Rödl & Partner

FEBRUAR 2018

ENTREPRENEUR

IM FOKUS: DATENSCHUTZ-GRUNDVERORDNUNG

BEITRÄGE AUS UNSEREN GESCHÄFTSFELDERN...

RECHTSBERATUNG Einhaltung von Datenschutz-Vorgaben | Kontrolle von Beschäftigten in Europa

STEUERBERATUNG § 203 StGB: IT-Dienstleister und Cloud-Computing | Steuerlicher Datenschutz

STEUERDEKLARATION UND BPO Konforme Datenverarbeitung | DSGVO in Polen, Rumänien und Italien

UNTERNEHMENS- UND IT-BERATUNG Kundendaten: Anonymisieren und Pseudonymisieren | ERP-Lösungen

WIRTSCHAFTSPRÜFUNG DSGVO und Abschlussprüfung | Sicherheit für Geschäftsführer, Vorstand, Aufsichtsrat

INHALT

AUSGABE FEBRUAR 2018

3 EDITORIAL

4 RECHTSBERATUNG

4 Einhaltung von Datenschutz-Vorgaben – Zwischen unsäglichem Übel und großartiger Gelegenheit

6 Kontrolle von Beschäftigten in Europa – Informationspflichten in Polen nach nationalen und europäischen Vorgaben

8 STEUERBERATUNG

8 § 203 StGB: Neuerung im Gesetz – Inanspruchnahme von IT-Dienstleistern und Cloud-Computing vereinfacht

10 Steuerlicher Datenschutz – Was die Finanzbehörden dürfen

12 STEUERDEKLARATION UND BUSINESS PROCESS OUTSOURCING

12 Datenschutzkonforme Datenverarbeitung – Technische Umsetzung der Dokumentationspflichten

14 DSGVO in Polen, Rumänien und Italien – Revolutionäre Änderungen in der Personal- und Lohnbuchhaltung

16 UNTERNEHMENS- UND IT-BERATUNG

16 Anonymisieren und Pseudonymisieren von Kundendaten – Praxisbeispiel aus dem Datenschutz

18 Die DSGVO im Ökosystem der ERP-Lösungen – Auswirkung auf das Zusammenspiel zwischen Unternehmen und Dienstleister

20 WIRTSCHAFTSPRÜFUNG

20 DSGVO und Abschlussprüfung – Veränderungen nicht nur für den Datenschutzbeauftragten

22 Umsetzung der DSGVO – So verschaffen Sie sich als Geschäftsführer, Vorstand oder Aufsichtsrat Sicherheit

24 INTERVIEW

24 Rita Santaniello und Nadia Martini:„Datenschutz als Wettbewerbsvorteil für Unternehmen – Einheitliche Regelung in der EU"

26 GASTKOMMENTAR

26 Prof. Dr. Alexander Roßnagel: „Datenschutz-Grundverordnung – Alle Zielsetzungen werden verfehlt"

28 EINBLICKE

28 Fakten zur DSGVO

Als passende **Bildstrecke** unserer aktuellen Ausgabe haben wir das Thema **„Sicherheit in der Nautik"** gewählt.

IMPRESSUM – ENTREPRENEUR

Ausgabe Februar 2018
ISSN 2199-8345

Herausgeber:
Rödl & Partner GbR
Äußere Sulzbacher Str. 100
90491 Nürnberg
Tel.: +49 (911) 91 93 – 0
www.roedl.de

Verantwortlich für den Inhalt:

Prof. Dr. Christian Rödl
christian.roedl@roedl.de
Äußere Sulzbacher Str. 100
90491 Nürnberg

Redaktion und Layout:

Unternehmenskommunikation:

Anja Soldan
anja.soldan@roedl.com
Ines Seitz
ines.seitz@roedl.com
Katrin Schmidt
katrin.schmidt@roedl.com
Thorsten Widow
thorsten.widow@roedl.com

für die Geschäftsfelder:

Patrick Satzinger
patrick.satzinger@roedl.de
Britta Dierichs
britta.dierichs@roedl.de
Christin Weller
christin.weller@roedl.de
Michael Kolbenschlag
michael.kolbenschlag@roedl.de
Dr. Andreas Schmid
andreas.schmid@roedl.de

Grafiken:

Nadine Viehmann
nadine.viehmann@roedl.de

Liebe Leserin, lieber Leser,

mit dem Fund von Erdöl kam es zu einer Industrie, die revolutionär war. Rund um das Rohöl als Rohstoff entwickelten sich nicht nur neue und erweiterte Antriebskonzepte, sondern in dem Bereich der petrochemischen Industrie eine neue Palette an zuvor völlig unbekannten Produkten.

Mit der bahnbrechenden Technik des Internets und des schnellen Datentransfers haben sich ebenfalls Geschäftsmodelle in rasend schneller Zeit verändert. Bestehende und althergebrachte Geschäftsmodelle wie der Vertriebshandel wurden revolutioniert und erfolgen heute mehrheitlich online.

Unternehmen, die diese schnellen Veränderungen nicht umgesetzt haben, wurden von den Entwicklungen überrollt und sind heute nicht mehr existent. Die disruptive Kraft der Innovation führt aber auch zur Entstehung völlig neuer Konzepte. Es entstehen Geschäftsmodelle, die als „Plattformen" agieren. Bspw. hat das weltgrößte Taxiunternehmen „Uber" keinerlei Taxen und der weltgrößte Hotelbetrieb „Airbnb" keinerlei eigene Hotels. Sie sind lediglich Onlineplattformen, die jedoch nur funktionieren, wenn gewährleistet ist, dass ein schneller Datenaustausch und eine Wertschöpfung über die genutzten Daten gewährleistet ist.

Konsequenterweise ist die Inhaberschaft der Daten und die hiermit verbundene Möglichkeit, Geschäftsmodelle damit umzusetzen, ein wesentlicher wertbildender Faktor. Das betrifft jedoch nicht nur Geschäftsdaten, sondern auch Personendaten. Um solche Personendaten besser zu schützen, wird die Europäische Datenschutz-Grundverordnung (DSGVO) eingeführt. Damit ändert sich vollständig das bisherige Konzept im Datenschutzrecht. Bislang gab der Gesetzgeber sehr klare Regelungen vor, wie der Datenschutz umzusetzen ist. Künftig wird ein Rechtsrahmen vorgegeben und die Unternehmen wurden verpflichtet, ein eigenes Datenschutzkonzept zu entwickeln und sodann in einer Dokumentation auch festzuhalten. Die gesetzliche Verpflichtung besteht und muss eingeführt werden. Es verbieten sich schematische Einführungsmodelle. Vielmehr sind unternehmensspezifische Aspekte zu berücksichtigen, denn letztlich können durch die Einführung der gesetzlichen Vorgaben Mehrwerte im Unternehmen realisiert werden.

Dr. José A. Campos Nave

EINHALTUNG VON DATENSCHUTZ-VORGABEN

Zwischen unsäglichem Übel und großartiger Gelegenheit

Von Alexander von Chrzanowski, Rödl & Partner Jena

Regelmäßig sind Unternehmen gefordert, sich an Veränderungen des rechtlichen und wirtschaftlichen Umfelds anzupassen. Im Mai 2018 betrifft das umfangreiche Anforderungen bei der Verarbeitung personenbezogener Daten. Überlegungen zu einer risikobasierten Befolgung der Datenschutzanforderungen lassen sich dabei zugleich mit den Vorteilen eines modernen Datenschutzes kombinieren.

Unternehmen prüfen üblicherweise die wahrscheinlichsten Ursachen für zivilrechtliche oder behördliche Inanspruchnahmen, bestimmen deren Eintrittswahrscheinlichkeit und ihre Auswirkungen auf den Geschäftsbetrieb. Je nach Ergebnis der Prüfung passen sie sich an oder nehmen Risiken bewusst in Kauf. Die Risiken sind abhängig von der Größe des Unternehmens, Art und Ort des Geschäftsbetriebs, der Konfrontationsfreude von Betroffenen, Wettbewerbern und staatlichen Stellen sowie den jeweils unternommenen Bemühungen zur Einhaltung der gesetzlichen Vorgaben.

Trotz dieser individuell zu beurteilenden Faktoren birgt das künftige europäische Datenschutzrecht ein hohes Risiko bei der Verletzung lediglich formaler Anforderungen. Hierzu zählen etwa die vielfältigen Pflichten zu Informationen und Erklärungen gegenüber Betroffenen, die Bestellung eines Datenschutzbeauftragten, Vereinbarungen mit Dritten zur Datenübermittlung oder das Vorhalten einer Übersicht personenbezogener Datenverarbeitungen im Unternehmen. Die Nichteinhaltung der formalen Anforderungen ist für Aufsichtsbehörden wie Beteiligte leicht erkennbar.

Unternehmerische Gründe für den Datenschutz

Neben der individuellen Feststellung von Haftungsrisiken und deren Reduzierung gibt es aus Unternehmersicht auch Vorteile, sich aktiv mit dem Schutz der Daten von Mitarbeitern, Kunden und Dritten zu befassen. Unternehmen können den Datenschutz als Werteversprechen ausgestalten und sich mit einer entsprechenden Unternehmensdarstellung positiv von Wettbewerbern abgrenzen. Ein Erfüllen oder Übertreffen gesetzlicher Anforderungen zugunsten von Mitarbeitern und Kunden kann das Ansehen des Unternehmens stärken und vertrauensbildend wirken.

Die nachweisbare Einhaltung von Datenschutzvorschriften stellt einen Unternehmenswert an sich dar, vergleichbar der Registrierung und Zusammenstellung des geistigen Eigentums einer Gesellschaft. So werden bei Unternehmenstransaktionen – etwa dem Erwerb oder der Veräußerung von Unternehmensanteilen – die bestehenden Risiken eines Geschäftsbetriebs bei Due Diligences üblicherweise vom Erwerber geprüft und bewertet. Aufgrund des erheblichen Bußgeldrahmens werden sich derartige Prüfungen künftig auch angemessen mit der Einhaltung des Datenschutzes im Unternehmen befassen müs-

sen. Innerhalb des häufig knappen zeitlichen Rahmens solcher Prüfungen ermöglicht eine vorhandene, aktuelle Dokumentation die Beurteilung der Datenschutzorganisation im Unternehmen. Selbst wenn dabei Mängel auftreten, bietet die Zusammenstellung zumindest eine Chance zur Bewertung des Vorhandenen und ggf. Fehlenden. Das vollständige Fehlen einer solchen Dokumentation wird dagegen Zweifel an der generellen Einhaltung des Datenschutzes im Unternehmen aufwerfen, was ein deutlich größeres Risiko darstellt und damit bei der Bewertung des Unternehmensanteils nachteilig zu Buche schlägt.

Alexander von Chrzanowski

Rechtsanwalt,
Fachanwalt für IT-Recht,
Fachanwalt für Arbeitsrecht
+49 (3641) 403 – 530
alexander.chrzanowski@roedl.com

Für international tätige Unternehmen kann es zudem sinnvoll sein, Datenschutz nicht lediglich lokal zu betrachten, um allein die jeweiligen einzelstaatlichen Mindestanforderungen einzuhalten. Dann ist es möglich, mit einem unternehmenseinheitlichen Standard die Anforderungen einer Vielzahl von Ländern zugleich einzuhalten und nur einander unvereinbaren gesetzlichen Anforderungen individuell zu begegnen. Zwar werden dadurch im Einzelfall gesetzliche Spielräume nicht ausgenutzt und vereinzelt ein höheres als das lokal erforderliche Datenschutzniveau erreicht, dafür entfallen für die Unternehmen die Kosten individueller lokaler Anpassungen und deren dauerhafte Aktualisierungen.

Fazit

Letztlich können Unternehmen das Risiko von Datenvorfällen sowie die Auseinandersetzung mit den Begehrlichkeiten interessierter Kreise – Betroffene, Strafverfolgungs- und Aufsichtsbehörden – durch die bewusste Reduzierung der überhaupt verarbeiteten oder vorgehaltenen Daten verringern. Was nicht vorhanden ist, kann nicht verlorengehen, braucht nicht herausgegeben zu werden und reduziert Arbeiten außerhalb des unternehmerischen Kerngeschäfts.

Unternehmen müssen sich ihre Risiken und Chancen bei der Einhaltung des Datenschutzes bewusst machen. Dabei sind eigene Positionen regelmäßig zu prüfen und erforderlichenfalls anzupassen. Für die formalen, leicht prüfbaren Anforderungen der Datenschutz-Grundverordnung sollten Unternehmen rechtzeitig überzeugende Lösungen finden.

KONTROLLE VON BESCHÄFTIGTEN IN EUROPA

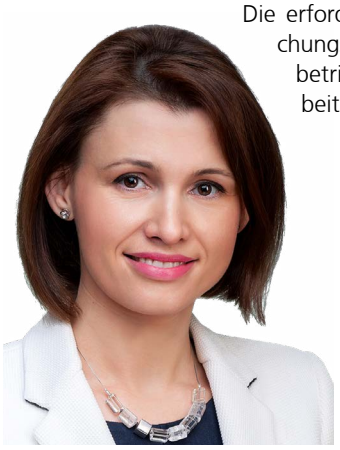
Informationspflichten in Polen nach nationalen und europäischen Vorgaben

Von Katarzyna Małaniuk und Dr. Michael Braun, Rödl & Partner Posen und Hof

Wir leben in Zeiten kontinuierlicher Überwachungsmöglichkeiten im Alltag. Das geschieht auf der Straße, beim Einkaufen, auf dem Parkplatz, beim Eingang zu Gebäuden und Wohnungen sowie am Arbeitsplatz. Den Anforderungen einer Überwachung am Arbeitsplatz widmen wir uns nachfolgend.

In Polen gibt es bislang keine arbeitsrechtlichen Vorschriften, die die Überwachung am Arbeitsplatz direkt zulassen und es war strittig, ob eine Überwachung überhaupt rechtlich zulässig ist. Das bedeutet aber nicht, dass die Beschäftigten gar nicht kontrolliert werden. In Literatur und Rechtsprechung gibt es unterschiedliche Meinungen. In der Praxis wird die Überwachung von Arbeitnehmern oft mit dem Hinweis auf das polnische Datenschutzgesetz durchgeführt. Demnach ist die Verarbeitung von Personendaten nur zulässig, wenn es zur Erfüllung der rechtlich begründeten Ziele durch den Verantwortlichen erfolgt und dabei die Rechte und Freiheiten der betroffenen Person nicht beeinträchtigt.

Hierzu wird in der Rechtsprechung die Auffassung vertreten, dass die betroffene Person über die Überwachung vorab zu informieren ist. Zudem müssen die gewählten Mittel verhältnismäßig sein und der Grad der Beeinträchtigung der Privatsphäre beurteilt werden. Die erforderlichen Informationen zu Überwachungsmaßnahmen sollen auch in innerbetriebliche Vorschriften (bspw. eine Arbeitsordnung) aufgenommen werden.



Katarzyna Małaniuk

Rechtsanwältin
+48 (61) 62 44 – 969
katarzyna.malaniuk@roedl.pro

Bemerkenswert ist, dass der polnische Gesetzgeber in dem Entwurf des Einführungsgesetzes zur Datenschutz-Grundverordnung (DSGVO) eine Einwilligung der Arbeitnehmer zur Überwachung durch Videoaufnahmen sowie eine Einwilligung für Erteilung zusätzlichen Personendaten vorsieht.

Informationspflichten nach der DSGVO

In der DSGVO werden die Informationspflichten viel detaillierter geregelt. Nach Art. 13 DSGVO ist der Arbeitgeber dazu verpflichtet, dem Beschäftigten als betroffene Person umfassend über die Überwachung zu informieren.

Hieraus folgt, dass polnische Arbeitgeber die Informationen zur Arbeitnehmerüberwachung in ihren innerbetrieblichen Regelungen stark ausbauen müssen. Die erweiterte Informationspflicht gemäß DSGVO soll nach Ansicht der Literatur jedoch nur für die Zukunft gelten: Demnach ist der Verantwortliche generell nicht zur Aktualisierung der nach dem 25. Mai 2018 erteilten Informationen verpflichtet.

Europäische Menschenrechtskonvention: Informationspflichten

Da die Kontrolle der Beschäftigten auch deren Privatsphäre beeinträchtigen kann, sind Entscheidungen des Europäischen Gerichthofs für Menschenrechte zum „Recht auf Achtung des Privatlebens und Korrespondenz" (Art. 8 EMRK) zu beachten. In der Entscheidung vom 5. September 2017 in der Sache Barbulescu v. Romania (AZ: 61496/08) hat das Gericht Kriterien genannt, die bei einer Kommunikationsüberwachung von Beschäftigten zu beachten sind. Folgendes ist relevant, um Erkenntnisse einer Überwachung – etwa in einem Kündigungsrechtsstreit – zu verwenden:

1. Vorabinformation über eine Überwachung: Der Betroffene ist klar und im Voraus über die Art der Überwachung zu informieren.

2. Ausmaß der Überwachung: Erfolgt lediglich die Überwachung des Kommunikationsflusses oder auch dessen Inhalts? Werden alle oder

nur Teile der Kommunikation überwacht? Wie ist die Dauer der Überwachung und die Anzahl von Personen mit Zugang zu den gewonnenen Informationen?

3. Begründung für die Überwachung: Bestehen legitime Gründe für die individuelle Überwachung des Beschäftigten? Die Überwachung von Kommunikationsinhalten ist invasiver als das bloße Feststellen der Kommunikation und erfordert daher eine gewichtigere Begründung.

4. Erforderlichkeit der ergriffenen Maßnahmen: Lässt sich das Ziel auch durch weniger einschneidende Maßnahmen und Methoden erreichen (z. B. ohne direkten Zugriff auf den gesamten Inhalt der Kommunikation)?

5. Folgen für den Arbeitnehmer und die beabsichtigte Verwendung der Ergebnisse – insbesondere, ob sie zur Erreichung des erklärten Ziels der Maßnahme verwendet wurden.

6. Existenz angemessener Garantien: Ist sichergestellt, dass nicht auf den Inhalt der Kommunikation zugegriffen werden kann, wenn der Arbeitnehmer nicht im Voraus hierüber informiert wurde?

Fazit

Das zeigt, dass schon jetzt die Überwachung von Beschäftigten anhand ähnlicher Kriterien wie der DSGVO durch Gerichte nachgeprüft werden kann, obwohl die DSGVO erst vor der Tür steht. Daher sollten Arbeitgeber die Anpassungen in diesem Bereich dringend vornehmen, statt bis zum 25. Mai 2018 abzuwarten.

§ 203 StGB: NEUERUNG IM GESETZ

Inanspruchnahme von IT-Dienstleistern und Cloud-Computing vereinfacht

Von Norman Lenger und Konrad Klein, Rödl & Partner Köln und Nürnberg

Bisher bewegten sich Berufsgeheimnisträger (z. B. Ärzte, Anwälte oder Wirtschaftsprüfer), die bei ihrer Berufsausübung IT-Dienste von Externen nutzten (bspw. E-Mail oder Cloud-Computing) in einer rechtlichen Grauzone. Die Neuregelung des § 203 Strafgesetzbuch (StGB) bringt nun Klarheit – wenn auch nicht vollumfänglich.

Mit dem Beschluss vom 29. Juni 2017 zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen und der anschließenden Billigung durch den Bundesrat am 22. September 2017 wurde die Reform des § 203 StGB endgültig beschlossen. Die Norm regelt Verletzungen der Schweigepflicht durch Berufsgeheimnisträger wie Anwälte, Ärzte, Notare, Steuerberater und Wirtschaftsprüfer.

Wie war die Rechtslage bisher?

Generell gilt für die Berufsgeheimnisträger eine (strafrechtliche) Verpflichtung zur Verschwiegenheit. Die Weitergabe von anvertrauten Informationen und Geheimnissen war bisher lediglich für berufsmäßig tätige Gehilfen rechtskonform. Sofern Externe Zugriff auf diese Informationen erhalten könnten, war die Einwilligung des betroffenen Mandanten erforderlich. Im Zeitalter der Digitalisierung ist das Bild der kleinen Kanzlei bzw. Arztpraxis mit dem Gehilfen und dem damit einhergehenden Informationsfluss jedoch nicht mehr zeitgemäß. Heute werden für die effiziente Bearbeitung Informationen über Provider per E-Mail übertragen und auf Servern gespeichert, die von IT-Dienstleistern oder Cloud-Anbietern gehostet werden.

Was ändert sich durch die Reform?

Mit der Reform hat der Gesetzgeber nicht nur die strafrechtlichen Regelungen in § 203 StGB, sondern darüber hinaus auch die strafprozessualen Zeugnisverweigerungsrechte und Beschlagnahmeverbote (§§ 53a, 97 StPO) sowie ferner im Rahmen seiner gesetzgeberischen Zuständigkeit verschiedene berufsrechtliche Vorschriften den geänderten praktischen Bedürfnissen angepasst.

Die Neuregelung erleichtert die Inanspruchnahme von externen Dienstleistungen. Durch die Erfüllung bestimmter Voraussetzungen wird die Weitergabe von Informationen an Mitwirkende ermöglicht. Eine solche Weitergabe ist immer dann möglich, soweit die Offenlegung der Informationen für die ordnungsgemäße Ausübung der Tätigkeit der mitwirkenden Personen erforderlich ist.

Die Formulierung „soweit" lässt den Schluss zu, dass es sich dabei nicht nur um eine generelle Prüfung des „Ob", sondern auch um eine einzelfallbezogene Prüfung des Umfangs der Offenbarung handelt. Zu berücksichtigen ist allerdings ein gewisser Abstraktionsgrad: Maßgeblich für die Erforderlichkeit ist die Tätigkeit des jeweiligen Dienstleisters. So geht der Gesetzgeber in seiner Begründung ebenfalls davon aus, dass die Einrichtung oder Wartung von IT-Anlagen durch externe Spezialisten grundsätzlich erforderlich ist.

Zudem sind die mitwirkenden Personen sorgfältig auszuwählen und müssen ebenfalls zur Geheimhaltung verpflichtet werden. Das kann vertraglich erfolgen, entweder durch das Hauptleistungsvertrags oder als Gegenstand einer gesonderten Vereinbarung. Die Einwilligung des Mandanten bzw. Patienten ist nunmehr nicht mehr notwendig – vielmehr rückt die vertragliche Ausgestaltung mit den Beschäftigten und den Dienstleistern in den Fokus.

Ist der Weg nun frei für die Digitalisierung?

Die Reform orientiert sich stark an den reellen Arbeitsabläufen und berücksichtigt den stetigen Wandel und Fortschritt. Sie ist daher grundsätzlich positiv zu bewerten. Dennoch bleiben weiterhin Unklarheiten bestehen. Da zum einen laut Gesetzestext die Offenlegung der Informationen an Mitwirkende ausschließlich gestattet ist, wenn sie erforderlich ist, bleibt immer ein Diskussionsspielraum bei der Frage der Notwendigkeit von Sicherheitsstandards und Verschlüsselungsmaßnahmen. Zum anderen flankieren weitergehende gesetzliche Anforderungen das Thema Datenschutz. Handelt es sich bei demjenigen, dessen Geheimnis es zu wahren gilt, um eine natürliche Person, findet auch das Bundesdatenschutzgesetz (BDSG) sowie ab Mai 2018 die Datenschutz-Grundverordnung (DSGVO) Anwendung. Danach ist der Berufsgeheimnisträger zusätzlich verpflichtet, mit dem jeweiligen IT-Dienstleister einen Auftragsdatenverarbeitungsvertrag (§ 11 BDSG, Art. 28 DSGVO) abzuschließen. Vorsicht ist zudem beim Auslandsbezug geboten!

Es entspricht gängiger Praxis, dass Dienstleister beim IT-Outsourcing bzw. internationale Unternehmen auch zur konzerninternen Datenverarbeitung auf Mitarbeiter und Unterauftragnehmer im Ausland zurückgreifen. Zwar stehen dem die Berufsverschwiegenheitspflichten aus § 203 StGB n. F. nicht entgegen, etwaige Einschränkungen können sich aber aus den jeweils einschlägigen berufsrechtlichen Vorschriften ergeben. So gibt § 62a Abs. 4 StBerG (§ 50a Abs. 4 WPO) Steuerberatern (Wirtschaftsprüfern) auf, der Verschwiegenheitspflicht unterliegende Daten nur im Ausland verarbeiten zu lassen, wenn der dort bestehende Geheimnisschutz mit dem im Inland vergleichbar ist.

Somit bestehen weiterhin Risiken bei der Inanspruchnahme von IT-Dienstleistungen und Cloud-Diensten, obgleich die Gesetzeslage etwas mehr Rechtssicherheit bietet. IT-Sicherheit ist in Anbetracht der aktuellen Regelungen ein zentrales Thema, v. a. für IT-Dienstleister. Der Nachweis eines angemessenen Sicherheitsniveaus, bspw. durch die Zertifizierung nach ISO 27001 oder die Bestätigung der Wirksamkeit des internen Kontrollsystems von IT-Dienstleistern (**IDW PS 951**), gewinnt durch die Neuregelung weiterhin zunehmend an Bedeutung.

Norman Lenger

Rechtsanwalt, Fachanwalt
für Steuerrecht,
Compliance Officer (TÜV)
+49 (221) 94 99 09 – 518
norman.lenger@roedl.com

STEUERLICHER DATENSCHUTZ

Was die Finanzbehörden dürfen

Von Britta Dierichs, Rödl & Partner Nürnberg

Die deutsche Finanzverwaltung verarbeitet in großem Umfang personenbezogene Daten. Daher muss auch das Besteuerungsverfahren auf das Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) im Mai 2018 vorbereitet werden. Sowohl der Gesetzgeber als auch das Bundesfinanzministerium haben reagiert und den steuerlichen Datenschutz angepasst.

Das steuerliche Datenschutzrecht fußt mit dem Inkrafttreten auf 2 Säulen: den obligatorischen Regelungen der DS-GVO selbst sowie den durch das Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer vom 17. Juli 2017 angepassten Vorschriften der , (AO). Hierzu hat das Bundes-finanzministerium mit einer Änderung des Anwendungserlasses der AO vom 12. Januar 2018 Anwendungsrichtlinien für die Finanzverwaltung erlassen. Alle Regelungen treten zum 25. Mai 2018 in Kraft. Das neugefasste Bundesdatenschutzgesetz (BDSG) gilt nur insoweit, als die AO ausdrücklich verweist. Ein anderes Bild ergibt sich, wenn nicht der Datenschutz durch die Finanzbehörden selbst betroffen ist: Hat z. B. der Arbeitgeber Daten im Rahmen des Lohnsteuerverfahrens zu übermitteln, sind die Regelungen des BDSG zu beachten. Ziel des neuen steuerlichen Datenschutzes ist es, den gegenwärtigen Zustand auch unter Geltung der DSGVO aufrecht erhalten zu können.

Rödl & Partner

Britta Dierichs

Diplom-Kauffrau,
Steuerberaterin
+49 (911) 91 93 – 12 60
britta.dierichs@roedl.com

Anwendungsbereich

Der steuerliche Datenschutz wird einheitlich geregelt. Die AO gilt sowohl für Bundes- als auch Landesfinanzbehörden für die Verwaltung bundesgesetzlich geregelter Steuern – also alle wesentlichen Steuerarten. Die Landesdatenschutzgesetze kommen grundsätzlich nicht zur Anwendung. Der neue steuerliche Datenschutz erfasst nicht nur lebende natürliche Personen, sondern auch verstorbene sowie juristische Personen und sonstige Personenvereinigungen. Insoweit wird die DSGVO als entsprechend anwendbar erklärt.

Rechtsgrundlage

Für die Verarbeitung personenbezogener Daten benötigt die Finanzverwaltung künftig eine ausdrückliche Rechtsgrundlage, die mit § 29b AO-neu geschaffen wurde. Sie erfasst auch die Verarbeitung besonderer Kategorien personenbezogener Daten, also besonders sensibler Daten wie Gesundheitsdaten, die z. B. bei der Geltendmachung als außergewöhnliche Belastung anfallen. Die hierfür erforderlichen Garantien für die Wahrung der Rechte der Betroffenen werden insbesondere durch das weiterhin geltende Steuergeheimnis (§ 30 AO) erfüllt, dessen enger Rahmen die Daten vor einer unberechtigten Offenbarung und Verwertung schützt.

Um die bisherigen Arbeits- und Austauschwege der Finanzverwaltung zu sichern, wurde mit § 29c AO-neu die Weiterverarbeitung von Daten durch die Finanzverwaltung auch für Zwecke ermöglicht, für die sie ursprünglich nicht erhoben wurden. Ohne § 29c Abs. 1 Nr. 1 AO wäre z. B. unsicher, ob die mit der ESt-Erklärung erhobenen Daten auch für Zwecke der Umsatzsteuer verwendet werden dürften. Mit Nr. 4 wird die Grundlage für die Verwendung von Daten für die Entwicklung, Überprüfung und Änderung automatisierter Verfahren der Finanzbehörden geschaffen. Nr. 5 erlaubt die Weiterverarbeitung für Aufsichts-, Steuerungs- und Disziplinarbefugnisse oder für Ausbildungs- und Prüfungszwecke. Die Verarbeitung von rechtmäßig erhobenen Daten aus dem Steuerverfahren für im öffentlichen Interesse liegende statistische Auswertungen ist bereits nach der DSGVO zulässig. Für besondere Kategorien personenbezogener Daten wird in § 31c AO-neu dafür die erforderliche Gesetzesgrundlage geschaffen und die flankierenden Anforderungen werden geregelt.

Steuergeheimnis

Die bisherigen Offenbarungstatbestände werden durch weitere Fälle ergänzt. Ohne § 30 Abs. 4 Nr. 1a AO-neu würde ein Finanzbeamter, der Daten eines Steuerpflichtigen an eine vorgesetzte Behörde z. B. zum Zweck der Einholung der Zustimmung für eine Steuerstundung übermittelt, gegen das Steuergeheimnis verstoßen. Dasselbe gilt für die Datenherausgabe für Programmentwicklungen (Nr. 2c) oder die Offenbarung von Daten an die zuständige Datenschutz-Aufsichtsbehörde (Nr. 1b). Allerdings wird die Offenbarung zu Statistikzwecken über § 31c AO-neu hinausgehend eingeschränkt auf die gesetzlichen Aufgaben des Statistischen Bundesamts; für Studien der Wirtschaftsforschungsinstitute bspw. bleiben personenbezogene Steuerdaten weiterhin tabu.

Betroffenenrechte

§ 32a AO-neu modifiziert die durch die DSGVO vorgegebenen Informationspflichten der Finanzverwaltung bei der Weiterverarbeitung von Daten zu einem anderen Zweck. Keine Information erfolgt z. B., wenn sie die Verschleierung steuerlicher Sachverhalte ermöglichen oder geplante Prüfungsmaßnahmen offenbaren würde. Die Auskunftsrechte über gespeicherte und verarbeitete personenbezogene Daten werden in § 32c AO-neu eingeschränkt. Versagungsgründe beziehen sich insbesondere auf einen unverhältnismäßigen Aufwand für die Finanzbehörden. Das wird flankiert durch die Möglichkeit des Betroffenen, eine Prüfung durch die zuständige Aufsichtsbehörde einzuleiten (§ 32a Abs. 4 AO-neu).

Modifikationen erfahren auch die Rechte auf Berichtigung sowie Löschung in § 32f AO-neu. Es besteht z. B. kein Löschungsanspruch mehr, wenn bestrittene Daten einem bereits bestandskräftigen Steuerbescheid zugrunde liegen. Es ist jedoch eine entsprechende Dokumentation und ein Hinweis bei der Weiterverarbeitung vorgesehen.

Datenschutzaufsicht und Rechtsweg

Finanzämter müssen auch wegen des steuerlichen Datenschutzes einen Datenschutzbeauftragten bestellen. Die Kontaktdaten sind zu veröffentlichen. Die Datenschutzaufsicht über die Finanzbehörden obliegt dem „Bundesbeauftragten für den Datenschutz und Informationsfreiheit" (BfDI). Dessen Maßnahmen zum Datenschutz sind jedoch nicht sofort vollziehbar, ihre Wirksamkeit kann durch eine Klage der Finanzbehörde aufgeschoben werden, bis die Rechtslage abschließend gerichtlich geklärt ist. Für alle Streitigkeiten, sowohl zwischen betroffenen Personen und den Finanzbehörden als auch zwischen ihnen und dem BfDI ist der Finanzrechtsweg eröffnet, ohne dass es der Durchführung eines Vorverfahrens bedarf (§ 32i AO neu).

DATENSCHUTZKONFORME DATENVERARBEITUNG

Technische Umsetzung der Dokumentationspflichten

Von Monika Völkel, Rödl & Partner Plauen

Ab dem 25. Mai 2018 ist die neue Datenschutz-Grundverordnung (DSGVO) umzusetzen. Sie bringt umfangreiche Änderungen des Datenschutzrechts zum Schutz personenbezogener Daten mit sich. Ziel ist es, u. a. das Datenschutzrecht an den technologischen Fortschritt anzupassen. Die Verantwortlichen müssen künftig die Einhaltung der Datenschutzvorgaben nachweisen. Sie sind verpflichtet, ihre Prozesse so einzurichten und zu dokumentieren, dass den Aufsichtsbehörden die datenschutzkonforme Datenverarbeitung nachgewiesen werden kann.

Monika Völkel

Diplom-Betriebswirtin (FH),
Wirtschaftsprüferin,
Steuerberaterin
+49 (37 41) 163 – 260
monika.voelkel@roedl.com

Nach Art. 5 Abs. 2 und Art. 24 Abs. 1 DSGVO verantwortet die Unternehmensleitung die Einhaltung der Grundsätze für die Verarbeitung der personenbezogenen Daten und muss deren Einhaltung nachweisen. Die Rechenschaftspflicht beinhaltet, dass die Unternehmen jederzeit befolgen können müssen, dass bei der Verarbeitung personenbezogener Daten die technisch-organisatorischen Anforderungen und Datenschutzgrundsätze der DSGVO erfüllt werden. Aus dieser neuen Pflicht folgt eine Beweislastumkehr gegenüber den Aufsichtsbehörden. Kann der Nachweis nicht erbracht werden, können Schadensersatz und Bußgelder folgen.

Die Datenschutzdokumentation sollte die Grundsätze für die Verarbeitung personenbezogener Daten im Unternehmen, u. U. identifizierte Datenschutzrisiken, interne Sicherheitsrichtlinien zu Datenschutz und IT, Risiko- und Datenschutzfolgeabschätzungen, Nachweise über Schulungen sowie Regeln für Kontrollen und Optimierung aller Datenschutzmaßnahmen umfassen.

Verfahrensverzeichnis

Das Verfahrensverzeichnis heißt in der DSGVO „Verzeichnis der Verarbeitungstätigkeiten" und ist eine Übersicht über die laufenden Datenverarbeitungen im Unternehmen. Der Verantwortliche ist verpflichtet ein schriftliches oder elektronisches Verzeichnis aller Verarbeitungstätigkeiten zu führen. Das war bereits in der Vergangenheit Pflicht (Bundesdatenschutzgesetz). Die Aufsichtsbehörden werden es bei Kontrollen fordern. Die Beschreibung der technischen und organisatorischen Maßnahmen ist entsprechend vorzunehmen. Auftragsverarbeiter haben ein gesondertes Verzeichnis der Auftragsverarbeitungstätigkeiten zu erstellen – es ist deutlich weniger umfangreich als das des Verantwortlichen.

Datenschutz durch Technikgestaltung und Voreinstellungen

Gemäß Art. 25 DSGVO müssen IT-Systeme so gestaltet sein, dass die Datenschutzgrundsätze wirksam umgesetzt werden. Als Beispiel für geeignete technische und organisatorische Maßnahmen wird die Pseudonymisierung genannt. In Art. 4 Nr. 5 DSGVO wird sie definiert als „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden". Zudem ist die Pseudonymisierung ein geeignetes Mittel zum Persönlichkeitsschutz. Des Weiteren sollten die IT-Systeme so voreingestellt sein, dass grundsätzlich lediglich solche Daten verarbeitet werden, die für den jeweiligen Zweck tatsächlich benötigt werden.

Nach Art. 32 DSGVO schließen die technischen und organisatorischen Maßnahmen u. a. Folgendes ein:

- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen und technischen Zwischenfall rasch wiederherzustellen;
- Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen zur Gewährleitung der Sicherheit der Verarbeitung.

Die Maßnahmen müssen ein angemessenes Schutzniveau gewährleisten. Bei der Beurteilung des Niveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Datenverarbeitung verbunden sind.

Die konkret daraus abzuleitenden technischen Folgerungen sind in Zusammenarbeit mit den jeweiligen EDV-Dienstleistern zu klären. Die Neuregelungen bringen weitreichende Pflichten mit sich, die es zu meistern und technisch umzusetzen gilt.

DSGVO IN POLEN, RUMÄNIEN UND ITALIEN

Revolutionäre Änderungen in der Personal- und Lohnbuchhaltung

Von Renata Kabas-Komorniczak, Jarosław Kamiński und Marta Wiśniewska, Rödl & Partner Warschau

Ab Mai 2018 werden in der Europäischen Union einheitliche Vorschriften zum Schutz und zur Verarbeitung personenbezogener Daten gelten. Die Datenschutz-Grundverordnung (DSGVO) bestimmt, wie der Schutz und die Sicherheit zu gewährleisten sind. Die Wichtigkeit des Themas ist unbestreitbar, die alltägliche Praxis ließ häufig zu wünschen übrig – auch im Bereich Personal- und Lohnbuchhaltung, in dem grundsätzlich personenbezogene Daten gesammelt und verarbeitet werden. Das betrifft nicht nur Unternehmen selbst, sondern auch Externe, die Daten im Auftrag anderer verarbeiten (z.B. Outsourcingunternehmen).

Im Nachfolgenden widmen wir uns den wichtigsten Grundsätzen zur Verarbeitung personenbezogener Daten in der Personal- und Lohnbuchhaltung der ausgewählten Rechtssysteme in Polen, Rumänien und Italien.

Aktuelle Grundsätze der Verarbeitung personenbezogener Daten

Sowohl in Polen und Italien als auch in Rumänien ist die Datenverarbeitung von Arbeitnehmern erlaubt. Jedoch müssen die allgemeinen Datenschutzregelungen (ab 25. Mai 2018 die Bestimmungen der DSGVO) in allen Staaten eingehalten werden, da den betroffenen Personen durch den unbefugten Zugang zu den personenbezogenen (auch sensiblen) Daten Schaden entstehen kann. Zudem müssen Arbeitgeber angemessene und passende technische Sicherheitsmaßnahmen ergreifen, die den Schutz der Beschäftigtendaten gewährleisten. In Polen ist es zudem wichtig, dass der Arbeitgeber vom künftigen oder aktuellen Arbeitnehmer grundsätzlich nur solche Daten einholen darf, die in den nationalen Vorschriften (insbesondere im polnischen Arbeitsgesetzbuch) bestimmt sind.

Für den italienischen Gesetzgeber ist es z. B. von Bedeutung, dass der Arbeitgeber spezifische interne Verfahrensanweisungen für die Nutzung elektronischer Werkzeuge des Unternehmens einzuführen hat, um das Bewusstsein der Mitarbeiter zu schärfen. Die von der italienischen Datenschutzbehörde festgelegten Regeln beinhalten u. a.

› eine Privatsphärenfolgenabschätzung für die Rechte der Arbeitnehmer und die Identifizierung spezifischer Internetseiten, die der Beschäftigte nicht besuchen darf, sowie

Renata Kabas-Komorniczak

Tax Consultant (Polen)
+48 (22) 696 28 – 00
renata.kabas@roedl.pro

› ein Verbot der Datenverarbeitung mithilfe von Hard- und Software, die auf die systematische, per Fernzugriff erfolgende Kontrolle von Arbeitstätigkeiten abzielt.

In Rumänien müssen Arbeitgeber bei der Verarbeitung personenbezogener Beschäftigtendaten ebenfalls bestimmte, grundlegende Datenschutzgrundsätze beachten, bspw. Transparenz, Verhältnismäßigkeit oder Finalität. Auch das Bewusstsein des Personals muss sensibilisiert werden – d. h. Mitarbeiter, zu deren täglichen Aufgaben die Verarbeitung personenbezogener Beschäftigtendaten gehört, sollten im Bereich der Datenschutzregelungen geschult werden.

Besondere Vorschriften der DSGVO

Gemäß Art. 88 DSGVO kann jeder Mitgliedstaat den Schutz personenbezogener Daten bei der Beschäftigung auch detaillierter regeln, als es die DSGVO verlangt. Das insbesondere im Management oder bei Bewerbungsverfahren, der Erfüllung von Arbeitsverträgen, der Planung und Organisation der Arbeit, der Gleichheit und Diversität sowie der Gesundheit und Sicherheit am Arbeitsplatz.

In Polen wurden bislang lediglich Änderungsentwürfe ausgearbeitet. Es wird u. a. geplant, die Verarbeitung biometrischer Daten von Arbeitnehmern zuzulassen, wenn der Arbeitnehmer damit einverstanden ist – ein Fehlen der Zustimmung kann weder zu einer schlechten Behandlung führen noch sonstige negative Folgen nach sich ziehen. Der Änderungsentwurf sieht außerdem vor, dass Arbeitgeber den Arbeitsort überwachen dürfen. Der Arbeitgeber darf die Überwachung jedoch nicht mit dem Ziel einführen, die Arbeit zu kontrollieren, sondern nur um den Arbeitnehmern und dem Unternehmensvermögen Sicherheit zu gewährleisten. Der Umfang der Daten, die der Arbeitgeber sammeln darf, wird sich ebenfalls ändern – bspw. bei der Verarbeitung von Telefonnummern und E-Mail-Adressen, die während des Bewerbungsverfahrens gespeichert wurden.

Die rumänische Regierung hat einen Gesetzesentwurf zur öffentlichen Debatte gestellt: Darin sollen die zwingenden Vorschriften der DSGVO in die Landesgesetzgebung überführt werden. Er enthält jedoch keine spezifischen Regelungen für Beschäftigungs- bzw. Lohnabrechnungsangelegenheiten.

In Italien gibt es zurzeit noch keine spezifische Verordnung zur Implementierung des Art. 88 DSGVO. Die italienische Regierung arbeitet aber daran, das Landesrecht durch die Verabschiedung spezifischer Gesetzesverordnungen innerhalb der nächsten 6 Monate an die DSGVO anzupassen – das ergibt sich aus einem ganz neuen Gesetz (Gesetz Nr. 163/2017), das am 21. November 2017 veröffentlicht wurde. In der Praxis verfügt die Regierung über folgende Rechte:

› Widerruf von Datenschutzregelungen, die nicht mit der DSGVO in Einklang stehen;
› Änderungen des italienischen Datenschutzgesetzes, um diejenigen DSGVO-Regelungen zu implementieren, die nicht unmittelbar durchsetzbar sind;
› Angleichung der Straf- und Verwaltungssanktionen an diejenigen, die in der neuen Datenschutzverordnung vorgesehen sind.

Outsourcing von Personal- und Lohnbuchhaltung

Die Personal- und Lohnbuchhaltung wird in der Praxis häufig ausgelagert. Aufgrund der DSGVO sollte der Arbeitgeber – als Verantwortlicher für die Verarbeitung von Beschäftigtendaten – nur solche Outsourcingunternehmen beauftragen, die die Anforderungen der DSGVO erfüllen. Eine Bestimmung kann das Vorhandensein eines Datenschutzbeauftragten sein, was in manchen Fällen obligatorisch ist. Eine Pflicht der Bestellung des Datenschutzbeauftragten ergibt sich unmittelbar aus der DSGVO bzw. aus nationalen Vorschriften.

Die nationalen Aufsichtsbehörden können zudem Richtlinien erlassen, die Unternehmen bei der Bewertung behilflich sind, ob die Bestellung eines Datenschutzbeauftragten unabdingbar ist oder nicht. Bspw. hat die rumänische Datenschutzbehörde bereits eine Richtlinie erlassen, die – auch wenn die DSGVO die Pflicht zur Ernennung eines Datenschutzbeauftragten ausdrücklich nur in bestimmten Situationen oder für bestimmte Datenverantwortliche vorsieht – empfiehlt, dass jedes Unternehmen solch einen Auftragsverarbeiter ernennen sollte, da das für den Datenverantwortlichen von großem Vorteil ist.

Dieselbe Auffassung vertritt die italienische Datenschutzbehörde: Sie legt Unternehmen die Ernennung eines Auftragsverarbeiters dringend ans Herz – selbst wenn es optional ist. So kann nachgewiesen werden, dass der Verantwortliche und der Auftragsverarbeiter das Rechnungslegungsprinzip befolgen und gleichzeitig kann das Risiko einer Geldbuße ausgeschaltet werden. Die polnische Aufsichtsbehörde hat bisher keine solchen Richtlinien aufgestellt.

Angesichts der bisherigen Stellungen der europäischen Aufsichtsbehörden sollten Unternehmen, die Outsourcing-Dienstleistungen in der Lohnbuchhaltung erbringen, unseres Erachtens einen Auftragsverarbeiter ernennen. Arbeitgeber, die Personal- und Lohnbuchhaltung outsourcen wollen, sollten Dienstleiter auch unter Berücksichtigung dieser Frage verifizieren – dadurch können sie ihrerseits die Sorgfaltspflicht besser nachweisen.

ANONYMISIEREN UND PSEUDONYMISIEREN VON KUNDENDATEN

Praxisbeispiel aus dem Datenschutz

Von Matthias Ammon, Rödl & Partner Nürnberg

Am 25. Mai 2018 tritt die Datenschutz-Grundverordnung (DSGVO) in Kraft: Spätestens dann müssen Business-Softwarelösungen fähig sein, personenbezogene Daten zu anonymisieren bzw. zu pseudonymisieren. Der Beitrag zeigt am Beispiel der Rödl & Partner-Softwarelösung „Targenio" die Möglichkeiten auf.

Targenio ist eine Lösung für die Digitalisierung und Automatisierung recherche- und wissensintensiver Vorgänge in Unternehmen. Das schließt das Verarbeiten von Kundendaten mit ein. Es wurde für Unternehmen entwickelt, die hohe Kundenkontakt-Volumen verarbeiten (mehr als 1.000 pro Woche).

Anonymisieren von Kundendaten

Bei der Kundenkommunikation werden oft personenbezogene Daten erhoben und gespeichert. Die Speicherung dieser Daten ist für die Bearbeitung eines Anliegens notwendig, falls das nicht im Erstkontakt erledigt wurde. Dagegen ist die Speicherung von personenbezogenen Daten nicht notwendig bei z. B. Verfügbarkeits- oder Preisanfragen zu einem Artikel.

Somit ist schon bei der Annahme von Anliegen auf die zweckgebundene und beschränkte Erhebung von Kundendaten zu achten (Art. 5 DSGVO).Werden personenbezogene Daten (bspw. Name, Adresse, E-Mail-Adresse, Telefonnummer) gespeichert, so sind sie laut DSGVO in vorgegebenen Fristen aus IT-Systemen wieder zu entfernen. Die erlaubten Speicherfristen sind von der Kundengruppe sowie dem letzten Kontaktzeitpunkt abhängig (Privatkunden 2 Jahre; Geschäftskunden 10 Jahre). Beim Anonymisieren der Kundendaten gibt es 2 mögliche Szenarien:

1. Hatte ein Privatkunde innerhalb von 2 Jahren keinen Kontakt zum Unternehmen, so müssen seine Kundendaten nach Ablauf der 2 Jahre entfernt werden.

2. Hatte ein Privatkunde vor 3 Jahren Kontakt zum Unternehmen und innerhalb der letzten beiden Jahre erneut, so dürfen seine Kundendaten gespeichert bleiben.

Es bleibt dem Unternehmen frei, die Kundendaten im IT-System tatsächlich zu löschen oder zu anonymisieren. Bei der Anonymisierung darf weder aus dem eventuell verbleibenden Kundendatensatz selbst, noch aus den Anliegendaten ein Rückschluss auf die personenbezogenen Daten möglich sein. Eine Löschung der Daten ist i. d. R. technisch einfacher zu implementieren und nachzuweisen als eine Anonymisierung. Allerdings geht bei einer Löschung der Daten auch die Auswertbarkeit verloren.

Die Anonymisierung personenbezogener Daten in IT-Systemen setzt meist eine Analyse der Anliegendaten voraus, da während der Anliegenbearbeitung die Kundendaten nicht nur verwendet, sondern anliegenspezifisch ergänzt oder geändert werden. Beispiele sind das Speichern vom oder an den Kunden gesendete E-Mails bzw. Briefe zum jeweiligen Anliegen als Anhang oder das Erfassen personenbezogener Daten (Gesprächsnotizen, Erreichbarkeit etc.) durch den Anwender.

Komplexer wird die Anonymisierung bei der Koppelung von IT-Systemen über Schnittstellen zu einem Verbund: Bspw. beim Einsatz einer zentralen Kundendatenbank oder bei der Weitergabe von Anliegendaten an ein zentrales Auswertungssystem („Data Warehouse"). Die Vorschriften der DSGVO sind dann auf den Verbund anzuwenden, d. h. die Fristen zum Entfernen der Kundendaten müssen über IT-Systeme hinweg synchronisiert werden. Das macht zusätzlich eine systemübergreifende Abstimmung erforderlich.

Pseudonymisieren von Kundendaten

Die Pseudonymisierung wird häufig eingesetzt, um Kundendatenbestände für IT-Softwaretests zu erzeugen. Dabei werden personenbezogene Daten (z. B. E-Mail-Adressen) durch eine Phantasieadresse ersetzt, so dass es ohne Hilfsmittel nicht möglich ist, auf die echte Adresse zu schließen. Die Echtdatensätze und die Zusammenhänge zwischen ihnen bleiben bestehen – die Inhalte werden „verfälscht".

Neben der Analyse der zu pseudonymisierenden Daten ist auch die inhaltliche Datenintegrität wichtig. Manche Anwendungen, die auf die verfälschten Daten zugreifen, benötigen inhaltlich zueinander passende Daten. Das ist z.B. bei der postalischen Richtigkeit einer Kundenadresse zu berücksichtigen, d.h. bei der Pseudonymisierung einer Adresse dürfen Straße, Hausnummer und Postleitzahl phantasievoll verfälscht werden, müssen inhaltlich jedoch zueinander passen.

Die Implementierung beider Themen in Targenio-Projekten erfolgt kundenspezifisch in enger Abstimmung mit dem Fachbereich, der für die Dateninhalte des jeweiligen IT-Systems zuständig ist, sowie mit dem Datenschutzbeauftragten des Unternehmens.

Matthias Ammon

Leiter Wartung und Betrieb
+49 (911) 597 96 – 118
matthias.ammon@roedl.com

BITTE BEACHTEN SIE:

- Die minimierte Erhebung von Kundendaten erleichtert das Anonymisieren und Pseudonymisieren.
- Schaffen Sie in Ihrem Unternehmen ein Bewusstsein für den verantwortungsvollen Umgang mit Kundendaten.
- Die DSGVO bietet große Chancen für die Kundenbindung.

DIE DSGVO IM ÖKOSYSTEM DER ERP-LÖSUNGEN

Auswirkung auf das Zusammenspiel zwischen Unternehmen und Dienstleister

Von Jens Hinkelmann und Hannes Hahn, Rödl & Partner Nürnberg und Köln

Die Datenschutz-Grundverordnung (DSGVO) fordert viel von Unternehmen: Die rechtlichen Grundlagen müssen für eine datenschutzkonforme Verarbeitung gelegt werden, neue Prozesse sind einzurichten, damit den Betroffenenrechten Genüge getan werden kann. Inwieweit das Ökosystem der im eigenen Unternehmen betriebenen ERP-Systeme angepasst werden muss, beleuchtet dieser Beitrag. Dabei wird die Frage beantwortet, welche positiven Auswirkungen die DSGVO hierauf langfristig haben wird.

Blickt man auf die Berichterstattungen rund um die DSGVO innerhalb der letzten 12 Monate, so schwant einem, dass ein Bürokratiemonster sondergleichen vor der unternehmerischen Haustür steht und kurz davor ist, zu läuten. Gleich hinter ihm steht ein Vertreter der Aufsichtsbehörde, der den Bußgeldbescheid formularbasiert in Händen hält, versehen mit einem „Radio-Button" für die Auswahl zwischen 2 und 4 Prozent vom weltweiten Gesamtumsatz als Sanktion.

Dass man der Verordnung auch etwas Gutes abgewinnen kann, darauf kommt man zunächst nicht. Daher demonstrieren wir am Beispiel des Ökosystems eines ERP-Systems, wie sich die IT-Welt auf lange Sicht positiv verändern wird.

ERP-Systeme und DSGVO: Die Vorteile

Lassen Sie uns die Vorteile anhand folgender Themengebiete kurz beleuchten:

› Entscheidungsfindung zur Anschaffung eines ERP-Systems: Die DSGVO fordert vermehrt die Auseinandersetzung mit dem Schutz der personenbezogenen Daten schon zum Zeitpunkt des „Designs" („Privacy by Design"). Sie beginnt zumindest bei der Erarbeitung des Pflichten- oder Lastenhefts zur Auswahl eines neuen ERP-Systems. Und das ist gut so, denn kein Unternehmen kann es sich leisten, erst nach einem „Go-Live" die Schutzmaßnahmen miteinzubeziehen. Erfolgt das schon zu einem frühen Zeitpunkt, so werden hohe Folgekosten vermieden. Ein guter Dienstleister kennt die Fallstricke und hilft, das Unternehmen davor zu schützen.

› Auswahl eines Dritten: Der Einbezug einer Consultingfirma (Implementierung, Customizing, Individualprogrammierung) muss als Auftragsverarbeitung bewertet werden, da der Dritte i. d. R. mit personenbezogenen Daten in Berührung kommt. Die DSGVO sieht eine gesamtschuldnerische Haftung bei Datenschutzverletzungen vor. Falls also bei einer Implementierung eine Verletzung durch den Dritten entsteht, kann sich das Unternehmen nur schwer aus der Verantwortung ziehen. Daher ist auf die Auswahl des Dritten eine erhebliche Sorgfalt zu legen – und das hat auf Dauer eine enorme Auswirkung auf die Anbieter solcher Leistungen.

› Entwicklung von Grob- und Feinkonzepten: Die Sicherstellung der Anforderungen muss in die Konzepterstellung einfließen. In den sog. „Proof-of-Concepts" müssen die Kosten für einen wirksamen Schutz mit eingeplant und eingepreist werden. Nur so lassen sich auf Dauer Fehlentscheidungen oder teure Nachrüstungen vermeiden. Daher werden wir zu den Standard-Kapiteln dieser Konzepte zunehmend Punkte wie Datenschutz, technisch und organisatorische Maßnahmen, Risikobewertung, Folgenabschätzung etc. vorfinden.

› Betriebsmodelle: Die Auseinandersetzung mit den Anforderungen der DSGVO wird die Unternehmen mehr denn je dazu bewegen, sich über das jeweilige Betriebsmodell Gedanken zu machen. Die geforderte Risikobewertung wird beeinflussen, welche Sicherheitsmaßnahmen Unternehmen für angemessen halten. Sind der eigene Rechenzentrumsbetrieb oder das Hosting bei einem Dritten die sicherere Variante? Was aber noch bedeutender ist, ist die Tatsache, dass sich auch die Anbieter solcher Lösungen vermehrt mit den Schutzmechanismen und den Folgen einer gemeinsamen Haftung auseinandersetzen müssen.

› Support und Wartung: Das betrifft ggf. vorhandene Sicherheitslücken, die sich durch Wartungs- und Supportprozesse ergeben könnten. Sie werden zunehmend auf den Prüfstand gestellt. Was passiert bei einem Zugriff auf Daten bei einem Supportprozess? Wird die Sicherheit der Systeme durch einen Wartungsvorgang gefährdet?

Jens Hinkelmann

Vorstand der Rödl
Consulting AG
+49 (911) 597 96 – 0
jens.hinkelmann@roedl.com

› Beendigung: In jedem Fall fordert die DSGVO, sich mit dem Zustand der Beendigung von Systemen und Dienstleistungsbeziehungen auseinanderzusetzen. Trennt sich das Unternehmen vom Rechenzentrumsdienstleister oder von einer Consultingfirma, muss sichergestellt sein, dass alle Systeme gestoppt und die Daten übergeben und unwiderruflich gelöscht werden. Sind alle Zugänge für Dritte wirksam gesperrt (Off-Boarding)? Wurde das überprüft? Ist das nachvollziehbar dokumentiert?

Fazit

Die Ausführungen zeigen, dass die DSGVO einen nachhaltigen und positiven Einfluss auf Unternehmen haben wird. Die zahlreichen Vorteile sollten im Auge behalten und intern besprochen werden, um das Unternehmen frühzeitig sowie optimal auf die DSGVO vorzubereiten. Nutzen Sie die Anforderungen als Steuerungsinstrument nach innen und außen zu den Geschäftspartnern.

DSGVO UND ABSCHLUSSPRÜFUNG

Veränderungen nicht nur für den Datenschutzbeauftragten

Von Armin Wilting, Rödl & Partner Köln

Grundsätzlich könnte man sagen, dass die Datenschutz-Grundverordnung (DSGVO) und die Abschlussprüfung keine Gemeinsamkeiten aufweisen und daher das Thema DSGVO für den Abschlussprüfer nicht relevant ist. Durch die DSGVO ändern sich aber die Aufgaben des Datenschutzbeauftragten: Er muss künftig eine aktivere Rolle im Unternehmen übernehmen. Aus Sicht der Abschlussprüfer ist er ein Bestandteil des internen Kontrollsystems. Zudem sind die möglichen Bußgelder deutlich erhöht worden und können somit auch für den Abschluss relevant werden.

Armin Wilting

Wirtschaftsprüfer, Steuerberater, Leiter IT-Prüfung
+49 (221) 94 99 09 – 0
armin.wilting@roedl.com

Die Prüfung der Einhaltung datenschutzrechtlicher Vorschriften ist auch nach Inkrafttreten der DSGVO keine Aufgabe der Abschlussprüfung. Allerdings setzt sich der Abschlussprüfer im Rahmen des risikoorientierten Prüfungsansatzes auch mit dem rechnungslegungsbezogenen internen Kontrollsystem des Mandanten auseinander. Der Datenschutzbeauftragte ist ein Teil des internen Kontrollsystems, genauer gesagt, des internen Überwachungssystems. Nach der DSGVO zählt zu den internen Aufgaben des Datenschutzbeauftragten auch die Überwachung der Einhaltung von Vorgaben. Dabei muss sich der Datenschutzbeauftragte auch mit den technischen Maßnahmen zur Einhaltung des Datenschutzes beschäftigen.

Gleiche Ziele bei Abschlussprüfung und Datenschutz

Im Rahmen der Abschlussprüfung muss sich der Abschlussprüfer gemäß dem „IDW Prüfungsstandard: Abschlussprüfung bei Einsatz von Informationstechnologie" (**IDW PS 330**) mit der IT-Sicherheit beschäftigen. Konkret zu prüfen ist die Einhaltung der in der „IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie" (IDW RS FAIT 1) definierten Anforderungen:

- Authentizität,
- Vertraulichkeit,
- Integrität,
- Verfügbarkeit,
- Autorisierung und
- Verbindlichkeit.

Hierbei handelt es sich um Anforderungen, die sich weitgehend mit denen des Datenschutzes decken. Somit bekommt der Abschlussprüfer auch einen Einblick in die Maßnahmen zum Datenschutz und kann bei seinen Prüfungshandlungen auch Probleme feststellen, die den Datenschutz betreffen.

Nutzung der Ergebnisse des Datenschutzbeauftragten

Der Abschlussprüfer kann überlegen, ob er sich bei der Abschlussprüfung auf Überwachungsmaßnahmen des Datenschutzbeauftragten stützt. Dabei könnten die gleichen Überlegungen angestellt werden, die auch bei der Verwertung der Ergebnisse der internen Revision gelten – danach wäre etwa zu beurteilen, ob Vorgehen und Umfang der Arbeiten des Datenschutzbeauftragten angemessen waren.

Berichtspflichten des Abschlussprüfers

Sofern der Abschlussprüfer feststellt, dass Anforderungen des Datenschutzes nicht eingehalten werden, muss er überlegen, ob es sich um schwerwiegende Gesetzesverstöße oder bedeutsame Schwächen des internen Kontrollsystems handelt. Ist das der Fall, muss er gemäß dem „IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Erstellung von Prüfungsberichten" (IDW PS 450 n. F.) im Prüfungsbericht darüber berichten.

Outsourcing

Immer häufiger werden Teilbereiche der Unternehmen ausgelagert. Dabei liegt häufig Auftragsdatenverarbeitung vor, bei der die Anforderungen von § 11 Abs. 2 BDSG zu beachten sind. Dort sind konkrete Vorgaben für die Vertragsgestaltung definiert. Da der Abschlussprüfer bei Auslagerungen ein Verständnis darüber erlangen muss, ob sie für die Abschlussprüfung relevant sind, wird er sich auch mit diesem Thema beschäftigen. Wir stellen während der Abschlussprüfung sehr häufig – insbesondere bei Auslagerungen innerhalb von Konzernen – fest, dass die vertragliche Gestaltung nicht den rechtlichen Anforderungen entspricht. Solche Verstöße bedeuten immer auch Verstöße gegen den Datenschutz.

Auswirkungen der Veränderungen im Datenschutz

Wesentliche Veränderungen aufgrund der DSGVO betreffen

- die Informationspflichten der Unternehmen,
- das Recht auf Vergessenwerden,
- die Rechenschaftspflichten und
- die Datenschutz-Folgenabschätzung mit den Informationspflichten gegenüber den Behörden.

Das führt zu einer Ausweitung der Aufgaben des Datenschutzbeauftragten.

Aus dem Blickwinkel des Abschlussprüfers ist eine weitere Veränderung von Relevanz, nämlich die Verschärfung der Sanktionen. In der Vergangenheit war das maximale Bußgeld (300.000 Euro) häufig für den Jahresabschluss unwesentlich. Durch die Änderung können jetzt bis zu 4 Prozent des weltweiten Konzernumsatzes als Strafzahlung verhängt werden. Bestehen entsprechende Risiken und werden sie nicht zutreffend im Abschluss abgebildet, muss der Abschlussprüfer ggf. Konsequenzen für den Bestätigungsvermerk in Erwägung ziehen.

BITTE BEACHTEN SIE:

- Unternehmen müssen sich rechtzeitig an die geänderten Anforderungen aufgrund der DSGVO anpassen.
- Auch vor dem Hintergrund der deutlich erhöhten Strafzahlungen sollte der Datenschutz erheblich an Gewicht gewinnen.
- Sprechen Sie mit Ihrem Abschlussprüfer, sofern Sie Bedenken bei der Einhaltung und Umsetzung von Anforderungen des Datenschutzes haben.

UMSETZUNG DER DSGVO

So verschaffen Sie sich als Geschäftsführer, Vorstand oder Aufsichtsrat Sicherheit

Von Hannes Hahn, Rödl & Partner Nürnberg

Der Datenschutz wird durch die Datenschutz-Grundverordnung (DSGVO) aus dem Mauerblümchen-Dasein katapultiert und fordert neben rechtlichen zunehmend auch organisatorische und technische Fähigkeiten von allen Beteiligten. Insbesondere bedarf es für den Nachweis eines wirksamen Datenschutzes einer guten Datenschutzmanagementorganisation. Verschaffen Sie sich als Verantwortlicher Sicherheit, ob Ihr Unternehmen den Anforderungen gerecht wird.

Der Datenschutz und das dazugehörige Management ist ein System, das für alle Beteiligten eine Herausforderung darstellen kann. Neben rechtlichen Anforderungen sind erhebliche organisatorische und funktionale Sachverhalte zu bewältigen. Unternehmen sind gefordert, ihre personenbezogenen Daten datenschutzkonform zu verarbeiten. Sie müssen die Betroffenenrechte einhalten, sich bei Datenschutzverletzungen anforderungsgerecht verhalten und noch vieles mehr.

Für die Verantwortlichen in einem Unternehmen kann sich bei der Komplexität des Themas schon die Frage stellen, ob die eigene Organisation auf dem richtigen Weg ist und bei der Umsetzung der gesetzlichen Anforderungen auch rechtzeitig ankommt. Hierzu ist eine Art „laufende Positionsbestimmung" mit Hinweisen auf Handlungsbedarf sinnvoll.

Vom Assessment…

Für den Einstieg in die Umsetzung der DSGVO empfehlen wir ein erstes Assessment, das den Status Quo erfasst, den Handlungsbedarf erkennen lässt und sich auf folgende Themengebiete bezieht:

- Umfeld, Aufbauorganisation (Governance, Datenschutzbeauftragter);
- datenschutzkonforme Verarbeitung (z. B. Zweck, Rechtmäßigkeit, Verzeichnis der Verarbeitungstätigkeiten);
- Betroffenenrechte;
- Meldung von Datenschutzverletzungen;
- Privacy by Default/Design;
- Analyse und Bewertung datenschutzrechtlicher Risiken;
- technische und organisatorische Maßnahmen (Verschlüsselung, Pseudonymisierung, Vertraulichkeit, Integrität, Belastbarkeit, Verfügbarkeit, Überwachung, Stand der Technik/Wirksamkeit);

BITTE BEACHTEN SIE:

- Führen Sie frühzeitig ein Assessment zum Stand der Umsetzung der DSGVO durch.
- Informieren Sie sich laufend über die Abarbeitung des Handlungsbedarfs.
- Schließen Sie mit der Prüfung durch einen Wirtschaftsprüfer ab, bei der Sie eine Berichterstattung erhalten, die für das Unternehmen und ggf. dessen Geschäftspartner Nutzen stiften kann.

- Löschen von Daten/Datenportabilität;
- Übermittlung/Offenlegung;
- Sensibilisierung/Information und Kommunikation;
- Nachweis- und Rechenschaftspflichten.

…über den Handlungsbedarf…

Nach einem solchen Assessment bietet es sich an, die Abarbeitung der Handlungsbedarfe laufend im Sinne einer „Positionsbestimmung" zu verfolgen. Sind alle Maßnahmen umgesetzt, kann das Assessment wiederholt werden und schließlich ein Wirtschaftsprüfer mit einer Prüfung beauftragt werden.

…zur Prüfung durch den Wirtschaftsprüfer

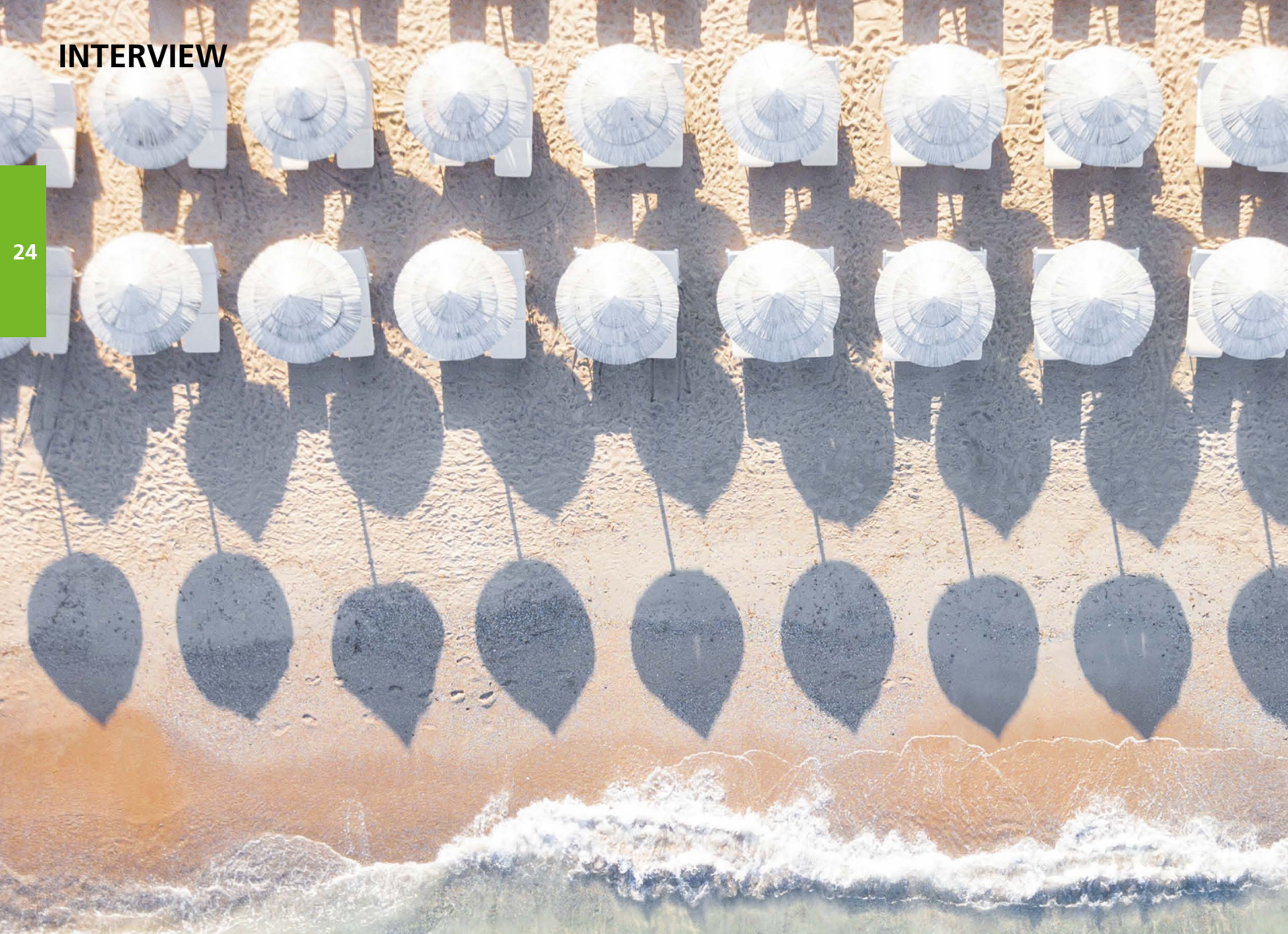
Die Datenschutz-Grundverordnung, die zugehörigen Erwägungsgründe sowie die nationalen Gesetze (z. B. in Deutschland die Neufassung des Bundesdatenschutzgesetzes) liefern eine belastbare Ausgangslage, um den in einem Unternehmen vorgefundenen Ist-Zustand zu beurteilen. Der vor Kurzem veröffentlichte Entwurf eines „**IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung**" (IDW EPS 860) bietet eine gute Grundlage für die Durchführung einer solchen Prüfung mit entsprechender Berichterstattung in Form eines Prüfungsvermerks oder Prüfungsberichts. Sie beinhaltet einen bedeutenden Vorteil für das Unternehmen, denn

- das Management kann sich ggf. entlasten,
- die Geschäftspartner können informiert und überzeugt werden,
- die Kunden können sich im Falle einer Auftragsverarbeitung von der Datenschutzkonformität überzeugen und
- das Image des Unternehmens wird durch den eigenen Datenschutz weiter verbessert.

Aus einer Kombination von Assessment, Projektbegleitung und Prüfung durch den Wirtschaftsprüfer kann das Unternehmen einen bedeutenden Mehrwert generieren: einen Nachweis über eine wirksame Datenschutzmanagementorganisation.

Hannes Hahn

CISA - CSP - DSB, IT-Auditor
IDW, Rödl IT Secure GmbH
+49 (221) 94 99 09 – 200
hannes.hahn@roedl.com



DATENSCHUTZ ALS WETTBEWERBSVORTEIL FÜR UNTERNEHMEN

Einheitliche Regelung in der EU

Rita Santaniello und Nadia Martini antworten

Rita Santaniello und Nadia Martini sind Avvocati (bei Rödl & Partner in Mailand und Mitglieder der Anwaltskammer Mailand. Sie unterstützen international führende Unternehmen bei der Implementierung der DSGVO.

Rita Santaniello verfügt über Erfahrungen in der Betreuung bei gerichtlichen sowie außergerichtlichen Verfahren mit ausländischen Parteien. Sie berät bei datenschutzrechtlichen Fragen im Arbeits- und Wettbewerbsrecht.

Nadia Martini unterstützt italienische und ausländische Mandanten in gerichtlichen und außergerichtlichen Belangen zu den Themen Datenschutz, Copyright und Industrial Property Law.

Im Dezember 2015 hat sich die Europäische Union auf eine Vereinheitlichung des europäischen Datenschutzrechts verständigt. Die EU-DSGVO ist am 24. Mai 2016 in Kraft getreten und ab dem 25. Mai 2018 anzuwenden. Was genau ist die EU-DSGVO?

Die EU-DSGVO stellt die Antwort auf eine Vielzahl von Bedürfnissen der letzten Jahre dar und hat 2 grundlegende Ziele: Einerseits soll sie eine Richtlinie ersetzen, die der heutigen technologischen Realität nicht mehr gewachsen ist, da sie vor Existenz des Internets konzipiert wurde. Andererseits will sie der Notwendigkeit Genüge tun, in einem vereinten Europa eine einheitliche Regelung zu schaffen, die es Unternehmen ermöglicht, nicht 28 verschiedene nationale Gesetze anwenden zu müssen.

Mit der Anwendung der EU-DSGVO treten zahlreiche Veränderungen für Unternehmen ein. Was muss künftig beachtet werden?

Vorab sollte betont werden, dass die durch die DSGVO eingeführten Hauptveränderungen eine kulturelle Revolution initiieren, die das Konzept des Datenschutzes verändert: von einer bloßen Formalität – bei der es ausreichte, sich den apriorisch festgelegten Gesetzesregelungen anzupassen – zu einem Grundverständnis, aufgrund dessen die Unternehmen die notwendigen Schritte für die durchzuführenden Verarbeitungen selbst abschätzen.

Aufgrund des „Accountability Prinzips" können Unternehmen nicht mehr nur ihre „Hausaufgaben" machen, sondern müssen in einer viel flexibleren Umgebung agieren, in der dem Datenschutz wettbewerbsfähige Bedeutung zukommt.

Welche Unternehmen sind davon betroffen?

Grundlegend neu ist die Ausweitung des Geltungsbereichs der Disziplin: Die neue Verordnung betrifft Unternehmen, die personenbezogene Daten bei ihrer Tätigkeit in einer EU-Niederlassung verarbeiten sowie Unternehmen ohne EU-Niederlassung, die Daten von sich in der EU befindenden Personen verwerten, um ihnen Waren oder Dienstleistungen anzubieten – unabhängig von einer Zahlungsverpflichtung – oder deren Verhalten zu beobachten.

Bis zur Anwendungspflicht sind es noch gut 3 Monate. Was droht Unternehmen, die sich nicht rechtzeitig darauf einstellen?

Da die DSGVO den Erfordernissen der heutigen Realität – gekennzeichnet durch die Präsenz von Unternehmensgiganten – entspricht, ist es nicht überraschend, dass sie eine Reihe von finanziellen Sanktionen vorsieht, die nicht nur das Einzelunternehmen, sondern die gesamte zugehörige Unternehmensgruppe betreffen. Um auch Großkonzerne zu sensibilisieren, können sie bis zu 20 Mio. Euro oder 4 Prozent des jährlichen Gesamtumsatzes (falls er höher ist) erreichen.

Auch der Beschäftigtendatenschutz wird angepasst. Welche wichtigen Aspekte sollten Arbeitgeber künftig beachten?

Wesentlich ist die Einführung neuer Rechte der betroffenen Person und folglich der Arbeitnehmer: Sie können nicht nur Auskunft über die verarbeiteten Daten sowie Art und Zweck der Verarbeitung fordern, sondern auch die Korrektur oder Löschung falscher bzw. überflüssiger Daten verlangen.

Am wichtigsten für die Arbeitgeber – und für alle Verantwortlichen – ist auch, dass sie die für ihre Situation angemessenen Sicherheits- und Organisationsmaßnahmen unabhängig zu bewerten und anzuwenden haben. Die große Neuheit liegt in der Abwesenheit von gesetzlich vorgegebenen allgemeingültigen Maßnahmen zugunsten einer größeren Elastizität, die sich aus der Bewertung individueller Situationen ergibt.

Welche Vorteile bringt die EU-DSGVO für Unternehmen und Verbraucher?

Bei Unternehmen entwickelt sich der Datenschutz dank der DSGVO zu einem Wettbewerbsvorteil: Das Prinzip des „Privacy by Design", die Möglichkeit der Anpassung von Verhaltenskodizes, die Einhaltung von Zertifizierungsverfahren sowie die neuen Benachrichtigungsverfahren im Falle eines „Data Breach" stellen in der Tat geeignete Mittel dar, um Kunden und – im Allgemeinen – potenzielle Verbraucher zu gewinnen und ihnen Sicherheit zu gewähren, da sie ihrerseits gravierende Mittel haben, um von den sie betreffenden Datenverstößen zu erfahren.

Rita Santaniello

DATENSCHUTZ-GRUNDVERORDNUNG

Alle Zielsetzungen werden verfehlt

Prof. Dr. Alexander Roßnagel kommentiert

Prof. Dr. Alexander Roßnagel ist Universitätsprofessor für „Öffentliches Recht" mit dem Schwerpunkt „Recht der Technik und des Umweltschutzes" an der Universität Kassel. Er ist wissenschaftlicher Leiter der „Projektgruppe verfassungsverträgliche Technikgestaltung (provet)" und Direktor des wissenschaftlichen Zentrums für Informationstechnik-Gestaltung (ITeG). Zudem ist er Sprecher des Forums „Privatheit und selbstbestimmtes Leben in der digitalisierten Welt". Von 2003 bis 2011 war er Vizepräsident der Universität Kassel.

Prof. Dr. Alexander Roßnagel führt zahlreiche Forschungsprojekte zum Grundrechtsschutz in der digitalen Gesellschaft und zur verfassungsverträglichen Technikgestaltung durch. Daneben ist er Autor diverser Publikationen. Zuletzt war er Herausgeber der Veröffentlichung „Das neue Datenschutzrecht – Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze" (erschienen im **Nomos Verlag** 2018, ca. 477 S.).

Am 25. Mai 2018 ist es soweit: Dann gilt die Datenschutz-Grundverordnung (DSGVO) unmittelbar in der gesamten Europäischen Union. Zugleich tritt das alte Bundesdatenschutzgesetz (BDSG) außer und ein neues in Kraft. Formal wird sich also alles ändern. Was heißt das aber für die Praxis?

Die DSGVO führt viele Regelungen der bisherigen Europäischen Datenschutzrichtlinie von 1995 fort. Da das deutsche Datenschutzrecht der Richtlinie entsprach, bleibt dessen Grundansatz erhalten und viele Regelungen der DSGVO sind mit denen des bisherigen Datenschutzes vergleichbar. Neu ist die Ausweitung des räumlichen Anwendungsbereichs durch das Marktortprinzip. Die DSGVO gilt also für die Verarbeitung personenbezogener Daten aller Personen, die sich in der Union aufhalten. Neu sind auch einige Pflichten der Datenverarbeiter, wie die datenschutzgerechte Systemgestaltung und datenschutzfreundliche Voreinstellungen, die Datenschutzfolgenabschätzung sowie zusätzliche Dokumentationspflichten. Diese Pflichten gelten allerdings unter vielen Vorbehalten. Hinzu kommt der Versuch, durch etliche verfahrensbezogene Regelungen den Vollzug des Datenschutzrechts in der Union zu vereinheitlichen. Für Verstöße gegen die Verordnung drohen künftig drastische Sanktionen: bis zu 20 Mio. Euro oder im Fall eines Unternehmens bis zu 4 Prozent seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs.

Mit der DSGVO verfolgt die EU 3 Zielsetzungen: Sie will zum einen das Datenschutzrecht unionsweit vereinheitlichten, zum anderen eine einheitliche Datenschutzpraxis erreichen und dadurch gleiche Wettbewerbsbedingungen bieten und zudem den Datenschutz angesichts der Herausforderungen der technischen Entwicklung modernisieren sowie den Schutz der Grundrechte verbessern. Sie wird jedoch alle 3 Zielsetzungen verfehlen:

Für eine Vereinheitlichung des Datenschutzrechts ist die DSGVO zu abstrakt und zu unterkomplex. Sie will in 51 Artikeln des materiellen Datenschutzes alle Datenschutzprobleme in allen Gesellschafts-, Wirtschafts- und Verwaltungsbereichen regeln. Dieser Ansatz unterschätzt die enorme Komplexität des Regelungsbedarfs. Er beseitigt die Vielfalt und Differenzierung bisheriger Regelungen und erzeugt dadurch große Rechtsunsicherheit. Im Gesetzgebungsprozess wurden diese Defizite erkannt und 70 Öffnungsklauseln eingebaut. Sie erlauben den Mitgliedstaaten eigenständige Regelungen. Dadurch können sie zwar die notwendige Komplexität und Detaillierung der Vorgaben erreichen, um ausreichende Rechtssicherheit zu gewährleisten, ein einheitliches Datenschutzrecht in der Union ist so aber nicht zu erreichen.

Für eine unionsweit gleiche Praxis des Datenschutzes bedarf es der konkreten Regulierung spezifischer Datenschutzprobleme. Ansonsten werden die hoch abstrakten Vorgaben, je nach bisheriger Datenschutzkultur, von Mitgliedstaat zu Mitgliedstaat unterschiedlich konkretisiert – mit der Folge unterschiedlicher Datenschutzpraktiken. Nur da, wo die Aufsichtsbehörden aller Mitgliedstaaten sich auf konkrete Vorgaben einigen können, besteht die Chance einheitlicher Praxislösungen. Allein mit der DSGVO kann keine Wettbewerbsgleichheit geschaffen werden.

Auch eine Modernisierung des Datenschutzrechts hat die Verordnung versäumt. In keiner Regelung werden die spezifischen Grundrechtsrisiken moderner IT, z. B. smarte Informationstechniken im Alltag, künstliche Intelligenz, selbstlernende Assistenzsysteme, Big Data, Cloud Computing oder datengetriebene Geschäftsmodelle, angesprochen oder gar gelöst. Die gleichen Zulässigkeitsregeln, Zweckbegrenzungen oder Rechte der betroffenen Person gelten für die Kundenliste beim „Bäcker um die Ecke" ebenso wie für die risikoreichsten Formen der Datenverarbeitung in Weltkonzernen und mächtigen Behörden. Insofern zeichnet sich die DSGVO durch eine Risikoneutralität bezogen auf Grundrechtsgefährdungen betroffener Personen aus.

Im Ergebnis führt die DSGVO nicht zu einem praxisrelevanten, einheitlichen und risikogerechten Datenschutzrecht, sondern zu einer von Mitgliedstaat zu Mitgliedstaat unterschiedlichen Ko-Regulierung des Datenschutzes zwischen Union und Mitgliedstaaten. Dadurch kommt den nationalen Gesetzgebern besondere Verantwortung zu. Allerdings hat der deutsche Gesetzgeber mit dem neuen BDSG die Chance vertan, die Regelungen der Verordnung risikogerechter zu gestalten und zu präzisieren.

Fakten zur DSGVO

Mit der Datenschutz-Grundverordnung (kurz: DSGVO; Englisch: „General Data Protection Regulation", kurz: GDPR) kommen EU-weit umfangreiche Änderungen auf die Unternehmen zu. Bisherige Regelungen wie das deutsche Bundesdatenschutzgesetz (BDSG) sind dann nicht mehr anwendbar und als europäisches Recht hat die DSGVO gegenüber nationalen Vorschriften Vorrang. Nur in Einzelfällen ist die Neueinführung nationaler Sonderregelungen erlaubt. Die neuen Anforderungen können zur Herausforderung werden und müssen frühzeitig Beachtung finden. Lesen Sie hier mehr zu ausgewählten Bestandteilen, die mit Anwendbarkeit der DSGVO beachtet werden müssen.

Das Wichtigste zuerst:

Wann?

Die DSGVO befindet sich seit 25. Mai 2016 in Kraft. Die darin geregelte Übergangsfrist beträgt 2 Jahre, so dass noch

106 Tage

bis zum 25. Mai 2018 – dem Tag der Anwendbarkeit – verbleiben.

Sind deutsche Unternehmen vorbereitet?

Laut einer **Bitkom-Studie** aus dem Herbst 2017 war zum damaligen Zeitpunkt die Mehrheit der deutschen Unternehmen noch nicht auf die Umsetzung der DSGVO vorbereitet:

› Lediglich 3 Prozent der Unternehmen konnten 51 bis 100 Prozent verwirklichen.
› 72 Prozent der Befragten hatten 0 bis 20 Prozent realisiert.

Daher werden der Umfrage zufolge viele die DSGVO nicht pünktlich implementieren können.

30 Prozent sind positiv gestimmt und werden nach eigener Aussage bis zum 25. Mai 2018 größtenteils bis vollständig vorbereitet sein.

54 Prozent sind unzureichend gewappnet und werden die Anpassungen nur teilweise verwirklicht haben.

Quellen: Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (www.bfdi.bund.de); www.bitkom.org; www.haufe.de, www.roedl.de.

Elementare Bestandteile:

Marktortprinzip: Die DSGVO gilt auch für Anbieter mit Sitz außerhalb der EU, wenn sie ihre Angebote an Bürger in der EU richten (z. B. Facebook und Google).

Rechenschaft: Unternehmen müssen nachweisen können, dass sie die datenschutzrechtlichen Vorgaben einhalten.

Informations- und Hinweispflichten: Unternehmen müssen Betroffene von der Verarbeitung ihrer personenbezogenen Daten umfassender und genauer als bisher über die Erhebung und Verwendung informieren und Auskunft erteilen (Art. 12 bis Art. 15 DSGVO).

Verfahrensregeln: U.a. **Privacy by Design und by Default** – Datenschutzanforderungen sind frühzeitig in Entwicklungs- und Change-Prozesse einzubinden.

Folgenabschätzung: Unternehmen haben eine Datenschutz-Folgenabschätzung vorzunehmen, wenn durch die geplante Verarbeitung ein hohes Risiko für die Rechte von natürlichen Personen absehbar ist.

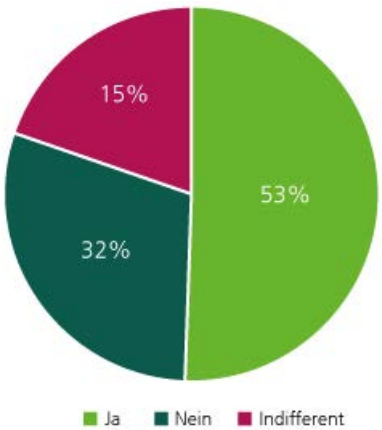
Sanktionen: Künftig müssen alle Datenschutz-Pannen innerhalb von 72 Stunden nach Kenntnis gemeldet werden, sofern ein Datenschutzrisiko besteht. Bei Verstößen können Bußgelder von bis zu 20 Mio. Euro oder 4 Prozent des globalen Jahresumsatzes verhängt werden.

Datenschutzbeauftragter: Die Bestellung eines betrieblichen Datenschutzbeauftragten bleibt für Unternehmen mit mehr als 9 Beschäftigten verpflichtend, die automatisiert personenbezogene Daten verarbeiten. **Seine Rolle ändert sich aber.**

Konzerndatenschutz: Durch den „gemeinsam Verantwortlichen" lassen sich andere Umsetzungsformen finden. Die Datenverarbeitung innerhalb von Unternehmensgruppen wird vereinfacht.

Lesen Sie mehr in unserem **Themenspecial „Datenschutz-Grundverordnung – Neue Bahnen für das Öl der Industrie 4.0"**.

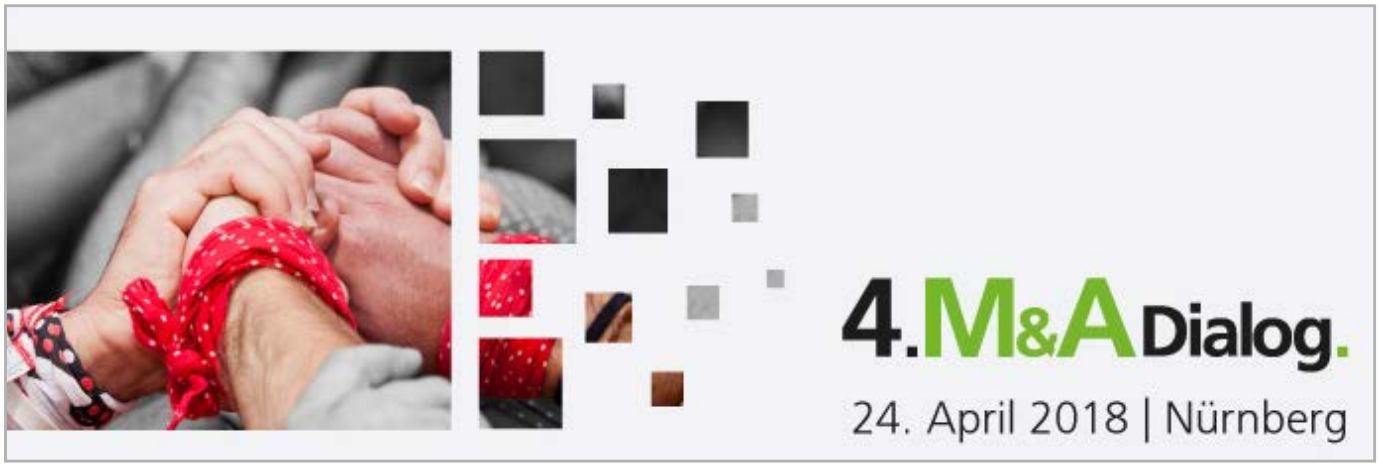
Umfrage auf www.roedl.de: Brauchen wir mehr Datenschutz in Deutschland?



Stand: 1. Februar 2018

Weitere Umfragen auf www.roedl.de »

Event-Highlights im April und Mai 2018



„Jeder Einzelne zählt" – bei den Castellers und bei uns.

Menschentürme symbolisieren in einzigartiger Weise die Unternehmenskultur von Rödl & Partner. Sie verkörpern unsere Philosophie von Zusammenhalt, Gleichgewicht, Mut und Mannschaftsgeist. Sie veranschaulichen das Wachstum aus eigener Kraft, das Rödl & Partner zu dem gemacht hat, was es heute ist.

„Força, Equilibri, Valor i Seny" (Kraft, Balance, Mut und Verstand) ist der katalanische Wahlspruch aller Castellers und beschreibt deren Grundwerte sehr pointiert. Das gefällt uns und entspricht unserer Mentalität. Deshalb ist Rödl & Partner eine Kooperation mit Repräsentanten dieser langen Tradition der Menschentürme, den Castellers de Barcelona, im Mai 2011 eingegangen. Der Verein aus Barcelona verkörpert neben vielen anderen dieses immaterielle Kulturerbe.

Rödl & Partner

www.roedl.de