BWL-Beratertipp des Monats

Ausgabe Mai/Juni 2018

Das aktuelle Thema

DSGVO – Bedeutung für Beleg- und Rechnungswesen – der Einstieg

Sehr geehrte Kollegin, sehr geehrter Kollege,

am 25.05.2018 ist es soweit: Die EU-Datenschutz-Grundverordnung (DSGVO) tritt insgesamt und ohne Übergangsfrist in Kraft. Gleichzeitig wird das bisher geltende Bundesdatenschutzgesetz 1990 durch das neue Bundesdatenschutzgesetz 2018 (BDSG-neu) komplett ersetzt. Die EU-Verordnung umfasst 99 Artikel und 88 Seiten im Amtsblatt der Europäischen Union L 119/88 vom 04.05.2016. Dazu kommen dann noch die 85 Paragraphen des neuen Bundesdatenschutzgesetzes 2018, die im Bundesgesetzblatt vom 05.06.2017 auch noch einmal 36 Seiten einnehmen.

Im Detail kommt jetzt doch vieles überraschend, was wohl nicht zuletzt damit zusammenhängt, dass wir uns im „Musterländle“ des Datenschutzes Deutschland bisher vielleicht zu wenig um die neuen Regelungen gesorgt haben: Was sollte denn noch strenger werden als es bei uns im internationalen Vergleich schon ist? Seit Anfang 2018 häufen sich jetzt allerdings die praktischen Hinweise und ersten Checklisten und Handreichungen, die doch den einen oder anderen Brennpunkt erkennen lassen und vor allem den enormen Dokumentationsaufwand aufzeigen.

Trotz manchem bedrohlichen Szenario hat es wenig Zweck, jetzt in Panik und Hektik zu verfallen. Einige gutgemeinte Vorschriften sind in der Praxis technisch wahrscheinlich noch gar nicht umsetzbar. Bei den Dokumentationspflichten muss man sich fragen, ob man wirklich schon alles perfekt fertig haben muss, wenn z.B. die berufsständischen Vertretungen der Steuerberater Anfang März noch mitteilen, dass sie bei der Erarbeitung (!) von Vorschlägen und Mustern speziell für die Belange des Berufsstandes sind. Allerdings ist das alles kein Grund, die Angelegenheit nicht ernst zu nehmen oder auf die lange Bank zu schieben. Vielmehr muss man jetzt sofort mit der konsequenten Bestandsaufnahme und Umsetzung beginnen.

Im vorliegenden Beratertipp beginnen wir daher mit der Bestandsaufnahme und dem Einstieg nach dem Motto: „Ein Anfang ist gemacht“, damit Sie sich auf den sicherlich nicht ganz kurzen Weg der Umsetzung machen können.

Bei der Umsetzung wünsche ich Ihnen einen guten Start und gutes Gelingen.

Mit freundlichen Grüßen

Böttges – Papendorf

Dr. D. Böttges-Papendorf

Sie lesen in diesem Monat:

Inhalt Seite

Beachten Sie auch unsere Onlinekomponente unter www.bwlberatung.de, außerdem die für Sie als Abonnenten des Loseblattwerks kostenlosen Downloads.
In diesem Monat u.a.

- BMWi: Die EU-Datenschutz-Grundverordnung – Checkliste für die Umsetzung in Unternehmen
- Arbeitshilfe: Prüfliste DS-GVO Anforderungen gem. BayLDA
- BayLDA: Beispielvorlage WEG – Muster für das Verzeichnis von Verarbeitungstätigkeiten
- BayLDA: Beispielvorlage Ärzte – Muster für das Verzeichnis von Verarbeitungstätigkeiten

Tipp: Informieren Sie Ihre Mandanten im Rahmen eines Mandantenabends zum Thema DSGVO.
Die fertige PowerPoint-Präsentation dazu inkl. Redeskript gibt’s hier bzw. unter bit.ly/2HnAUWf.

Deubner Steuern & Praxis

Der „BWL-Beratertipp des Monats“ ist ein monatlicher Sonderservice für die Abonnenten des Loseblattwerks **„Betriebswirtschaftliche Beratung durch den Steuerberater“** aus dem Deubner Verlag Köln.
Herausgeberin: Steuerberaterin Dr. Dorothee Böttges-Papendorf; Redaktion: Dipl.-Wirtsch.-Inf. Sibylle Hänchen und Dipl.-Kfm. Axel Lendle.

Beratungsidee des Monats: Sicher am Start mit der DS-GVO am 25.05.2018

EU-Datenschutz-Grundverordnung (DSGVO) – Rechtsgrundlagen

Rechtsgrundlage für die neuen Regelungen zum Datenschutz ab 25.05.2018 ist die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Die Verordnung wurde veröffentlicht im Amtsblatt der Europäischen Union vom 04.05.2016 Nr. L 119/1. Es handelt sich um eine **Verordnung**, d.h. im Gegensatz zu einer Richtlinie ist die Verordnung unmittelbar anwendbares Recht im gesamten Bereich der EU. Sie geht damit eventuellen nationalen Regelungen vor. Der Text ist auf den Rechtsseiten der EU in Deutsch als pdf zum Download verfügbar.

Ergänzende Regelungen: Das neue Bundesdatenschutzgesetz (BDSG-neu)

Es ist nur folgerichtig, dass damit das bisher geltende Bundesdatenschutzgesetz (1990) obsolet und mit dem Datum 25.05.2018 aufgehoben wird. Statt dessen kommt ein neues Bundesdatenschutzgesetz (BDSG-neu bzw. BDSG 2018), das eigentlich den sperrigen Namen Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU 2016/279) und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und - Umsetzungsgesetz (EU-DSAnp UG-EU) vom 30.06.2017) trägt und im Bundesgesetzblatt 2017 Nr. 44 vom 05.07.2017, Seite 2097 ff. veröffentlicht ist. Dieses Gesetz ist so „geheim“ und geschützt, dass bei Redaktionsschluss aus offiziellen Quellen nur die Nur-Leseversion des Bundesanzeiger Verlags aus dem Bundesgesetzblatt im Internet www.bundesgesetzblatt.de verfügbar war.

Die „Baustellen“ aus Steuerberatersicht

Aus Steuerberatersicht sind speziell drei Anwendungskreise zu berücksichtigen:

1. Anwendung in der eigenen Kanzlei des Steuerberaters
2. Anwendung im Verhältnis zum Mandanten als Auftragsbearbeiter
3. Anwendung beim Mandanten soweit Rechnungswesen relevant.

Steuerberater sind auf der einen Seite besonders betroffen, da sie aufgrund der Natur der ihnen überlassenen Daten in die strengsten Kategorien des Datenschutzes fallen. Auf der anderen Seite haben sie nicht die Probleme, die Daten zweckentfremdet zu verwenden, da Steuerberater schon aus berufsrechtlichen Gründen Daten weder an Dritte verkaufen noch für außerberufliche Zwecke verwenden – wobei schon das Versenden von Geburtstagskarten ohne ausdrückliche Einwilligung des Mandanten allerdings zwiespältig gesehen werden kann. Aufgrund der strengen – und bei Verletzung strafbewehrten – beruflichen Verschwiegenheitspflicht sind Steuerberater und ihre Mitarbeiter aber auf jeden Fall sensibilisiert für das Thema. Neu hinzukommen allerdings technische Fragen. Denn es geht jetzt auch um die Datensicherheit in elektronischen Speichern und vor allem bei der Übermittlung und dem Transfer von Daten von einem Medium ins andere und zwischen unterschiedlichen Akteuren (Mandant, Steuerberater, Finanzamt, Sozialversicherungsträger, Banken, Rechenzentren und Clouds). Hier ist muss der Steuerberater gewährleisten, dass keine Schutzlücken entstehen, auch wenn er selbst nicht der technische Experte und Betreiber ist.

Wo anfangen? – Umsetzungsschwerpunkte setzen

Selbstverständlich muss „alles“ bereits ab dem 25.05.2018 theoretisch perfekt sein, und davon gehen wir als Berufsstand, der traditionell mit geschützten Daten zu tun hat von der Sache her aus. Trotzdem wird es Prüf- und Anpassungsbedarf geben und vor allem Dokumentationserfordernisse sind zu erfüllen, damit im Falle einer Prüfung die entsprechenden „Compliance“-Nachweise erbracht werden können. Das Bundesministerium für Wirtschaft und Energie hat eine Checkliste mit zehn Punkten zur Umsetzung der DSGVO in Unternehmen herausgegeben, die wesentliche Ansatzpunkte für den Einstieg aufzeigt. Die Prüfpunkte sind in der Übersicht auf Seite 3 dargestellt.

Diese Punkte abzuarbeiten, kann schon mal nicht falsch sein. Anregungen, wie man dabei ergebnisorientiert und effizient vorgehen kann, sind zu den einzelnen Punkten aufgeführt. Die Originaltexte des BMWi finden Sie in der Internetbeilage.

Umsetzung: Handreichung des BayLDA für Kleinunternehmen und Vereine

Das Bayerische Landesamt für Datenschutzaufsicht hat außerdem Anfang 2018 Handreichungen für kleine Unternehmen und Vereine mit konkreten Umsetzungshinweisen und Mustern entwickelt und veröffentlicht. Bisher sind konkrete Beispiele für folgende Branchen abrufbar, an denen man sich für den eigenen Bedarf orientieren kann:

- Vereine
- Kfz-Werkstatt
- Handwerksbetrieb
- Steuerberater
- Arztpraxis
- WEG-Verwaltung
- Produktionsbetrieb
- Genossenschaftsbank
- Online-Shop
- Bäckerei
- Beherbergungsbetrieb
- Einzelhändler

Stand 28.03.2018, www.lda.bayern.de/de/kleine-unternehmen.html.

Die zehn Prüfpunkte der Checkliste des BMWi zur Umsetzung der DS-GVO* in Unternehmen abarbeiten

1. Kommunikation und Sensibilisierung

Hier kann der Einstieg durch eine Datenschutzanweisung für die Mitarbeiter erfolgen. Das kann einhergehen mit einer Auffrischung der Verschwiegenheitserklärung, die jetzt ergänzt werden muss durch eine Datenschutzanweisung nach den Vorgaben der DSGVO. Hierfür gibt es keine offiziellen Mustervorlagen, und auch die schriftliche Abfassung ist nicht zwingend erforderlich, jedoch aus Nachweisgründen anzuraten. Muster für Vertraulichkeitserklärungen werden teilweise von berufsständischen Organisationen angeboten oder in entsprechenden Seminaren verteilt. Außerdem hat die Gesellschaft für Datenschutz- und Datensicherheit e.V. hierfür eine Praxishilfe zusammengestellt, die als Grundlage für eine derartige Erklärung verbunden mit der erforderlichen Mitarbeiterschulung dienen kann. Die GDD-Praxishilfen DS-GVO sind zum Download verfügbar auf www.gdd.de. **Diese Informations-, Verpflichtungs-, Sensibilisierungs- und Schulungsmaßnahme sollte unbedingt noch bis zum 24.05.2018 erfolgen.**

2. Bestandsaufnahme

Der nächste Schritt zur Identifizierung möglichen Änderungsbedarfs ist die Bestandsaufnahme aller Prozesse, in denen personenbezogene Daten verarbeitet und gespeichert werden. Das sind insbesondere Mandanten- und Kundendaten. Hier beginnt die Fleißarbeit. Das wird sicher einige Zeit in Anspruch nehmen. Der **Fragebogen zur Umsetzung der DS-GVO zum 25. Mai 2018** des BayLDA hilft bei der Bestandsaufnahme. Wer bereits bisher datenschutzbewusst gearbeitet hat, sollte von den Prozessen i.a. auf der sicheren Seite sein. Was fehlen dürfte, ist die Dokumentation entsprechend den neuen Anforderungen. Prüfen: **Prozess in Ordnung (sofort)? Prozessdokumentation vorhanden (evtl. nachbessern)?**

3. Rechtsgrundlagen prüfen

Grundsätzlich darf man personenbezogene Daten nicht verarbeiten und speichern, es sei denn, es gibt hierfür eine besondere Rechtsgrundlage (sog. Verbot mit Erlaubnisvorbehalt). Als Rechtsgrundlage kommt insbesondere die Einwilligung des Betroffenen (unter Beachtung entsprechender Formvorschriften) in Betracht. **Außerdem ist die Datenverarbeitung zulässig, wenn sie zur Erfüllung eines Vertrags mit dem Betroffenen erforderlich ist**. Prüfen: Liegt für alle Datenverarbeitungsprozesse innerhalb des Unternehmens eine entsprechende Rechtsgrundlage vor?

4. Anforderung an die datenschutzrechtliche Einwilligung

Für die Einwilligung sind die entsprechenden Vorschriften der DSGVO zu beachten (vgl. Art. 7 und 8) sowie die Informationspflichten gemäß Artikel 13 DSGVO. Vgl. zur **Einwilligung** – speziell auch in den unverschlüsselten Mail-Versand – GDD-Praxishilfe DS-GVO VIII, Stand 02/2018.

5. Verträge und Regularien überprüfen

Die bestehenden Verträge und Regelungen zur Auftragsdatenverarbeitung sind zu überprüfen und zu überarbeiten, ebenso wie die Vertragsmuster z.B. bei der Auftragsannahme.

6. Datenschutz-Folgenabschätzung

Eine formelle Datenschutz-Folgeabschätzung ist erforderlich, wenn die Datenverarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für Rechte und Freiheiten betroffener Personen bergen. Für die vom Bayerischen Landesamt für Datenschutzaufsicht dargestellten Fallstudien von KMU wird das Bestehen besonderer Risiken i.d.R. verneint. Ein Anwendungsfall erhöhter Sorgfaltspflichten kann die Benutzung gemeinsamer IT-Infrastrukturen mit Dritten sein (vgl. dazu die Orientierungshilfe Mandantenfähigkeit V 1.0 vom 11.10.2012.

7. Melde- und Konsultationspflichten, Bestellung eines Datenschutzbeauftragten

Es ist die Verpflichtung zur Bestellung eines Datenschutzbeauftragten neu zu prüfen. Bei Unternehmen, in denen **weniger als zehn Personen** regelmäßigen Umgang mit personenbezogenen Daten haben, ist eine solche Bestellung nicht erforderlich. Im Übrigen ergeben sich die Melde- und Konsultationspflichten gegenüber den Aufsichtsbehörden aus den Artikeln 33, 36 und 37 DSGVO.

8. Betroffenenrechte und Informationspflichten

Zu beachten sind das Recht auf Löschung (Art. 17 DSGVO), das Recht auf Datenübertragbarkeit auf einen Dritten (Art. 20 DSGVO) sowie die Informationspflichten gegenüber den Betroffenen (Art. 13, 14 DSGVO). **Eine Löschpflicht besteht nicht, solange gesetzliche Aufbewahrungsfristen bestehen.** Hier ist es wichtig, dass die Daten so organisiert sind, dass eine Trennung nach Personen leicht möglich ist und bei Personen außerdem noch zwischen Daten, die gelöscht werden dürfen und Daten, deren vorzeitige Löschung eine Aufbewahrungsverpflichtung gegenüber steht. Speziell hier dürfte es bei integrierten Systemen teilweise technische Probleme geben. Zutage getreten sind diese z.B. bei Arztpraxen und bei der Trennung von Patientendaten, die für das Rechnungswesen relevant sind, von den Gesundheitsdaten, die der absoluten Verschwiegenheitspflicht unterliegen. Hier wird man sich regelmäßig technisch auf dem Laufenden halten müssen und bis dahin für sich eine möglichst passende Lösung finden müssen.

9. Dokumentation

Das wichtigste neue Verzeichnis ist in Artikel 13 geregelt, das **Verarbeitungsverzeichnis**: Ein solches sollte in jedem Unternehmen künftig vorhanden sein. Außerdem sind Datenschutzvorfälle zu dokumentieren und die Weisungen im Rahmen von **Auftragsverarbeitung**sverhältnissen.

10. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (TOM)

Für die Zukunft sollte bereits bei Einrichtung und Ausgestaltung der Datenverarbeitung frühzeitig auf die datenschutzrechtlichen Erfordernisse geachtet werden. Dies wird jetzt ausdrücklich in Artikel 25 DSGVO unter der Überschrift „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ gefordert. Stichworte sind Privacy by Design, Privacy by Default und Pseudonymisierung. Das heißt, es soll durch **technische und organisatorische Maßnahmen (TOM)** gewährleistet werden, dass auch für weniger technikaffine Nutzer ein möglichst großen Schutz ihrer Privatsphäre gewährleistet wird, ohne dass diese selbst komplizierte Einstellungen vornehmen müssen.

* Prüfpunkte gem. BMWi „Die EU-Datenschutz-Grundverordnung – Checkliste für die Umsetzung in Unternehmen“, s.a. Internet-Beilage, Download 14.04.2018, mit eigenen Erläuterungen für mögliche konkrete Umsetzungsmaßnahmen.

Arbeitshilfe: Prüfliste DS-GVO Anforderungen des BayLDA

In seinen Fallstudien für KMU geht das Bayerische Landesamt für Datenschutzaufsicht (www.lda.bayern.de) nach folgendem Schema vor:

Kurzbeschreibung des Unternehmens
(Branche, Größe, Anzahl Mitarbeiter, Kunden, Einzugsgebiet, IT und externe IT-Partner)

Darstellung der wesentlichen Verarbeitungstätigkeiten
(typische Tätigkeiten mit Verarbeitung personenbezogener Daten sind z.B. Lohn- und Gehaltsabrechnung der Mitarbeiter, Verarbeitung von Kunden-/Patienten-/Mandantendaten von Privatkunden zur Auftragsabwicklung und Rechnungsstellung, Verarbeitung von Daten von Firmenkunden und deren Kunden/Mitarbeitern zur Auftragsabwicklung und Rechnungsstellung, Betrieb einer Webseite über Dienstleister mit und ohne Kontaktformular oder interaktive Funktionen wie Terminvereinbarung, Online-Shop, Zahlungsabwicklung, Buchhaltungsdienstleistungen über externe Dienstleister und Rechenzentren)

Checkliste: Wesentliche DS-GVO-Anforderungen für KMU

A Datenschutzbeauftragter (DSB)
Muss ein DSB vom Unternehmen benannt werden?
- ☐ ja (wenn mehr als 10 Personen regelmäßigen Umgang mit personenbezogenen Daten haben)
- ☐ nein (wenn weniger als 10 Personen im regelmäßigen Umgang mit personenbezogenen Daten)

B Verzeichnis von Verarbeitungstätigkeiten
Ist ein solches Verzeichnis erforderlich?
- ☐ ja (wegen regelmäßiger Verarbeitung personenbezogener Daten)
- ☐ nein (dürfte in der Praxis kaum noch vorkommen)

C Datenschutz-Verpflichtung von Beschäftigten
Ist eine solche Verpflichtung durchzuführen?
- ☐ ja (da alle/die meisten Mitarbeiter mit personenbezogenen Daten umgehen; schriftlich aus Nachweisgründen empfohlen; regelmäßige Auffrischungen)
- ☐ nein (dürfte ein Ausnahmefall sein)

D Informations- und Auskunftspflichten
Bestehen irgendwelche Informationspflichten?
- ☐ ja (insb. bei Vertragsabschluss sowie auf der Webseite in der Datenschutzerklärung)
- ☐ nein (dürfte ein Ausnahmefall sein)

E Löschen von Daten
Gibt es eine Anforderung zur Datenlöschung?
- ☐ ja (Normalfall, aber erst nach Ablauf gesetzlicher Aufbewahrungspflichten; ggf. aufbewahrungspflichtige und andere Daten unterscheiden und trennen)
- ☐ nein

F Sicherheit
Müssen die Daten besonders gesichert werden?
- ☐ ja (immer: **Standardmaßnahmen**; spezielle Maßnahmen z.B. beim Transport oder Auslagerung auf mobile Geräte, in Clouds, Übertragung an Dritte auf Verschlüsselung und evtl. abweichende Standards in „Drittländern“ (= Nicht-EU und EWR) achten)
- ☐ nein

G Auftragsverarbeitung
Ist ein Vertrag zur Auftragsverarbeitung notwendig?
- ☐ ja (typischer Fall externe IT-Dienstleister für Webseite und IT-Wartung; auch externe Buchführungsdienstleister und Rechenzentren)
- ☐ nein

H Datenschutzverletzungen
Müssen bestimmte Vorfälle gemeldet werden?
- ☐ ja (aber nur bei relevanten Risiken – eine einfache Online-Meldung beim BayLDA ist möglich; evtl. berufliche Verschwiegenheitspflichten beachten)
- ☐ nein

I Datenschutz-Folgeabschätzung (DSFA)
Ist eine DSFA vom Steuerberater durchzuführen?
- ☐ ja (bei hohem Risiko bei der Datenverarbeitung, z.B. wenn sich Daten in Clouds oder anderen gemeinsam mit Dritten genutzten „mandantenfähigen“ IT-Infrastrukturen befinden; vgl. zur Datenschutzfolgenabschätzung Kurzpapier Nr. 5 der DSK Datenschutzkommission sowie Orientierungshilfe Mandantenfähigkeit Version 1.0 vom 11.10.2012, Download über www.lda.bayern.de am 16.04.2018).
- ☐ nein (wenn kein hohes Risiko bei der Datenverarbeitung besteht)

J Videoüberwachung (VÜ)
Besteht eine Ausschilderungspflicht bezüglich VÜ?
- ☐ ja (wenn Videoüberwachung besteht)
- ☐ nein (da keine Videoüberwachung vom Unternehmen durchgeführt wird)

Natürlich sind alle Punkte gleich wichtig und zu beachten. Bei der Schwerpunktsetzung sollte man aber die Prüfpunkte A bis D vorrangig angehen. Dann hat man schon mal das organisatorische Datenschutzkonzept stehen. Wenn das technische Datenschutzkonzept mit den Standardmaßnahmen wie Firewall, Virenschutz, regelmäßige Updates und Nutzungskontrolle dazu kommt, sollten in jedem Fall die Grundlagen stimmen. Verbessern kann man laufend.

Aktuelle Zinssätze (Stand 17.04.2018)

Art des Zinses	%	Rechtsgrundlage/ Quelle
Basiszinssatz seit 01.07.2016	-0,88 p.a.	§ 247 Abs. 1 BGB/ Deutsche Bundesbank Zinssätze
Hauptrefinanzierungs-Fazilität seit 16.03.2016 Spitzenrefinanzierungs-Fazilität seit 16.03.2016	0,00 p.a. 0,25 p.a.	Deutsche Bundesbank, EZB-Zinssätze
Anleihen der öffentlichen Hand mit Restlaufzeit über 9–10 Jahre (02/2018)	0,7	Deutsche Bundesbank, Kapitalmarktstatistik, März 2018
ERP-Gründerkredit – Startgeld – 5 Jahre – nominal (effektiv) ERP-Gründerkredit Universell: je nach Bonität nominal (effektiv)	2,05 (2,07) ab 1,00 (1,00)	Seit 14.10.2014 bzw. 01.04.2015. Alle Werte aktuell siehe Konditionen-Anzeiger der KfW www.kfw.de.
Kapitalisierungsfaktor (Multiplikator) für das vereinfachte Ertragswertverfahren, rückwirkend ab 01.01.2016 (statt zuletzt alte Rechtslage 17,86) entspricht Zins	13,75 7,27	§ 203 Abs. 1 BewG i.d.F. des Gesetzes vom 04.11.2016, BGBl I v. 09.11.2016, 2464

Vorschau: DSGVO – Aktuelle Brennpunkte und Lösungsansätze im Rechnungswesen