliche Erlaubnis erfolgen, so berücksichtigt der Verantwortliche – um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist – unter anderem jede Verbindung zwischen den Zwecken, den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, die Art der personenbezogenen Daten, die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen und das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören können.

Rechte der Betroffenen

Der Verantwortliche für die Datenverarbeitung hat die Interessen des Betroffenen also nicht nur mitzudenken, sondern auch auf die Geltendmachung der in der DSGVO enthaltenen Rechte der Betroffenen einzugehen und angemessen zu reagieren. Der Katalog der Rechte beginnt mit dem Recht auf präzise, transparente, verständliche und leicht zugängliche Information in verständlicher Sprache. Zukünftig werden also schwammige oder nichtssagende Texte vor der Einwilligung nicht mehr zulässig sein, weil sie die Wirksamkeit der Einwilligung gefährden. In diesem Zusammenhang sei darauf hingewiesen, dass die deutschen Datenschutzbeauftragten am 14. September 2016 beschlossen haben, dass vor dem 25. Mai 2018 rechtswirksam erteilte Einwilligungen fortgelten. Schwierig wird hier mitunter der hinreichend dokumentierte Nachweis sein.

Die Betroffenenrechte seien hier nur kurz aufgezählt: Recht auf Information bei Erhebung, bei anderweitiger Erhebung, bei Zweckänderung; Recht auf Auskunft; Recht auf Berichtigung; Recht auf Löschung (Recht auf Vergessenwerden); Recht auf Einschränkung der Verarbeitung (Sperrung); Recht auf Datenübertragbarkeit; Widerspruchsrecht bei besonderer Situation in Fällen der Verarbeitung im öffentlichen Interesse oder bei Abwägung, Profiling oder Direktwerbung und ein grundsätzliches Verbot automatisierter Entscheidungen im Einzelfall, es sei denn, es liegt eine Einwilligung, ein Vertrag oder ein Gesetz vor. Auch dies hat Einfluss auf die zukünftige Gestaltung von Datenverarbeitung, allein was beispielsweise Vergessenwerden oder die Datenübertragbarkeit angeht.

Auftragsverarbeitung, Verarbeitungsverzeichnis, Folgenabschätzung

Nach der Darstellung dieser Grundlagen kann es nun an die Neuerungen in einzelnen Bereichen der Verarbeitung gehen. Ein zentraler Bereich ist nun die Auftragsverarbeitung. Nicht nur die Bezeichnung ist eine neue, auch die Regelungen hierzu sind geändert. So begeben sich Auftragsverarbeiter, die unter Verstoß gegen die DSGVO agieren, in eigene Verantwortlichkeiten. Die Auftragsdatenverarbeitung darf nur auf Grundlage einer vertraglichen Vereinbarung, die auch elektronisch geschlossen werden kann, nach den inhaltlichen Vorgaben der DSGVO erfolgen. Dazu gehören beispielsweise die genaue Beschreibung der Aufgaben des Auftragsverarbeiters und hinreichende Garantien von diesem für angemessene technische und organisatorische Maßnahmen (TOM). Diese TOM-Anforderung gilt damit auch im Bereich des Cloud-Computing. Auch hier wird verlangt, dass der Cloud-Nutzer nur mit Cloud-Anbietern zusammenarbeitet, die hinreichend Garantien dafür bieten, dass geeignete TOM so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Bei jeder Art von Cloud-Lösung ist diese Prüfung vorzunehmen, da generelle Aussagen hier kaum möglich sind.

Neu benannt wurde auch das vom BDSG bekannte Verfahrensverzeichnis. Es heißt nun Verarbeitungsverzeichnis und ist bei Verantwortlichen mit mehr als 250 Mitarbeitern Pflicht. Aber auch unterhalb dieses Schwellenwerts kann ein Verzeichnis der Verarbeitungstätigkeiten notwendig werden, wenn die vorgenommene Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder eine Verarbeitung sensible Daten oder Daten über strafrechtliche Verurteilungen und Straftaten betrifft. Hier ist eine sorgsame Prüfung erforderlich.

Ebenso wurde aus der BDSG-Vorabkontrolle nun eine Folgenabschätzung. Sofern ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht, ist diese erforderlich. Dies muss kein finanzieller Schaden sein, es geht auch um Diskriminierung, Identitätsdiebstahl, Rufschädigung, Verlust der Vertraulichkeit, Aufhebung der Pseudonymisierung oder den Verlust der Kontrolle über die eigenen Daten. Das Ergebnis der Risikoanalyse und die daraus resultierenden Maßnahmen sind zu dokumentieren. Gegebenenfalls ist auch die Aufsichtsbehörde zu konsultieren, wenn ein hohes Risiko besteht. Hier sowie bei den Verarbeitungsverzeichnissen können Vorlagen der Aufsichtsbehörden genutzt werden.

Datensparsamkeit und Datensicherheit

Die DSGVO gibt weitere Grundsätze für die Gestaltung der Datenverarbeitung vor: Durch technische und organisatorische Möglichkeiten muss sichergestellt sein, dass der Datenschutz verwirklicht wird. „Privacy by Design“ soll die Verarbeitung so ge-

stalten, dass der Datenschutz bereits in der Grundkonstruktion berücksichtigt ist. „Privacy by Default" soll insbesondere bei Online-Anwendungen sicherstellen, dass bei Vorgaben stets die datenschutzfreundlichste Variante voreingestellt ist. Die Beachtung dieser Grundsätze wird bei der Bemessung von Bußgeldern eine Rolle spielen und ist daher nicht nur ein Selbstzweck.

Artikel 32 der DSGVO beschäftigt sich mit der Verpflichtung zur Datensicherheit, wonach geeignete technische und organisatorische Maßnahmen zu treffen sind, die dem Stand der Technik entsprechen und nach Kosten und Risiko verhältnismäßig sind. Die Datensicherheit betrifft aber auch die Aspekte der weitgehenden Pseudonymisierung, der Sicherstellung der Fähigkeiten von Systemen und Diensten, der Wiederherstellung der Verfügbarkeit und des Zugangs zu Daten sowie von Verfahren zur Überprüfung der Gewährleistung der Sicherheit der Verarbeitung. Auch hier wird die Aufsicht mehr als ein Auge auf den Nachweis der Einhaltung dieser Voraussetzungen haben.

Von Bedeutung ist dabei auch die Festlegung von Prozessen bei Verletzung des Schutzes personenbezogener Daten, also „Unfällen" bei der Sicherheit von Daten. Die DSGVO schreibt vor, dass binnen 72 Stunden nach Kenntnis über einen Verstoß die zuständige Aufsichtsbehörde zu verständigen ist. Hierzu wird es ein Online-Tool bei den Datenschutzbeauftragten geben. Die Meldung kann nur unterbleiben, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Hier ist anzuraten, diese Prognose-Entscheidung genau zu dokumentieren.

Sofern mit der Verletzung des Datenschutzes voraussichtlich ein hohes Risiko für den Betroffenen verbunden ist, muss dieser ebenfalls informiert werden. Dies kann unterbleiben, wenn der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat, etwa durch Verschlüsselung, oder wenn der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko aller Wahrscheinlichkeit nach nicht mehr besteht. Ferner wenn die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden. Dies bedeutet für jeden Verantwortlichen, dass er ein Notfall-Management einführen muss, das die notwendigen Prozesse mit den dazugehörigen Verantwortlichkeiten definiert und entsprechende Informationsmaßnahmen vorbereitet.

Zur betrieblichen Organisation gehört ferner in bestimmten Fällen ein Datenschutzbeauftragter, wie er seit dem BDSG bekannt ist. Der Schwellenwert, bei dessen Überschreiten ein Datenschutzbeauftragter einzusetzen und nun auch der Aufsicht zu benennen ist, bleibt bei zehn Personen, die regelmäßig Zugriff auf die personenbezogenen Daten nehmen. Außerdem ist ein Datenschutzbeauftragter zu benennen, unter anderem wenn die Kerntätigkeit des Verantwortlichen eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich macht oder die Kerntätigkeit im Umgang mit besonders sensiblen Daten liegt. Die Berufung kann auch freiwillig erfolgen. In jedem Fall ist sie aber intern und extern bekannt zu machen.

Schließlich noch ein kurzer Blick auf die Weitergabe von Daten an Dritte. Die Weitergabe innerhalb der Europäischen Union ist weitgehend unproblematisch, da sie als Inland gilt. Die Übermittlung von Daten ist grundsätzlich nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die Bedingungen der DGSVO einhalten. Tragender Gedanke ist, dass das Schutzniveau der DGSVO nicht untergraben werden soll, wie insbesondere in den Erwägungsgründen ausgeführt wird: Die EU-Kommission darf mit Wirkung für die gesamte Union beschließen, dass ein bestimmtes Drittland oder eine internationale Organisation ein angemessenes Datenschutzniveau bietet. In derartigen Fällen dürfen personenbezogene Daten ohne weitere Genehmigung an dieses Land oder diese internationale Organisation übermittelt werden. Gibt es einen solchen Angemessenheitsbeschluss nicht, sollte der Verantwortliche oder der Auftragsverarbeiter als Ausgleich für den in einem Drittland bestehenden Mangel an Datenschutz geeignete Garantien für den Schutz der betroffenen Person vorsehen. Diese geeigneten Garantien können darin bestehen, dass auf verbindliche interne Datenschutzvorschriften, auf von der Kommission oder von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln oder auf von einer Aufsichtsbehörde genehmigte Vertragsklauseln zurückgegriffen wird. Diese Garantien sollten sicherstellen, dass die Datenschutzvorschriften und die Rechte der betroffenen Personen auf eine der Verarbeitung innerhalb der Union angemessene Art und Weise beachtet werden; dies gilt auch hinsichtlich der Verfügbarkeit von durchsetzbaren Rechten der betroffenen Person und von wirksamen Rechtsbehelfen einschließlich des Rechts auf wirksame verwaltungsrechtliche oder gerichtliche Rechtsbehelfe sowie des Rechts auf Geltendmachung von Schadenersatzansprüchen in der Union oder in einem Drittland. Dieses Thema bedarf einer eingehenden Erörterung, insbesondere im Verkehr mit den USA angesichts der „Privacy Shield"-Politik, die den Rahmen dieses Beitrags sprengen würde.

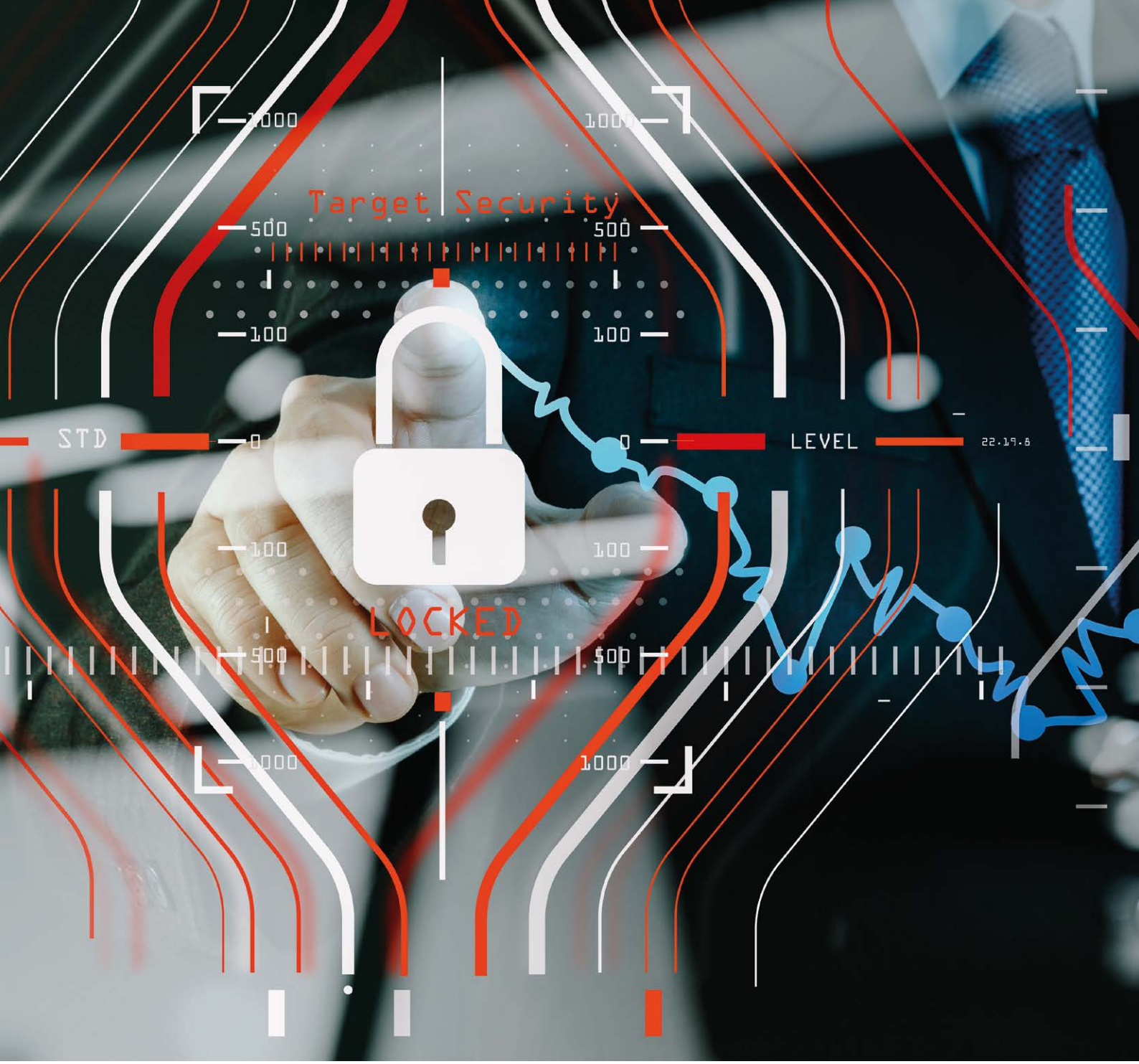
Abschließend stellt sich also die Frage, was zu tun ist, um am 25. Mai 2018 vorbereitet zu sein. Zunächst sollten eine Bestandsanalyse erfolgen und alle Prozesse der Verarbeitung von Daten erfasst werden. Sodann können diese mit einer GAP-Analyse darauf geprüft werden, welche Prozesse noch auf den Stand der DSGVO zu bringen sind. Die notwendigen Abläufe und Prozesse in den Abteilungen sowie in der IT sind anzupassen. Verträge, insbesondere Auftragsdatenverarbeitungsverträge, sind auf den neuen Stand zu bringen. Dies gilt auch für andere rechtlich relevante Dokumente und vor allem für die Informationen bei Einwilligungen. Das Unternehmen sollte ein Leitbild für den Datenschutz entwickeln und Mitarbeitende sowie Führungskräfte auf die DSGVO-Änderungen vorbreiten.

Letztlich bedingt die Anwendbarkeit der DSGVO ab Ende Mai genau das, was der Gesetzgeber intendiert hat: eine intensive Beschäftigung mit dem Thema „Datenschutz" und den Aufbau oder die Überarbeitung der gesamten Datenschutzorganisation in einem Unternehmen. Schon aus den in diesem Beitrag aufgezeigten Punkten ergibt sich ein großer Prüfungs- und Dokumentationsaufwand.

Weiterführende Informationen

- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_de
- Kranig, Sachs, Gierschmann, Datenschutz-Compliance nach der DS-GVO, Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden, 230 Seiten, Verlag Bundesanzeiger, ISBN 978-3846207604, 44 Euro

Carsten J. Diercks
cj@diercksrechtsanwalt.de



Die neue EU-Datenschutz-Grundverordnung – eine Chance für Unternehmen

Christian Vellmer, PROMATIS Gruppe

Am 25. Mai dieses Jahres beginnt eine neue Zeitrechnung für den Datenschutz in Europa. Die Datenschutz-Grundverordnung (DSGVO) kommt auf alle Unternehmen in Europa zu und wird das wirtschaftliche Handeln miteinander nachhaltig verändern. Personenbezogene Daten werden nicht mehr nur verkauft oder getauscht, sie müssen ab diesem Tag überprüft und hinterfragt werden. Wie wird sich das auf das tägliche Umfeld der Unternehmen auswirken und was ist eigentlich zu tun, um immensen Strafen zu entgehen? Dieser Beitrag beschäftigt sich mit dieser Fragestellung und wird aufzeigen, dass die kommende Datenschutz-Grundverordnung gar nicht so viel verändert, wie bisher kundgetan wird.

Kernpunkte der neuen DSGVO	
Harmonisierung des Datenschutzrechts	Vereinheitlichung von 28 nationalen Rechten
Weltweite Anwendbarkeit	Organisationen innerhalb und außerhalb der EU unter bestimmten Voraussetzungen
Stärkung der Betroffenenrechte	Recht auf Löschung kann vom Nutzer jederzeit verlangt werden
Verbindliche Meldepflicht	Gegenüber Behörden innerhalb von 72 Stunden, Nutzern unverzüglich
Gesamtschuldnerische Haftung	Von verantwortlichen Stellen und Auftragsverarbeitern
Opt-in Einwilligung	Transparenz und Verbindlichkeit für den Nutzer
Datenübermittlung	Datenschutzrechte an Daten gebunden, weltweite Anwendung
Hohe Bußgelder	Bis zu 4% des weltweiten Jahresumsatzes oder 20 Mio. €
Bedürfnis nach Datensicherheit	Forderung nach Datenschutz durch Technikgestaltung und Sicherheit der Verarbeitung

Abbildung 1: Anforderungen der neuen DSGVO

25. Mai 2018 – wie ein Damoklesschwert schwebt dieser Termin über den Unternehmen. Die Datenschutzbeauftragten flattern nervös von einer Abteilung zur nächsten und versuchen in den verbleibenden Wochen, ihr Unternehmen datenschutzkonform zu gestalten. Zwischenzeitlich haben auch die wenig datenschutzinteressierten Mitarbeiter mitbekommen, dass an diesem Stichtag die neue Datenschutz-Grundverordnung in Kraft tritt, ein europaweites Gesetz, das massiv Einfluss auf die gesamten IT-Prozesse nimmt.

Doch woher kommt diese Hektik, obwohl der Beschluss doch schon seit zwei Jahren bekannt ist? Ganz einfach, das ist die Fünf-vor-zwölf-Taktik der Unternehmen, die – bewusst oder unbewusst – das Thema erstmal zur Seite geschoben haben und darauf bauten, nicht beachtet zu werden. Die Umsetzung der neuen Vorgaben ist ein Kostenfaktor für die Unternehmen, der nicht unerheblich ist. Diese Vorgehensweise geht jetzt nicht auf, denn plötzlich ist die DSGVO in aller Munde – quer durch alle Medien. Ein Grund dafür ist, dass wirtschaftliche Faktoren zu berücksichtigen sind und somit die Thematik an Brisanz gewinnt. So müssen die Unternehmen bei Nichteinhaltung der Regularien vier Prozent des weltweiten Jahresumsatzes oder zwanzig Millionen Euro Strafe zahlen – das sind Dimensionen, die aufschrecken lassen!

Eine europaweite Verordnung, die jeden betrifft

Laut einer IDC-Studie im November 2017 sind 44 Prozent der Unternehmen in Deutschland auf die neue Datenschutzverordnung nicht vorbereitet beziehungsweise sehen den Änderungen gelassen entgegen. Doch nun heißt es, sich aktiv mit der Thematik auseinanderzusetzen, denn die neue DSGVO umfasst 99 Artikel, die mit mehr als 170 Anmerkungen ein komplexes und inhaltsreiches Kompendium darstellt, das es in jedem Unternehmen umzusetzen gilt. Ziel dieses Werks ist, für ein einheitliches Datenschutzrecht innerhalb der EU zu sorgen und insbesondere die Rechte und Kontrollmöglichkeiten bei der Erhebung und Verarbeitung personenbezogener Daten zu stärken. Für Unternehmen bedeutet das eine erhöhte Transparenz sowie eine umfassende Informationspflicht in Bezug auf den Umgang mit Daten. Diese Vorgaben sind bindend und die Bußgelder bei Nichteinhaltung erheblich.

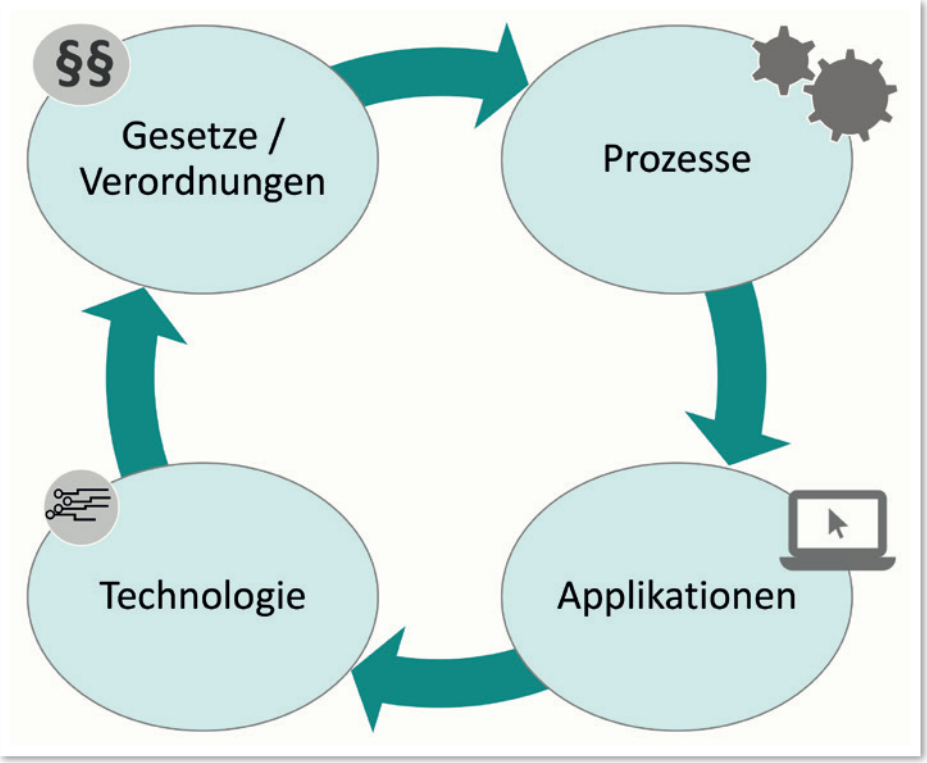


Abbildung 2: Erfolgsfaktoren im Zusammenspiel

Rechtliche Anforderungen und Grundsätze der DSGVO

Die DSGVO sieht in Artikel 5 eine Vielzahl von allgemeinen Grundsätzen vor. Sie stellen so etwas wie die Grundregeln für die Verarbeitung von personenbezogenen Daten dar und helfen insbesondere bei der Auslegung von Regelungen der DSGVO. Normiert sind die Themen „Rechtmäßigkeit, Verarbeitung

nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit". So müssen personenbezogene Daten folgende Kriterien erfüllen:

- Auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.
- Für festgelegte, eindeutige und legitime Zwecke erhoben sein und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.
- Auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.
- Sachlich richtig und auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.
- In einer Form gespeichert sein, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.
- In einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

Verstöße gegen die in Artikel 5 der DSGVO normierten Grundsätze können Maßnahmen der Aufsichtsbehörden nach sich ziehen. Die Anforderungen und Auswirkungen für Unternehmen sind insbesondere vor dem Hintergrund dieser Sanktionen erheblich *(siehe Abbildung 1)*.

Auswirkungen auf die Unternehmen

Unternehmen, die mit personenbezogenen Daten arbeiten, was praktisch in jedem Betrieb der Fall ist, müssen also sehr genau darauf achten, die genannten Vorgaben einzuhalten. Geeignete technische und organisatorische Maßnahmen sind zu treffen, um die Rechte der Betroffenen zu bewahren. Dies betrifft nicht nur organisatorische Schritte wie beispielsweise die Datenerhebung, sondern es wird auch eine transparente Darstellung aller relevanten Prozesse sowie die Anpassung aller technischen Geräte und Software gefordert. Die betrieblichen, technischen, organisatorischen und rechtlichen Anforderungen der neuen DSGVO fordern von den Unternehmen sichere Konzepte.

Intelligente Lösungen statt operativer Hektik

Statt in blinden Aktionismus zu verfallen, ist es erforderlich, die verbleibende Zeit gut zu planen, denn im Grunde befasst sich die DSGVO ja nur mit der Verarbeitung von personenbezogenen Daten. Das hört sich nicht so gewaltig an – kratzt man jedoch ein wenig an der Oberfläche, zeigt sich, wo überall in dem enormen und verzweigten Netzwerk der Unternehmens-IT diese Daten zu finden sind.

Um die Anforderungen gesetzeskonform umzusetzen, gibt es nun zwei Möglichkeiten: entweder selbst die unzähligen Stellen in der umfassenden digitalen Unternehmenswelt mühsam zu suchen, um danach die Änderungen individuell zu realisieren, oder die Aufgabe an einen Experten zu übertragen. Dabei müssen bestimmte Voraussetzungen erfüllt sein: ein tiefes Verständnis der Gesetze sowie der Anwendungsbereiche gepaart mit fundiertem Know-how der gesamten Unternehmensprozesse und Datenstrukturen.

Die Vorgehensweise der externen Spezialisten orientiert sich meistens an der klassischen Handhabung: Analyse, Konzeption, Umsetzung. Auch hier nichts Neues, wenn der Fokus des Verfahrens auf der Analyse liegt, denn je detaillierter und systematischer die Untersuchungen der Systeme durchgeführt werden, desto schneller und somit auch effizienter kann die Umsetzung erfolgen *(siehe Abbildung 2)*.

Optimierung der Prozesse

Ein weiterer Vorteil einer umfassenden Analyse liegt in dem Erkennen von Schwachstellen, unnötigen Prozessen und Daten, redundanten Vorgängen und vielen weiteren Punkten, die eine IT-Landschaft belasten. Um für Unternehmen pragmatische und valide Konzepte erstellen zu können, ist eine systematische Intelligenz erforderlich, die sowohl die Gesetzesvorgaben als auch die Prozessstrukturen innerhalb des Unternehmens kennt. Diese Methodik spiegelt sich auch in der Umsetzung wider, praxisorientierte Lösungen mit minimalem Aufwand zu implementieren. Das ist die große Chance, die durch die Einführung der DSGVO für die Unternehmen besteht. Aufgrund der detaillierten und vor allem systematischen Betrachtung können Prozesse optimiert, Daten minimiert und die Transparenz erhöht werden. Mit diesem Vorgehen können Unternehmen ihr jahrelanges Ignorieren der DSGVO in einen einmaligen Vorteil wandeln und die gesamte IT-Landschaft innerhalb kürzester Zeit gesetzeskonform, valide, schlank und bereinigt gestalten.

Christian Vellmer
Christian.vellmer@promatis.de

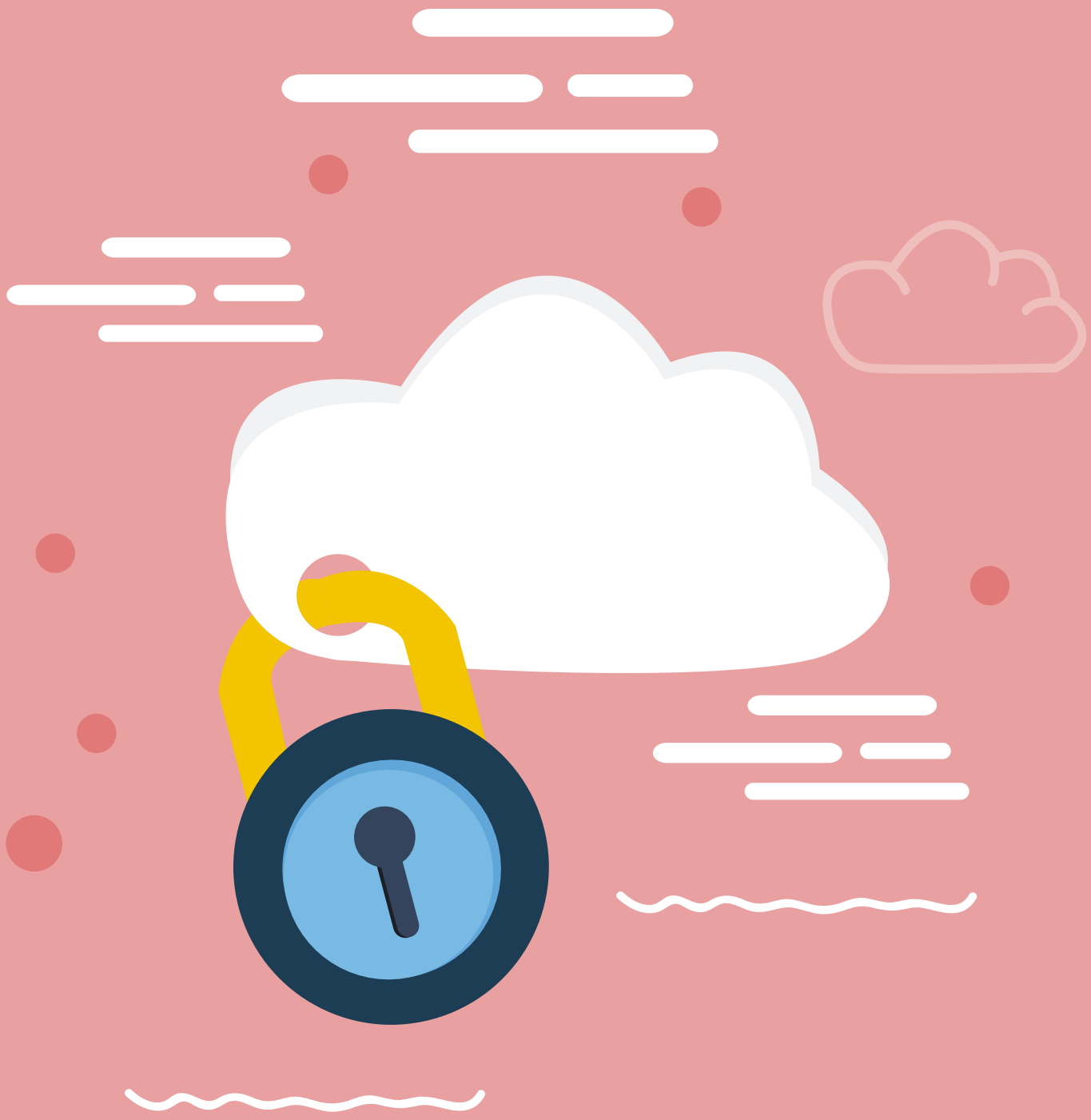
Der DOAG Jahresbericht 2017 ist online

Highlights, Neuigkeiten, Herausforderungen: Der Jahresbericht 2017 gibt dazu Auskunft. Auf 32 Seiten lassen die DOAG-Verantwortlichen das vergangene Jahr Revue passieren. Vorstandsvorsitzender Stefan Kinnen sieht den Verein auf einem sehr guten Weg, wie er in seinem Vorwort im Jahresbericht betont. Im Hinblick auf die Cloud richteten Mitglieder jetzt auch andere Fragen und Erwartungen an den Verein: „Neben technischen und methodischen Themen sind nun auch rechtliche sowie wirtschaftliche Aspekte relevant." Bei Themen wie IT-Sicherheit, Datenschutz und notwendige Zertifizierungen bleibe die DOAG „nachhaltig am Ball, um unseren Mitgliedern beim schrittweisen Weg in die Cloud wertvolle Hilfestellungen geben zu können." Auch wiederkehrende Fragestellungen aus dem Alltag – wie die Qualität des Oracle Supports oder Lizenzfragen in virtuellen Umgebungen – wird die DOAG laut Kinnen im Blick behalten.

Der DOAG Jahresbericht 2017 ist ab sofort hier verfügbar: *„https://www.doag.org/formes/pubfiles/10046451/docs/DOAG/Delegiertenversammlungen/2018/2017-DOAG-Jahresbericht-Web.pdf"*.

Oracle-Lösungen zur Datensicherheit

Ernst Lorenz, Oracle Deutschland B.V. & Co. KG



Am 25. Mai 2018 tritt die EU-Datenschutz-Grundverordnung in Kraft. Schon jetzt, in der Vorbereitungsphase, hat sich das Bewusstsein für IT-Sicherheit aufgrund der Häufung von Cyber-Crime-Attacken stark intensiviert. Kriminelle Angriffe auf Daten und Anwendungen sind in der Ausführung mittlerweile so raffiniert, dass auch der Schutz und die Abwehr „nachgerüstet" werden müssen. Seitens seiner Produktstrategie hat Oracle von Beginn an eine ganzheitlich angelegte Sicherheitsphilosophie verfolgt. Der Artikel zeigt auf, wo die von Oracle angebotenen Sicherheitstechniken möglicherweise helfen können, die Anforderungen und Ziele der EU-Datenschutz-Grundverordnung zu adressieren.

Die Datenschutz-Grundverordnung umfasst 99 Artikel und 173 sogenannte „Erwägungsgründe". Schon allein dieses Zahlenverhältnis von normativen Festlegungen zu Erläuterungen zeigt, wie komplex die Anwendungssachverhalte sind. Die eigentliche Herausforderung für die Umsetzung der Verordnung stellen jedoch die Varianz und Komplexität der heutigen IT-Systeme dar. Diese Systeme wurden nicht im juristischen Erwartungshorizont der EU-DSGVO entworfen. Um jetzt ab 25. Mai 2018 der Verordnung zu entsprechen und potenziell hohe Haftungsrisiken zu vermeiden, können Nachbesserungen bei der Sicherheit der IT-Systeme erforderlich sein.

Risikokategorien im Kontext der IT-Systeme

Der juristische Kontext der EU-DSGVO erwartet Sicherheit an verschiedenen Stellen der IT-Systeme. Wenn Unternehmen diesen Sicherheitsanforderungen nicht entsprechen, gehen sie nicht unerhebliche Risiken ein. Artikel 83 behandelt die „Allgemeine(n) Bedingungen für die Verhängung von Geldbußen" und bestimmt, dass getroffene technische Vorkehrungen bei der Entscheidung über Geldbußen berücksichtigt werden sollen.

Eines der größten Risiken im Sicherheitsverständnis der EU-DSGVO ist der Datendiebstahl. Unabhängig von den Sanktionen geht dieser häufig auch mit einem immensen Reputationsschaden für das Unternehmen einher. Die Kategorie „Datendiebstahl/ Data Breaches" soll hier als synonymer Begriff für alle Arten von Angriffen auf die zu schützenden personenbezogenen Daten verstanden werden. Weitere Erwartungen an die Sicherheit lassen sich den Kategorien „Sorgfalt in der IT" und „Meldepflicht" zuordnen. Technisch gesehen sind die drei Hauptbereiche wichtig:

- Verhinderung und Vermeidung von Datenschutzverletzungen
- Nachweiserbringung und Dokumentierung des Umgangs mit personenbezogenen Daten
- Bericht und Benachrichtigung im Pannenfall

Angriffe können sowohl von extern, also von außerhalb der IT-Systemgrenzen, als auch von autorisierten Benutzern innerhalb des Systems erfolgen. Aus technischer Sicht ist für die Auswahl geeigneter Sicherheitsmittel neben den Angriffsszenarien auch die Art der potenziell an den Daten verursachten Schäden maßgeblich.

Grundsätzlich können zwei Arten von Schutzverletzungen erfolgen: Diebstahl von Personendaten und deren Manipulation. Dabei kann sich die Manipulation als noch gravierender als der Datendiebstahl auswirken. Arti-

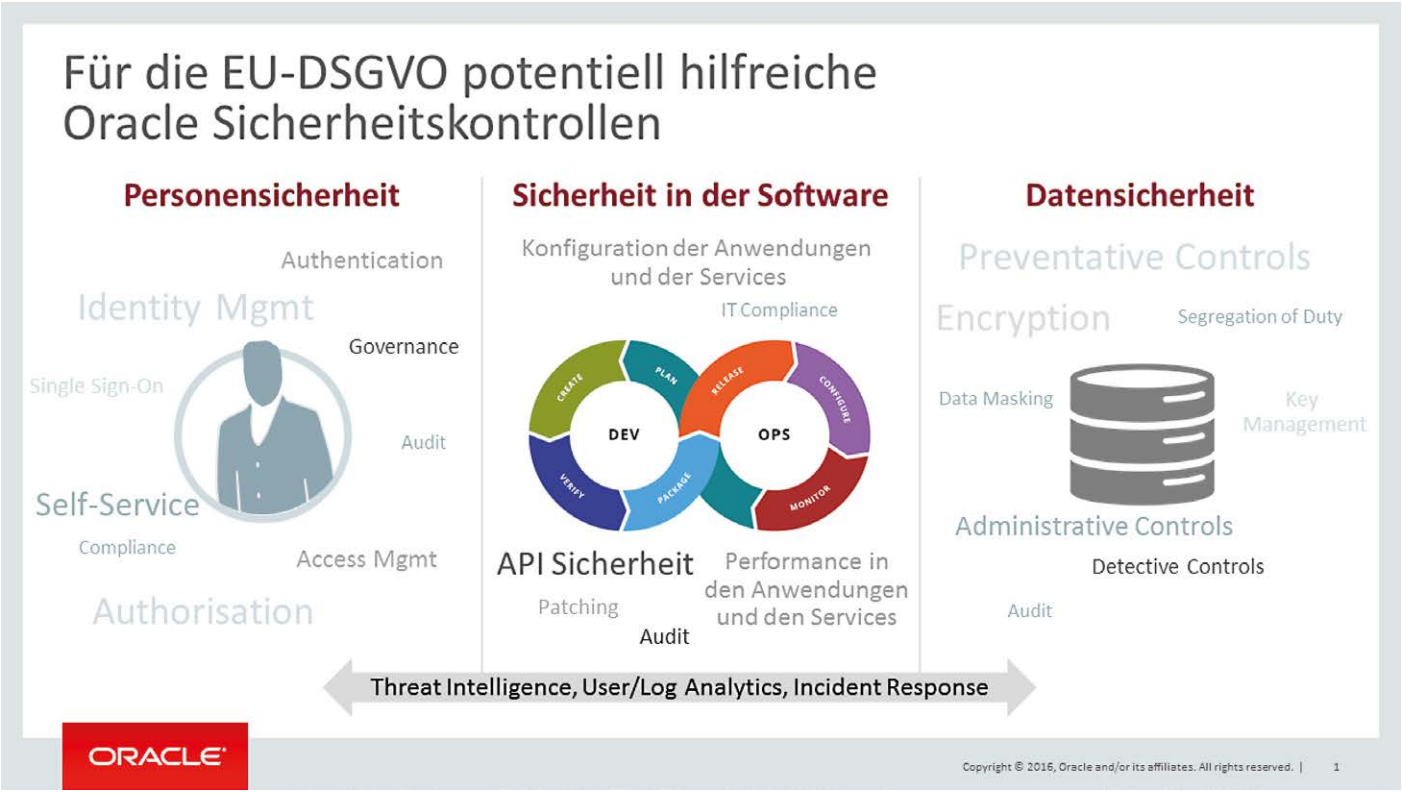


Abbildung 1: So können Oracle-Lösungen zur Datensicherheit beitragen

kel 34 der DSGVO über die „Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person" trägt dem Rechnung. Problematisch wird es insbesondere, wenn hochsensible Personendaten manipuliert werden, diese Manipulation aber nicht sofort erkannt wird. Im Falle spezieller Angriffe wie Ransomware fällt die Manipulation sofort auf, weil der Datenbestand des Unternehmens in krimineller Absicht verschlüsselt wird und nicht mehr zugänglich ist. Unternehmen müssen sich dann den Zugang zu ihren Daten wieder freikaufen.

Sorgfaltspflichten in der Verarbeitung, Dokumentation und Berichterstattung

In einer von IDC 2017 herausgegebenen Studie wird sehr pointiert dargestellt, warum sich die EU-DGSVO nicht nur auf die Verhinderung von Datendiebstahl und -manipulation reduziert [1]. Auch mangelnde Sorgfalt in der Datenverarbeitung kann beanstandet werden. Unternehmen sollten deshalb die drei Dimensionen „Angriffsabwehr", „Schadenminimierung" und „Sorgfalt im Verfahrensbetrieb" über den Einsatz technischer und organisatorischer Sicherheitsmittel absichern [2].

Aufgrund seiner langjährigen Erfahrung ist Oracle der Überzeugung, dass die Sicherheit am effizientesten gemäß den Prinzipien „Nearest to the data" und „Least privilege", also Daten- und Zugriffssicherheit, zu implementieren ist, weil das Angriffsziel immer direkt auf die Daten gerichtet ist. *Abbildung 1* zeigt dazu einen Funktionsüberblick.

Technische Oracle-Sicherheitsmittel

Verschlüsselung der Daten kann zum Beispiel im Fall eines Datendiebstahls das Risiko eines Schadens für betroffene Personen verringern. Die gestohlenen Daten sind unkenntlich gemacht und daher regelmäßig wertlos. Bei der Maskierung von bestimmten Feldinhalten werden bestimmte personenbezogene Informationen in der Verarbeitung verfälscht, um die negativen Auswirkungen eines Datenverlusts zu begrenzen. Werden Feld-Inhalte randomisiert, ist der eigentliche Informationsgehalt der Daten zerstört, sodass sie möglicherweise an Dritte weitergegeben werden können; dennoch ermöglicht es die Oracle-Lösung, die relationalen Datenbeziehungen für Test und Entwicklung zu erhalten. Beim Subsetting von Daten-Untermengen werden sensible Daten nur sehr gezielt und minimiert bereitgestellt. So lassen sich potenzielle Angriffsflächen verringern und damit der Schutz vergrößern. Eine ähnliche Strategie wird verfolgt, wenn auf kritische Feld-Attribute Label-Vergaben zur Bildung von Risiko-Kategorien erfolgen. Über das Label wird dann, analog zu den Risikozuordnungen, der Zugriff auf die Daten kontrolliert und protokolliert.

Klassische Zugriffs- und Rechte-Steuerungen, wie Benutzername und Passwort, sind zwar nach wie vor notwendig, aber in den modernen Systemumgebungen bei weitem nicht mehr ausreichend. Wenn im Internet mit wechselnden Endgeräten auf die Daten zugegriffen wird, sollten die Daten zusätzlich, neben abgesicherten Zugriffskontrollen wie zum Beispiel der Zwei-Faktor-Authentifizierung, entsprechend obigen Sicherheitsmitteln geschützt sein. Die Internet-Verarbeitungsszenarien sind maßgeblich dafür verantwortlich, dass sich die klassischen Systemgrenzen der IT-Systeme zunehmend auflösen. Diese Unschärfe in der Abgrenzung der Systeme erfordert völlig neue Überwachungs- und Absicherungsmittel *(siehe Abbildung 2)*.

Deshalb müssen sich Unternehmen jetzt auch zunehmend überlegen, wie sie ihre Cloud-Strategie in Einklang mit den Erwartungen der EU-DSGVO bringen; insbesondere, welche Rolle die unterschiedlichen Cloud-Betriebsmodelle hinsichtlich Sicherheit und Risiko im IT-Aufbau für das Unternehmen darstellen. Wie wird zum Beispiel die Datensicherheit in hybriden Umgebungen (On-Premises, Cloud) hergestellt? Wie wird die Verarbeitung im Gesamtsystem überwacht, insbesondere wenn über sogenannte „Shadow-IT" potenziell Daten unkontrolliert abfließen können? Wie wird, analog zu den Vorgaben der DSGVO, die Verarbeitung auditiert und dokumentiert? Speziell auch hinsichtlich

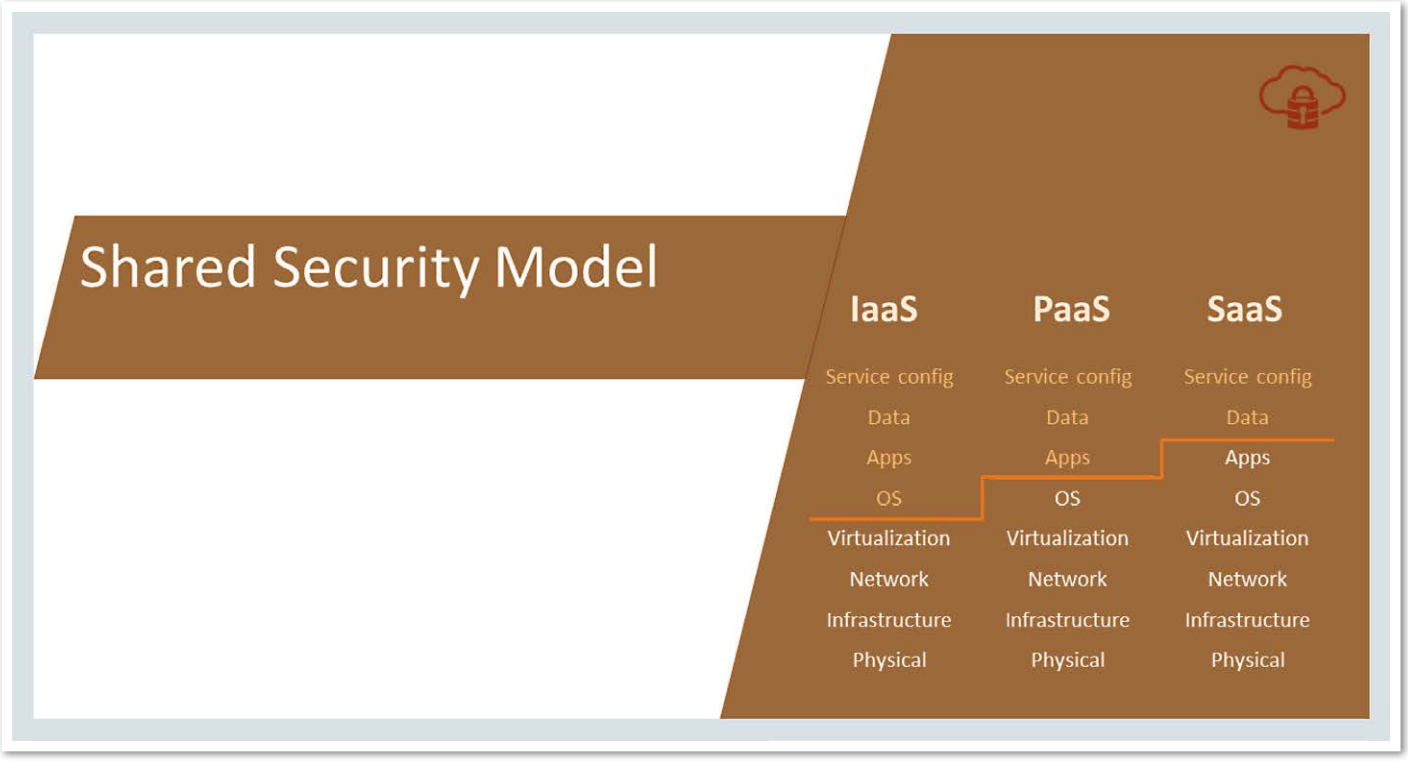


Abbildung 2: Unterschiedliche Betriebsmodelle und verteilte Verantwortung

der besonders zu schützenden personenbezogenen Daten, gemäß den Vorgaben der Verordnung nach den Artikeln 30 und 35 [3]. Dazu gehört dann auch die Vorbereitung darauf, wie Pannenfälle (Risiko-Kategorie „Meldepflicht“) zu dokumentieren sind und wie an die Aufsichtsbehörden berichtet wird.

Betriebsmodelle im Kontext der DSGVO-Akteure

Die EU-DSGVO weist eine sehr klare und eindeutige Architektur auf. Sie ähnelt einem Pflichtenheft, wie man es aus der Informatik kennt. In Artikel 4 „Begriffsbestimmungen“ und in den Erwägungsgründen 26 bis 37 werden unter anderem die Akteure der Verordnung und ihre juristischen Verhältnisse zueinander definiert. Dabei unterliegen die Akteure bestimmten Verantwortlichkeiten, sie müssen bestimmte Aufgaben erfüllen und unterliegen spezifischen Rollenerwartungen.

Den eigentlichen Kern der EU-DSGVO bilden die beiden Hauptakteure „Verantwortlicher“ und „Auftragsverarbeiter“. Der Verantwortliche muss entscheiden, welche Risiken im IT-System abzudecken und welche Datensicherungsmittel dafür einzusetzen sind. Gegenüber den Daten-Subjekten und ihren Rechten und Freiheiten an ihren personenbezogenen Daten existiert das Prinzip der „Beweislastumkehr“. Nicht das Daten-Subjekt muss nachweisen, dass seine/ihre Daten nicht ausreichend gesichert scheinen. Der Verantwortliche muss die rechtmäßige Verarbeitung und vor allem die erforderliche Datensicherheit nachweisen können, gegebenenfalls auch gegenüber der Aufsichtsbehörde (Artikel 5, Absatz 2).

Aus Sicht der Rollenverteilung der DSGVO ist das Unternehmen gerade auch im Betriebsmodell „On-Premises“ immer Verantwortlicher. Über Zulieferer, wie zum Beispiel Oracle, können für den On-Premises-Betrieb entsprechende ergänzende Sicherheitsprodukte zur Datenbank, zur Middleware, zum Identity Management, zur Überwachung und zum Reporting erworben werden. Wichtig für das Verständnis des On-Premises-Modells ist, dass die Entscheidung darüber, wie das datenschutzrechtlich geforderte Sicherheitsniveau herzustellen ist, ausschließlich in der Verantwortung des Unternehmens liegt.

Verlagert das Unternehmen Teile seiner IT in Cloud-Betreibermodelle, ist der Cloud-Betreiber Akteur im Sinne der DSGVO (Auftragsverarbeiter). Unternehmen können dann die von dem Cloud-Provider getroffenen Sicherheitsvorkehrungen bei der Prüfung ihrer Datenschutz-Compliance berücksichtigen. Oracle als On-Premises-Lösungsanbieter und Cloud Provider bietet seinen Kunden diesbezüglich die volle Durchgängigkeit der technischen Sicherheitsmittel über alle Betreibermodelle hinweg an. So werden zum Beispiel alle im Oracle-Cloud-Umfeld betriebenen Datenbanken per Default verschlüsselt.

Über Oracle Key Vault kann sich der Kunde zum alleinigen Besitzer aller benötigten Sicherheitsschlüssel machen und hat damit die vollständige Kontrolle über seine Daten. Dies wird ergänzt durch entsprechend starke und restriktive Authentifizierung- und Autorisierungs-Mechanismen sowie darauf aufbauende Zugriffskontrollen, über die kontrolliert werden kann, wer im On-Premises- und Cloud-Umfeld auf welche Instanzen und Daten zugreifen darf.

Persönliche Rechte, Überwachung, Auditing, Dokumentation und Benachrichtigung

Neben den bisher aufgezeigten Sicherheitserwartungen der EU-DSGVO gibt es zwei weitere Anforderungsbereiche. Diese betreffen die bereitzustellende Sicherheit im fachlich funktionalen Kontext. Die gesetzliche Grundlage dafür findet sich in den Artikeln 5 „Grundsätze für die Verarbeitung personenbezogener Daten“ und 7 „Bedingungen für die Einwilligung“ der Verordnung. In *Abbildung 3* sind beide sicherheitsrelevan-

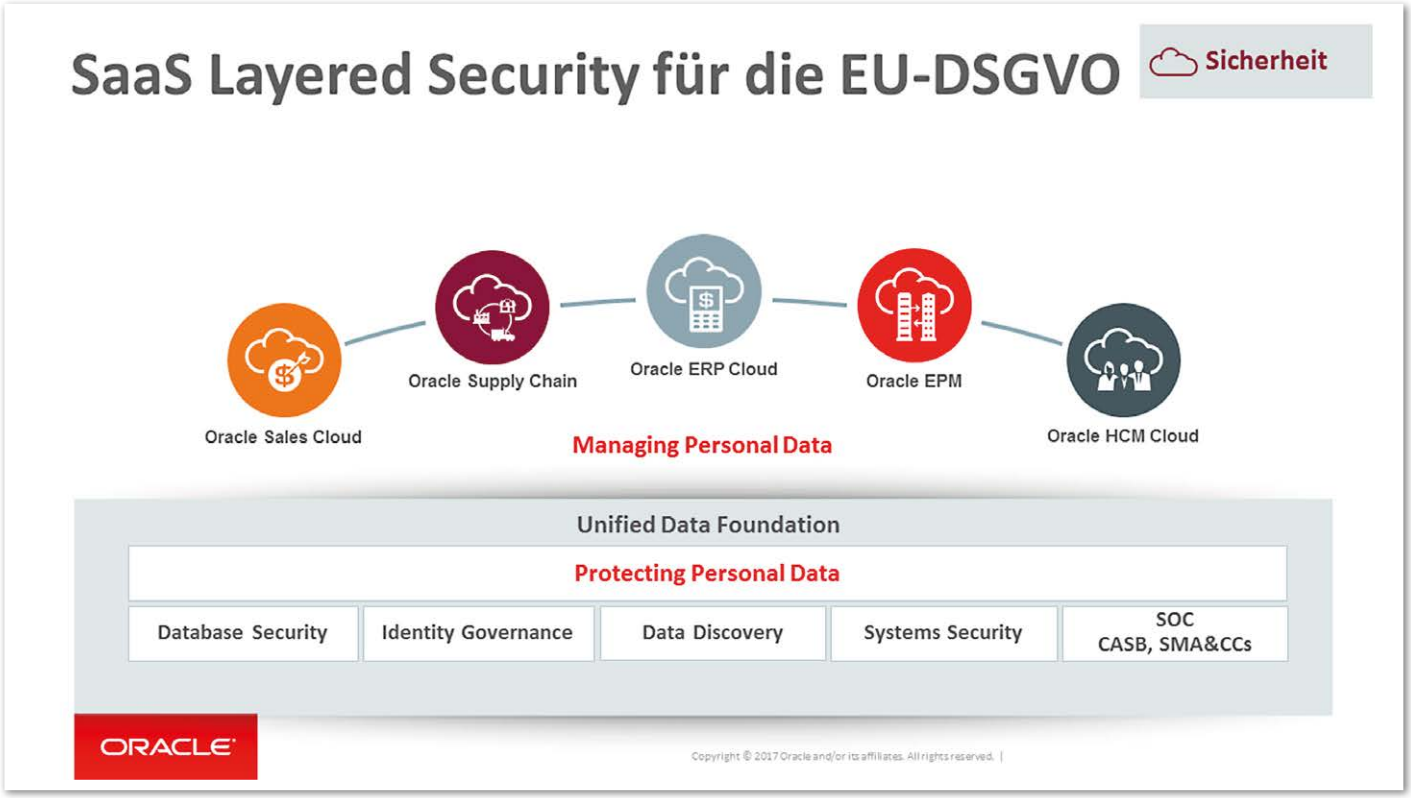


Abbildung 3: Sicherheit im fachlich funktionalen Bereich

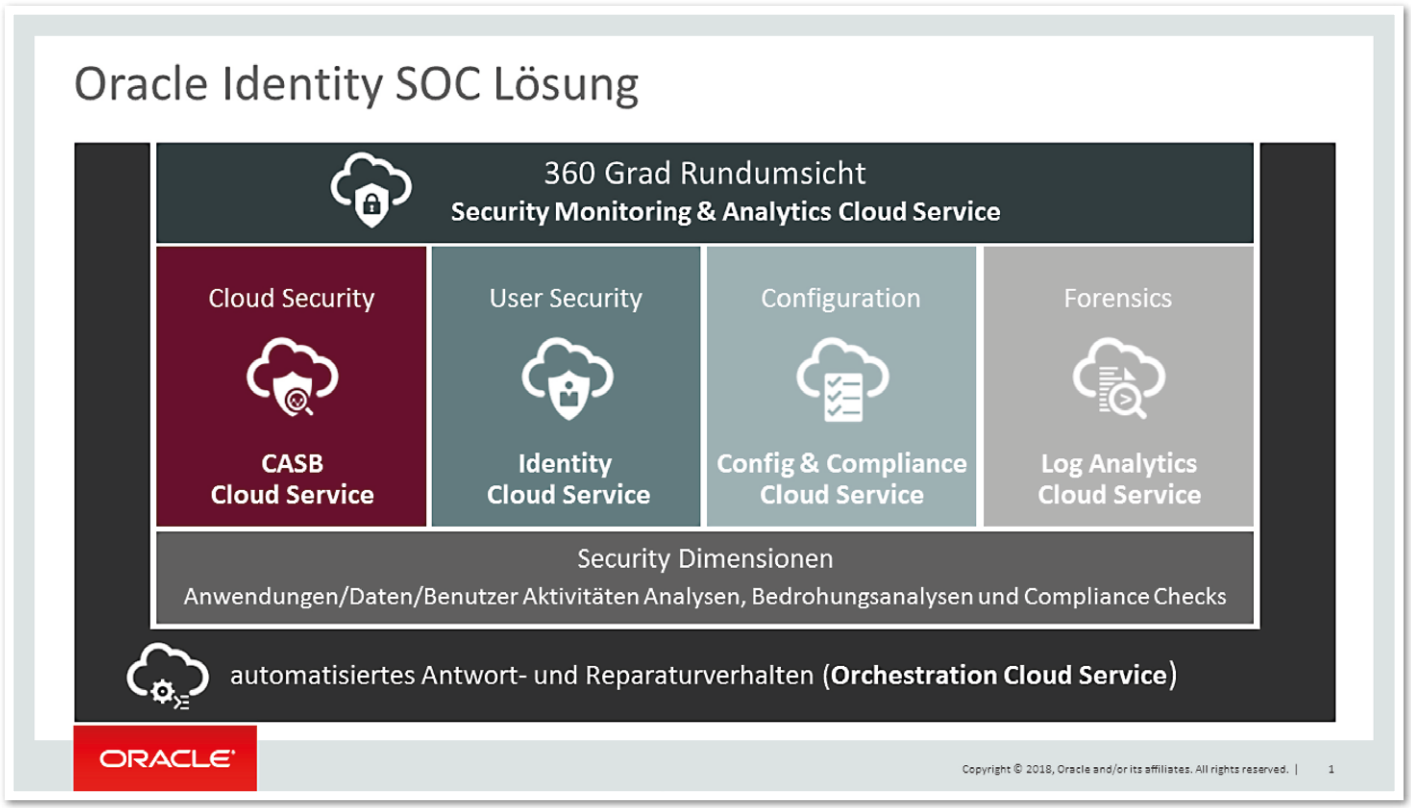


Abbildung 4: Angriffsabwehr und Systemschutz

ten Hauptkategorien in Beziehung zueinander gesetzt. Nach oben hin, in Richtung der Anwendungen, versteht sich Sicherheit als „Managing Personal Data". Nach unten hin, in Richtung der Infrastruktur, realisiert sich Sicherheit im Kontext der Infrastruktur als „Protecting Personal Data".

„Managing Personal Data" muss im Sinne der EU-DSGVO die fachlichen Rechte der Person an ihren Daten umsetzen. Das beginnt mit Funktionen zur Verwaltung der Einwilligung, die eine Person für die Verarbeitung ihrer personenbezogenen Daten abgibt. Dazu gehört auch die Implementierung für die Daten-Migration, entsprechend dem Recht auf Datenübertragbarkeit gemäß Artikel 20. Die Artikel 16 bis 19 der Verordnung [4] spezifizieren das Recht auf Berichtigung, auf Löschung, auf Einschränkung in der Verarbeitung sowie auf entsprechende Mitteilungspflicht im Verarbeiten der personenbezogenen Daten.

Im Kontext der funktionalen Sicherstellung dieser individuellen Rechte der Person gewinnen dann insbesondere auch die Auflagen der EU-DSGVO hinsichtlich Auditing, Dokumentation und Benachrichtigung ihre hohe Bedeutung. Nicht nur die EU-DSGVO, auch andere Compliance-Regelungen schreiben diesbezüglich den Unternehmen im Rahmen ihrer branchenüblichen Vorgaben [5] ein detailliertes Reporting in der Datenverarbeitung vor. Rechte sind also nicht nur entsprechend funktional abzubilden, sondern es ist auch die detaillierte Nachvollziehbarkeit und Berichtsführung hinsichtlich der Compliance gefordert.

Oracle-Datenbanken auditieren alle Zugriffe auf die Datenbanken im sogenannten „Audit-Log". Auf dessen Basis können dann Sicherheitshinweise bei sicherheitskritischen Ereignissen an die Administration gemeldet werden oder nachträglich forensische Untersuchungen, im Falle von Datenmissbrauch, durchgeführt werden.

Die von Oracle angebotene Audit-Vault-Lösung kann Verarbeitungsdaten sowohl von On-Premises- als auch von Cloud-Datenbanken sammeln. Es lassen sich Oracle- und auch Nicht-Oracle-Datenbanken protokollieren, ebenso wie Operating-System- und Network-Logs sowie die Log-Dateien der Anwendungen. Auf deren Basis können über den Audit Vault Database Firewall Server (AVDF) Audit-Reports erstellt werden. Diese sind im Rahmen der Compliance-Regelungen als Nachweis verwendbar.

Schutz des IT-Gesamtsystems

Durch die Häufung der kriminellen Angriffe wird das für die Unternehmen auch insbesondere im Blickwinkel der Datenschutz-Grundverordnung wichtig. Als Cloud-Provider muss sich Oracle mittlerweile auch verstärkt auf das Sicherheitsmanagement im IT-Gesamtzusammenhang konzentrieren, das unter dem Begriff „Security Operation Center" (SOC) zusammengefasst ist. Wichtige Prinzipien, denen der SOC-Ansatz maßgeblich folgt, sind:

- Zentralisierung und Standardisierung der sicherheitsrelevanten Informationen
- Machine Learning für die Überwachung und Krisenintervention

Die Konzepte für das SOC gibt es mit SIEM [6] und UEBA [7] schon seit einigen Jahren. Bei SIEM wird ein Ansatz des Sicherheitsmanagements verfolgt, der darauf abzielt, eine ganzheitliche Sicht auf die Sicherheit in der Informationstechnologie eines Unternehmens zu entwickeln. UEBA ist ein Machine-Learning-Modell, das helfen kann, Sicherheitsanomalien aufzudecken und Cyber-Attacken zu identifizieren. Im großen Stil eines RZ-Betriebs geht das nur, wenn alle die Sicherheit betreffenden Daten standardisiert und vergleichbar gemacht sind.

Im Jahr 2017 hat Gartner im Rahmen einer Forschungsarbeit dieses komplexe Zusammenspiel der Angriffsabwehr beschrieben. Entsprechend Gartner lässt sich das

„CARTA-Verständnis“ [8] folgendermaßen zusammenfassen: „Die Strategie des Verteidigungsansatzes muss der kontinuierlichen Risikoanpassung und der kontinuierlichen Prüfung darauf, ob dem System noch vertraut werden kann, folgen.“ In komplexen Systemen funktioniert das nur über Machine-Learning-Ansätze, bei denen standardisiert und permanent auf Abweichungen überwacht wird. „CARTA“ steht für „Continuous Adaptive Risk and Trust Assessment“. *Abbildung 4* fasst diese Gesamtsicht nochmals abschließend zusammen.

Weitere Informationen

[1] IDC Perspective – „Ten Myths regarding GDPR: Sifting Fact from Fiction“, Kuan Hon, Duncan Brown, June 2017, IDC #EMEA42628217

[2] Artikel 25 „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“.

[3] Artikel 30 „Verzeichnis von Verarbeitungstätigkeiten“, Artikel 35 „Datenschutz-Folgenabschätzung“

[4] Artikel 16 „Recht auf Berichtigung“, Artikel 17 „Recht auf Löschung“, Artikel 18 „Recht auf Einschränkung der Verarbeitung“, Artikel 19 „Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung“

[5] Zum Beispiel „Health Insurance Portability and Accountability Act“ (HIPAA) oder „Sarbanes-Oxley Act“ (SOX)

[6] „Security Information and Event Management“ (SIEM)

[7] „User and Entity Behavior Analytics“ (UEBA)

[8] Gartner – „Use a CARTA Strategic Approach to embrace Digital Business Opportunities in an Era of Advanced Threats“, Neil MacDonald, Felix Gaehtgens, May 2017, ID #G00332400

Ernst Lorenz
ernst.lorenz@oracle.com

In sieben Schritten zu EU-DSGVO-Verfahrenshandbuch & Co.

Mag. Wolfgang Klinger und DI (FH) Ernst Stippl, Sphinx IT Consulting GmbH

Es gibt viele Gründe, sich nicht mit langweiliger Dokumentation zu beschäftigen. Doch die DSGVO ist in diesem Punkt ganz klar: Personenbezogene Daten und deren Verarbeitungen müssen dokumentiert sein. Dieser Leitfaden hilft in sieben Schritten, die DSGVO-relevanten Dokumente rechtzeitig fertigzustellen, um auch nach dem 25. Mai 2018 ruhig schlafen zu können.

Wie verspeist man einen Elefanten? – In kleinen Häppchen!

Die DSGVO ist ziemlich umfangreich und besser in strukturierten Teilen zu genießen; das ist bekömmlicher und kann auch sehr zum Vorteil des Unternehmens sein: Das große Aufräumen im Sinne der DSGVO bringt Übersicht, Transparenz, spart Ressourcen und schafft Platz für Neues. Ist es wirklich sinnvoll, Marketing-Aussendungen an möglichst viele Adressaten zu schicken? Ist eine kleinere, wirklich interessierte Zielgruppe nicht ohnehin die bessere Alternative? Sind die Heerscharen von Office-Dokumenten, die auf diversen Servern gestrandet sind, nicht sowieso besser in einem Dashboard mit genau geregelten Zugriffsrechten aufgehoben? Die DSGVO kann Anlass dafür sein, sich mit Projekten zu befassen, die bisher immer auf die lange Bank geschoben wurden.

Es gibt teilweise Unschärfen in der DSGVO. Wie diese letztendlich zu interpretieren sind, wird sich – wie bei jedem juristischen Text – erst in zukünftigen Gerichtsurteilen herausstellen. Es gibt aber auch Abschnitte mit klaren Vorgaben, etwa bezüglich der zu erstellenden Dokumente, allen voran das „Verzeichnis von Verarbeitungstätigkeiten". Diese Dokumente sind im Bedarfsfall vorzuweisen, also dann, wenn die Behörde eine entsprechende Anfrage stellt. Es ist jedenfalls besser, vorbereitet zu sein, um einen guten Start in der Zusammenarbeit mit der Behörde hinlegen zu können. Der Artikel stellt eine Möglichkeit vor, sich der Erstellung dieser Dokumente anzunähern.

Schritt 1: Betroffene Daten erheben

Zunächst muss klar sein, welche Daten im Unternehmen überhaupt gespeichert sind. „Personenbezogen" ist dabei sehr umfassend zu sehen – es inkludiert auch IP-Adressen, Cookies, Fotos und Kundennummern. Alles, was eine Person eindeutig identifizierbar macht, fällt darunter. Dabei sind auch harmlos erscheinende Daten zu berücksichtigen, die in Kombination miteinander plötzlich wieder zur eindeutigen Identifizierbarkeit führen können.

Zu klären ist: Welche Daten werden von Mitarbeitern, Kunden, Lieferanten oder Geschäftspartnern gespeichert? Sind auch besonders sensible Daten dabei, wie etwa Gesundheitsdaten oder Religionsbekenntnis?

Das Vorgehen: Es ist nicht ganz einfach und klingt aufwendig, kann aber durch automatisiertes Durchsuchen von Datenbeständen und geführtes Einbeziehen wissender Mitarbeiter gut unterstützt werden. Personenbezogene Daten werden von Applikationen verwaltet oder sind als identifizierbare Datenbestände (Dateien) auffindbar.

Ergebnis: die Liste der Daten, die im Unternehmen von der DSGVO betroffen sind.

Schritt 2: Verarbeitungen beschreiben

Welche Verarbeitungen werden mit den in Schritt 1 identifizierten Daten durchgeführt? Gibt es Daten, die nicht mehr verwendet werden? Dann ist es am besten, diese zu löschen. Der Grundsatz der Datenminimierung zieht sich wie ein roter Faden durch die DSGVO. Das heißt, es soll sowohl der Zugriff auf Daten als auch deren Speicherung nur im wirklich notwendigen Ausmaß erfolgen – es muss also immer einen Grund dafür geben. Zu klären ist:

- Wer ist für welche Daten verantwortlich?
- Für welchen Zweck werden welche Daten gespeichert?
- Was genau passiert mit welchen Daten (Art der Verarbeitung)?
- Wie lange werden welche Daten gespeichert und warum?
- Wer hat Zugriff auf die Daten und an wen werden sie weitergegeben?

Das Vorgehen: Jetzt beginnt die Hauptarbeit! Eine gute Vorlage für das Verfahrenshandbuch gibt es beispielsweise bei der WKO *(siehe „www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verarbeitungsverzeichnis-verantwortliche.html")*. Die Autoren empfehlen, hier ein paar Euro in eine Software-Lösung zu investieren. Man wird damit durch die Fragen gut geführt und mehrere Leute können gleichzeitig daran arbeiten. Man kann auch einen DSGVO-Kundigen von extern hinzuziehen, der aktiv mitarbeitet oder den Fortschritt verfolgt und Tipps gibt. Auch spätere Anpassungen sind viel leichter und das Verfahrenshandbuch kann immer auf dem letzten Stand gehalten werden.

Ergebnis: das Verfahrenshandbuch (Verzeichnis der Verarbeitungstätigkeiten) mit allen vorgeschriebenen Inhalten.

Schritt 3: Richtige Reaktion bei Anfragen von Betroffenen festlegen

Es gibt eine kurze Liste an Rechten, die Betroffene, von denen das Unternehmen Daten gespeichert hat, einfordern können. Diese Liste ist zwar nicht lang, aber es ist wichtig, sich vorab zu überlegen, wie diesen Rechten entsprochen werden kann. Im Anlassfall kann ein Betroffener eines seiner folgenden Rechte einfordern:

- Informationspflicht
- Auskunftsrecht
- Recht auf Berichtigung
- Recht auf Löschung („Recht auf Vergessenwerden")
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht

Das Vorgehen: Für die Erhebung dieser Informationen ist mindestens eine Person nötig, die sich mit den Abläufen in der Firma auskennt, und eine, die mit den IT-Systemen gut vertraut ist. Moderierte Intensiv-Workshops in Kombination mit Hausaufgaben für diese Kollegen bringen aus Erfahrung der Autoren am schnellsten die gewünschten Ergebnisse.

Ergebnis: eine Prozess-Beschreibung für den DSGVO-konformen Ablauf für jede dieser Anfragen sowie Arbeitsanweisungen und Schulung für die verantwortlichen Mitarbeiter.

Schritt 4: IT-Anwendungen und -Systeme auf DSGVO-Konformität untersuchen

Die obigen Schritte auf Anfragen von Betroffenen sind in manchen Umgebungen nicht uneingeschränkt umsetzbar; vor allem das Recht auf Löschung kann eine Anpassung der Systeme erfordern. Logisches Löschen durch Setzen eines Löschkennzeichens kann zumindest als temporäre Lösung dienen, wenn physisches Löschen nicht ohne Weiteres implementierbar ist. Wichtig ist, den Zugriff auf die logisch gelöschten Daten zuverlässig zu verhindern. Vorhandene IT-Anwendungen müssen daher auf Erfüllung der DSGVO-Vorgaben geprüft werden:

- Welche Anwendungen sind im Einsatz?
- Wie werden die Betroffenenrechte mit diesen Anwendungen verwirklicht (beispielsweise die saubere Löschung von Daten)?
- Gibt es „Office-Applikationen" (Word, Excel etc.), die personenbezogene Daten verarbeiten, die oft verstreut auf den Filesystemen herumliegen?

Das Vorgehen: Auflistung der DSGVO-relevanten Funktionen in einem Applikationskatalog. Gleichzeitig wird überprüft, in welchem Maße die vorhandenen Applikationen die DSGVO-Personenrechte unterstützen.

Ergebnis: eine Liste der Applikationen, aus der ersichtlich wird, welche DSGVO-

konform sind und welche nicht. Dadurch können die Investitionen für Applikations-Versionen transparent gemacht werden, um sie DSGVO-konform zu machen.

Schritt 5: Richtige Reaktion bei Missbrauch der Daten festlegen

Wenn Daten gestohlen werden, ist rasches Handeln angesagt, denn die DSGVO schreibt enge Fristen vor. Daher ist es wichtig, für den Anlassfall vorbereitete Abläufe bei der Hand zu haben, die überlegt ausgearbeitet sind. Denn wenn es so weit ist, gibt es ohnehin Stress genug. Folgendes ist zu tun:

- Feststellen, welche Daten wie kompromittiert wurden. Hier kann in weiterer Folge forensische Arbeit nötig sein, für die eventuell Unterstützung von außen erforderlich ist.
- Meldung an die Aufsichtsbehörde, Muster siehe *„www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-data-breach-notification-behoerde.html"*
- Meldung an die Betroffenen, Muster siehe „Muster: *www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-data-breach-notification-betroffene.html"*

Das Vorgehen: Als Basis dient eine geeignete Vorlage (Anwalt, WKO etc.), die an das Unternehmen angepasst wird. Am wichtigsten sind die Erstellung einer Checkliste oder Arbeitsanweisung sowie die Schulung der Mitarbeiter, die an der Analyse und Aufarbeitung eines Datendiebstahls involviert sein werden. Sie müssen im Anlassfall unter Stress schnell und richtig reagieren können.

Ergebnis: Prozessbeschreibungen für die DSGVO-relevanten Meldungen, Arbeitsanweisung und Schulung für verantwortliche Mitarbeiter sowie eine Definition von Maßnahmen (technisch, organisatorisch), um das Risiko für solche Vorfälle zu senken.

Schritt 6: Sicherheit der mobilen Endgeräte überprüfen

Mobile Endgeräte führen leicht zu unkontrollierter Verbreitung von Daten, der Schutz auf diesen Geräten wird oft übersehen. Besonders kritisch sind Geräte, auf denen Apps vom Anwender frei installiert werden dürfen und die möglicherweise Daten auslesen und weiterreichen, ohne das an die große Glocke zu hängen. Das ist bei Apps leider nicht die Ausnahme, sondern fast schon die Regel. Mobile Device Management (MDM), das etwa das Löschen aus der Ferne ermöglicht, sowie die Einschränkung der Benutzerrechte am Gerät sind hier wesentliche Faktoren.

Wie sicher sind Laptops, Tablets, Handys & Co. und wie kann technisch und organisatorisch sichergestellt werden, unerlaubten Zugriff auf personenbezogene Daten zu verhindern?

Das Vorgehen: Anlegen eines Software- und Datenverzeichnisses mit Schwerpunkt auf Sicherheitsfunktionen.

Ergebnis: Definition von Maßnahmen (technisch, organisatorisch), um das Risiko für unerlaubte Zugriffe oder unbeabsichtigten Datenverlust zu senken, und ein Zeitplan für die Umsetzung.

Schritt 7: Spezialfälle prüfen

Als letzter Schritt ist zu prüfen, ob auch nichts übersehen wurde. Durch die Art der Verarbeitung (etwa Video-Aufzeichnungen oder Profiling) oder bei speziellen Daten (wie Gesundheitsdaten) können durch Kombination zusätzliche Informationen entstanden sein, die ebenfalls berücksichtigt werden müssen. Unter Umständen sind für diese Informationen eigene Dokumentationen nötig. Es ist zu klären, welche Spezialfälle auf das Unternehmen zutreffen, für die weitere Dokumente im Sinne der DSGVO vorhanden sein müssen.

Das Vorgehen: Es werden die in Schritt 1 und 2 erhobenen Informationen so kombiniert, dass dadurch mögliche Spezialfälle sichtbar werden. Beispiele dafür wären die Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten oder die Frage, ob eine Datenschutz-Folgenabschätzung durchgeführt werden muss.

Ergebnis ist eines oder mehrere der folgenden Dokumente:

- Dokumentation der Einwilligungserklärungen *(siehe „https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Einwilligungserklaerung-.html")*
- Dokumentation der Sicherheitsmaßnahmen
- Dokumentation der Risikoabschätzung
- Dokumentation von Arbeitsanweisungen
- Mustervertrag für die Auftragsverarbeitung *(siehe „https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag-auftragsverarbeitung.html")*
- Dokumentation der Geheimhaltungspflicht *(siehe „https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verpflichtungserklaerung-datengeheimnis.html")*

Ein abschließender Tipp

Am besten ist es, alle Überlegungen und Entscheidungen, die zur DSGVO angestellt werden, gleich im Verzeichnis von Verarbeitungstätigkeiten zu dokumentieren. Es ist das zentrale Dokument zur DSGVO-Konformität und erleichtert die Nachvollziehbarkeit aller Entscheidungen in Bezug auf den Datenschutz, wenn alles an einem Ort zusammengefasst ist. Auch wenn es Überlegungen gibt, die für das Unternehmen als nicht relevant erachtet wurden, sollten diese trotzdem zu Dokumentationszwecken inklusive Begründung in das Verzeichnis aufgenommen werden.

Fazit

Das Sieben-Punkte-Programm ist eine pragmatische Vorgehensweise, die einfache Methoden, bewährte Vorlagen, eine schlanke Software-Lösung und Mitarbeiter-Schulung umfasst. Damit ist man bezüglich aller Dokumentationspflichten im Sinne der DSGVO „auf der sicheren Seite". Im Zuge des Sieben-Punkte-Programms werden zusätzliche Erkenntnisse gewonnen, die Unternehmen in Form von Verbesserungsvorschlägen und neuen Ideen viel nützen können:

- Die Verbesserung von Abläufen sorgt für höhere Effizienz und Transparenz
- Mehr Informationen aus vorhandenen Daten zu ziehen, hilft bei der laufenden Verbesserung der Dienstleistung oder der Produkte
- Ausmisten unnötiger Daten oder Verarbeitungen schafft Luft für Neues und entlastet die Mitarbeiter
- Das Schaffen der Awareness bei Mitarbeitern ist eine gute Vorbeugungsmaßnahme gegen Datenverlust durch Angriffe von innen und außen
- Das Erhöhen der Betriebssicherheit senkt das Risiko von Geschäftsausfällen

Mag. Wolfgang Klinger
wolfgang.klinger@sphinx.at

DI (FH) Ernst Stippl
ernst.stippl@sphinx.at

Datenschutz-Grundverordnung für Datenbank-Administratoren

Alexander Kornbrust, Red Database Security

Am 25. Mai 2018 tritt die europäische Datenschutz-Grundverordnung (DSGVO, engl. GDPR) [1] in Kraft. Diese Verordnung umfasst 99 Artikel und 173 Erwägungsgründe (Abmilderungen/Einschränkungen). Der Artikel konzentriert sich auf das Thema „Administration von Datenbanken", da dort in der Regel personenbezogene Daten abgelegt sind.

Der Autor gibt keinen rechtlichen Beistand. Die nachfolgenden Informationen sind jedoch nach bestem Wissen und Gewissen zusammengestellt. Dabei wird auf folgende Fragen eingegangen:

- Was ist die DSGVO in wenigen Sätzen?
- Was hat ein DBA mit der DSGVO zu tun?
- Warum ist die DSGVO so schwierig umzusetzen?
- Was muss man minimal umsetzen?
- Wie findet man (automatisiert) personenbezogene Daten?
- Wie lässt sich die Abfrage einer Person nach ihren Daten umsetzen?

Man kann über die DSGVO ganze Bücher schreiben. Nachfolgend eine kurze, informelle Zusammenfassung über die Motivation der EU-Behörde und die Zielsetzung hinter dieser Verordnung. Das erste Hauptziel der DSGVO ist es, jedem Bürger das Recht zu geben, die Daten, die über ihn von Firmen/Organisationen in der EU gespeichert sind, zu sehen (Artikel 15), zu ändern/korrigieren (Artikel 16) und zu löschen (Artikel 17), falls diese rechtlich nicht mehr benötigt werden. Zudem kann die Verarbeitung der Daten eingeschränkt werden (Artikel 18).

Das zweite Hauptziel ist die Sicherstellung, dass Hackerangriffe (intern und extern) nicht mehr unter den Tisch gekehrt werden können, da die zuständige Aufsichtsbehörde innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls informiert werden muss (Artikel 33). Zusätzlich sind die vom Datenleck betroffenen Personen (Artikel 34) direkt oder durch öffentliche Bekanntmachung zu informieren.

Um diese beiden Ziele sicherzustellen, wurden die hohen Strafen hinzugefügt (Artikel 83). Gleichzeitig existiert ein Recht auf Schadensersatz bei betroffenen Personen (Artikel 82). Hinzu kommen allerlei Dokumentationspflichten (wie Verfahrensverzeichnis, Backup/Restore-Konzept etc.), die von den Firmen/Organisationen erfüllt werden müssen.

Der Datenbank-Administrator und die DSGVO

Im Grunde hat ein Datenbank-Administrator sehr wenig mit der DSGVO zu tun, da er normalerweise nicht für die (personenbezogenen) Systeminhalte verantwortlich ist. Anforderungen (Artikel 32) wie zeitnahes Restore

betroffener Systeme und Kapazitätsplanung sind in der Regel standardmäßig implementiert; der Datenbank-Administrator könnte sich also gemütlich zurücklehnen. Da er aber normalerweise hilfsbereit, wissend und vorausschauend ist, sollte er die Datenschützer und Anwendungsverantwortlichen nach Möglichkeit mit seinem Datenbank-Know-how bei der Umsetzung der DSGVO unterstützen.

DSGVO-Projekte sind deshalb so schwierig zu realisieren, weil es in den Köpfen der DSGVO-Verantwortlichen (Datenschutz, Juristen, Projektteam) nur ganz wenige (betroffene) Datenbanken gibt, in denen personenbezogene Daten vorhanden sind. In großen Firmen existieren oft mehr als hundert Datenbanken, in Konzernen sogar zwischen tausend und zehntausend (von relational bis zu Big Data). Diese Datenbanken enthalten nach Erfahrung des Autors zu einem großen Anteil personenbezogene Daten (je nach Definition beispielsweise Vorname, Nachname, E-Mail-Adresse etc.). In diesen Systemen sind Hunderte bis Tausende Tabellen mit personenbezogenen Daten üblich, die alle betrachtet werden müssen – auch wenn es zum Teil unterschiedliche Meinungen gibt („Diese Personendaten zählen nicht", „Das weiß der Kunde sowieso nicht", „Das sind ja nur ein paar Daten", „Wir machen nur Produktionssysteme"). Unter diese Datenbanken fallen natürlich auch die Q/A-, Pre-Live-, Test- und Entwicklungssysteme, sofern diese nicht vollständig anonymisiert sind, was normalerweise selten erfolgt, da man nicht genau weiß, wo überhaupt welche personenbezogenen Daten liegen.

Die minimale Umsetzung

Da bei Erscheinen dieses Artikels nur noch wenig Zeit für die Umsetzung bleibt, sollte man sich über die Priorität der DSGVO-Implementierung Gedanken machen. Wenn man x Leute fragt, wird man x+1 verschiedene Meinungen dazu erhalten. Der Artikel geht auf die Anforderungen ein, die ab 25. Mai 2018 eine Außenwirkung zeigen. Auch innerhalb weniger Wochen kann man viel erreichen, wenn man es wirklich will und einen Plan hat.

Anfrage einer Person nach ihren Daten

Da es sehr wahrscheinlich ab dem 25. Mai 2018 Anfragen zu Personendaten geben wird, sollte man den entsprechenden Workflow einsatzbereit haben. Die Antworten müssen spätestens nach einem Monat (Artikel 12) dem Anfragenden (kostenlos) zugesandt werden. Bei einer größeren Menge von Anfragen gibt es maximal zwei Monate mehr Zeit für die Beantwortung, Anfragen vom 25. Mai 2018 müssen also bis allerspätestens 25. August 2018 beantwortet sein.

Verzeichnis der Verarbeitungstätigkeiten für die Aufsichtsbehörde

Gemäß Artikel 30 ist ein Verzeichnis aller Verarbeitungstätigkeiten schriftlich zu führen, wenn eine Mindestanzahl an Mitarbeitern (mehr als 250, Erwägungsgrund 13) vorliegt. Dieses Verarbeitungsverzeichnis lässt sich beispielsweise aus einem Konfigurationsmanagementsystem (CMDB) erstellen und gemäß DSGVO um die üblicherweise fehlenden Informationen ergänzen (etwa Kategorie personenbezogener Daten, Dauer der Datenhaltung etc.).

Verhalten nach einem Hackerangriff

Zumindest auf dem Papier sollte definiert sein, wer im Falle eines Falles in welcher Zeit informieren sollte, welche (Forensik-)Daten von wem und wo zu sammeln sind und wer für die Kommunikation mit den Aufsichtsbehörden zuständig ist. Sollte es bereits einen Incident-Management-Prozess geben, empfiehlt es sich, die Datenschutz-Grundverordnung einzubauen.

Audit einer Wirtschaftsprüfungsgesellschaft

Da eine maximale Strafe von vier Prozent des Gesamtumsatzes ein (großes) Risiko für ein Unternehmen darstellt, werden die Wirtschaftsprüfungsgesellschaften zu diesem Thema prüfen. Da solche Prozesse oftmals Papierprüfungen sind, sollte man die entsprechenden Dokumente vorhalten beziehungsweise im Vorhinein erstellen (Artikel 32: Sicherheit der Verarbeitung, Backup/Recovery, regelmäßige Überprüfung etc.). Da Audits nicht gleich im Mai 2018 stattfinden werden, hat man bei diesem Punkt mehr Zeit.

Automatisiert personenbezogene Daten finden

Um die Anfrage einer Person nach ihren Daten beantworten zu können, sollte man sich einen Workflow überlegen. Dieser könnte wie folgt aussehen:

- Anfrage einer Person (per E-Mail, Webseite etc.)
- Identität der Person überprüfen (etwa anhand von Vertragsdaten, Video-Ident-Verfahren, Personalausweis [2], durch persönlichen Besuch etc.)
- Suche nach Daten dieser Person in (allen) Datenbanken
- Erstellung eines (maschinenlesbaren) Berichts
- Zusenden des Berichts zum Anfragenden

Dieser Workflow ist relativ einfach zu verstehen und in der Theorie einfach umzusetzen. Sobald man ihn jedoch realisieren soll, stößt man auf ein paar Probleme:

Deutsch	Englisch	Französisch
Vorname	Firstname	prenom
Nachname	Lastname	nom
Straße	Street	rue
PLZ	Zip	codepostal
Ort	Town	ville
Stadt	City	
Gebdat	Dob	ne
Geburtsdatum	Dateofbirth	datenaissance
...	...	...

Tabelle 1

```
Select * from acc.t_inv_osuser where vorna='Alexander' and
nachn='Kornbrust';
Select * from damrepo.osusers where vorname='Alexander' and
nachname='Kornbrust';
Select * from dam.kunden where firstname='Alexander' and
lastname='Kornbrust';
...
```

Listing 1

- Was sind personenbezogene Daten?
- Wo sind diese Daten abgelegt?
- Wie komme ich an diese Daten?

Die Definition der personenbezogenen Daten muss jede Firma/Organisation für sich selbst festlegen und auch regelmäßig aktualisieren. Hier gibt es zwar einen kleinsten gemeinsamen Nenner (Vorname, Nachname, Adresse, Geburtsdaten etc.), die Ansicht über weitergehende personenbezogene Daten (GPS-Daten, IP-Adressen etc.) ist innerhalb einer Firma allerdings oft unterschiedlich.

Sobald diese Daten definiert sind, sollte man eine Liste dieser Begriffe in unterschiedlichen Sprachen anlegen, da Datenbank-Entwickler oft die eigene Muttersprache zur Bezeichnung verwenden *(siehe Tabelle 1)*. Dabei ist zu beachten, dass es oft mehrere Synonyme für einen Begriff gibt (Lastname, namelast, lname, familyname, surname etc.), die alle zu überprüfen sind. Ob ein Begriff üblicherweise verwendet wird, lässt sich gut mithilfe einer Suchmaschine ausprobieren (beispielsweise durch die Suche nach „create table" „vorname varchar").

Sobald die personenbezogenen Daten definiert sind, kann man die Metadaten (Tabellen und Spaltennamen) der Datenbanken (Oracle, MSSQL, MySQL, SAP etc.) nach diesen Schlüsselwörtern durchsuchen. Dies kann mit Programmen wie Oracle Security Assessment Tool (nur Oracle, englisch) [3] oder gdprscan (mehrere Plattformen, mehrsprachig) [4] erfolgen. Der automatisierte Ansatz ist hier der manuellen Anfrage an die unterschiedlichen Fachabteilungen vorzuziehen, da er schneller und oft zuverlässiger ist.

Die Fundstellen in (nicht-leeren) Tabellen gilt es zu identifizieren; anschließend die Orte, in denen sich personenbezogene Daten befinden; also eine nicht-leere Tabelle mit Vorname, Nachname, Handynummer enthält in der Regel personenbezogene Daten. Normalerweise sind die Kunden überrascht, was alles in ihren Datenbanken gefunden wurde. Zum einen findet man am Anfang oft False-Positives (Suche nach „%ort%" findet auch „Port", „%RASSE%" auch „Strasse" etc.), was sich jedoch durch Finetuning/Ausnahmen verbessern lässt. Zum anderen findet man personenbezogene Daten oft in den privaten Schemata der Entwickler (Kopie der Produktionstabelle), in Backup-Tabellen („EMP_BCK", „EMP_03012011" etc.) oder im Oracle Recylce-Bin (das weiterhin zugreifbar bleibt). Diese Fundstellen sollten von den entsprechenden Fachabteilungen/Verantwortlichen kontrolliert und verbessert werden. Nicht notwendige Tabellen mit personenbezogenen Daten (Backup, Recycle Bin, private Kopien etc.) sind am besten gleich zu löschen.

Das Finden der Daten einer anfragenden Person mit manuellen Prozessen ist enorm zeitaufwendig – wenn man beispielsweise in zehn unterschiedlichen Abteilungen mit insgesamt hundert verschiedenen Anwendungen nachfragt, ob es Daten über einen „Hans Meier, geb. 23.12.1977" gibt. Diese Daten sind zu sammeln und weiterzuleiten. Hier entstehen pro Anfrage zum Teil Aufwände von mehreren Personentagen.

Alternativ kann man die bei der Analyse der Metadaten gewonnenen Daten mithilfe von dynamischen SQL-Befehlen abfragen, da man nun weiß, welche personenbezogenen Daten in welchen Tabellen beziehungsweise Spalten abgelegt sind. Dabei werden für jede Datenbank und jede Tabelle dynamische SQL-Befehle ausgeführt. *Listing 1* zeigt ein Beispiel.

Die Suche kann dann über mehrere Datenbanken erfolgen. Gegenüber der manuellen Abfrage von hundert Anwendungen bedeutet dies eine erhebliche Erleichterung und Zeitersparnis.

Fazit

Die europäische Datenschutz-Grundverordnung stellt enorme Anforderungen an jede Firma/Organisation. Anstatt den Kopf in den Sand zu stecken, sollte man sich auf die dringendsten Probleme wie Anfrage-Prozess und das Verarbeitungsverzeichnis konzentrieren, um ab dem 25. Mai 2018 nicht in den Fokus der zuständigen Datenschutzbehörde zu geraten. Datenbank-Administratoren können die Datenschützer beziehungsweise das DSGVO-Projektteam dabei stark unterstützen, indem sie sowohl das Finden von personenbezogenen Daten (per Metadaten-Analyse) als auch die Suche nach Daten einer bestimmten Person (per dynamischen SQL) automatisieren.

Weiterführende Links

[1] DSGVO: *https://dsgvo-gesetz.de*
[2] Personalausweis: *https://www.datenschutz-praxis.de/wp-content/uploads/s_November_14_web1.pdf*
[3] Oracle DSAT: *https://docs.oracle.com/cd/E76178_01/SATUG/toc.htm*
[4] GDPRSCAN: *http://www.gdprscan.de*

Alexander Kornbrust
ak@red-database-security.com

Data Analytics 2018: Der Zukunft ein Stück näher

Am 19. und 20. März 2018 fand die gemeinsame Data Analytics Konferenz von Oracle und der DOAG im Phantasialand in Brühl statt. Unter dem Motto „Daten als Motor der Digitalisierung" übertraf die 13. Data Warehouse Konferenz mit rund 250 Besuchern und 14 Ausstellern die Erwartungen.

Zukünftige Innovationen und Digitalisierung zogen sich durch die gesamte Veranstaltung wie ein roter Faden; besonders erfreulich: Neben Oracle-Experten und Großunternehmen hielten Kunden knapp 50 Prozent der Vorträge. Praxisnah berichteten beispielsweise Dominic Marx und Andreas Howanietz von DB Cargo über ihre Reise in die Cloud und welche Stolpersteine es auf dem Weg zu überwinden galt. Sie teilten ihre Erkenntnisse und gaben wertvolle Tipps und Tricks. Professor Hartmut Westenberger von der TH Köln stellte seine Studie zum Thema BI-Strategie und Industrialisierung vor. Die darauffolgende Frage- und Diskussionsrunde sprengte fast den Zeitrahmen und spiegelte das große Interesse wider.

Das Programm war vielfältig: Neben klassischen, technischen Themen fanden auch aktuelle Fragestellungen zu Machine Learning, Design Thinking, Geodaten, Datenschutzgrundverordnung und viele weitere Gehör. In der Eröffnungs-Keynote stellte Sohan de Mel, Vice President of Product Strategy und Business Development bei Oracle, das autonome Datenmanagement der Zukunft vor und sprach somit gleich das Hauptthema der Veranstaltung an.

Die Aktivitäten der Deutschsprachigen SAP-Anwendergruppe e.V. für die Umsetzung der EU-DSGVO

Dr. Mario Günter, Deutschsprachigen SAP-Anwendergruppe e.V.

Laut einer aktuellen Umfrage der Deutschsprachigen SAP-Anwendergruppe e.V. (DSAG) unter ihren Mitgliedern haben bisher gerade einmal etwas mehr als die Hälfte der befragten Firmen eine Vorgehensweise zur Umsetzung der EU-DSGVO in ihrem Unternehmen.

„Die neuen Vorschriften bringen einige Veränderungen mit sich – zum Beispiel mehr Verantwortung für den Nachweis der Rechtskonformität der Verarbeitung und der Datensicherheit. Darauf und auf die Systemkonformität werden die Wirtschaftsprüfer schauen. Es darf zum Beispiel im Berechtigungsmanagement keine generelle Freigabe geben. Unternehmen, die noch nicht aktiv geworden sind, sollten das schnellstmöglich nachholen", rät Mario Günter, Geschäftsführer der DSAG. Doch obwohl mehr als zwei Drittel der Befragten (73 Prozent) angeben, dass sie wissen, welche Anforderungen an die IT die EU-DSGVO mit sich bringt, haben bisher gerade einmal 53 Prozent der befragten Unternehmen eine Roadmap zur Umsetzung *(siehe Abbildung 1)*.

Einen Grund dafür sieht Mario Günter in den vielen noch zu klärenden Fragen. „Umfrage-Teilnehmer haben beispielsweise angemerkt, dass es aktuell noch keine Rechtsprechung zur EU-DSGVO gibt und sie Verständnisfragen haben. Hier fehlt es wohl an Transparenz", erläutert er. Daher sei nun zu befürchten, dass viele Unternehmen auf den letzten Drücker anfingen, die EU-DSGVO umzusetzen, ohne sich sauber und umfassend informiert zu haben.

Dementsprechend niedrig ist die Zahl derer, die wirklich zuversichtlich sind, dass ihr Unternehmen es schafft, sich fristgerecht bis zum Stichtag entsprechend den EU-Datenschutz-Vorgaben aufzustellen. Das sind 39 Prozent der Befragten. Dass knapp 61 Prozent der Umfrageteilnehmer wenig zuversichtlich sind, überrascht Mario Günter nicht. „Mit 99 Artikeln und 173 Erwägungsgründen, die alle beachtet werden müssen, braucht die EU–Datenschutz-Grundverordnung einfach eine lange Vorbereitungszeit", erläutert der Geschäftsführer. Deshalb sei auch die im Mai auslaufende zweijährige Übergangsfrist festgelegt worden, was zunächst einmal nach einer langen Zeit klänge. „Doch bei der Umsetzung der EU-DSGVO ist ein Jahr Projektdauer normal. Das ist natürlich auch vielen unserer Mitgliedsunternehmen inzwischen bewusst und sorgt für entsprechende Sensibilität", so Günter.

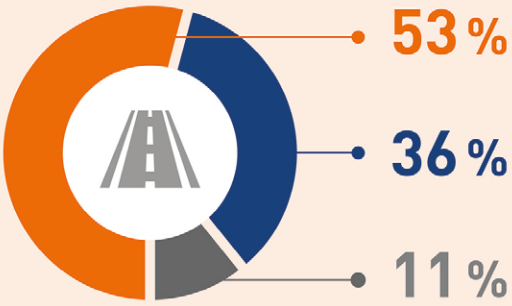
Bisher sind laut Umfrage erst knapp 4 Prozent der Befragten auf die Einführung vorbereitet und entsprechen bereits zum jetzigen Zeitpunkt den Anforderungen der Verordnung. Rund 66 Prozent der Befragten haben einige Vorbereitungen für die EU-DSGVO-Einführung getroffen, auch wenn sie noch nicht komplett konform sind. „Auch wir als Verband der Deutschsprachigen SAP-Anwender sind in der Umsetzung der Verordnung. Wir haben zum Beispiel in einem ersten Schritt eine Bestandsaufnahme in Bezug auf die Einhaltung heute noch bestehender Datenschutzgesetze und auf die DSGVO gemacht und dann weitere Maßnahmen evaluiert und umgesetzt", so Mario Günter.

Betroffen von der EU-DSGVO seien ja nicht nur Mitarbeiter- und Mitgliederdaten, sondern auch alle Bereiche, die personenbezogene Daten speichern, wie zum Beispiel Vertrieb, Marketing oder Buchhaltung. Da die Verordnung auch in den Personalwirtschafts-Lösungen der SAP oder in Human-Resources-Lösungen Anwendung findet, gibt es im Grunde kein Unternehmen, das die EU-DSGVO nicht umsetzen muss. Darüber hinaus betrifft die Einführung sämtliche Unternehmen mit SAP ERP- und Industrie-Lösungen, in denen Business-to-Customer-Geschäftsbeziehungen bestehen, wie zum Beispiel bei Versorgungs-, Telekommunikations- und Versicherungsunternehmen. „Da es für die Umsetzung der Verordnung in SAP ERP- und Industrie-Lösungen keine standardisierte Lösung im Rahmen eines Auslieferungskonzeptes gibt, raten wir unseren Mitgliedsunternehmen, die eigenen Unternehmensprozesse und Datenstrukturen zu überprüfen", erläutert Mario Günter.

EU-DATENSCHUTZ-GRUNDVERORDNUNG

AUS SICHT DER SAP-ANWENDER

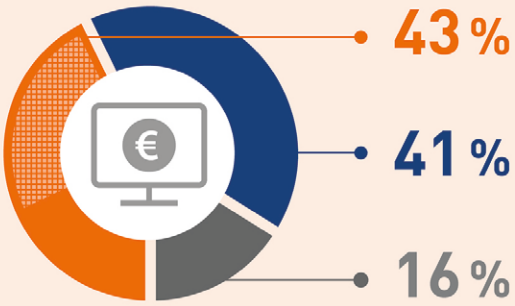
(DSAG-Mitgliederumfrage – November 2017)



53 Prozent der Unternehmen haben eine Roadmap zur Umsetzung.

36 Prozent der Unternehmen haben **keine** Roadmap zur Umsetzung.

11 Prozent der Befragten wissen nicht, ob ihr Unternehmen eine Roadmap zur Umsetzung hat.



43 Prozent haben zusätzliche Investitionen getätigt, um die Datenschutzanforderungen in ihrem Unternehmen umzusetzen. Etwas mehr als die Hälfte davon haben in die IT-Beratung investiert.

41 Prozent haben **keine** zusätzlichen Investitionen getätigt, um die Datenschutzanforderungen in ihrem Unternehmen umzusetzen.

16 Prozent wissen nicht, ob zusätzliche Investitionen getätigt wurden oder haben keine Angaben gemacht.

Wie zufrieden sind Sie mit der Unterstützung von SAP bezogen auf die Umsetzung der EU-DSGVO im SAP-System?

Wie zuversichtlich sind Sie, dass Ihr Unternehmen es schafft, sich fristgerecht entsprechend der EU-DSGVO aufzustellen?

61 %

Nicht sehr zuversichtlich / Gar nicht zuversichtlich

39 %

Sehr zuversichtlich / Zuversichtlich

Wissen Sie, welche Anforderungen an die IT die EU-Datenschutz-Grundverordnung mit sich bringt?

JA **73 %**

Wünschen Sie sich Datenschutz-Leitfäden, um Ihr SAP-System DSGVO-konform zu machen?

JA **89 %**

Datenbasis: Umfrage unter DSAG-Mitgliedsunternehmen der Arbeitsgruppe Datenschutz im Zeitraum Oktober/November 2017, 158 Teilnehmer (davon Unternehmen mit 0-499 Beschäftigten: 13%, 500-4.999 Beschäftigten: 38%, 5.000 oder mehr Beschäftigten: 41%, keine Angaben: 8%).

Abbildung 1: Die EU–Datenschutz-Grundverordnung aus Sicht der SAP-Anwender

Weitere Informationen unter www.dsag.de

Investitionsbereitschaft hoch

Wie etwa 43 Prozent der Befragten hat auch die DSAG zusätzliche Investitionen getätigt, um die EU–Datenschutz-Grundverordnung umzusetzen. Mehr als die Hälfte (54 Prozent) der Befragten, die investiert haben, steckten laut Umfrage zusätzlich Geld in die IT-Beratung. Zudem haben etwa 40 Prozent der Umfrageteilnehmer in Non-IT-Beratung investiert, knapp 14 Prozent in IT-Lizenzen und etwa 18 Prozent in sonstige Bereiche wie Hardware, Datenschutz-Software oder Personal.

Mario Günter überrascht die Bereitschaft, Geld auszugeben, wenig: „Je nachdem, gegen welche Norm ein Unternehmen verstößt, können künftig Bußgelder in Millionenhöhe fällig werden. Für solche Summen können die meisten Unternehmen nicht mal eben Rückstellungen bilden – es gilt Rechtskonformität herzustellen. Umso wichtiger ist es, sich mit der EU-DSGVO intensiv auseinanderzusetzen." Dabei begleitet die DSAG die SAP-Anwender unter anderem mit Veranstaltungen und einer Landingpage („*www.dsag.de/eu-dsgvo*", DSAG-Mitgliedschaft erforderlich), die alle relevanten Informationen entsprechend bündelt.

SAP-Anwender fordern mehr Unterstützung

Rund 89 Prozent der Befragten wünschen sich Datenschutz-Leitfäden, um ihre SAP-Systeme verordnungskonform zu machen. „Die Umfrage-Ergebnisse bestätigen, was wir zur EU-DSGVO bereits herausgehört hatten: Unsere Mitglieder erwarten einerseits von SAP die uneingeschränkte Umsetzung der Vorschriften. Andererseits erhoffen sie sich von SAP und durch den Austausch innerhalb der DSAG wichtige Hinweise und Tipps für ihre eigenen Datenschutzprojekte", erläutert Mario Günter.

Insbesondere, was die Unterstützung seitens SAP anbelangt, sehen die Mitglieder Nachholbedarf. Während nur etwas mehr als 11 Prozent der Befragten mit der Unterstützung durch SAP sehr zufrieden oder zufrieden sind, erwarten etwa 72 Prozent mehr. Sie sind nur mäßig oder gar nicht zufrieden mit dem, was SAP bezogen auf die Umsetzung der Datenschutz-Grundverordnung im SAP-System bietet. Sie erhoffen sich einerseits bessere Unterstützung seitens des Herstellers bezogen auf die Softwarelösungen, detaillierte Informationen zu den SAP-Standardtools und ein klares Statement, welche Unterstützung von SAP zu erwarten ist. Somit sind die Ergebnisse ein Spiegelbild der Diskussionen in den entsprechenden DSAG-Gremien.

DSAG fordert kostenfreie und effiziente Lösung

Die DSAG hat von SAP eine kostenfreie und effiziente Möglichkeit gefordert, um die Richtlinien der EU-DSGVO umzusetzen. Diese Forderung wird von zahlreichen Mitgliedsunternehmen unterstützt. Die DSAG steht im Austausch mit dem SAP-Vorstand, um sicherzustellen, dass die Abdeckung der EU–Datenschutz-Grundverordnung im Rahmen der Legal Compliance erfolgen wird. Innerhalb des DSAG-Vorstands ist das Thema bei Gerhard Göttert angesiedelt. Der Vorstand für den Bereich Anwendungsportfolio erklärt: „Wir brauchen Klarheit, welche Möglichkeiten unsere Mitglieder haben, die gesetzlichen Forderungen umzusetzen. Dass wir wenige Monate vor Ende der Übergangsfrist noch Klärungsbedarf mit SAP haben, ist nicht zufriedenstellend. Die Zeit drängt und wir brauchen nun rasch eine einfach umsetzbare und kostenfreie Lösung."

DSAG erreicht lizenzkostenfreie Lösung

Lange forderte die DSAG von SAP eine kostenfreie und effiziente Möglichkeit, um Anforderungen aus der EU–Datenschutz-Grundverordnung in SAP-Software umzusetzen. Im Januar 2018 ist SAP dieser Forderung nachgekommen. Ein großer Erfolg für die SAP-Anwender im deutschsprachigen Raum.

„Auf dem DSAG-Jahreskongress im September 2017 hat SAP unsere Forderung aufgegriffen und zugesagt, dass ihre Kunden in die Lage versetzt werden, Anforderungen aus der EU-DSGVO effizient und ohne zusätzliche Lizenzkosten zu erfüllen", so Gerhard Göttert, Mitglied des DSAG-Vorstands. Bis zu diesem Zeitpunkt gab es seitens SAP noch kein lizenzkostenfreies Angebot zur Umsetzung. Für die SAP-Anwender ein unbefriedigender Zustand, den es schnellstmöglich zu ändern galt – auch vor dem Hintergrund, dass die Frist, die Anforderungen aus der EU–Datenschutz-Grundverordnung umzusetzen, am 25. Mai 2018 endet.

Anforderungen aufwandsarm umsetzen

Viele der DSAG-Mitgliedsunternehmen sahen sich gezwungen, in zusätzliche Produkte von SAP zu investieren, um die gesetzlichen Anforderungen zu erfüllen. Insbesondere vor dem Hintergrund, dass ohne SAP NetWeaver Information Lifecycle Management (ILM) die Umsetzung der Vorgaben nur mit hohem Zusatzaufwand machbar ist. Das ILM wird unter anderem zum Sperren und Löschen von personenbezogenen Daten benötigt. „Wir brauchten also dringend Klarheit, welche Möglichkeiten unsere Mitglieder haben, die gesetzlichen Anforderungen kostenfrei und effizient umzusetzen", so Gerhard Göttert. Dabei war für die SAP-Anwender klar, dass die Lieferungen und die Verfügbarkeit einer aufwandsarmen Lösung zur Erfüllung von Anforderungen aus der EU-DSGVO über die Wartungsgebühren abgedeckt sein müssen.

DSAG-Forderung erfüllt

Dieser Forderung der DSAG kam schlussendlich auch SAP nach. „Wir sind zufrieden, dass SAP unseren Forderungen nachgekommen ist und sich kundenorientiert gezeigt hat", sagt Gerhart Göttert. Konkret hat SAP die Lizenz für SAP NetWeaver Runtime um die Retention-Management-Funktionen von ILM erweitert. Mit dieser Lösung und weiteren Standardfunktionen der SAP-Software – wie beispielsweise dem Berechtigungsmanagement – ist es möglich, die Projekte zur Realisierung der technischen und organisatorischen Maßnahmen in den Firmen umzusetzen.

Für Kunden, die ILM zur Erfüllung der gesetzlichen Anforderungen im Rahmen der EU–Datenschutz-Grundverordnung einsetzen, besteht eine Kompensationsregelung. Vor dem Hintergrund, dass viele Kunden ihre Umsetzungs-Projekte bereits beginnen und ihre Software lizenzieren mussten, ist die Kompensations-Regelung ein großer Erfolg für alle Anwender, da sie alle Kunden finanziell gleichstellt.

Über die DSAG

Die Deutschsprachige SAP-Anwendergruppe e. V. (DSAG) in Walldorf versteht sich als eine unabhängige Interessenvertretung aller SAP-Anwender in Deutschland, Österreich und der Schweiz. Ziel der DSAG ist es, darauf hinzuwirken, dass bedarfsgerechte SAP-Lösungen geschaffen werden, sowie den Erfahrungs- und Informationsaustausch sowohl der SAP-Kunden untereinander als auch mit SAP zu fördern. Die 1997 als eingetragener Verein gegründete DSAG zählt heute über 3.300 Mitgliedsunternehmen mit über 60.000 Mitgliedspersonen und hat sich als eine der größten SAP-Anwendergruppen weltweit etabliert. Weitere Informationen unter *„www.dsag.de"*, *„www.dsag.at"* und *„www.dsag-ev.ch"*.

Dr. Mario Günter
info@dsag.de

DWH-Modernisierung mithilfe eines Data Lake – die verschiedenen Umsetzungsmöglichkeiten in der Praxis

Fabian Hardt, OPITZ CONSULTING Deutschland GmbH

Inmitten von Digitalisierung und Industrie 4.0 haben sich die Anforderungen für die Speicherung und die anschließende Analyse an klassische, seit vielen Jahren etablierte Data-Warehouse-Systeme maßgeblich geändert. Bleibt dennoch der klassische Ansatz weiterhin das Mittel der Wahl oder sind Unternehmen gezwungen, die bestehende Data-Warehouse-Architektur zu modernisieren oder langfristig sogar zu ersetzen? Der Artikel geht dieser Frage nach und beleuchtet die jeweiligen Vor- und Nachteile anhand eines Praxisbeispiels.

Für Unternehmen kann es im Vorfeld einer Modernisierungsentscheidung hilfreich sein, sich die Möglichkeiten einmal genauer anzusehen. Wie sollte etwa eine Modernisierung aus technischer Sicht aufgebaut sein, um die stetig steigenden Anforderungen weiterhin angemessen erfüllen zu können? Im weiteren Verlauf werden einige Beispiel-Architekturen vorgestellt und deren Vor- und Nachteile betrachtet. Dabei wird deutlich, welche verschiedenen Möglichkeiten es bei der Modernisierung in der Praxis gibt und in welcher Konstellation Data Lakes zu Kosteneinsparungen in einer bestehenden Systemlandschaft führen können. Bevor es um die Frage geht, inwiefern ein Data Lake ein klassisches Oracle Data Warehouse (DWH) ersetzen oder vielleicht eher eine perfekte Ergänzung darstellen kann, ist es wichtig, beide Systeme klar voneinander abzugrenzen.

Mit Data Lakes große Datenmengen flexibel verarbeiten

Von einer hohen Abstraktionsebene aus betrachtet, handelt es sich bei einem Data Lake um eine alternative Datenspeicherungsmethode, die mithilfe sogenannter „Big-Data-Frameworks" arbeitet. In der Praxis kommen in einem Data Lake häufig Hadoop-Systeme zum Einsatz, kombiniert mit Software-Tools wie Apache Spark und Apache Kafka sowie mit einer Lambda-Architektur, um Daten auch in Echtzeit in angemessener Latenz verarbeiten zu können. Ein Data Lake erfüllt damit deutlich besser die typischen Big-Data-Anforderungen als ein klassisches DWH, da er aufgrund der hohen Skalierbarkeit deutlich besser für die Verarbeitung großer Datenmengen geeignet ist. Zudem ist ein Data Lake deutlich flexibler, was die Integration neuer Datenstrukturen und -typen angeht. Das ist dem „Schema on Read"-Paradigma geschuldet, auf das im nachfolgenden Abschnitt näher eingegangen wird.

„Schema on Read" vs. „Schema on Write"

Ein klassisches DWH beziehungsweise eine relationale Datenbank folgt dem sogenannten „Schema on Write". Hier ist das Zielschema im DWH vorgegeben und die Daten werden mit den Schritten „Extrahieren, Transformieren, Laden" (ETL) in die Form dieses Schemas gebracht. Das vorliegende Datenmodell und die darunterliegenden Strukturen orientieren sich vor allem an den Anforderungen der Nutzer. Der Vorteil dieses Paradigmas ist die automatisch hohe Datenqualität, die festgelegte Tabellenstrukturen und technische Hilfsmittel wie Constraints gewährleisten. Daten, die im Aufbau von diesen Strukturen abweichen, können nicht eingefügt werden. Der Nachteil: Das Vorgehen bei diesem Schema-Typ ist wenig agil. Bei jeder Veränderung der Quelldaten ist eine Anpassung der gesamten ETL-Strecke nötig.

Ein Data Lake hingegen folgt dem sogenannten „Schema on Read"-Paradigma. Hier erfolgt die Schematisierung erst beim Auslesen der Daten. Die Quelldaten liegen ohne Datenverlust vor und können zu einem späteren Zeitpunkt verarbeitet werden. Die Reihenfolge wäre jetzt also „Extrahieren, Laden, Transformieren" (ELT). In der Folge besteht bei Änderungen an den Quellsystemen keine direkte Abhängigkeit. Somit droht kein Datenverlust, wenn die Struktur der Quelldaten von der Struktur der Zieldaten abweicht. Lediglich bei der nachfolgenden Verarbeitung muss die Logik entsprechend angepasst werden, damit alle Daten ohne großen Aufwand nachträglich verarbeitet werden können. Ein Nachteil dieser „Schemalosigkeit" ist die fehlende Prüfung auf Datenintegrität. Nicht gefüllte Attribute oder falsche Datentypen in einer Spalte werden erst beim Auslesen der Daten erkannt und sind somit in der Ladelogik entsprechend zu berücksichtigen [1].

Mithilfe des „Schema on Read"-Vorgehens ist ein Erkenntnisgewinn aus den vorliegenden Daten jederzeit möglich, auch wenn zunächst keine Zusammenhänge vermutet wurden [2]. In der Praxis macht ist eine Kombination aus „Schema on Read" und „Schema on Write" sinnvoll. Das Resultat sind Architekturen, wie sie in *Abbildung 1* dargestellt sind. Es gibt einen „Rohdaten-Bereich" (Raw Data), in dem die Quelldaten zunächst im Ausgangszustand abgelegt werden. Parallel dazu wird eine „Data Refinery" betrieben. Diese dient als Preprocessing Area, ähnlich der Staging Area im DWH. Als letzter Baustein ist der „qualitätsgesicherte Bereich" (Refined Data) zu sehen. Dieser ist essenziell; er wird gesondert kontrolliert und verwaltet. In diesen Bereich gelangen nur Daten, die durch Data Cleansing – teilweise in Echtzeit – aufbereitet wurden. Häufig wird dieser Bereich auch „Data Reservoir" genannt und als separater Datenbereich betrachtet [3].

Damit ein Data Lake zu einem Data Reservoir wird, sind folgende Dinge zu beachten:

- Es ist ein Katalog erforderlich, der den Inhalt des Data Lake klassifiziert und Metadaten zu den Objekten bereitstellt.

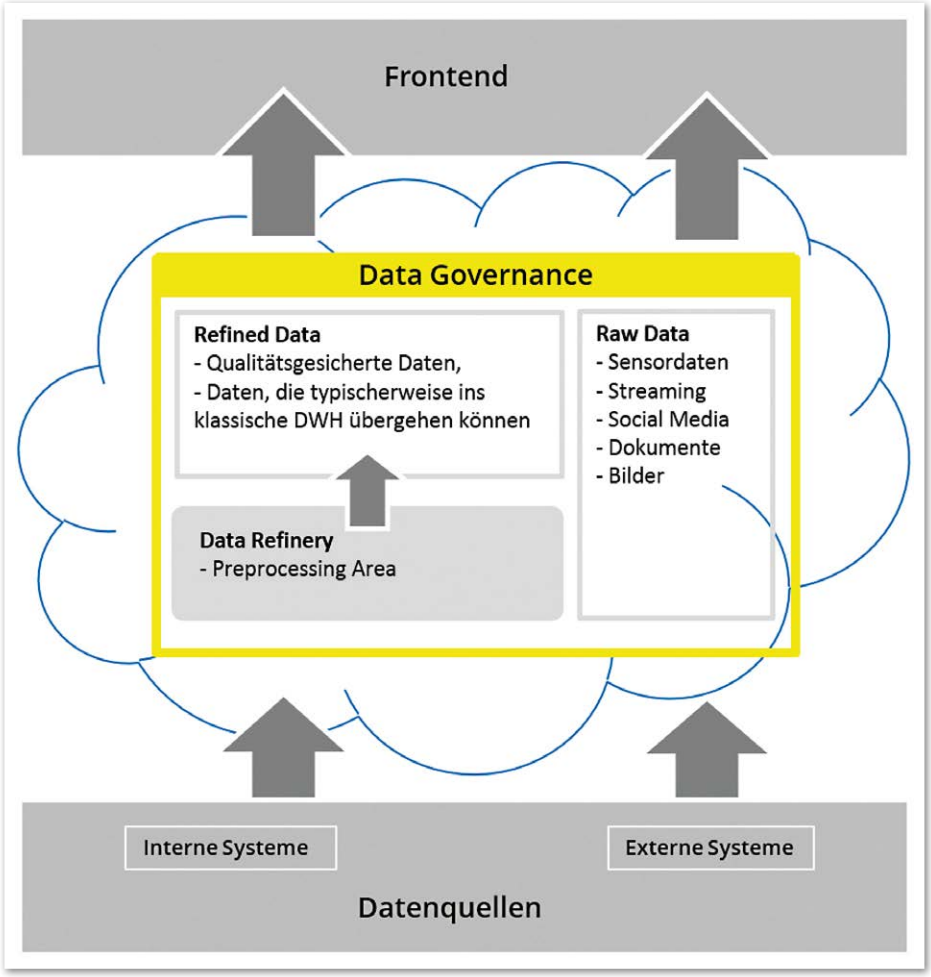


Abbildung 1: Data-Lake-Detailansicht

- Es gibt innerhalb des Reservoirs ein Berechtigungskonzept, analog zum DWH. Auch hier darf die Fachabteilung nur ihre eigenen Daten einsehen. Innerhalb des Reservoirs ist sowohl die zeitliche als auch die inhaltliche Konsistenz sichergestellt.
- Es besteht die Möglichkeit, ein Data Reservoir fachlich orientiert anzulegen; dies geschieht wie bei fachlich angelegten Data Marts im DWH. Diese sind für einen speziellen Zweck implementiert und bilden zum Beispiel einen Kernprozess des Unternehmens ab.

Das hybride Architektur-Szenario

Unter einer hybriden Architektur versteht man eine parallele Datenverarbeitung in einem Data Lake oder DWH *(siehe Abbildung 2)*. Hierbei wird die Kernkompetenz des jeweiligen Systems zu einem Maximum ausgeschöpft. Der hybride Ansatz nutzt somit die Vorteile beider Architekturen und ermöglicht auf diese Weise schnellere Innovationszyklen. Trotzdem lassen sich das DWH und sein teurer Speicher verkleinern, indem man einige Daten wie zum Beispiel unverdichtete Massendaten in den Data Lake verschiebt. Das bestehende DWH muss bei diesem Ansatz nicht direkt architektonisch verändert werden; alle Systeme für die Datenbeladung, Auswertungen und betriebliches Berichtswesen können weiterhin existieren.

Ein klassisches Beispiel wäre an dieser Stelle das Exportieren von berechneten KPIs, also sogenannter „Faktendaten". Diese sind im DWH-Prozess bereits vom Fachbereich abgenommen und somit diversen Qualitätssicherungsmaßnahmen unterzogen worden. Mithilfe eines Offloading-Verfahrens stehen diese Kennzahlen auch in einem Data Lake zur Verfügung.

Offloading als Kernelement der DWH-Modernisierung

Das Offloading-Vorgehen gewinnt im Zuge der Digitalisierung zunehmend an Bedeutung, weil an digitalen Geschäftsprozessen stets verschiedenste IT-Systeme beteiligt sind. Es wird künftig also nicht mehr ausreichen, ein DWH als die „Single Source of Truth" zu betrachten, zumindest nicht, solange es nicht eine umfassende Modernisierung erfahren hat. Im Zusammenspiel mit einem Data Lake kann das DWH befähigt werden, auch Informationen aus neuartigen Datenquellen zu verarbeiten und diese Informationen ganzheitlich zu ver-

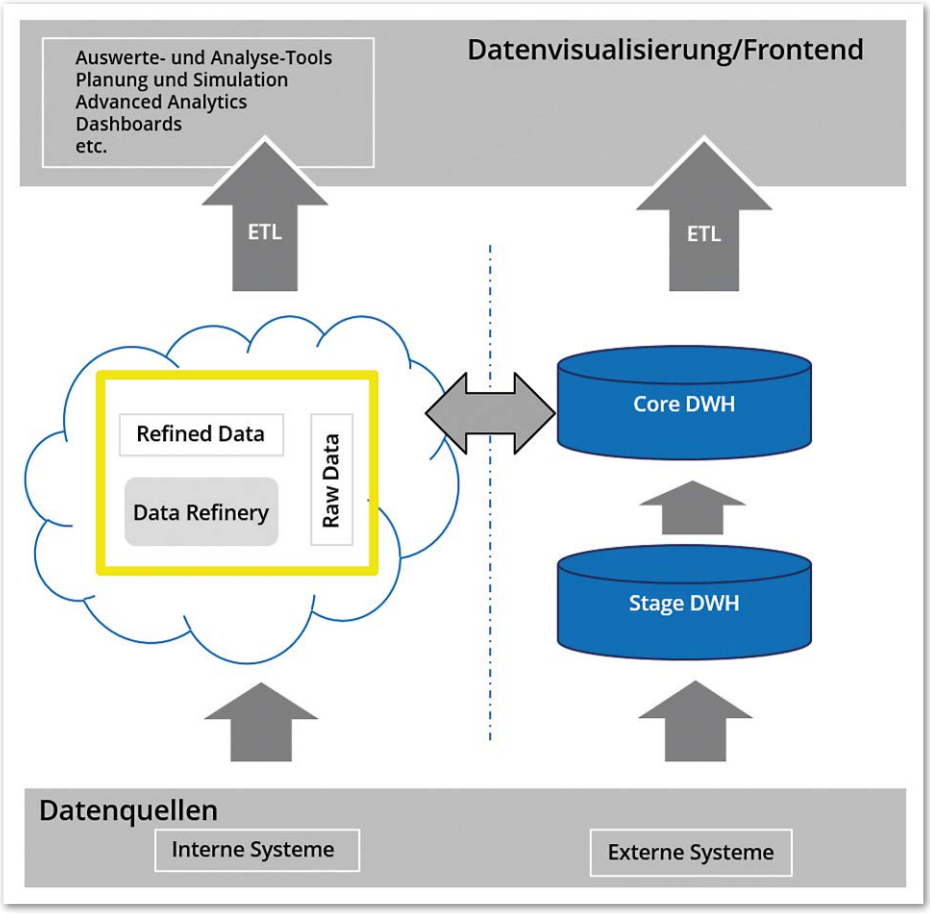


Abbildung 2: Hybride Architektur aus DWH und Data Lake

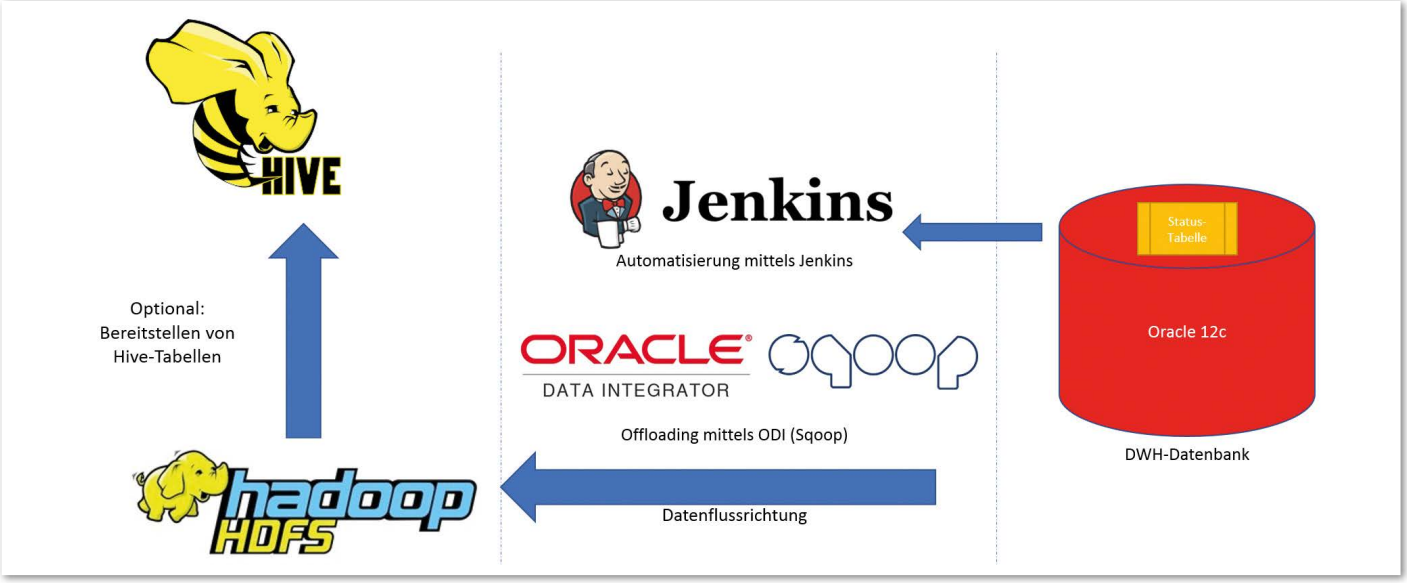


Abbildung 3: Unabhängiges Mastersystem

einen. Alternativ ist auch die Bildung von Datensilos möglich, um die Spezialisierung der verschiedenen Systeme zu nutzen und die Daten erst in einem gemeinsamen Frontend wieder zusammenzuführen. Es gibt verschiedene Möglichkeiten, ein Offloading-Vorgehen zu realisieren, und mehrere strategische Ansätze, um die technischen Hürden eines DWH-Offloading zu meistern:

- *Konzept für ein Mastersystem*
  An erster Stelle steht ein Konzept, aus dem ein sogenanntes „Mastersystem" hervorgeht. In vielen aktuellen Unternehmensinitiativen wird ein Big-Data-System als neues strategisches Mastersystem definiert, oftmals in Form eines Data Lake. In diesem Fall ist also ein DWH-Offloading zu implementieren, um die ganzheitlichen Unternehmensdaten in den Data Lake zu überführen. Dieses Architektur-Szenario bietet ein hohes Maß an Flexibilität, da ein Data Lake deutlich besser mit Echtzeit- und semistrukturierten Daten umgehen kann als das bestehende DWH-System. In diesem Fall findet ein Offloading der Daten vom DWH in den Data Lake statt.

- *Datenfluss vom Data Lake ins DWH*
  Als zweite Variante können Daten aus dem Data Lake ins DWH fließen. Es findet also ein Offloading in Richtung DWH statt. Dies kann vor allem dann sinnvoll sein, wenn eine Massendaten-Verarbeitung auf dem Big-Data-System durchgeführt werden soll und die hochgradig verdichteten Daten (Fakten) langfristig im DWH zu Auswertungszwecken erforderlich sind.

- *Neues Mastersystem*
  Eine dritte Möglichkeit kann sein, ein ganz neues System als Mastersystem zu etablieren, das die Metadaten der beiden Systeme hält und auch das Offloading in eine oder sogar beide Richtungen entsprechend überwacht und automatisiert. *Abbildung 3* zeigt einen technischen Vorschlag zur Realisierung einer solchen Systemlandschaft. Es wird ein neuer Master-Server aufgesetzt, der aus einer Oracle-Datenbank und einem Jenkins-Server besteht. Die Datenbank verwaltet sämtliche Metadaten, also Berechtigungen, technische Monitoring-Daten sowie fachliche Ladestände – genau die Metadaten, die eine Aussage darüber treffen, bis zu welchem Zeitraum die Daten erfolgreich zwischen den Systemen synchronisiert wurden.

Ein Praxisbeispiel für das Zusammenspiel von Data Lake und DWH

Dieser Abschnitt stellt ein hybrides Architektur-Szenario vor, das für einen Kunden des Autors aus der Telekommunikationsbranche entwickelt wurde und dort im produktiven Einsatz ist. Es besteht aus einem klassischen Data Mart und einem Data Lake als DWH-Core-Ersatz.

Die Kombination dieser beiden Systeme wurde gewählt, da die Berechnung von KPIs auf Call Data Records (CDRs) bisher ein technisch aufwendiger Prozess war, verbunden mit teuren Lizenzen und sehr langen Laufzeiten. Um den Mehrwert eines Data Lake in

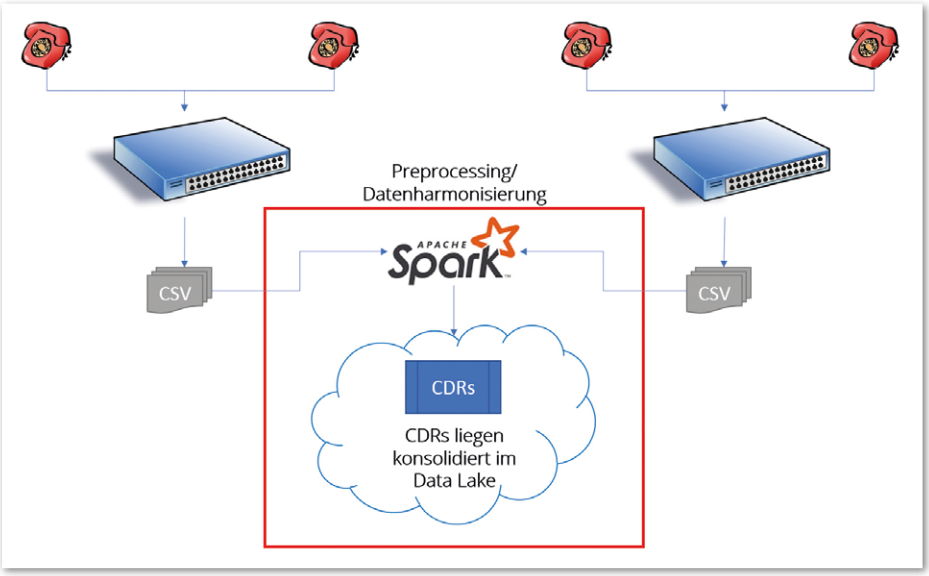


Abbildung 4: Der Erzeugungsprozess von Call Data Records

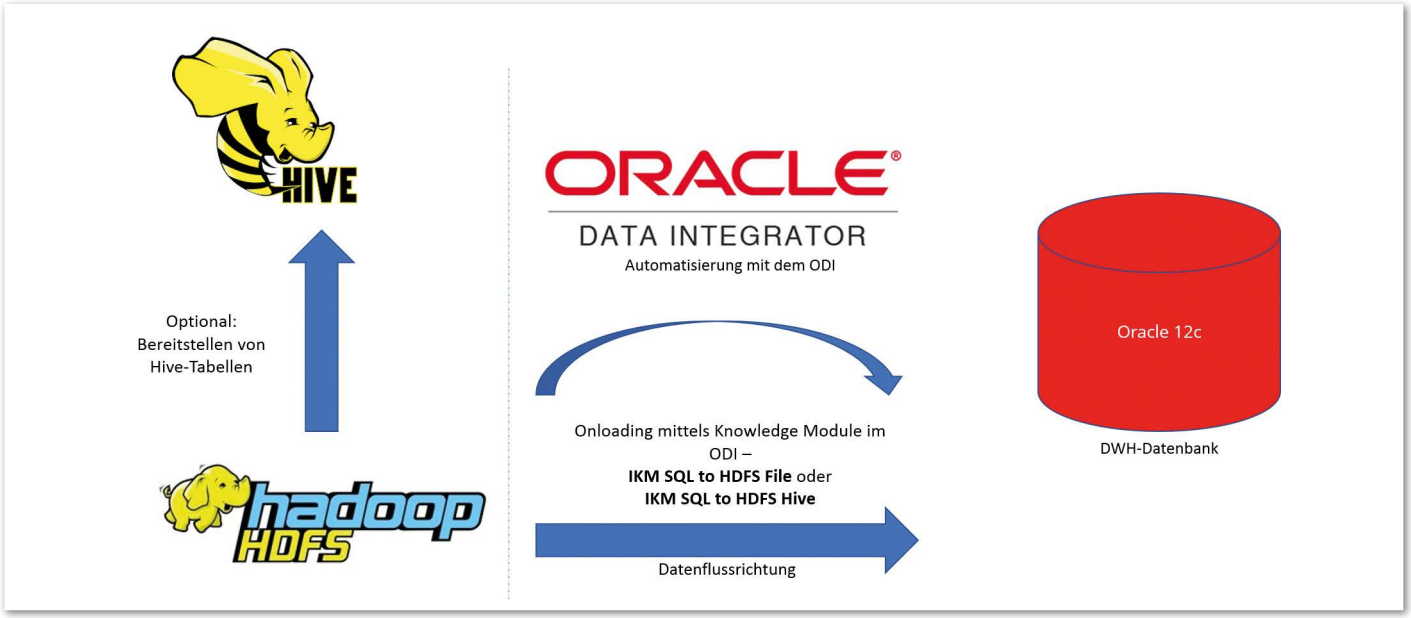


Abbildung 5: DWH-Onloading-Prozess

diesem Anwendungsfall nachzuvollziehen, ist zunächst ein gewisses Grundverständnis um den Erzeugungsprozess von CDRs vonnöten.

Abbildung 4 stellt den Prozess grafisch dar. Bei jedem Anruf werden die Detail-Informationen zur aufgebauten Verbindung von sogenannten Switches protokolliert und in Dateien abgespeichert. Da ein Telekommunikationsanbieter in der Regel Switches von diversen Herstellern im Einsatz hat, liegen die Daten in sehr unterschiedlichen Formaten vor. Dies betrifft sowohl die Struktur als auch den fachlichen Inhalt der Dateien. Daher müssen diese für eine Weiterverarbeitung harmonisiert und zusammengeführt werden. In der Regel findet dieser Vorgang in einer sogenannten „Mediationsphase" statt.

Das Ergebnis dieses Prozesses ist normalerweise eine sehr große Tabelle in einem relationalen Datenbank-System, die sämtliche Rohdaten zu den protokollierten Verbindungen enthält. Aufgrund der sehr hohen Datenmenge, die hier anfällt, handelt es sich um einen relativ kostenintensiven Verarbeitungsschritt. Diese Kosten werden durch teure Enterprise-Lizenzen und hohe Hardware-Anforderungen verursacht.

Die bereits angesprochene Mediationsphase mündet in einen sogenannten „Billing-Prozess". Dort werden die CDR-Daten um weitere Kundendaten angereichert, um die anfallenden Kosten einem bestimmten Kundenkonto zuordnen zu können. Erweiterte Auswertungsmöglichkeiten auf CDR-Basis sind an dieser Stelle meist nicht vorgesehen, weshalb viele Unternehmen auf die Idee kommen, diese Daten zusätzlich im Unternehmens-DWH zu verarbeiten, mit dem Ziel, weitergehende Kennzahlen zur Netzqualität oder zum allgemeinen Nutzerverhalten zu ermitteln. Sowohl aus Performance- als auch aus Datenschutzgründen werden die Daten dann oft nur temporär ins DWH geladen und nur so lange dort gespeichert, bis die Kennzahlen für den entsprechenden Tag erfolgreich berechnet wurden.

Genau an dieser Stelle war es für den Kunden sinnvoll, die Konsolidierung der Daten an eine zentrale Stelle auszulagern. Ein Big-Data-System eignete sich in diesem Fall sehr gut, da die Verarbeitung über dieses hochgradig parallelisiert und auf viele Rechenknoten verteilt werden kann. Die Dateien der Switches können direkt im Big-Data-System, beispielsweise mit einem Software-Tool wie Spark, verarbeitet und abschließend in einem Data Lake als zentralem Datenspeicherort abgelegt werden. Um Redundanzen bei der Verarbeitung dieser großen Datenmengen zu vermeiden, ist es empfehlenswert, sowohl die Billing-Daten als auch die weiteren KPIs, die zuvor im DWH berechnet wurden, im Big-Data-System zu berechnen. Anschließend können diese mit einem geeigneten Offloading/Onloading-Verfahren ins Zielsystem transferiert werden *(siehe Abbildung 5)*.

Sofern ein klassisches Oracle DWH inklusive des Oracle Data Integrator (ODI) im Einsatz ist, ist es auf recht einfach Weise möglich, ein Onloading (aus Sicht des DWH-Systems) durchzuführen und die Kennzahlen in die bestehende Datenlandschaft zu integrieren. Die aggregierten CDRs, die im Data Lake vorliegen, können mit dem Software-Tool Scoop, das bereits in den Knowledge-Modulen des ODI zum Einsatz kommt, ins DWH übertragen werden.

Auf diese Weise lassen sich die Tabellen im Data Lake ganz einfach in die Datentransformations-Logik im DWH integrieren und im regelmäßigen DWH-Batchprozess mitverarbeiten. So können Faktendaten, die bereits im Data Lake berechnet wurden, im DWH weiterverarbeitet werden. Ein Beispiel dafür ist die weitere Aggregation der Daten. Typischerweise werden die Verbrauchsdaten von Einzelkunden auch auf Monatswerte aggregiert und mit den Planumsätzen in Beziehung gebracht.

Quellen

[1] Sandmann, Big Data im Banking: Data Lake statt Data Warehouse?: *https://bankinghub.de/banking/technology/big-data-im-banking-data-lake-statt-data-warehouse*

[2] Pasupuleti/Purra, Data Lake Development with Big Data, Packt Verlag, Birmingham, 2015

[3] Reiss/Reimann, Das Data Lake Konzept: Der Schatz im Datensee: *https://www.it-daily.net/it-management/big-data-analytics/11222-das-data-lake-konzept-der-schatz-im-datensee*

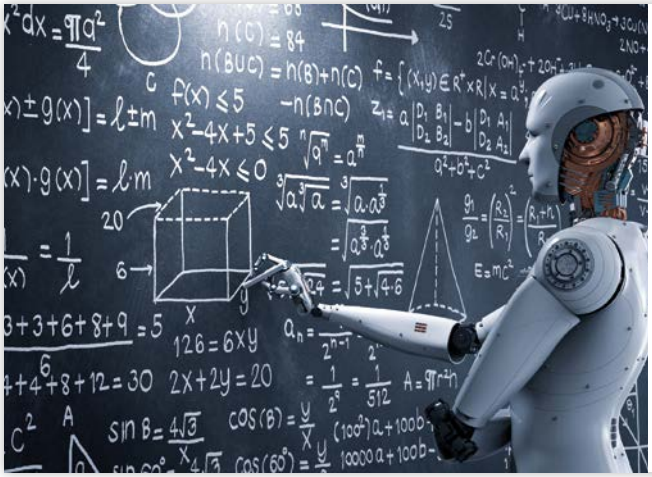
Fabian Hardt
fabian.hardt@opitz-consulting.com

20. - 21. September 2018 in Dresden

DOAG BIG DATA Days

Daten, der Treibstoff der digitalen Gesellschaft

Bis
10. August
Frühbucher-Rabatt



BIG DATA

Informieren Sie sich über die Rolle der Oracle-Datenbank-Technologie und die Verarbeitung von großen Datenmengen durch spezielle Features der Datenbank-Version 18c.

VISUALISIERUNG/ REPORTING

Werkzeuge für die Visualisierung (Oracle Business Intelligence, APEX, ADF, JET) und das Reporting (Oracle BI Publisher, Reports) bieten vielfältige Möglichkeiten.

GEODATEN

Nutzen Sie die Möglichkeit, unter anderem an Talks aus den Themenbereichen Geoinformation in der Cloud und hybriden Umgebungen, Linked Open Geodata oder Location Intelligence teilzunehmen.

Weitere Informationen und Anmeldung unter:
www.doag.org/go/bigdatadays


ORAWORLD
Das e-Magazine für alle Oracle-Anwender!
EOUC
EMEA ORACLE USERGROUP COMMUNITY
• Spannende Geschichten aus der Oracle-Welt
• Technologische Hintergrundartikel
• Leben und Arbeiten heute und morgen
• Einblicke in andere User Groups weltweit
• Neues (und Altes) aus der Welt der Nerds
• Comics, Fun Facts und Infografiken
Jetzt Artikel einreichen oder Thema vorschlagen!
Bis 9. August 2018
Jetzt e-Magazine herunterladen
www.oraworld.org