Mag. Matthias Aichinger, MBA
Ing. Andreas Dolezal

Datenschutz in der Praxis

Datenschutz-Leitfaden mit 60 wertvollen Tipps für die Praxis

von Unternehmern für Unternehmer

Inhalt

Rechtshinweis

Dieses Handbuch stellt keine abschließende und vollständige Information dar. Eine individuelle, unternehmensspezifische Betrachtung sowie gegebenenfalls die Inanspruchnahme von spezialisierten (Rechts-)Beratern kann durch dieses Handbuch nicht ersetzt werden. Dieses Handbuch stellt keine Rechtsberatung dar, und gibt den Wissens- und Erfahrungsstand der Autoren auf Basis der zum Zeitpunkt des Verfassens geltenden gesetzlichen Bestimmungen (Juli 2018) wieder. Trotz sorgfältiger Prüfung aller Inhalte sind Irrtümer und Fehler nicht auszuschließen, ebenso wird für die Richtigkeit des Inhalts keine Gewähr übernommen. Eine Haftung der Autoren ist ausgeschlossen.

Im Sinne der besseren Lesbarkeit wird entweder die männliche oder die weibliche Form von personenbezogenen Wörtern gewählt. Damit wird keinesfalls das jeweils andere Geschlecht benachteiligt. Frauen und Männer mögen sich von den Inhalten dieses Buches gleichermaßen angesprochen fühlen.

Datenschutz per Gesetz

Datenschutz im Sinne der geltenden Datenschutzgesetze bezeichnet den Schutz personenbezogener Daten von natürlichen Personen (um ganz genau zu sein: von geborenen sowie lebenden Personen), ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsortes.

Seit 25. Mai 2018 wird dazu in der gesamten Europäischen Union (EU) sowie dem Europäischen Wirtschaftsraum[1] (EWR) die Verordnung[2] (EU) 2016/679, besser bekannt als Datenschutz-Grundverordnung, oder kurz DSGVO, angewandt. Sie umfasst 173 Erwägungsgründe und 99 Artikel, und löst die EU-Datenschutzrichtlinie (95/46/EG) ab, auf der das bisherige österreichische Datenschutzgesetz (DSG 2000) beruht.

Die Datenschutz-Grundverordnung wurde bereits am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlicht und ist am zwanzigsten Tag nach der Veröffentlichung, also am 24. Mai 2016, in Kraft getreten.

Die „Übergangsfrist", die es Unternehmern und Unternehmen ermöglicht hat die Vorschriften in die Praxis umzusetzen, endete zwei Jahre nach Inkrafttreten der DSGVO, also am 24. Mai 2018. Seit Freitag, den 25. Mai 2018, werden die neuen Datenschutzvorschriften angewandt.

---

[1] Der Europäische Wirtschaftsraum, kurz EWR, umfasst die derzeit 28 EU-Mitgliedstaaten sowie Island, Liechtenstein und Norwegen.

[2] Eine Verordnung der EU ist unmittelbar anwendbar und bedarf grundsätzlich keiner weiteren nationalen Umsetzung. Sie gilt 1:1 in allen EU-Mitgliedstaaten. Im Gegensatz dazu geben Richtlinien der EU einen Rechtsrahmen als Mindeststandard vor, der erst in nationale Gesetze gegossen werden muss, bevor er in Kraft treten kann.

Über die gesetzlichen Normen hinaus stellt der Europäische Datenschutzausschuss (EDSA) ein Gremium dar, über den sich die Aufsichtsbehörden (in Österreich die Datenschutzbehörde) der Mitgliedstaaten abstimmen und Orientierungshilfen sowie Leitlinien und Vorlagen zu gewissen Instrumenten der DSGVO erlassen.

Und schließlich ist auch immer mit dem Europäischen Gerichtshof (EuGH) zu rechnen, der in der Vergangenheit mit seinen Entscheidungen das europäische Datenschutzrecht maßgeblich mitgeprägt hat.

An all den neuen Gesetzen und zahlreichen Stellen, die in die Gesetzgebung eingebunden sind, ist klar zu erkennen, dass Datenschutz und Datensicherheit zu einem zentralen Anliegen der EU geworden ist.

Entbürokratisierung

Eine der grundlegenden Intentionen des europäischen Gesetzgebers für das Schaffen der neuen, strengen Datenschutzregeln war die Entbürokratisierung. Gerade jenen, die sich bereits intensiv mit dem Umsetzen in die Praxis beschäftigt haben, mag das vielleicht unglaubwürdig erscheinen. Aber auf Basis der Verordnung, die viel Ermessensspielraum bietet, können sich Unternehmer und Unternehmen jetzt ihren Datenschutz grundsätzlich eigenständig – ohne Datenschutzbehörden konsultieren zu müssen – organisieren. Das versteht die EU unter Entbürokratisierung.

Fallweise beklagen sich Unternehmer jetzt allerdings, dass die Last der Entscheidungen an sie delegiert wird und sich die EU damit elegant aus der Verantwortung verabschiedet. Entscheidungen im Rahmen des weiten Ermessensspielraumes der DSGVO zu treffen, kann nämlich heikel, um nicht zu sagen Existenz bedrohend, sein. Denn der Strafrahmen wurde um den Faktor 800 (!) erhöht.

Erwägungsgrund 13 der Datenschutz-Grundverordnung besagt zwar, dass der „*besonderen Situation der Kleinstunternehmen sowie der*

Ist ab 25. Mai 2018 wirklich alles neu?

Nein, ganz und gar nicht. Viele Datenschutzvorschriften über die jetzt diskutiert und fallweise seitens Unternehmern gejammert wird, sind nicht neu. Vieles galt auch schon vor dem 25. Mai 2018. Bereits die aus dem Jahr 1995 stammende Datenschutz-Richtlinie 95/46/EG und das darauf beruhende Datenschutzgesetz 2000 (DSG 2000) enthalten viele Regeln, die sich auch in der Datenschutz-Grundverordnung wiederfinden.

So sind beispielsweise schon im DSG 2000 „Datensicherheitsmaßnahmen" ebenso zu finden wie das spezielle Handhaben von sensiblen („besonders schutzwürdigen") Daten. Auch das Auskunftsrecht, das Recht auf Richtigstellung oder Löschung sowie das Widerspruchsrecht kennt bereits das seit dem Jahr 2000 geltende Datenschutz-Gesetz.

Wer zum Beispiel über eine so genannte DVR-Nummer verfügt – sich also in das Datenverarbeitungsregister (DVR) eingetragen hat – der sollte bereits über ein Verzeichnis seiner Verarbeitungstätigkeiten verfügen. Ein solches Verzeichnis war nämlich die Grundlage für den Erhalt einer DVR-Nummer.

Aus der Praxis für die Praxis

Die alten DVR-Nummern sind mit dem Anwenden der Datenschutz-Grundverordnung gegenstandlos geworden. Es ist nicht mehr notwendig diese zum Beispiel in Ihren Geschäftsdokumenten anzuführen.

Früher: „zahnlose“ Behörde & geringe Strafen

Die Vermutung liegt nahe, dass sich die Mehrzahl der Unternehmer und Unternehmen um das Umsetzen der Datenschutzvorschriften nicht gekümmert haben, weil bei Verstößen kaum mit Strafen zu rechnen war.

Bis 24. Mai 2018 war die Datenschutzbehörde – salopp formuliert – eher eine zahnlose Organisation mit eingeschränkten Befugnissen. Auch der Strafrahmen war mit maximal 25.000 Euro wohl zu gering, um Unternehmer und Unternehmen zum Umsetzen der aufwendigen Datenschutzvorschriften zu motivieren. Die eher unwahrscheinlichen und vergleichsweise geringen Strafen sprachen gegen den zeitlichen und finanziellen Aufwand für die Umsetzung.

Daher haben viele Unternehmer erst im Vorfeld der Anwendung der DSGVO mit dem Umsetzen begonnen.

Heute: „gnadenlose“ Behörde & enorme Strafen

Seit 25. Mai 2018 verfügen betroffene Personen, deren personenbezogene Daten verarbeitet werden, per Gesetz über noch umfassendere Rechte. Zum Beispiel das Recht auf Datenübertragbarkeit. Ebenso wurden die Informationspflichten gegenüber Betroffenen ausgeweitet.

Die Österreichische Datenschutzbehörde, die ihren Sitz in der Wickenburggasse 8 im 8. Wiener Gemeindebezirk hat, wurde deutlich aufgewertet. Sie ist jetzt eine unabhängige, weisungsfreie Aufsichtsbehörde, deren Aufgaben und Befugnisse erheblich erweitert wurden. Zu den Befugnissen der Datenschutzbehörde zählen:

- Untersuchungsbefugnisse einschließlich des Betretungsrechts bestimmter Räumlichkeiten, die Datenschutzbehörde kann

Anwendungsbereich der DSGVO

Die Datenschutz-Grundverordnung unterscheidet zwischen sachlichem (Artikel 2 DSGVO) und räumlichem Anwendungsbereich (Artikel 3 DSGVO).

Sachlicher Anwendungsbereich

Als sachlichen Anwendungsbereich definiert die Verordnung die „*ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten*" sowie das manuelle Verarbeiten von personenbezogenen Daten, wenn sie „*in einem Dateisystem gespeichert sind oder gespeichert werden sollen.*"

In typischem Juristendeutsch legt die DSGVO also fest, dass sowohl Daten, die elektronisch verarbeitet werden, als auch Daten auf Papier unter die Bestimmungen fallen, wenn sie in einem Datensystem aufbewahrt werden. Für Ihre alphabetisch geordneten Kundenakten in Aktenordnern gelten also dieselben Vorschriften wie für Kundendaten, die Sie auf Ihrer Festplatte elektronisch speichern.

Erwägungsgrund 27 hält darüber hinaus fest, dass die Verordnung nicht für die personenbezogenen Daten Verstorbener gelten soll.

Räumlicher Anwendungsbereich

Als räumlichen Anwendungsbereich definiert die DSGVO – vereinfacht gesagt – jedes Verarbeiten von personenbezogenen Daten durch Unternehmer (natürliche Personen) und Unternehmen (juristische Personen) mit Sitz in der Europäischen Union sowie das Verarbeiten der Daten all jener Personen, die sich in der EU befinden,

unabhängig davon, ob die Verarbeitung innerhalb oder außerhalb der Europäischen Union stattfindet.

Für Nicht-Juristen mag das jetzt spitzfindig und überdefiniert klingen, aber in der Praxis bedeutet es folgendes:

- Alle in der EU ansässigen und tätigen Unternehmer und Unternehmen sind vom räumlichen Anwendungsbereich umfasst.
- Auch nicht in der EU ansässige Unternehmen müssen die Vorschriften der DSGVO berücksichtigen, wenn sie ihre Waren oder Dienstleistungen in der EU ansässigen Personen anbieten (und daher deren Daten – gegebenenfalls nicht einmal in der EU – verarbeiten).

Der zweite Teil des räumlichen Anwendungsbereiches führt dazu, dass sich zum Beispiel auch Konzerne wie Alphabet (Mutterkonzern von Google), Facebook (und damit auch Instagram und WhatsApp) sowie Amazon mit den europäischen Vorschriften zum Datenschutz intensiv auseinandersetzen müssen. Selbst wenn diese Dienstleister ihre europäischen Standorte aufgeben würden, bieten sie ihre Dienstleistungen weiterhin EU-Bürgern an, verarbeiten dabei deren Daten und müssen die Pflichten der DSGVO berücksichtigen.

EU-US Datenschutzschild

Das so genannte EU-US Datenschutzschild, im Original *EU-US Privacy Shield* genannt, wird immer dann zum Thema, wenn Daten in die Vereinigten Staaten von Amerika (USA) übermittelt werden.

Das EU-US Datenschutzschild ist die Nachfolgeregelung der Safe-Harbor-Entscheidung, welche der Europäische Gerichtshof am 6. Oktober 2015 für ungültig erklärt hat, weil persönliche Daten europäischer Internetnutzer in den USA nicht ausreichend vor dem Zugriff der Behörden geschützt sind.

Wichtige Begriffe

Zum besseren Verständnis der nunmehr geltenden Datenschutzvorschriften ist es wichtig, dass Ihnen die wesentlichen Begriffe und Definitionen geläufig sind. Für das Umsetzen der Vorschriften in die Praxis sind die Grundbegriffe unverzichtbar.

Personenbezogene Daten

(Artikel 4 Ziffer 1 DSGVO)

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen. Als identifizierbar wird eine natürliche (geborene und lebende) Person angesehen, die direkt oder indirekt identifiziert werden kann. Das kann mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten oder zu einer Online-Kennung (zum Beispiel IP-Adresse) möglich sein.

Personenbezogene Daten sind also unter anderem (wenn Sie sich auf eine natürliche Person beziehen):

- Name und Post- beziehungsweise Wohnadresse
- Telefonnummer und E-Mail-Adresse
- Sozialversicherungsnummer
- Ausweisnummer
- Gesichtsbild
- IP-Adresse
- Polizzennummer einer Versicherung
- Steuernummer beim Finanzamt
- Konto- und Depotnummer sowie IBAN

- KFZ-Kennzeichen
- IMEI Seriennummer eines Smartphones
- UID Nummern (wenn der Firmenwortlaut auf eine natürliche Person lautet – wie zum Beispiel im Falle der Autoren)
- Reservierungsnummer für eine Hotel-Buchung

Auch anhand von besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind, kann eine betroffene Person identifiziert werden. Diese zuletzt genannten personenbezogenen Daten fallen in die Kategorie der „besonderen" Daten, die besonderen Schutz genießen und deren Verarbeitung zusätzliche Pflichten mit sich bringt.

Aus der Praxis für die Praxis

Es spielt keine Rolle, ob Sie als Verantwortlicher eine betroffene Person anhand ihrer personenbezogenen Daten selbst (direkt) identifizieren können. Auch wenn Sie selbst auf Basis der Ihnen bekannten Daten die betroffene Person nicht identifizieren können – sondern zum Beispiel nur ein externer Dritter oder eine Behörde – gelten Betroffene anhand dieser Daten als indirekt identifizierbar und die personenbezogenen Daten müssen von Ihnen entsprechend geschützt werden!

Sie müssen sich also nicht nur fragen, ob Sie selbst die betroffene Person eindeutig identifizieren können, sondern ob irgendjemand in der Lage ist den Betroffenen eindeutig zu identifizieren.

Grundprinzipien der DSGVO

Grundsätzlich verlangt die Datenschutz-Grundverordnung in Artikel 5, dass personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben sowie in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

Rechtmäßigkeit

Das Verarbeiten von personenbezogenen Daten natürlicher Personen ist grundsätzlich verboten, außer der Verantwortliche kann sich auf eine gültige Rechtsgrundlage berufen. Bereits das abgelöste Datenschutzgesetz 2000 hatte dieses so genannte „Verbot mit Erlaubnisvorbehalt" zum Inhalt.

Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren (transparenten) Weise verarbeitet werden. Das Verarbeiten der Daten muss rechtmäßig sein, das heißt es muss mindestens eine der Rechtsgrundlagen gemäß Artikel 6 oder Artikel 9 (besondere Datenkategorien) oder Artikel 10 (strafrechtlich relevante Daten) DSGVO gegeben sein. Diese sind zum Beispiel:

- **Vertragserfüllung und vorvertragliche Maßnahmen**:

  Ein Vertrag, der zwischen den Parteien abgeschlossen ist beziehungsweise dessen Anbahnung (mit Kunden, Lieferanten, Beschäftigten, Bewerbern).

- **Gesetzliche Grundlage**:

  Eine rechtliche (gesetzliche) Verpflichtung des Verantwortlichen, zum Beispiel steuerliche Aufbewahrungspflichten gemäß Bundesabgabenordnung (BAO) und gesetzlich vorgesehene Dokumentations- oder Meldepflichten.

- **Berechtigtes Interesse**:

  Ein berechtigtes Interesse an der Verarbeitung, zum Beispiel Postversand von Informationen an bestehende Kunden.

- **Einwilligung/Zustimmung**:

  Die freiwillige, informierte, jederzeit widerrufliche Einwilligung zum Beispiel in Zusammenhang mit dem Versand von E-Mail Newslettern an Kunden und Interessenten.

- **Lebenswichtiges Interesse** der betroffenen Person, zum Beispiel im Zusammenhang mit medizinischen Notfällen.
- **Öffentliches Interesse** beziehungsweise die Ausübung öffentlicher Gewalt.

In Ihrem beruflichen Alltag als Unternehmer werden die ersten vier der genannten Rechtsgrundlagen die zentrale Rolle spielen. Und zwar in der angeführten Reihenfolge, denn widerrufliche Einwilligungen sollten nur das letzte Instrument für das Rechtfertigen der Datenverarbeitung sein.

Während den drei Rechtsgrundlagen Vertragserfüllung, gesetzliche Grundlagen und Einwilligung klare Fakten zu Grunde liegen (Vertrag, Gesetz, Einwilligungserklärung), lässt die Rechtsgrundlage berechtigtes Interesse sehr viel Interpretationsspielraum zu.

Erwägungsgrund 47 der DSGVO sieht berechtigtes Interesse einer Verantwortlichen jedenfalls nur dann als Grundlage rechtmäßiger Datenverarbeitung an, wenn die Interessen oder Grundrechte der betroffenen Person nicht überwiegen. Bei der Abwägung, ob berechtigtes Interesse vorliegen kann, sind die „*vernünftigen Erwartungen der betroffenen Personen*“ bezüglich ihrer Beziehung zum Verantwortlichen zu berücksichtigen. Auf jeden Fall sollte das Bestehen eines berechtigten Interesses besonders sorgfältig erwogen werden.

Berechtigtes Interesse könnte beispielsweise vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht. Erwägungsgrund 47 nennt in diesem Zusammenhang als Beispiel, wenn die betroffene

Rechte betroffener Personen

Die Datenschutz-Grundverordnung räumt betroffenen Personen, deren Daten Sie als Verantwortlicher verarbeiten, eine Vielzahl von Rechten ein, die volle acht Artikel umfassen. Sie werden beim Lesen erkennen, dass das Wahren beziehungsweise Erfüllen der Betroffenenrechte alles andere als eine einfache und unkomplizierte Aufgabe ist. Insbesondere dann, wenn zeitgleich mehrere betroffene Personen auf ihre Rechte pochen.

Aus der Praxis für die Praxis

Bereiten Sie sich schon beim Umsetzen der Datenschutzvorschriften auf das Wahren der Rechte von betroffenen Personen vor. Das Beauskunften, das Klären der Rechtmäßigkeit von Löschbegehren, usw. kann – insbesondere bei größeren Unternehmen und Organisationsstrukturen – sehr viel Zeit in Anspruch nehmen. Trotzdem soll natürlich der normale Geschäftsbetrieb nicht darunter leiden.

In unserer Praxis bewährt haben sich detaillierte Checklisten und vorformulierte Antwortschreiben, mit Hilfe derer sich sämtliche Anfragen hinsichtlich Betroffenenrechte vergleichsweise zügig abarbeiten lassen.

Recht auf Auskunft

(Artikel 15 DSGVO)

Jede natürliche Person hat das Recht, vom Verantwortlichen Auskunft zu erhalten, ob sie betreffende personenbezogenen Daten verarbeitet werden. Wenn das der Fall ist, dann hat die betroffene Person das Recht auf Auskunft über diese personenbezogenen Daten sowie auf folgende Informationen:

- die Verarbeitungszwecke,
- die Kategorien personenbezogener Daten, welche verarbeitet werden,
- die Empfänger oder Kategorien von Empfängern, gegenüber denen der Verantwortliche die personenbezogenen Daten offengelegt hat oder noch offenlegen wird, insbesondere bei Empfängern in Drittländern (nicht EU und EWR),
- die geplante Dauer, für die die personenbezogenen Daten gespeichert werden,
- das Bestehen des Rechts auf Berichtigung, Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung (im Rahmen der Beantwortung eines Auskunftsersuchens müssen Sie dem Antragsteller auch seine darüber hinaus bestehenden Rechte mitteilen),
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde,
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten,
- ob eine automatisierte Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 DSGVO durchgeführt wird sowie – in den betreffenden Fällen – aussagekräftige Informationen

Was ist in der Praxis konkret zu tun?

Einer der Beweggründe der Europäischen Union für die Datenschutz-Grundverordnung war beziehungsweise ist die Entbürokratisierung. Denn Unternehmen können sich jetzt auf Basis der neuen Vorschriften den Schutz personenbezogener Daten weitgehend selbst organisieren. In diesem Sinne bietet die DSGVO sehr viel Ermessensspielraum und reichlich Platz für Interpretationen. Beinahe unzählbar oft spricht die Datenschutz-Grundverordnung von „angemessenen" und „geeigneten" Maßnahmen.

Die Folge davon ist allerdings, dass sich zahlreiche Detailfragen aus den Vorschriften heraus nicht beantworten lassen. Es liegt damit im Ermessen des einzelnen Unternehmers und Verantwortlichen für seinen individuellen Tätigkeitsbereich die richtigen Schlüsse aus den Vorschriften zu ziehen und gut zu begründen. Ob einzelne Auslegungen dann tatsächlich die Zustimmung der Datenschutzbehörde finden, wird erst die gelebte – sowie geprüfte und gegebenenfalls ausjudizierte – Praxis zeigen.

Erstellen eines Verarbeitungsverzeichnisses

(Artikel 30 DSGVO)

Als Verantwortlicher für die von Ihnen verarbeiteten Daten sind Sie verpflichtet, so ein Verzeichnis zu erstellen. Der Inhalt umfasst mindestens:

- Name und Kontaktdaten des Verantwortlichen
- Gegebenenfalls Name und Kontaktdaten des benannten Datenschutzbeauftragten
- Zweck der Verarbeitungen
- Kategorien der betroffenen Personen

- Kategorien der personenbezogenen Daten
- Kategorien von (internen und externen) Empfängern, insbesondere in Drittländer außerhalb der EU beziehungsweise des EWR
- Fristen für das Aufbewahren und Löschen
- technische & organisatorische Maßnahmen zur Sicherheit der Verarbeitung und der personenbezogenen Daten.

Ausgangspunkt für dieses Verzeichnis von Verarbeitungstätigkeiten kann – falls Sie in der Vergangenheit eine DVR-Nummer hatten und alle damit verbundenen Pflichten erfüllt haben – die Meldung beim Datenverarbeitungsregister sein.

Wenn Sie mit dem Verarbeitungsverzeichnis hingegen bei null beginnen, dann nehmen Sie sich ausreichend Zeit dafür. Erstens werden Sie wahrscheinlich feststellen wie lange und eventuell auch komplex der Weg ist, den personenbezogene Daten heutzutage im Geschäftsalltag nehmen. Zweitens, weil das Verzeichnis der Verarbeitungstätigkeiten DAS zentrale Dokument ist, auf das Sie immer wieder zurückgreifen werden (müssen).

Aus der Praxis für die Praxis

Das Verzeichnis der Verarbeitungstätigkeiten ist kein starres Dokument, das lediglich einmal zu erstellen ist. Es muss im Zeitverlauf stets aktuell sein. Das Anpassen an aktuelle Gegebenheiten, das Aufnehmen neuer Verarbeitungstätigkeiten (und damit gegebenenfalls auch das Verarbeiten neuer Datenkategorien), die Zusammenarbeit mit neuen oder anderen Auftragsverarbeitern, neue Ziel- oder Kundengruppen, usw. erfordern das laufende Anpassen des Verwendungsverzeichnisses.

Je besser und durchdachter Ihr Verarbeitungsverzeichnis ist, desto einfacher wird es unter anderem die Rechte von betroffenen

Strafbestimmungen

Die vorgesehenen Geldbußen, welche in Artikel 83 DSGVO sowie den Paragrafen 62 und 63 DSG zu finden sind, stiegen erheblich, und zwar von bis zu 25.000 Euro (DSG 2000 bis 24. Mai 2018) auf bis zu 20.000.000 Euro oder 4 Prozent des weltweiten Konzern- beziehungsweise Gesamtumsatzes (es zählt jene Grenze, die höher ist). Geldbußen sollen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein. Wurde ein strafbarer Tatbestand vor der Geltung der Datenschutz-Grundverordnung verwirklicht, ist der Verstoß nach jener Rechtslage zu beurteilen, die für den Täter in ihrer Gesamtauswirkung günstiger ist.

Die DSGVO bietet der Datenschutzbehörde auch die Möglichkeit, Verantwortliche und Auftragsverarbeiter mittels Abhilfebefugnissen gemäß Artikel 58 Absatz 2 der DSGVO zur Einhaltung ihrer Pflichten nach der Datenschutz-Grundverordnung zu verhalten.

Im Datenschutz-Deregulierungsgesetz ist vorgesehen, dass die Datenschutzbehörde bei erstmaligen Verstößen auch verwarnen statt strafen kann. Allerdings ist davon auszugehen, dass die Behörde von der Möglichkeit der Verwarnung nur dann Gebrauch machen wird, wenn nachgewiesen werden kann, dass die Vorschriften der DSGVO grundsätzlich umgesetzt wurden. Müssen Sie der Behörde sagen, dass Sie noch keinen Gedanken an die DSGVO verschwendet haben, wird die Behörde wohl eine Geldbuße verhängen (müssen).

Geldbußen gemäß DSGVO

Bei der Verhängung einer Geldbuße - zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 DSGVO - und der Ent-