WHITEPAPER

Datenschutz-Grundverordnung: Die neuen Regelungen sicher anwenden

10 Punkte, die Sie als Unternehmer wissen müssen

LEXWARE

WHITEPAPER

Datenschutz-Grundverordnung: Die neuen Regelungen sicher anwenden

10 Punkte, die Sie als Unternehmer wissen müssen

Inhaltsverzeichnis

Einleitung

Wenn Sie der Meinung sind, dass Datenschutz-Verstöße reine Kavaliersdelikte sind, müssen Sie sich ab dem 25. Mai 2018 komplett umstellen. Denn ab diesem Stichtag ist die Datenschutz-Grundverordnung (DGSVO) der Europäischen Union anzuwenden. Bei Verstößen gegen die Datenschutz-Grundverordnung sind dann Geldbußen bis zu einer Höhe von 4 % des Umsatzes (oder maximal 20 Mio. Euro) möglich.

Dass auch Kleinunternehmern derart hohe Geldbußen drohen, ist unwahrscheinlich. Allerdings werden auch für sie die Strafen deutlich höher ausfallen als bisher. Hinzu kommt, dass das Thema Datenschutz durch die umfassende Berichterstattung in den Fokus der Öffentlichkeit gerückt ist. Dadurch werden mit Sicherheit die Anfragen Ihrer Kunden zunehmen, die wissen möchten, was denn mit ihren Daten geschieht. Und auch die Abmahnanwälte stehen schon in den Startlöchern.

Doch wer sich richtig auf die DSGVO vorbereitet, muss sich davor nicht fürchten. Schauen Sie sich einfach unsere wichtigsten Fragen und Antworten zum Datenschutz an. Wir haben für Sie zusammengefasst, worauf Sie als Unternehmer achten müssen, um sicher durch die neue Gesetzeslage zu manövrieren.

Als Unternehmer haben Sie tagtäglich mit unterschiedlichsten Daten zu tun: Kunden-, Mitarbeiter- oder Dienstleister-Daten. Daher besteht ein grundsätzliches Risiko, dass Datenschutz-Verstöße passieren. Neben einer soliden Absicherung in technischen Belangen sollten Sie auch Ihre Mitarbeiter gut einweisen. Denn als Chef tragen Sie die Gesamt-Verantwortung für gesetzeskonforme Abläufe im Unternehmen.

Damit Sie bei der Anwendung der DSGVO den typischen Stolperfallen möglichst aus dem Weg gehen, verschaffen Sie sich am besten einen guten Überblick, von welchen Regelungen der DSGVO Ihr Unternehmen betroffen ist. Dabei können Ihnen diese 10 wichtigen Informationen helfen, die wir zum Thema Datenschutz für Sie zusammengetragen haben.

1. Das umfasst der Begriff „personenbezogene Daten“

Der Begriff **personenbezogene Daten** bezeichnet Angaben über persönliche oder sachliche Verhältnisse einer natürlichen Person: Name, Adresse, Alter, Beruf, Staatsangehörigkeit, Religionszugehörigkeit, sexuelle Orientierung, Gesundheitszustand, Vermögensstand etc. Die DSGVO sieht vor, dass diese sensiblen Daten in möglichst geringen Mengen erhoben und verarbeitet werden. Das ist das Prinzip der Datenminimierung. Außerdem soll mit personenbezogenen Daten generell unter der Maßgabe von Rechtmäßigkeit, Treu und Glauben sowie Transparenz umgegangen werden.

WICHTIG:

Falls Ihr Unternehmen seinen Hauptsitz im EU-Ausland hat, bedeutet das nicht automatisch, dass die DSGVO nicht anzuwenden ist. Denn die DSGVO funktioniert nach dem Marktortprinzip. Das heißt, dass jedes Unternehmen sie anwenden muss, das Produkte oder Leistungen innerhalb der EU anbietet. (Aus diesem Grund müssen sich auch z.B. Facebook oder Google mit der Umstellung beschäftigen.)

2. Diese Rechte haben Personen in Bezug auf ihre Daten

Die DSGVO räumt natürlichen Personen bestimmte Rechte an ihren personenbezogenen Daten ein. Unternehmen müssen diese Rechte unbedingt beachten:

- Jede Person muss der Speicherung und Verarbeitung seiner Daten aktiv zustimmen. Hierbei reicht ein „stillschweigendes Einverständnis“ nicht mehr aus – z. B. durch das Akzeptieren Ihrer Datenschutzerklärung.
- Ihr Unternehmen hat bei einer entsprechenden Anfrage die Pflicht, einer Person bestimmte Auskünfte zu den Daten zu erteilen, die Sie von ihr gespeichert haben. Die Person darf Auskünfte zu den Daten selbst (welche Daten haben Sie?), zur Quelle (wie kamen Sie an die Daten?), zum Zweck (wozu speichern Sie die Daten?) und ggf. zum Empfänger (an wen geben Sie die Daten?) einfordern. **Wichtig dabei:** Ihre Antwort muss innerhalb eines Monats nach Eingang der Frage erfolgen!
- Wenn die personenbezogenen Daten, die Sie von der Person erhoben haben, fehlerhaft sind, kann die Person verlangen, dass die Daten berichtigt werden. In dem Fall müssen Sie die Daten unbedingt korrigieren.
- Wenn Sie die Daten unzulässigerweise gespeichert haben oder wenn Sie die Daten nicht mehr für den eigentlichen Zweck benötigen, für den Sie sie erhoben haben, sind Sie zum Löschen der Daten verpflichtet. Dies gilt auch, wenn die Person, von der Sie die Daten erhoben haben, ihre Einwilligung zur Datenspeicherung widerruft. Stehen einer Löschung die gesetzlichen Aufbewahrungspflichten entgegen, dann müssen Sie die Daten sperren. Das ist z. B. bei Rechnungen der Fall. Haben Sie die Daten an Dritte weitergegeben, ist es zudem wichtig, dass Sie diese über die Löschung informieren.

3. Richtig auf Datenschutz-Verletzungen reagieren

Selbstverständlich sollte es im Unternehmen am besten gar nicht erst zu Datenschutzverletzungen kommen. Realistischerweise können aber natürlich Fehler passieren (man denke z. B. an IT-Ausfälle). Daher sieht die DSGVO bestimmte Verhaltensweisen im Notfall vor: Stellen Sie fest, dass in Ihrem Unternehmen der Schutz von personenbezogenen Daten verletzt wurde, müssen Sie unverzüglich (innerhalb von 72 Stunden) die zuständige Aufsichtsbehörde informieren. Wenn Sie definitiv ausschließen können, dass die Rechte der betroffenen Personen verletzt wurden, können Sie auf die Meldung verzichten.

Auch die Betroffenen müssen unter Umständen über die Datenpanne informiert werden – und zwar immer dann, wenn „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten“ des Betroffenen besteht. Die Benachrichtigung muss dabei „in klarer und einfacher Sprache“ erfolgen. Wenn durch technische und organisatorische Maßnahmen, die vor der Datenpanne getroffen wurden, ausgeschlossen werden kann, dass Dritte die Daten einsehen können, müssen die Betroffenen nicht benachrichtigt werden. Das kann z. B. dann der Fall sein, wenn zwar ein USB-Stick oder eine CD mit Daten verloren wurde, die Daten aber so verschlüsselt sind, dass sie nicht ausgelesen werden können.

4. Diese Konsequenzen können auf einen Verstoß folgen

Gemäß DGSVO können Verstöße gegen den Datenschutz hart geahndet werden. Bußgeldzahlungen können bis zu 4 % des Umsatzes bzw. bis zu 20 Mio. Euro betragen. Damit gehen Datenschutz-Verstöße keinesfalls mehr als Kavaliersdelikt durch! Die genaue Höhe einer möglichen Geldstrafe hängt von verschiedenen Faktoren ab:

- in welcher Form, wie lange und wie schwer wurde gegen die DSGVO verstoßen. Dabei sind auch Art, Umfang und Zweck der Datenverarbeitung sowie die Zahl der betroffenen Personen und das Ausmaß des entstandenen Schadens einzubeziehen;
- wurde der Verstoß vorsätzlich oder fahrlässig herbeigeführt;
- welche Maßnahmen hat das Unternehmen getroffen, um den Schaden zu begrenzen;
- lag der Fehler wirklich beim Verantwortlichen bzw. dem Auftragsverarbeiter;
- welche technischen und organisatorischen Maßnahmen wurden getroffen, um den Fehler zu verhindern;
- wie hoch ist die Bereitschaft zur Zusammenarbeit mit der Aufsichtsbehörde, um Schadensbegrenzung zu betreiben;
- welche personenbezogenen Daten sind von dem Verstoß betroffen;
- in welcher Art und Weise wurde der Verstoß der Aufsichtsbehörde gemeldet (durch das Unternehmen selbst oder eine dritte Partei?);
- alle anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

In Anbetracht der möglicherweise hohen Summe des Bußgeldes raten wir jedem Kleinunternehmer dringend, vorbeugende Maßnahmen zu ergreifen, damit es idealerweise zu keinem wirtschaftlichen Schaden durch Datenschutz-Verstöße kommt. Neben der nachhaltigen Unterweisung der Mitarbeiter sollten Sie zudem unbedingt darauf achten, nur Softwarelösungen einzusetzen, die die DSGVO-Standards unterstützen.

5. Wer trägt die Verantwortung für den Datenschutz im Unternehmen?

Wer genau die Verantwortung für den Datenschutz trägt, hängt mitunter auch von Struktur und Größe des Unternehmens ab:

- Der **Geschäftsführer** trägt die Gesamtverantwortung für das Unternehmen – und damit auch für den Datenschutz. Er muss die passenden Rahmenbedingungen schaffen, in denen ein ausreichender Datenschutz möglich ist (z.B. technische Systeme).
- Bestimmte Unternehmen sind dazu verpflichtet, einen **Datenschutzbeauftragten** zu bestellen. Das trifft zu, wenn mindestens zehn Mitarbeiter permanent mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, was bei Kleinunternehmen wohl eher selten der Fall sein wird. Wenn Ihr Unternehmen keinen Datenschutzbeauftragten benötigt, stehen Sie als Geschäftsführer wiederum in der Haftung. Falls Ihr Unternehmen aber doch einen Datenschutzbeauftragten haben muss, drohen Ihnen Bußgelder von bis zu 50.000 Euro, wenn Sie versäumen, ihn einzuberufen. Sie können für diese Rolle auch auf Externe zurückgreifen.
- Wenn Sie **Mitarbeiter** haben, gilt natürlich, dass in gewisser Weise jeder Einzelne für den gesetzeskonformen Umgang mit Daten verantwortlich ist. Daher ist eine klare Einweisung der Mitarbeiter unbedingt notwendig. Hier bieten sich ebenfalls entsprechende Schulungen an. Verpflichten Sie Ihre Mitarbeiter bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

6. Maßnahmen zum Schutz personenbezogener Daten

Die DSGVO und das Bundesdatenschutzgesetz (BDSG) schreiben vor, dass Unternehmen sowohl in organisatorischer als auch in technischer Hinsicht angemessene Maßnahmen ergreifen, um den Schutz von personenbezogenen Daten sicherzustellen. Doch was gilt als „angemessene“ Maßnahmen? Die „Angemessenheit“ wird vom Stand der Technik, den Implementierungskosten sowie der Art, dem Umfang, den Umständen und dem Zweck der Verarbeitung beeinflusst.

Folgende Maßnahmen können sich daraus ableiten lassen:

1. die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
2. die Fähigkeit, sowohl die Vertraulichkeit, Integrität, Verfügbarkeit als auch die Belastbarkeit der Systeme und Dienste sicherzustellen, die für die Datenverarbeitung eingesetzt werden;
3. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall schnell wiederherzustellen;
4. ein Verfahren zur regelmäßigen Überprüfung und Auswertung, wie wirksam die Maßnahmen sind, die Sie zum Schutz von personenbezogenen Daten ergriffen haben.

7. Schutz der Daten von Mitarbeitern und Bewerbern

Beschäftigen Sie Mitarbeiter in Ihrem Kleinunternehmen? Dann haben Sie sicherlich auch persönliche Daten Ihrer Mitarbeiter erfasst, die Sie beispielsweise für die Entgeltabrechnung benötigen. Dies ist auch künftig unproblematisch, denn personenbezogene Daten von Beschäftigten dürfen verarbeitet werden, sofern dies für Zwecke der Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses erforderlich ist. Dabei müssen Sie die gesetzlichen und arbeitsvertraglichen Regelungen beachten.

Daten von Mitarbeitern, die hiervon nicht abgedeckt sind, dürfen dagegen nur erhoben und verarbeitet werden, wenn der Beschäftigte sein Einverständnis zur Speicherung oder Verarbeitung seiner Daten ausdrücklich gestattet hat. Er muss seine Einwilligung freiwillig abgegeben haben – und zwar normalerweise schriftlich. Außerdem sollten Sie Ihren Mitarbeiter in Textform darüber unterrichten, für welchen Zweck Sie die Daten verarbeiten und dass Ihr Mitarbeiter ein Widerrufsrecht hat.

Meistens sind die wichtigsten Daten zu einem Mitarbeiter in der Personalakte enthalten. Daher sollten Sie die Akte unbedingt vertraulich führen und sicher aufbewahren. Schützen Sie die Akte vor dem Zugriff Dritter. Zudem muss die Personalakte auch vollständig und nachvollziehbar sein.

Was Sie für den Schutz der personenbezogenen Daten Ihrer Mitarbeiter tun sollten:

- Standard-Schutzvorkehrungen treffen, wie z. B. Datensicherung, Virenscanner und Firewall
- eine nachvollziehbare Dokumentation aller Vorgänge, Unterlagen, E-Mails etc. anfertigen
- Schutz der Datenträger vor dem Zugriff von Unbefugten gewährleisten, z. B. durch eigene Laufwerke oder besonders geschützte Verzeichnisse
- abgeschlossene Karteischränke aufstellen, die nur Sie oder (falls vorhanden) ein Personalverantwortlicher einsehen kann

Wenn sich Kandidaten bei Ihnen bewerben, unterliegen die Bewerber-Daten ebenso dem Datenschutz. Das trifft gleichermaßen zu, wenn es eine Bewerbung auf eine von Ihnen ausgeschriebene Stelle oder eine Initiativbewerbung ist. Idealerweise speichern und verarbeiten Sie nur diejenigen Daten, die für den Bewerbungsprozess relevant sind. Denn manchmal lassen Bewerber einem Unternehmen mehr als die unbedingt erforderlichen Daten zukommen (insbesondere bei Initiativbewerbungen). Bei öffentlich zugänglichen persönlichen Daten, die Sie z. B. auf Webseiten, Foren oder in sozialen Netzwerken finden (XING, LinkedIn, Facebook), sollten Sie vorsichtig sein. Aktuell ist strittig, ob Sie diese Daten aktiv in das Bewerbungsverfahren einbeziehen dürfen. Ist das Bewerbungsverfahren beendet, sind die Daten der abgelehnten Bewerber zu löschen. Name, Anschrift und Geburtsdatum dürfen Sie weiterhin speichern, weil diese Daten gegebenenfalls in einem weiteren Bewerbungsverfahren genutzt werden können.

PRAXIS-TIPP zur Aufbewahrung von Bewerberdaten:

Abgelehnte Bewerber haben bei einem Verstoß gegen das allgemeine Gleichbehandlungsgesetz (AGG) die Möglichkeit, innerhalb von zwei Monaten Klage einzureichen und Schadensersatz zu verlangen. Deshalb sollten Sie den Ablauf Ihres Bewerbungsverfahrens und den Grund jeder Absage sicherheitshalber dokumentieren. Dies berücksichtigt die DSGVO dahingehend, dass Sie die Daten abgelehnter Bewerber bis zu 6 Monaten aufbewahren dürfen. Allerdings sollten Sie die entsprechenden Unterlagen für diesen Zeitraum sperren. Möchten Sie die Daten eines Bewerbers länger aufbewahren, z. B. weil Sie ihn in einen Bewerberpool aufnehmen möchten, bedarf es einer schriftlichen Einwilligung des Bewerbers.

Daten aus der E-Mail- und Internet-Nutzung der Mitarbeiter

In den IT-Systemen eines Unternehmens gibt es in der Regel die technische Möglichkeit, die Daten aus der Internet- und E-Mail-Nutzung der Beschäftigten einzusehen. Beispielsweise könnten Sie Daten zur Benutzeridentifikation, IP-Adressen, Zugriffszeiten, Datenmengen und Zieladressen in Erfahrung bringen. Doch hierbei müssen Sie auf die Bestimmungen der DSGVO genau aufpassen! Denn Ihr Recht, die private Internet- und E-Mail-Nutzung Ihrer Mitarbeiter einzusehen, hängt u. a. davon ab, ob Sie Ihren Mitarbeitern eine private Internet- und E-Mail-Nutzung erlaubt haben.

Haben Sie Ihren Mitarbeiter keine private Nutzung von Internet- und E-Mail-Diensten gestattet, kann der Mitarbeiter die IT-Infrastruktur nur zu rein **dienstlichen Zwecken** nutzen. In diesem Fall besagen DSGVO und BDSG, dass das Recht des Mitarbeiters auf informationelle Selbstbestimmung gegen die Interessen des Unternehmens an der Datenverarbeitung abzuwägen ist.

Wenn Sie Ihren Mitarbeitern jedoch die die p**rivate Nutzung** von E-Mail und Internet erlauben, gilt das Fernmeldegeheimnis der Beschäftigten. In diesem Fall sind Ihre Zugriffsrechte stark eingeschränkt. Sie dürfen die Daten aus der Internet- und E-Mail-Nutzung nur in dem Umfang verarbeiten, wie es für das Betreiben und Abrechnen des Internet- und E-Mail-Diensts notwendig ist.

In rein dienstliche E-Mails Ihrer Mitarbeiter dürfen Sie als Unternehmer Einsicht nehmen. Private E-Mails dürfen (bei Erlaubnis der Privatnutzung) hingegen nur dann eingesehen werden, wenn ein Verdacht auf einen Straftatbestand besteht.

8. Schutz von Kundendaten

Als Kleinunternehmer haben Sie oft einen sehr engen Kontakt zu Ihren Kunden. Daher wissen Sie, wie unangenehm und geschäftsschädigend sich problematische Zwischenfälle auswirken können, wenn Ihre Kunden davon erfahren. Schon aus unternehmerischer Sicht sollten Sie deshalb unter allen Umständen vermeiden, dass es zu Datenschutzverletzungen kommt, die die personenbezogenen Daten Ihrer Kunden betreffen. Zudem können die vertraglichen Bestimmungen eventuell genaue Regelungen zum Kundendatenschutz enthalten. Kommt es in so einem Fall zu einer Datenschutzverletzung, müssen Sie sogar mit einer Vertragsstrafe rechnen.

Behandeln Sie die Kontaktdaten des Kunden (z. B. seine persönliche E-Mail-Adresse oder eine nicht veröffentlichte Telefonnummer) deshalb unbedingt vertraulich und bewahren Sie sie immer möglichst sicher auf. Bei mobilen Endgeräten bedeutet dies, dass die Daten nicht dauerhaft auf Smartphones etc. gespeichert sein sollten. Zudem sollte eine Datenverschlüsselung bei der Speicherung bzw. in Cloudspeichern verwendet werden. Sollte es doch einmal vorkommen, dass der Schutz der Kundendaten verletzt wird, gehen Sie wie in Punkt 3 beschrieben vor und informieren Sie ggf. Datenschutzbehörde sowie betroffene Kunden.

Worauf Sie unbedingt achten sollten: Nicht selten sind gefälschte oder präparierte E-Mails im Umlauf, die beim Öffnen eine Schadsoftware in Ihre IT-Struktur einschleusen. Solche E-Mails sehen häufig wie Rechnungen, Bewerbungen oder Auftragsbestätigungen aus und können nach Aktivierung die Daten aus Ihrem Netzwerk an Dritte übertragen oder Ihr IT-System lahmlegen. Daher ist es neben dem Einsatz aktueller Virensoftware enorm wichtig, dass sowohl Sie selbst als auch Ihre Mitarbeiter ausreichend für das Risiko sensibilisiert sind und wissen, wie man verdächtige E-Mails erkennt.

9. Verwendung von Daten für Marketing- und Werbe-Maßnahmen

Immer mehr Kleinunternehmer betreiben inzwischen ihre eigene Website, vielleicht sogar mit einem Newsletter oder einem Kunden-Login. Melden sich Kunden online an, erhalten Sie interessante personenbezogene Daten, die Sie sicherlich auch zu Werbezwecken gerne weiterverwenden möchten. Die DSGVO enthält jedoch sehr strikte Bestimmungen zur Verarbeitung dieser Daten. Ohne das Einverständnis des Interessenten oder Kunden dürfen Sie personenbezogene Daten für Werbezwecke nur unter folgenden Bedingungen nutzen:

- Die Daten sind in allgemein zugänglichen Verzeichnissen wie Adress-, Rufnummern-, Branchen- oder vergleichbaren Verzeichnissen (Listenprivileg) veröffentlicht.

Und:

- Die Daten enthalten lediglich folgende Informationen: Zugehörigkeit zu einer Gruppe (z. B. Hobbys, wie Mountainbikefahrer), Berufs-, Branchen- oder Geschäftsbezeichnung, Name, Titel, akademischen Grad, Anschrift und Geburtsjahr (nicht Geburtsdatum!).

Und:

- Sie nutzen die Daten nur für die Bewerbung eigener Angebote, für berufliche Werbung an die geschäftliche Adresse oder für Spendenwerbung.
- Sie haben die Daten rechtmäßig erhoben und die erstmalig erhebende Stelle geht eindeutig als Datenquelle aus der Werbung hervor. Die erforderlichen Daten sind Firma bzw. Name sowie die ladungsfähige Anschrift. Nennen Sie die Datenquelle im Fußbereich des Werbebriefs.
- Sie weisen explizit auf das Widerspruchsrecht zur Datennutzung zu Werbezwecken hin. Macht der Kunde oder Interessent von dem Widerspruchsrecht Gebrauch, müssen Sie Datenverarbeitung sofort unterlassen!

Wenn diese Bedingungen nicht erfüllt sind, benötigen Sie eine schriftliche Einwilligung des Kunden oder Interessenten, um seine Daten für Werbezwecke zu nutzen. Eine elektronisch übermittelte Einwilligung (z. B. auf einer Internetseite) müssen Sie unbedingt dokumentieren und Sie müssen dem Nutzer die Möglichkeit zu Einsicht und Widerruf geben.

Was Sie bei Internet- und Onlinediensten unbedingt beachten müssen:

- Wenn Sie über Ihren Webauftritt oder einen Onlinedienst (z. B. Webshop) Daten einsammeln, dürfen Sie diese nur soweit erheben, wie sie zur Erbringung Ihrer Leistung notwendig sind.
- Informieren Sie den Nutzer darüber, welche seiner Daten Sie speichern und verarbeiten.
- Bei der Erhebung von personenbezogenen Daten ist entweder eine gesetzliche Erlaubnis oder die persönliche Einwilligung des Nutzers erforderlich.
- Wenn Sie einen Newsletter anbieten oder einen integrierten Webshop haben, brauchen Sie eine Datenschutzerklärung, weil hierbei immer Daten elektronisch verarbeitet werden.
- Falls Sie Dienste Dritter in Anspruch nehmen (z.B. Google Analytics), müssen Sie den Nutzer darüber aufklären und sein Einverständnis einholen.

10. Lieferanten und Outsourcing: Der richtige Umgang mit Dienstleister-Daten

Viele Kleinunternehmer haben enge geschäftliche Beziehungen zu ihren Lieferanten oder Dienstleistern. Dabei kommt es nicht selten vor, dass Sie personenbezogene Daten Ihrer Lieferanten speichern: Geburtstag, Privatanschrift, persönliche E-Mail-Adresse oder Mobiltelefonnummer. Diese persönlichen Angaben unterliegen selbstverständlich dem Schutz der personenbezogenen Daten.

Wenn Ihr Dienstleister im Rahmen seiner Tätigkeit für Sie auf Ihre intern verarbeiteten Daten zugreifen muss, sollten Sie den Dienstleister auf ausreichenden Datenschutz prüfen. Zudem sind Sie nach den Regelungen der DSGVO dazu verpflichtet, einen Vertrag über Auftragsverarbeitung mit dem Dienstleister zu schließen, wenn dieser personenbezogene Daten für Sie verarbeitet. Dies kann z. B. bei Gehaltsabrechnungsbüros, Werbeagenturen, Web-Hostern, Anbietern von Cloud-Diensten oder auch freien Mitarbeitern der Fall sein.

TIPP zur Beauftragung von Datenspeicherung:

Nutzen Sie den Service von Anbietern zur Datenspeicherung, informieren Sie sich am besten vorab darüber, wo und wie der Anbieter die Daten verarbeitet und speichert. Hierbei müssen Sie beachten, dass die DSGVO die Datenübermittlung in ein Drittland nur dann erlaubt, wenn die weitere Verarbeitung der Daten nach den Vorgaben der DSGVO erfolgt und der Schutz der Daten gewährleistet ist.

Fazit: Seien Sie gut vorbereitet, um hohe Strafen zu vermeiden

Durch die DSGVO besteht für viele Unternehmer dringender Handlungsbedarf in Sachen Datenverarbeitung. Falls Sie sich noch nicht intensiv mit dem Thema Datenschutz befasst haben, sollten Sie dies spätestens jetzt dringend tun. Denn die Zeit bis zum Inkrafttreten der DSGVO wird immer knapper und bei einer Verletzung der neuen Regelungen drohen hohe Geldstrafen und Reputationsverluste. Daher sollten Sie unbedingt Vorkehrungen treffen, um einem solchen wirtschaftlichen Schaden vorzubeugen.

Die in diesem Whitepaper angeführten Punkte sollten Sie dabei unbedingt prüfen und angehen. Von besonderer Wichtigkeit sind in diesem Rahmen die Frage, wie die korrekte Datenverarbeitung in Ihrem Betrieb aus technischer Sicht zu lösen ist, und zum anderen der Aufbau von Datenschutzwissen bei Ihren Mitarbeitern.

Auch wenn Sie noch überhaupt keine Datenschutz-Maßnahmen eingeleitet haben, sollten Sie nicht verzweifeln und die Flinte ins Korn schmeißen. Es rentiert sich für Sie auch jetzt noch, damit anzufangen und Ihre Bemühungen zu dokumentieren. Denn wenn Sie der zuständigen Datenschutzbehörde nachweisen können, dass Sie entsprechende Maßnahmen zur Umsetzung der DSGVO eingeleitet haben, kann es sein, dass die Prüfer bei einer ersten Kontrolle vielleicht noch einmal ein Auge zudrücken. Haben Sie dagegen noch gar nichts getan, ist die Wahrscheinlichkeit eines Bußgeldes sehr hoch.