

05|18

# Aktuelle Informationen für unsere Mandanten

Termine (Steuern und Sozialversicherungsbeiträge) .....	2
Wichtige Fakten über die DSGVO und das neue BDSG .....	2

## Termine (Steuern und Sozialversicherungsbeiträge)

TERMINE MAI 2018			
Steuerart	Fälligkeit	Überweisung	Scheck/bar
Lohnsteuer, Kirchensteuer, Solidaritätszuschlag	11.05.2018	14.05.2018	Keine Schonfrist
Umsatzsteuer	11.05.2018	14.05.2018	Keine Schonfrist
Gewerbsteuer	15.05.2018	18.05.2018	Keine Schonfrist
Grundsteuer	15.05.2018	18.05.2018	Keine Schonfrist
Sozialversicherungsabgaben	28.05.2018	Keine Schonfrist	Keine Schonfrist

TERMINE JUNI 2018			
Steuerart	Fälligkeit	Überweisung	Scheck/bar
Lohnsteuer, Kirchensteuer, Solidaritätszuschlag	11.06.2018	14.06.2018	Keine Schonfrist
Umsatzsteuer	11.06.2018	14.06.2018	Keine Schonfrist
Körperschaftsteuer, Solidaritätszuschlag	11.06.2018	14.06.2018	Keine Schonfrist
Einkommensteuer, Kirchensteuer, Solidaritätszuschlag	11.06.2018	14.06.2018	Keine Schonfrist
Sozialversicherungsabgaben	27.06.2018	Keine Schonfrist	Keine Schonfrist

**Steuern:** Bei verspäteter Zahlung bis zu 3 Tagen werden Zuschläge nicht erhoben (§ 240 Abs. 3 AO i.d.F StÄndG 2003). Diese Schonfrist entfällt bei Barzahlung und Zahlungen per Scheck. Seit 01.01.2007 gelten Zahlungen per Scheck erst drei Tage nach Eingang des Schecks als geleistet.

**Sozialversicherung:** Seit 2006 sind Beiträge spätestens am drittletzten Bankarbeitstag des laufenden Monats fällig. (Der 24.12. und 31.12. gelten nicht als bankübliche Arbeitstage)

## Wichtige Fakten über die DSGVO und das neue BDSG

In Kürze wird in Europa erstmals ein einheitlicher Datenschutz eingeführt. Dann startet die EU-Datenschutz-Grundverordnung (EU-DSGVO). Nachfolgend finden Sie die wichtigsten Fakten im Kurzüberblick zusammengefasst.

Wir können i.S. DSGVO nicht beraten. Sprechen Sie ggf. Ihren Rechtsanwalt, die Handelskammer oder Ihren Berufsverband an.

### **1. Wann tritt die DSGVO in Kraft und wie wirkt die EU-Datenschutzgrundverordnung in Deutschland?**

Die EU-Datenschutz-Grundverordnung ist bereits am 25.5.2016 in Kraft getreten. Nach der darin geregelten Übergangsfrist kommt sie allerdings erst zwei Jahre nach Inkrafttreten zur Anwendung. Das bedeutet, dass sie ab 25.5.2018 für alle gilt. Ab dem 25.5.2018 regelt die DSGVO EU-weit also einheitlich die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen.

Die für Unternehmen einschlägigen Regelungen des Bundesdatenschutzgesetzes werden weitgehend durch die Regelungen der DSGVO ersetzt. Da es sich bei dem neuen Gesetz um eine europäische Verordnung handelt, gilt sie direkt in allen Mitgliedstaaten. Die nationalen Gesetzgeber werden lediglich neue Gesetze erlassen, um die nationalen Vorschriften, die durch die Verordnung ersetzt werden, aufzuheben. Das heißt: Das bestehende BDSG wurde in weiten Teilen überarbeitet und tritt ebenfalls am 25.5.2018 in Kraft.

### **2. Gibt es eine Übergangsfrist?**

Nein, eine Übergangsfrist wird es nicht geben. Rein rechtlich ist sie ja bereits am 25.5.2016 in Kraft getreten. Sie entfaltet nur jetzt erst ihre Wirkung. Unternehmer müssen sich umgehend mit den notwendigen Maßnahmen zur Einhaltung der DSGVO befassen.

### **3. Betrifft die DSGVO jedes Unternehmen?**

Jedes Unternehmen muss am 25.5.2018 nachweisen, dass es den Datenschutz einhält. Nach Art. 2 DSGVO gilt die Verordnung für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Datensystem gespeichert sind oder gespeichert werden sollen. Damit sind praktisch alle erfasst: Händler, Shop-Betreiber, Unternehmer, Arztpraxen, Kanzleien, Vereine. Wenn eine elektronische Datenverarbeitung erfolgt, auch wenn sie nur aus einem Computer besteht oder Daten aus einem Karteikartensystem auf Papier verarbeitet werden, dann gilt die DSGVO.

### **4. Was sind personenbezogene Daten?**

Als „personenbezogene Daten“ gelten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. „Identifizierbar“ bedeutet, dass die Person nicht identifiziert werden muss. Es reicht aus, dass die Person mithilfe der zur Verfügung stehenden Daten identifiziert werden könnte.

Beispiele für personenbezogene Daten sind: Name, Adresse, Geburtsdatum, Bankdaten, etc. Aber auch Fingerabdruck, Irisscan und Krankengeschichte gehören dazu.

### **5. Wann „verarbeitet“ man überhaupt Daten?**

Der Begriff der Verarbeitung ist nach Art. 4 DSGVO weit gefasst. Danach ist jeder „mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“ eine Verarbeitung im Sinne des Gesetzes.

Beispiele für die Verarbeitung von Daten sind: Die Erstellung einer Kundendatei, Aufnahme der Daten zur Erstellung einer Rechnung oder das Anlegen oder Führen einer Mitarbeiterdatenbank.

So beinhaltet die Verarbeitung praktisch jede Art des Umgangs mit personenbezogenen Daten. Insbesondere wird jeder Umgang mit personenbezogenen Daten erfasst, die in Computern oder anderen digitalen Medien gespeichert sind.

## **6. Worauf basieren die Grundsätze für die Verarbeitung personenbezogener Daten?**

Bei der Datenverarbeitung in Europa gilt das sogenannte Verbot mit Erlaubnisvorbehalt. Das bedeutet, dass jede Verarbeitung personenbezogener Daten verboten ist, außer wenn sie per Gesetz (zum Beispiel aus BDSG, Telemediengesetz-TMG, DSGVO) oder durch eine Einwilligung erlaubt wurde.

In der DSGVO sind die Art. 5 und 6 quasi die entscheidenden Artikel, wann eine Verarbeitung erlaubt sein kann: Art. 5 Abs. 1 a-f stellt die Prinzipien – quasi die Kernelemente des Gesetzes – dar:

- **Transparenz** – Die Verarbeitung personenbezogener Daten muss für Betroffene nachvollziehbar sein.
- **Zweckbindung** – Unternehmen sollen Daten nur für den Zweck verarbeiten, für den sie erhoben worden sind. Das heißt, man muss sich bereits zu Beginn von Verarbeitungsprozessen Gedanken machen, wofür die Daten benötigt werden. Dies ist zu dokumentieren.
- **Datenminimierung** – Unternehmen müssen die Verarbeitung von personenbezogenen Daten auf das den Verarbeitungszweck notwendige Maß beschränken.
- **Richtigkeit** – Unternehmen müssen dafür sorgen, dass die personenbezogenen Daten korrekt sind. Dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.
- **Speicherbegrenzung** – Unternehmen dürfen personenbezogene Daten nur so lange speichern, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.
- **Integrität und Vertraulichkeit** – Daten müssen durch technische und organisatorische Maßnahmen vor unbefugter Verarbeitung, Zerstörung, Veränderung oder Verlust geschützt werden.

Nach Art. 6 DSGVO ist die Verarbeitung nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere konkrete Zwecke gegeben.
- Die Verarbeitung ist für die Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen erforderlich.
- Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich.
- Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.
- Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt.

- Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

### **7. Was ändert sich für die Unternehmen konkret?**

Eine der wichtigsten Neuerungen ist die Einführung der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO. Unternehmen sind danach verpflichtet, die Einhaltung der DSGVO nachzuweisen.

Daraus ergeben sich verstärkte Dokumentations- und Nachweispflichten:

- Die Führung eines Verzeichnisses von Verarbeitungstätigkeiten,
- die Durchführung von Datenschutz-Folgenabschätzungen sowie
- die Dokumentation von Datenschutzvorfällen.

Das aus dem BDSG bekannte Verfahrensverzeichnis – dort „Übersicht“ genannt – wird mit der DSGVO abgelöst durch ein schriftliches oder elektronisches Verzeichnis aller Verarbeitungstätigkeiten mit personenbezogenen Daten.

Ein Verzeichnis von Verarbeitungstätigkeiten gemäß DSGVO muss erheblich umfangreicher ausfallen, als das bisherige Verfahrensverzeichnis, wenn es als Grundlage dienen soll, um den Nachweispflichten der DSGVO nachzukommen. Das Verzeichnis kann durch die Aufsichtsbehörde jederzeit angefordert werden. Falls das Verzeichnis von Verarbeitungstätigkeiten nicht und unvollständig vorliegt drohen empfindliche Bußgelder.

Das Verfahrensverzeichnis betrifft sämtliche – auch teilweise – automatisierte Verarbeitungen sowie nichtautomatisierte Verarbeitungen personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Grundsätzlich ist jeder Verantwortliche z. B. Unternehmen, Freiberufler, Verein und Auftragsverarbeiter zur Erstellung und Führung eines solchen Verzeichnisses verpflichtet.

Ein Verzeichnis von Verarbeitungstätigkeiten enthält mehrere Verfahrensbeschreibungen. In den Verfahrensbeschreibungen werden die Verarbeitungsschritte von personenbezogenen Daten dokumentiert. Aus den Dokumenten muss hervorgehen, welche personenbezogenen Daten das Unternehmen mithilfe welcher Verfahren auf welche Weise verarbeitet und welche technisch-organisatorischen Maßnahmen zum Schutz dieser Daten dabei getroffen wurden.

Hierzu empfiehlt es sich, eine Übersicht aller im Unternehmen eingesetzten Anwendungen und IT-Verfahren und Dateien, in denen personenbezogene Daten verarbeitet werden, zu erstellen. Typische Beispiele sind Zeiterfassungssysteme, E-Mailverarbeitungen, CRM-Systeme, Personalverwaltung und Websitebesucheranalysen.

Eine gewisse Erleichterung gibt es für Unternehmen oder Einrichtungen mit weniger als 250 Mitarbeitern. Diese könnten von der Führung eines Verzeichnisses befreit sein, sofern die Verarbeitungen von personenbezogenen Daten

- kein Risiko für die Rechte und Freiheiten der betroffenen Personen bergen,
- nur gelegentlich erfolgen oder

- keine besonderen Datenkategorien z. B. Gesundheitsdaten oder strafrechtliche Verurteilungen und Straftaten betreffen.

Da nur eine dieser Fallgruppen für eine Pflicht zur Verzeichnisführung erfüllt sein muss, werden nur wenige Unternehmen und Einrichtungen von der Pflicht zur Führung eines Verzeichnisses entbunden sein. Vor allem die Ausnahme, dass die Verarbeitung nur gelegentlich erfolgen darf, wird dazu führen, dass ein Verzeichnis praktisch doch immer geführt werden muss. Allein Lohn- und Gehaltsabrechnungen erfolgen regelmäßig und nicht nur gelegentlich und da dabei auch Religions- und Gesundheitsdaten (Krankheitstage) betroffen sind, wird in praktisch allen Unternehmen und Einrichtungen ein Verzeichnis für Verzeichnisse erforderlich sein.

Für kleinere Unternehmen und Einrichtungen z. B. Handwerker, Ärzte und vor allem Vereine bedeutet dies einen erheblichen zusätzlichen bürokratischen Aufwand.

Weitere Änderungen sind: Die Informationspflichten gegenüber Betroffenen (z. B. die Datenschutzerklärung) sind umfangreicher, die Verträge mit Dienstleistern zur Auftragsverarbeitung müssen strengere Anforderungen erfüllen; das Recht auf Datenportabilität sowie die Fristen für die Bearbeitung der Anträge zur Ausübung der Rechte der Betroffenen sind zu beachten. Das bedeutet, man muss jederzeit Nachweis über seine Datenverarbeitungsprozesse führen und belegen, dass deren Zwecke, Art und Umfang und risikomindernde Maßnahmen dokumentiert und die Zulässigkeit geprüft worden sind.

#### **8. Was, wenn sich der Unternehmer nicht an die Vorschriften hält?**

Wer die datenschutzrechtlichen Vorschriften nicht einhält, dem drohen empfindliche Strafen: Verstöße können mit Bußgeldern von bis zu 20 Millionen EUR oder von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes geahndet werden. Die EU will damit ein deutliches Zeichen setzen.

Zusätzlich können weitere Einzelmaßnahmen in Betracht kommen: Zum Beispiel Bußgelder neben oder anstelle von Maßnahmen, wie Herausgabe von Informationen, Verwarnungen oder Beschränkungen der Verarbeitung.

#### **9. Wen trifft die Datenschutzreform vor allem?**

Wer bereits bis heute ein Verzeichnis der Datenverarbeitungen geführt hat, wird sich viel von dieser Fleißarbeit ersparen. Treffen wird es vor allem diejenigen, die sich bisher um den Datenschutz wenig Gedanken gemacht haben. Genau diese Zielgruppe wollte der Gesetzgeber erreichen.

SIEGERT | EDEN | KASTENS

Vorangegangene Mandanteninformationen dienen zur allgemeinen Information über aktuelle steuerliche Fragestellungen und Entwicklungen in Gesetzgebung und Rechtsprechung und sind als solche zu sehen. Diese fachlichen Informationen können den zugrundeliegenden Sachverhalt oftmals nur verkürzt wiedergeben und ersetzen daher nicht eine individuelle Beratung durch uns. Ein Mandatsverhältnis kommt durch die Nutzung bzw. das Einsehen dieser Informationen nicht zustande. Sollte sich aus den Informationen heraus konkreter Beratungsbedarf für Sie ergeben, stehen wir hierfür jederzeit zur Verfügung.