lexoffice
just smile

eBook DSGVO

Datenschutz-Grundverordnung: Die neuen Regelungen sicher anwenden

- Die 10 wichtigsten Punkte für Unternehmer
- Experteninterview mit RA Michael Rohrlich
- DSGVO 6-Punkte-Maßnahmenplan
- Fragen & Antworten zur DSGVO
- Tabelle Aufsichtsbehörden Datenschutz
- Muster & Vorlagen

LEXWARE

eBook DSGVO

Datenschutz-Grundverordnung: Die neuen Regelungen sicher anwenden

Inhaltsverzeichnis

Einleitung 2
1. Das umfasst der Begriff „personenbezogene Daten“ 3
2. Diese Rechte haben Personen in Bezug auf ihre Daten 3
3. Richtig auf Datenschutz-Verletzungen reagieren 4
4. Diese Konsequenzen können auf einen Verstoß folgen 4
5. Wer trägt die Verantwortung für den Datenschutz im Unternehmen? 5
6. Maßnahmen zum Schutz personenbezogener Daten 5
7. Schutz der Daten von Mitarbeitern und Bewerbern 5
8. Schutz von Kundendaten 7
9. Verwendung von Daten für Marketing- und Werbe-Maßnahmen 7
10. Lieferanten und Outsourcing: Der richtige Umgang mit Dienstleister-Daten 8
Fazit: Seien Sie gut vorbereitet, um hohe Strafen zu vermeiden 9
Experteninterview mit RA Michael Rohrlich 10
DSGVO 6-Punkte-Maßnahmenplan 14
Fragen & Antworten zur DSGVO 18
Tabelle Aufsichtsbehörden Datenschutz 25
Muster & Vorlagen 26

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.

10 Punkte, die Sie als Unternehmer wissen müssen

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.

Experteninterview mit Michael Rohrlich

Rechtsanwalt und TÜV Süd zertifizierter Datenschutzbeauftragter (DSB-TÜV)

Herr Rohrlich, die DSGVO bringt einige Neuerungen und Anforderungen mit sich, die auch kleine Unternehmen und Selbstständige betreffen. Was muss ein Betrieb konkret tun, damit er die DSGVO-Vorgaben umsetzt und Bußgelder vermeidet?

Es gibt verschiedene Maßnahmen, die zu treffen sind. Zunächst einmal sollte im Unternehmen der Ist-Zustand ermittelt werden. Es muss also überprüft werden, ob bereits einzelne Datenschutz-Maßnahmen – von denen es übrigens auch schon nach alter Rechtslage einige gab – im Unternehmen vorhanden sind. Dann muss dieser Ist-Zustand mit dem Soll-Zustand gemäß DSGVO verglichen werden, um erkennen zu können, was nun genau zu tun ist.

Alle Unternehmen mit mehr als 10 Mitarbeitern müssen einen Datenschutzbeauftragten bestellen. Auch kleinere Unternehmen können dazu verpflichtet sein. Das ist dann der Fall, wenn in einem gewissen Umfang besonders sensible Daten verarbeitet werden, wie etwa Gesundheitsdaten oder Informationen über die sexuelle Orientierung. Daher muss beispielsweise ein Zahnlabor mit nur 4 Mitarbeitern auch einen Datenschutzbeauftragten bestellen. Ein existierender Datenschutzbeauftragter muss spätestens ab dem 25.05.2018 der zuständigen Aufsichtsbehörde gemeldet werden.

Wichtig ist auch das Führen des sogenannten Verzeichnisses von Verarbeitungstätigkeiten. Dabei handelt es sich um das zentrale Dokument im Bereich Datenschutz, in dem alle Datenverarbeitungsvorgänge beschrieben und dokumentiert werden. Dieses Verzeichnis muss man der Aufsichtsbehörde auf Nachfrage vorlegen, um so seiner Nachweispflicht nachzukommen.

Dazu gehört auch die Beschreibung der vorhandenen technischen und organisatorischen Maßnahmen, mit denen man im Unternehmen den Datenschutz sicherstellt – z.B. die Zutrittskontrolle im Gebäude, die Sicherung des Serverraums, der Zugang zu Computern mit Kennung und Passwort, eine Firewall, eine Antiviren-Software, aktuelle Betriebssysteme und Anwendungssoftware etc.

Gilt das genauso für kleine Unternehmen oder müssen diese anders vorgehen? Was gilt für 1-Mann-Betriebe?

Die DSGVO gilt prinzipiell auch für kleine Unternehmen und sogar für Einzelunternehmer –unabhängig von Branche, Mitarbeiterzahl, Umsatz oder Organisationsform. Eine Ausnahme existiert nur für den rein privaten Bereich, z.B. die in Excel angelegte Geburtstagsliste von Freunden. Allerdings sieht die DSGVO an manchen Stellen Ausnahmeregelungen für Kleinunternehmen vor. Das gilt etwa für die Pflicht zum Führen des Verzeichnisses von Verarbeitungstätigkeiten. Diese gilt nicht für Unternehmen mit weniger als 250 Mitarbeitern. Allerdings gibt es von dieser Ausnahme auch Gegenausnahmen – z.B. dann, wenn aufgrund der Datenverarbeitung Risiken für die Betroffenen bestehen oder sensible Daten verarbeitet werden. Unter dem Strich lässt sich sagen, dass die eigentliche Ausnahme für Unternehmen mit weniger als 250 Mitarbeitern wohl eher selten greift, so dass im Grunde auch kleinere Unternehmen im Zweifel das Verzeichnis führen sollten.

Welche Bereiche im Unternehmen sind betroffen?

Datenschutz gilt online, aber natürlich auch offline. Daher sind alle Bereiche bzw. Arbeitsabläufe in Unternehmen betroffen, mit denen personenbezogene Daten verarbeitet werden. Nur reine Unternehmensdaten (Bilanz, Statistik etc.) sind ausgenommen. Unter „personenbezogenen Daten" versteht man alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Derjenige, dessen Daten verarbeitet werden, wird „Betroffener" genannt, das datenverarbeitende Unternehmen „Verantwortlicher".

Der Begriff der personenbezogenen Daten wird sehr weit verstanden. Dazu zählen also u.a.:

- persönliche Daten (Name, Anschrift, Geburtsdatum etc.)
- Kontaktdaten (Telefonnummer, Faxnummer, E-Mail-Adresse etc.)
- Finanzdaten (Bankverbindung, Gehaltsabrechnung etc.)
- Fotos mit erkennbar abgebildeten Personen
- Gesundheitsdaten (Krankmeldung, Diagnose, Überweisung etc.)
- Kfz-Kennzeichen
- IP-Adressen

Wenn man sich nicht sicher ist, ob es sich in einem bestimmten Fall um Daten mit Personenbezug handelt, sollte man im Zweifel davon ausgehen, dass dies der Fall ist. Denn es geht hierbei nicht nur um Daten von Kunden, sondern auch um solche von Mitarbeitern, Dienstleistern etc.

Der Begriff der Datenverarbeitung wird ebenfalls sehr weit ausgelegt. Darunter fallen nahezu alle Vorgänge in einem Unternehmen: von der Erhebung über das Organisieren, Speichern, Verknüpfen und Übermitteln bis hin zum Löschen bzw. Vernichten. Im Zweifel sollte man also auch hier davon ausgehen, dass eine bestimmte Tätigkeit unter den Begriff „Verarbeitung von Daten" fällt.

Typische Datenverarbeitungsvorgänge in Unternehmen sind etwa die Bearbeitung einer Bestellung, der Versand eines Newsletters, die Veranstaltung von Gewinnspielen, die Verwaltung von Mitarbeiterdaten oder auch die Verarbeitung von Daten in der Cloud (z.B. Dropbox, Microsoft Office 365 etc.). Ebenso stellen Finanzbuchhaltung, Urlaubsplanung, Reisekostenabrechnung oder Bewerbermanagement relevante Datenverarbeitungsvorgänge dar.

Müssen Unternehmen ihre bestehenden Datenschutzerklärungen erweitern? Wenn ja, wie bzw. um welche Punkte?

Wer eine nicht nur rein private Internetseite betreibt, muss neben einem Impressum auch eine Datenschutzerklärung bereitstellen. Dies war bislang schon so und wird sich auch unter der DSGVO nicht ändern. Allerdings müssen die Inhalte an die neue Rechtslage angepasst werden. Nach Maßgabe der DSGVO müssen Website-Besucher beispielsweise über Namen und Kontaktdaten des Unternehmens, einen eventuell vorhandenen Datenschutzbeauftragten, die Zwecke der Datenverarbeitung und deren Rechtsgrundlage, die Dauer der Datenspeicherung, die Betroffenenrechte (auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Datenportabilität) oder auch über das Beschwerderecht bei Aufsichtsbehörden informiert werden. Insbesondere müssen auf der Internetseite eingesetzte Technologien, wie z.B. Cookies, Analysesoftware, Werbung, Social Plugins, Kontaktformulare etc., im Rahmen der Datenschutzerklärung näher beleuchtet werden.

Was muss man konkret beachten, wenn man Werbung (Briefe/ E-Mailings) versenden möchte?

Bei dem Versand von Werbung ist zu unterscheiden, ob diese per Brief oder auf elektronischem Wege, also z.B. per E-Mail, verschickt wird. Beim postalischen Versand gilt das sogenannte Opt-Out-Prinzip. Das heißt: Es darf so lange Werbung verschickt werden, bis der Empfänger dem widerspricht. Beim elektronischen Versand ist es genau anders herum: Hier muss der Empfänger vorab ausdrücklich dem Erhalt von Werbe-E-Mails zustimmen, sonst darf kein Versand erfolgen. Da es diese Regelungen auch schon vor Inkrafttreten der DSGVO gab, wird sich in dieser Hinsicht nichts ändern.

Folgende Punkte sind beim E-Mail-Marketing zu beachten:

- Vollständige E-Mail-Signatur inkl. aller wichtigen Unternehmensangaben (vgl. Impressum)
- deutlicher Hinweis auf Werbung schon in der Betreffzeile
- keine unlauteren Inhalte (also korrekte Produktbeschreibungen, Preisangaben etc.)
- Beachtung der Datensparsamkeit (nur E-Mail-Adresse als Pflichtangabe erheben)
- Beachtung des Double-Opt-In-Prinzips (Versand erst nach Erhalt der Einwilligung und erfolgreicher Verifizierung der Mail-Adresse)

Wie hoch ist die Wahrscheinlichkeit, dass kleine Unternehmen wirklich kontrolliert werden?

Das ist schwer zu beantworten. Es ist so, dass wohl alle Datenschutzaufsichtsbehörden in Deutschland vermehrt Personal eingestellt haben, um ihren neuen Aufgaben nachkommen zu können. Aber sicherlich gibt es auch jetzt nicht so viele Mitarbeiter, dass alle Unternehmen aktiv kontrolliert werden können. Vermutlich werden zunächst einmal – wenn überhaupt – eher größere Unternehmen Ziel der Aufsichtsbehörden sein.

Aber sicherlich werden auch bei mittleren und kleineren Unternehmen stichprobenartige Kontrollen durchgeführt werden. Zudem lässt sich manches auch automatisiert erledigen, wie etwa die Überprüfung der Online-Datenschutzerklärung oder die Pflicht zur Meldung eines Datenschutzbeauftragten. Es kann auch sein, dass die Aufsichtsbehörden die Unternehmen in ihrem Zuständigkeitsgebiet anschreiben, die keinen Datenschutzbeauftragten gemeldet haben, nach Information der Behörde aber eigentlich einen solchen benennen müssten.

Mit welchen Strafen müssen kleine Unternehmen rechnen, wenn sie die Vorgaben nicht umsetzen? Drohen wirklich auch kleinen Unternehmen Bußgelder in Millionenhöhe?

Bei den Sanktionen macht die DSGVO grundsätzlich keinen Unterschied zwischen großen, mittleren oder kleinen Unternehmen. Je nach Verstoß stehen daher für alle gleichermaßen bis zu 10 Millionen Euro bzw. bis zu 20 Millionen Euro Geldbuße im Raum. Früher lag die Grenze bei 50.000 bzw. 300.000 Euro. Bußgelder sollen prinzipiell „wirksam, verhältnismäßig und abschreckend“ sein. Allerdings gibt es diverse Kriterien, die bei der Bemessung des konkreten Betrages zu beachten sind.

Dazu zählen u.a. folgende Aspekte:

- Art, Schwere und Dauer des Verstoßes unter Berücksichtigung von Art, Umfang oder Zweck der betreffenden Verarbeitung sowie der Zahl der Betroffenen und des Ausmaßes des erlittenen Schadens
- vorsätzliche oder fahrlässige Begehung
- vom Unternehmen getroffene Maßnahmen zur Minderung des Schadens
- eventuell einschlägige frühere Verstöße des Unternehmens
- Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und mögliche nachteilige Auswirkungen zu mindern
- Kategorien der betroffenen Daten
- Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und ggf. in welchem Umfang das Unternehmen den Verstoß mitgeteilt hat
- jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall (z.B. unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste)

Insgesamt wird ein internationaler Konzern daher ein viel höheres Bußgeld zahlen müssen, als ein kleiner Handwerksbetrieb oder ein mittelständisches produzierendes Unternehmen mit 30 Mitarbeitern. Doch die Sanktionen werden wohl für alle spürbar ausfallen, da sich Datenschutzverstöße nicht mehr „lohnen“ sollen.

Wird es eine Schonfrist geben, in der noch keine Bußgelder verhängt werden?

Auch das ist nicht leicht zu beantworten. Generell ist es so, dass die DSGVO bereits im Mai 2016 in Kraft getreten ist und eine zweijährige Übergangsfrist vorsieht. Daher entfaltet sie ihre volle Wirkung zum 25.05.2018. Ab dann müssen alle Anforderungen umgesetzt sein, das Gesetz sieht keine weitere Übergangsfrist vor. Ob und wann die Behörden die ersten Maßnahmen ergreifen, ist noch nicht ganz klar. Allerdings hat schon die eine oder andere Behörde angekündigt, nicht allzu lange nach dem Stichtag abzuwarten und die Unternehmen in ihrem Bundesland zeitnah anzuschreiben. Es ist also besser, schon mal mit der Umstellung auf die DSGVO anzufangen, auch wenn man nicht bis zum 25.05.2018 damit 100%-ig fertig wird. Denn das ist allemal besser, als noch gar nichts unternommen zu haben.

Rechtsanwalt Michael Rohrlich

www.ra-rohrlich.de

DSGVO-MASSNAHMENPLAN

„So gehen Sie die DSGVO-Umstellung in Ihrem Unternehmen an“

von Michael Rohrlich, Rechtsanwalt und TÜV Süd zertifizierter Datenschutzbeauftragter (DSB-TÜV)

Die EU-Datenschutzgrundverordnung (DSGVO) ist im Mai 2016 in Kraft getreten. Aufgrund einer zweijährigen Übergangszeit entfaltet sie ihre Wirkung zum 25.05.2018. Ab diesem Zeitpunkt wird es keine weitere „Schonfrist“ mehr geben. Sie gilt dann grundsätzlich für alle Unternehmen – unabhängig von Branche, Größe, Mitarbeiteranzahl oder Umsatz.

Damit Sie Ihr Unternehmen optimal auf die DSGVO vorbereiten können, haben wir Ihnen einen 6-Punkte-Maßnahmenplan erstellt.

1. Herausforderung annehmen

- **Wissen aneignen**
- **Personal, Zeit und Geld einplanen**
- **Verantwortliche bestimmen**

Die „Vogel-Strauß-Methode“ funktioniert nicht – die DSGVO kommt definitiv und muss beachtet werden. Sie enthält das sogenannte Nachweis-Prinzip. Das heißt: Sie müssen künftig in der Lage sein, der Aufsichtsbehörde auf Anfrage zu belegen, dass Sie rechtskonform handeln. Bisher musste Ihnen ein fehlerhaftes Verhalten erst nachgewiesen werden.

Für Sie bedeutet das: Es reicht nun nicht mehr aus, Datenschutz-Maßnahmen im Unternehmen umzusetzen, diese müssen auch dokumentiert werden.

Bauen Sie gezielt Grundlagenwissen auf

Es ist wichtig, dass Sie sich zunächst ein gewisses Grundlagenwissen aneignen, um das Projekt DSGVO effizient in Angriff nehmen zu können. Sie sollten die wichtigsten Begrifflichkeiten und Grundsätze kennen. Zum Beispiel sollten Sie wissen, wer als Betroffener und wer als Verantwortlicher bezeichnet wird und was man unter dem Rechtmäßigkeitsprinzip oder dem Zweckbindungsgrundsatz versteht.

Da stets die Geschäftsführung im Unternehmen für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich ist, sollte insbesondere in dieser Ebene das Basis-Know-how aufgebaut werden. Ist ein Datenschutzbeauftragter vorhanden, muss natürlich auch dieser sein Wissen auf den aktuellen Stand bringen. Aber: nicht jeder muss alles wissen. Die Informationen sollten also nicht nach dem „Gießkannenprinzip“ verteilt werden. Es reicht vollkommen aus, wenn z.B. die Marketingabteilung die Besonderheiten im Bereich Werbung oder die IT-Abteilung die speziellen technikbezogenen Themen kennen.

Planen Sie ausreichend Budget und Personal ein

Insbesondere wenn in Ihrem Unternehmen noch keinerlei Unterlagen in puncto Datenschutz existieren, sollten Sie den Aufwand zur Umstellung auf die DSGVO nicht unterschätzen und entsprechend ausreichende Mittel einplanen. Je größer Ihr Unternehmen ist, desto mehr Personal, Zeit und Geld muss bereitgestellt werden.

Während beispielweise in einem kleinen Handwerksbetrieb ein „DSGVO-Manager“ ausreicht, muss in einem mittelständischen Produktionsbetrieb mit 70 Mitarbeitern hingegen eher ein „Datenschutz-Team“ etabliert werden, in dem je ein Verantwortlicher aus den einzelnen Abteilungen (Personal, Buchhaltung, IT, Marketing etc.) in die DSGVO-Vorbereitung eingebunden wird.

2. Bestandsaufnahme durchführen

- **Prozesse analysieren**
- **Verzeichnis von Verarbeitungstätigkeiten anlegen**
- **Technische und organisatorische Maßnahmen dokumentieren**
- **Liste mit Dienstleistern anlegen**

Zunächst sollten Sie alle Arbeitsabläufe (Prozesse) in Ihrem Unternehmen auflisten, mit denen personenbezogene Daten verarbeitet werden. Typische Prozesse in Unternehmen sind u.a. das Führen von Personalakten, die Buchhaltung, das Durchführen von Bewerbungsverfahren, der Versand von Werbe-Mails, Videoüberwachung im Gebäude oder auch die Vernichtung von Papierunterlagen. Die einzelnen Prozesse sollten zumindest stichpunktartig beschrieben und/oder durch ein Ablaufdiagramm grafisch dargestellt werden (wer ein Qualitätsmanagement-Handbuch oder z.B. eine ISO9001-Zertifizierung o.ä. besitzt, verfügt dadurch schon über eine ganz gute Grundlage). Um die nötigen Informationen zu erhalten, können Sie beispielsweise „geleitete Interviews“ mit den einzelnen Verantwortlichen für Personal, Buchhaltung, IT, Marketing etc. durchführen. Ziel ist es, ein Verzeichnis von Verarbeitungstätigkeiten zu erstellen, das als zentrale Datenschutz-Management-Quelle und ggf. zur Erfüllung Ihrer Nachweispflicht dient.

Dokumentieren Sie Ihre TOM und Dienstleister

Neben den Beschreibungen der Prozesse müssen Sie auch Ihre vorhandenen technischen und organisatorischen Maßnahmen (kurz: TOM) dokumentieren. Dazu zählen beispielsweise eine Zutrittskontrolle zum Gebäude, die Sicherung des Serverraums, die Pflicht zum Anmelden am Computer mittels Kennung und Passwort, der Einsatz von Antiviren-Software und Firewall etc.

Außerdem sollten Sie eine Liste sämtlicher Dienstleister anfertigen, mit denen Sie zusammenarbeiten. Typischerweise sind das Cloud-Anbieter, E-Mail- bzw. Web-Hoster, IT-Dienstleister für die Drucker- / Kopierer-Wartung, externe Lohnbuchhalter, Entsorgungsunternehmen o.ä. Hier müssen zusätzlich zu den eigentlichen Dienstleistungsverträgen auch sogenannte Auftragsverarbeitungsverträge geschlossen werden. Diese Pflicht ist nicht neu und galt auch schon unter dem alten Bundesdatenschutzgesetz (BDSG). Bereits bestehende Verträge sollten Sie daher an die DSGVO anpassen.

3. Lücken erkennen und schließen

- **Verfahrensbeschreibungen gemäß DSGVO vervollständigen**
- **Technische und organisatorische Maßnahmen prüfen & ggf. anpassen**

Nachdem Sie die Bestandsaufnahme durchgeführt haben, müssen die Vorgaben der DSGVO in Ihrem Unternehmen umgesetzt werden, die noch nicht berücksichtigt werden. Das kann durch Maßnahmen geschehen, wie z.B. die Aktualisierung des Betriebssystems, die Wahl einer anderen Cloud-Anwendung oder die Verwendung eines Verschlüsselungszertifikats für die eigene Internetseite (insbesondere wichtig bei Webshops oder auch bei Verwendung eines Kontaktformulars). Unter Umständen ergibt die Prüfung aber auch, dass Sie bislang Werbe-Mails an Kunden verschicken, die Ihnen dafür gar nicht die Einwilligung erteilt haben.

4. Rechtsprüfung durchführen (lassen)

- **Verträge prüfen & anpassen (lassen)**
- **Neue Verträge erstellen (lassen)**
- **Ggf. Rechtsrat einholen**

In jedem Fall sollte eine rechtliche Prüfung erfolgen. Denn personenbezogene Daten dürfen grundsätzlich nicht verarbeitet werden – es sei denn, es liegt eine Einwilligung des Betroffenen vor. Es gibt allerdings einen gesetzlichen Ausnahmetatbestand, oder es bestehen überwiegende berechtigte Interessen des Verantwortlichen. Wichtige Erlaubnistatbestände in der DSGVO erlauben die Datenverarbeitung u.a.:

- zur Erfüllung eines Vertrages (z.B. Durchführung eines Kundenauftrags),
- aufgrund einer rechtlichen Verpflichtung (z.B. steuerrechtliche Aufbewahrungsfristen) oder
- zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe bzw. Ausübung öffentlicher Gewalt (z.B. „Knöllchen“ vom Ordnungsamt).

Der Schutz vor Betrug oder auch das Direktmarketing gelten nach Maßgabe der DSGVO übrigens als berechtigtes Interessen zur Verarbeitung personenbezogener Daten durch Unternehmen.

Geben Sie zu jedem Prozess die Rechtsgrundlage an

Im Rahmen des Verzeichnisses der Verarbeitungstätigkeiten muss zu jedem einzelnen Prozess die entsprechende Rechtsgrundlage angegeben werden, auf deren Basis die Verarbeitung der jeweiligen Daten erfolgt. Daher müssen Sie abklären, um welche Rechtsgrundlagen es sich handelt und ob ggf. Verträge aktualisiert werden müssen.

Darüber hinaus müssen Sie bei bestimmten Verarbeitungstätigkeiten, wie z.B. der Verarbeitung von besonders sensiblen Daten (Gesundheitsdaten o.ä.), Videoüberwachung öffentlicher Bereiche oder Profiling-Maßnahmen, eine sogenannte Datenschutz-Folgenabschätzung durchführen. Hierdurch soll das potentielle Risiko für die Betroffenen ermittelt werden. Je nach Ausmaß des ermittelten Risikos muss dann vor Durchführung der Datenverarbeitung die Aufsichtsbehörde darüber informiert werden.

5. Maßnahmen mit Außenwirkung

- **Online-Datenschutzerklärung anpassen**
- **Ggf. Datenschutzbeauftragten benennen und/oder melden**

Ob Sie die Datenschutzvorgaben einhalten oder nicht, lässt sich am besten anhand der Maßnahmen überprüfen, die für andere „sichtbar“ sind. Ob Sie bei der Abwicklung einer Kundenbestellung alles korrekt beachten, können Außenstehende nur schlecht beurteilen. Aber der Umstand, dass Sie einen Datenschutzbeauftragten brauchen und diesen dann auch der zuständigen Aufsichtsbehörde melden müssen, hat eine gewisse Außenwirkung und ist deshalb auch eher nachvollziehbar. Das Gleiche gilt für eine korrekte Datenschutzerklärung auf Ihrer Internetseite. Hier kann sogar eine automatisierte Prüfung durch die Aufsichtsbehörde oder auch von Ihrer Konkurrenz erfolgen. Diese Punkte sollten daher weit oben auf Ihre To-Do-Liste stehen und auch bis zum Stichtag 25.05.2018 DSGVO-konform umgesetzt werden.

6. Neue Arbeitsabläufe etablieren

- **Geschäftsabläufe zur Wahrung der Betroffenenrechte umsetzen**
- **Auf mögliche Datenpannen vorbereiten**
- **Prozesse zur regelmäßigen Prüfung einrichten**
- **Ggf. Datenschutz-Management-System einführen**

Ein wichtiger Aspekt der DSGVO sind die Rechte der Betroffenen, also der Personen, deren Daten Sie in Ihrem Unternehmen verarbeiten. Sie müssen insbesondere verschiedene Informationsrechte beachten, etwa bei der erstmaligen Erhebung von Daten, bei etwaigen Datenpannen oder eben auch in der Online-Datenschutzerklärung. Außerdem müssen Sie sicherstellen, dass z.B. bei Auskunftsanfragen oder auch bei Datenpannen Ihre Mitarbeiter alle wissen, wie vorzugehen ist. Hierzu können Sie etwa entsprechende Arbeitsanweisungen erteilen oder Prozessbeschreibungen im Datenschutz-Management-System hinterlegen (sofern vorhanden). Auch das frühzeitige Formulieren von Musterschreiben für die Erteilung von Auskünften oder Mitteilungen an die Aufsichtsbehörde ist sinnvoll, damit Sie im Falle des Falles schnell reagieren können.

Aktualisieren Sie Ihre Prozess-Dokumentationen bei Änderungen

Die DSGVO sieht vor, dass Sie Ihre Arbeitsabläufe regelmäßig überprüfen – zumindest immer dann, wenn sich daran etwas ändert oder Sie neue Prozesse einführen. Wechseln Sie z.B. den Mail-Provider oder installieren Sie ein Zeiterfassungssystem für Ihre Mitarbeiter, müssen Sie auch die entsprechenden Änderungen im Verzeichnis von Verarbeitungstätigkeiten aufnehmen.

Rechtsanwalt Michael Rohrlich

www.ra-rohrlich.de

FAQ-LISTE

Fragen und Antworten zur Datenschutz-Grundverordnung (DSGVO)

Welche Unternehmen sind von der DSGVO betroffen?

Von der neuen Verordnung sind alle Unternehmen in der EU betroffen, unabhängig von der Größe, Mitarbeiterzahl oder Umsatz des Unternehmens. Das heißt: Kleine Handwerksbetriebe mit zwei bis drei Mitarbeitern sind genauso betroffen wie große Konzerne.

Wann tritt die DSGVO in Kraft?

Die Verordnung ist bereits 2016 in Kraft getreten. Die EU hat den Unternehmen jedoch eine zweijährige Übergangsfrist gewährt. Ab 25. Mai 2018 ist sie dann in allen EU-Mitgliedsstaaten anwendbar.

Welche Daten unterliegen der DSGVO?

Das Datenschutzrecht gilt ausschließlich für personenbezogene Daten, denn das Ziel ist, die Privatsphäre des Einzelnen zu schützen. Demnach sind u.a. folgende Daten betroffen:

- Kundendaten
- Lieferantendaten
- Mitarbeiterdaten

Unternehmensdaten sind nicht geschützt.

Was genau sind personenbezogene Daten?

Im Detail sind folgende Daten gemeint:

- allgemeine Personendaten: Name, Geburtsdatum, Geburtsort, Postanschrift, E-Mail-Adresse, Rufnummern usw.
- Kennnummern: Sozialversicherungsnummer, Steueridentifikationsnummer, Nummer bei der Krankenkasse, Personalausweisnummer usw.
- Bankdaten: Kontostände, Kontonummern, Kreditinformationen, usw.
- körperliche Merkmale: Geschlecht, Haut-, Haar- und Augenfarbe, Statur usw.
- Vermögen und Besitz: Immobilien, Fahrzeuge, Grundbucheintragungen, Kfz-Kennzeichen, usw.
- Werturteile: Schul-, Hochschul- und Arbeitszeugnisse usw.
- Kundendaten: Bestellungen, Adressdaten, Kontodaten usw.
- Online-Daten: IP-Adresse, Standortdaten usw.
- u. v. m.

Darüber hinaus gibt es (laut § 4 Absatz 9 BDSG) die besonderen personenbezogenen Daten. Die Vorschriften zur Sammlung und Verarbeitung dieser Daten sind wesentlich strenger. Es handelt sich um folgende Daten:

- Angaben über rassische sowie ethnische Herkunft

- politische Ansichten
- religiöse und philosophische Überzeugung
- Gewerkschaftszugehörigkeit
- Angaben zur Gesundheit
- Angaben zur Sexualität

Wann darf ich personenbezogene Daten verarbeiten?

Oberster Grundsatz des alten wie neuen Datenschutzrechts ist das Verbotsprinzip: Jede Verarbeitung personenbezogener Daten ist verboten. Es sei denn, der Zweck der Datenspeicherung ist gerechtfertigt.

Das ist z. B. dann der Fall, wenn ein Vertrag mit der betroffenen Person besteht: Der Betreiber eines Online-Shops darf die Adressdaten des Kunden an einen Logistikdienstleister weitergeben, damit die Ware ausgeliefert werden kann. Die Datenspeicherung darf aber nur so erfolgen, wie es für die Vertragserfüllung notwendig ist.

Was sind die Kernforderungen der DSGVO?

Die Datenschutzgrundverordnung enthält eine Vielzahl komplexer Inhalte. Für Sie als Klein- unternehmer sind vor allem folgende Forderungen relevant:

Recht auf Vergessen /Löschung
Ein wichtiger Teil der DSGVO sind die Rechte der Betroffenen. Daten müssen auf Verlangen eines Kunden gelöscht werden, wenn der Zweck, für den die Daten gespeichert wurden, nicht mehr besteht. Aber auch dann, wenn der Kunde seine Einwilligung zur Datenspeicherung widerruft oder wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden.

Auskunftsrecht
Der Kunde kann, wie in der bisherigen Verordnung auch, jederzeit Auskunft darüber verlangen, welche Daten von ihm gespeichert und wie diese verarbeitet werden. Diese Auskunft muss unverzüglich erteilt werden. Dies bedeutet, dass in jedem Unternehmen ein Prozess geschaffen werden muss, der den Auskunftsansprüchen gerecht wird.

Meldepflicht
Die Meldepflicht von Datenpannen, die z. B. durch Hacker-Angriffe, Verlust eines Datenträgers oder mobilen Endgeräts verursacht werden, sind mit der neuen DSGVO deutlich umfangreicher geworden: Bisher war nur im Ausnahmefall eine Meldung erforderlich, nach neuem Recht muss jede Datenschutzverletzung binnen 72 Stunden der Behörde – unter Umständen auch den Betroffenen – gemeldet werden. Deshalb sollte jedes Unternehmen über einen internen Prozess verfügen, der im Falle von Datenlecks zum Einsatz kommt.

Was mache ich mit Daten in Dokumenten, für die Aufbewahrungsfristen bestehen?

Wenn Aufbewahrungspflichten für bestimmte Dokumente bestehen, dürfen diese gespeichert werden, auch wenn sie personenbezogene Daten enthalten. Die Pflicht zur Löschung wird in diesen Fällen ausgesetzt. Das ist zum Beispiel bei Rechnungen der Fall (Aufbewahrungspflicht 10 Jahre) und bei geschäftlichen Briefen /E-Mails (Aufbewahrungspflicht 6 Jahre).

Welche Bereiche im Unternehmen sind von der DSGVO betroffen?

Wichtige Bereiche im Unternehmen, auf die ein besonderes Augenmerk gelegt werden sollte, sind u.a.

- EDV
- Vertrieb
- Einkauf
- Personalabteilung

Was passiert, wenn ich die DSGVO nicht fristgerecht umgesetzt habe?

Experten gehen davon aus, dass bis zum Stichtag nicht alle Unternehmen die DSGVO bereits umgesetzt haben. Insofern werden Prüfer voraussichtlich nicht sofort von umfassenden Strafmaßnahmen Gebrauch machen. Unternehmer sind jedoch gut beraten, das Thema nicht zu ignorieren. Denn wer nachweisen kann, dass bereits an der Umsetzung der DSGVO gearbeitet wird, kann bei einer Prüfung auf Nachsicht und Unterstützung seitens der Behörden hoffen.

Doch Vorsicht: Nicht nur Behörden, sondern auch Kunden oder z. B. ehemalige Mitarbeiter können Auskunft über die gespeicherten Daten verlangen. Wer diesen Anforderungen nicht unverzüglich nachkommt, kann juristisch belangt werden. Experte warnen bereits jetzt davor, dass die Abmahnanwälte schon in den Startlöchern stehen.

Welche Bußgelder drohen tatsächlich?

Bisher waren Bußgelder von maximal 300 000 Euro vorgesehen, was in der Praxis meistens auf Beträge zwischen 5000 und 10 000 Euro hinauslief. Zukünftig sollen Verstöße gegen den Datenschutz erheblich schärfer bestraft werden. Der Höchstbetrag kann nun bis zu vier Prozent des Jahresumsatzes oder bis zu 20 Millionen Euro betragen – je nachdem, welche Summe höher liegt. Dadurch werden auch die tatsächlich zu zahlenden Bußgelder drastisch ansteigen.

Muss ich in meinem Unternehmen einen Datenschutzbeauftragen haben?

Wenn sich in Ihrer Firma mehr als 10 Mitarbeiter ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, sollten Sie einen Datenschutzbeauftragen vorweisen können. Unternehmen mit mehr als 20 Mitarbeitern benötigen zwingend einen Datenschutzbeauftragten. Hier sollte ein geeigneter Mitarbeiter entsprechend ausgebildet bzw. geschult werden.

Wer ist bei Verstößen gegen die DSGVO verantwortlich?

Prinzipiell ist der Inhaber oder Geschäftsführer eines Unternehmens verantwortlich und nicht der Datenschutzbeauftragte oder der Leiter der EDV! Stellen Sie daher in Ihrem Unternehmen sicher, dass die neuen Vorschriften von allen Mitarbeitern eingehalten werden.

FAQ ZUR DSGVO

Kunden fragen – unser Experte antwortet!

Haben auch Sie konkrete Fragen zur DSGVO? Der **Fachanwalt und Autor Dr. Martin Schirmbacher** hat bereits zahlreiche Fragen beantwortet, die unsere Kunden in seiner Online-Schulung gestellt haben. Profitieren auch Sie von diesem Wissen!

Allgemeine Fragen

Wie soll ein Ein-Mann-Unternehmen bezüglich DSGVO vorgehen?

Auch für ein Ein-Mann-Unternehmen gilt die DSGVO. Allerdings ist ein Datenschutzbeauftragter nicht zu bestellen. Mein Rat ist, die in meinem Fachartikel geschilderten Pflichten umzusetzen und insbesondere Datenschutzinformationen auf der Website zu aktualisieren. Viele Interessenverbände haben inzwischen Muster zur Verfügung gestellt. Falls Sie hier nicht fündig werden, sollten Sie sich Rechtsrat einholen.

Link zum Fachartikel: www.lexware.de/artikel/datenschutzgrundverordnung-was-ist-das-eigentlich-und-was-bedeutet-die-einfuehrung-fuer-unternehmen

Aufbewahrungsfristen nach deutschem Recht vs. DSGVO: was gilt?

Hier gilt nicht entweder/oder! Wenn das deutsche Recht eine Pflicht zur Aufbewahrung von Unterlagen vorsieht, liegt in der Regel auch eine Rechtfertigung nach der DSGVO vor. Allerdings muss im Einzelnen geprüft werden, worauf sich die Löschfrist bezieht. Nur solche personenbezogenen Daten dürfen gespeichert bleiben, die aufgrund des jeweiligen Gesetzes von der Aufbewahrungspflicht umfasst sind.

Welche Behörde prüft denn, ob die Vorschriften nach DSGVO eingehalten werden?

Zuständig ist jeweils die Aufsichtsbehörde am Sitz des Unternehmens. In Deutschland hat jedes Bundes land eine für den Datenschutz im nicht öffentlichen Bereich zuständige Behörde. Eine vollständige Liste gibt es hier: www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html

An wen kann ich mich wenden, wenn ich weitere Fragen zur DSGVO habe?

Die Datenschutzbehörden sind grundsätzlich gehalten, Unternehmen bei der Umsetzung der Vorgaben der DSGVO zu unterstützen. Einzelne Fragen kann man daher an die Aufsichtsbehörde richten. Ansonsten ist empfehlenswert, Datenschutzberater oder spezialisierte Rechtsanwälte zu konsultieren.

Fragen zur Verfahrensdokumentation

Wer muss eine Verfahrensdokumentation erstellen?

Jedes Unternehmen, das personenbezogene Daten verarbeitet, muss im Zweifel in der Lage sein nach zuweisen, dass es sich datenschutzkonform verhält. Es besteht eine Verpflichtung, ein Verzeichnis über die Verarbeitungstätigkeiten zu führen, wenn das Unternehmen mehr als 250 Mitarbeiter hat. Doch auch Unternehmen mit weniger Angestellten müssen ein solches Verzeichnis führen, wenn die Verarbeitung nicht nur gelegentlich erfolgt oder besondere Datenkategorien, etwa Gesundheitsdaten, verarbeitet

werden. Wann eine Verarbeitung nicht nur gelegentlich erfolgt, ist bisher nicht klar. Man wird davon ausgehen müssen, dass die allermeisten Unternehmen ein Verzeichnis führen müssen.

Wie muss eine Verfahrensdokumentation aussehen?

Der Mindestinhalt des Verzeichnisses ergibt sich aus Art. 30 DSGVO. Danach muss Name und Zweck der Datenverarbeitung und die Rechtsgrundlage angegeben werden. Für jedes einzelne Verfahren müssen die betroffenen Personengruppen und die konkrete Art der Daten angegeben werden. Gesondert zu kennzeichnen ist, wenn es sich um besondere Arten personenbezogener Daten handelt (z. B. Gesundheitsdaten).

Zudem bietet es sich an, jedem Verfahren eine kurze Beschreibung beizufügen. Diese muss nicht jedes Detail enthalten, es sollte aber deutlich werden, wie die Datenverarbeitung erfolgt. Hierzu kann es sinnvoll sein, aus dem Verzeichnis auf eine ausführlichere Prozessbeschreibung zu verweisen.

Bisweilen schwierig aber notwendig ist die Angabe, wie lange die Daten zu speichern sind. Dazu bedarf es zunächst eines Löschkonzepts, aus dem sich die einzelnen Löschfristen ergeben.

Weitere Informationspflichten beziehen sich auf die Angabe einer allgemeinen Beschreibung der eingesetzten technischen und organisatorischen Maßnahmen für den Datenschutz. Hierbei spielt insbesondere ein Zugriffsberechtigungskonzept eine wichtige Rolle. Angegeben werden muss zudem, wenn die Daten außerhalb der europäischen Union verarbeitet werden sollen.

Das Verzeichnis kann elektronisch, etwa in Excel oder Word geführt werden. Viele Verbände haben für ihre Mitglieder Musterverzeichnisse entwickelt. Der Anwaltsverein hat zum Beispiel eines für Anwaltskanzleien veröffentlicht: www.anwaltverein.de/de/praxis/datenschutz

Fragen zu Kundendaten

Muss ich bei meinen Kunden eine Einwilligungserklärung einholen oder ggf. nur bei neuen Kunden nach dem 25. Mai 2018?

Ob eine Einwilligung erforderlich ist oder ob die Datenverarbeitung etwa auf einen Vertrag oder berechtigte Interessen gestützt werden kann, muss für jeden einzelnen Datenverarbeitungsvorgang isoliert betrachtet werden. Für Newsletter- Werbung per E-Mail ist in jedem Falle eine Einwilligung erforderlich. Dabei gelten jedoch in der Regel bisher eingeholte Einwilligungen weiter.

Muss jeder Kunde angeschrieben und darüber informiert werden, welche Daten wir von ihm speichern?

In der Tat sieht die Verordnung vor, dass die Betroffenen über jede Datenverarbeitung zu informieren sind. Online kann dies über die Website erfolgen. Bei Katalogbestellungen sollte die Erklärung zum Datenschutz im Katalog abgedruckt werden. Am Point-of-Sale können Datenschutzinformationen ausgelegt werden. Schwierig ist die Information aber zum Beispiel am Telefon. Inwieweit Medienbrüche zulässig sind und etwa ein Verweis auf die Website erfolgen kann, ist bisher unklar.

Reicht es, wenn auf der Homepage eine Datenschutzerklärung zu finden ist oder muss man diese von seinen Kunden unterschreiben lassen?

Für Online-Bestellungen ist es ausreichend, wenn die Hinweise zum Datenschutz in der Datenschutzerklärung zu finden sind. Dabei sollte die Erklärung unmittelbar bei der Datenerhebung verlinkt sein. Eine ausdrückliche Bestätigung wie: „Ich habe die Datenschutzerklärung gelesen und bin damit einverstanden“, oder gar eine Unterschrift sind nicht erforderlich.

Darf ich öffentlich zugängliche Daten in meinem CRM-System speichern?

Datenschutzrechtlich stellt sich die Frage nur bei personenbezogenen Daten. Für reine Unternehmens kennzahlen etwa gibt es keine datenschutzrechtlichen Beschränkungen.

Auch die Erhebung und Nutzung von öffentlich zugänglichen personenbezogenen Daten ist grundsätzlich gestattet. Problematisch kann aber die gezielte Anreicherung von bereits vorhandenen Informationen im CRM sein. Hier sollte man sich genau anschauen, ob eine einwilligungsbedürftige Profilbildung vorliegt. Außerdem muss der Betroffene über die Datenerhebung informiert werden.

Darf ich meinen Kunden noch zum Geburtstag gratulieren/frohe Weihnachten wünschen?

Unproblematisch ist das, wenn eine Einwilligung des Kunden vorliegt. Ansonsten ist es in der Tat schwierig. Möglich ist allenfalls ein postalischer Gruß. Und dafür sind die beteiligten Interessen miteinander abzuwägen. Während für die Unternehmen der Kundenservice und die Umsatzmehrung spricht, haben die Kunden ein Interesse daran, dass ihr Geburtsdatum nicht für Werbezwecke verwendet wird.

Am Ende kommt es auf die vernünftigen Erwartungen der Kunden an. Wer sich in einer intensiven Kundenbeziehung befindet und bisher Geburtstagswünsche erhalten hat, wird damit auch in Zukunft rechnen. Wer z. B. sein Geburtsdatum angeben musste, um die Volljährigkeit zu prüfen, wird nicht mit einem Geburtstagsgruß rechnen.

Fragen zum Datenschutzbeauftragten

Welche Unternehmen benötigen einen Datenschutzbeauftragten?

In Deutschland brauchen alle Unternehmen einen Datenschutzbeauftragten, bei denen mehr als 10 Mitarbeiter ständig mit der Datenverarbeitung befasst sind.

Außerdem muss ein Datenschutzbeauftragter ernannt werden, wenn die Kerntätigkeit des Unternehmens in einer Datenverarbeitung liegt, die mit der Überwachung von Personen zusammenhängt. Auch wenn die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten, insbesondere Gesundheitsdaten besteht, muss ein Datenschutzbeauftragter bestellt werden. Darunter fallen jedenfalls Krankenhäuser und Labore.

Benötigen Unternehmen/Freiberufler, die besonders sensible Daten verarbeiten, wie etwa Steuerberater, Ärzte und Anwälte, einen Datenschutzbeauftragten auch bei weniger als 10 Mitarbeitern?

Nein. Allein die Tatsache, dass auch sensible Daten verarbeitet werden, führt nicht zur Pflicht, einen Datenschutzbeauftragten benennen zu müssen.

Wer im Unternehmen soll/darf Datenschutzbeauftragter werden – GF, IT-ler, Assistentin?

Die Anforderungen an einen Datenschutzbeauftragten sind nicht hoch. Die Person muss ein Mindestmaß an Sachkunde aufweisen, sollte also jedenfalls eine entsprechende Schulung durchlaufen haben. Allerdings sind Mitglieder der Geschäftsleitung davon ausgeschlossen, Datenschutzbeauftragter zu werden. Auch der IT-Leiter sollte nicht die Stelle sein, die die Einhaltung der Datenschutzvorschriften im Unternehmen prüft.

Fragen zu Mitarbeiterdaten

Sollte man zur Sicherheit einen § in den Arbeitsvertrag aufnehmen, damit die Mitarbeiter unterschreiben können, dass sie mit der Datenverarbeitung einverstanden sind?

Es kommt darauf an, für welche Datenverarbeitung die Einwilligung gelten soll. Für die Standardprozesse ist das nicht erforderlich – und auch nicht sinnvoll. Eine Einwilligung im Arbeitsverhältnis ist meist problematisch. Oberstes Gebot ist die Freiwilligkeit. Nur wenn die Einwilligung wirklich aus freien Stücken erfolgt, ist sie wirksam. Außerdem kann sie jederzeit widerrufen werden, weshalb sie deutlich weniger als Rechtsgrundlage für die Verarbeitung von Daten im Arbeitsverhältnis geeignet ist.

Muss ich jeden Mitarbeiter darüber informieren, was wir im Personalstammblatt speichern?

Ja. Das kann zum Beispiel als Anlage zum Arbeitsvertrag geschehen.

Spezielle Fragen

Welche Auswirkungen hat die DSGVO auf (Zahn-) Arztpraxen?

Arztpraxen sind zunächst einmal Unternehmen wie andere auch, so dass die allgemeinen Voraus setzungen gelten. Die Bundeszahnärztekammer hat ein Merkblatt veröffentlicht, in dem viele Details angesprochen sind: www.bzaek.de/fileadmin/PDFs/b/datenschutz_zahnarzt.pdf

DSGVO bei Vereinen – auf was ist zu achten?

Auch für Vereine gilt die DSGVO. Das bedeutet zum Beispiel, dass ggf. ein Datenschutzbeauftragter zu bestellen ist und insbesondere das Mitgliedermanagement auf den Prüfstand gehört.
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg stellt hierzu folgende Informationen zur Verfügung:
www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf

Was müssen wir als Kleinunternehmen (Druckerei unter 10 Mitarbeiter) tun, wenn wir Adressdaten von Kunden zum Druck von Mailings erhalten. Reicht eine Einwilligungserklärung für die Verwendung der Adressen?

Als Druckerei verarbeitet Sie die Daten im Auftrag Ihrer Kunden. Sie sollten sich einen Standardvertrag für eine Datenverarbeitung im Auftrag fertigen lassen und den Kunden jeweils akzeptieren lassen. Das geht auch online und möglicherweise sogar als Annex zu Ihren AGB.

Hinweis:

Die Beantwortung der Fragen erfolgt nach bestem Wissen und neuestem Kenntnisstand. Die Komplexität und der ständige Wandel der Rechtsmaterie machen es jedoch unabdingbar, insoweit jegliche Haftung und Gewähr auszuschließen.

Tabelle der deutschen Aufsichtsbehörden für Datenschutz

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Husarenstr. 30 • 53117 Bonn

Tel.: 0228 997799-0
Fax: 0228 997799-550
E-Mail: poststelle@bfdi.bund.de
Web: www.bfdi.bund.de

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27 • 91522 Ansbach

Tel.: 0981 531300
Fax: 0981 53981300
E-Mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de

Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg
Königstr. 10a • 70173 Stuttgart

Tel.: 0711 615541-0
Fax: 0711 615541-15
E-Mail: poststelle@lfdi.bwl.de
Web: www.baden-wuerttemberg.datenschutz.de

Berliner Beauftragte für Datenschutz und Informationsfreiheit
Friedrichstr. 219 • 10969 Berlin

Tel.: 030 13889-0
Fax: 030 2155050
E-Mail: mailbox@datenschutz-berlin.de
Web: www.datenschutz-berlin.de

Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg
Stahnsdorfer Damm 77 • 14532 Kleinmachnow

Tel.: 033203 356-0
Fax: 033203 356-49
E-Mail: Poststelle@LDA.Brandenburg.de
Web: www.lda.Brandenburg.de

Landesbeauftragter für Datenschutz und Informationsfreiheit der Hansestadt Bremen
Arndtstr. 1 • 27570 Bremerhaven

Tel.: 0421 3612010 oder 0471 5962010
Fax: 0421 49618495
E-Mail: office@datenschutz.bremen.de
Web: www.datenschutz.bremen.de

Der Hamburgischer Beauftragte für Datenschutz und Informationsfreiheit
Klosterwall 6 (Block C) • 20095 Hamburg

Tel.: 040 42854-4040
Fax: 040 4279-11811
E-Mail: mailbox@datenschutz.hamburg.de
Web: www.datenschutz-hamburg.de

Der Hessische Datenschutzbeauftragte
Gustav-Stresemann-Ring 1 • 65189 Wiesbaden

Tel.: 0611 1408-0
Fax : 0611 1408-900 oder -901
E-Mail: poststelle@datenschutz.hessen.de
Web: www.datenschutz.hessen.de

Der Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern
Schloss Schwerin • Lennéstr. 1 • 19053 Schwerin

Tel.: 0385 59494-0
Fax: 0385 59494-58
E-Mail: info@datenschutz-mv.de
Web: www.datenschutz-mv.de

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstr. 5 • 30159 Hannover

Tel.: 0511 120-4500
Fax: 0511 120-4599
E-Mail: poststelle@lfd.niedersachsen.de
Web: www.lfd.niedersachsen.de

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
Kavalleriestr. 2-4 • 40213 Düsseldorf

Tel.: 0211 38424-0
Fax: 0211 38424-10
E-Mail: poststelle@ldi.nrw.de
Web: www.ldi.nrw.de

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
Hintere Bleiche 34 • 55116 Mainz

Tel.: 06131 208-2449
Fax: 06131 208-2497
E-Mail: poststelle@datenschutz.rlp.de
Web: www.datenschutz.rlp.de

Unabhängiges Datenschutzzentrum Saarland
Fritz-Dobisch-Str. 12 • 66111 Saarbrücken

Tel.: 0681 94781-0
Fax: 0681 94781-29
E-Mail: poststelle@datenschutz.saarland.de
Web: www.datenschutz.saarland.de

Der Sächsische Datenschutzbeauftragte
Bernhard-von-Lindenau-Platz 1 • 01067 Dresden

Tel.: 0351 493-5401
Fax: 0351 493-5490
Email: saechsdsb@slt.sachsen.de
Web: www.datenschutz.sachsen.de

Landesbeauftragter für den Datenschutz Sachsen-Anhalt
Leiterstr. 9 • 39104 Magdeburg

Tel.: 0391 81803-0
Fax: 0391 81803-33
E-Mail: poststelle@lfd.sachsen-anhalt.de
Web: www.datenschutz.sachsen-anhalt.de

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstr. 98 • 24103 Kiel

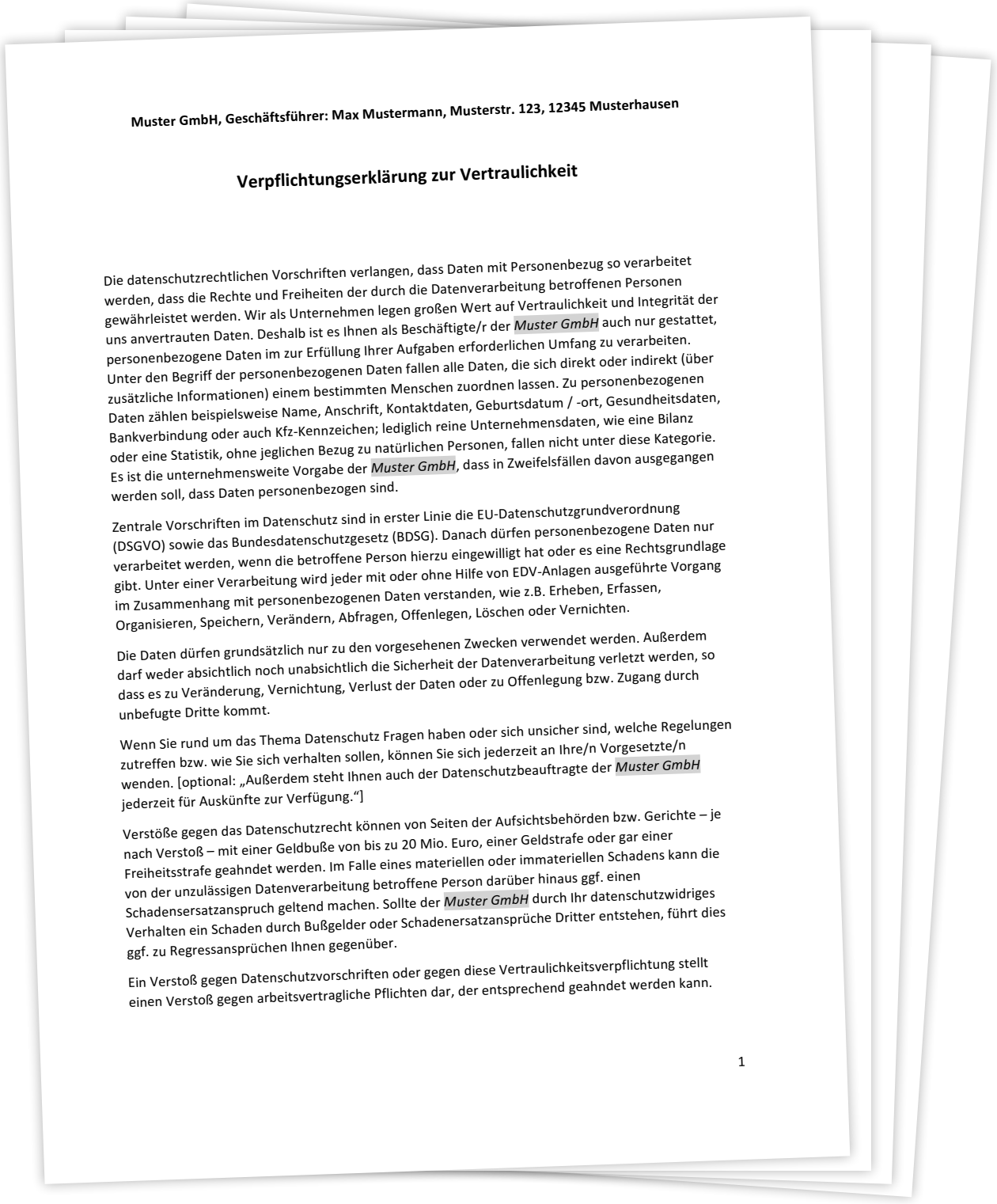
Tel.: 0431 988-1200
Fax: 0431 988-1223
E-Mail: mail@datenschutzzentrum.de
Web: www.datenschutzzentrum.de

Stand: 02/2018 – ohne Gewähr für Richtigkeit und Vollständigkeit

Verpflichtungserklärung zur Vertraulichkeit

(4-seitiges Word Dokument)

Download: https://www.lexoffice.de/dsgvo-vorlage-1



Muster GmbH, Geschäftsführer: Max Mustermann, Musterstr. 123, 12345 Musterhausen

Verpflichtungserklärung zur Vertraulichkeit

Die datenschutzrechtlichen Vorschriften verlangen, dass Daten mit Personenbezug so verarbeitet werden, dass die Rechte und Freiheiten der durch die Datenverarbeitung betroffenen Personen gewährleistet werden. Wir als Unternehmen legen großen Wert auf Vertraulichkeit und Integrität der uns anvertrauten Daten. Deshalb ist es Ihnen als Beschäftigte/r der *Muster GmbH* auch nur gestattet, personenbezogene Daten im zur Erfüllung Ihrer Aufgaben erforderlichen Umfang zu verarbeiten. Unter den Begriff der personenbezogenen Daten fallen alle Daten, die sich direkt oder indirekt (über zusätzliche Informationen) einem bestimmten Menschen zuordnen lassen. Zu personenbezogenen Daten zählen beispielsweise Name, Anschrift, Kontaktdaten, Geburtsdatum / -ort, Gesundheitsdaten, Bankverbindung oder auch Kfz-Kennzeichen; lediglich reine Unternehmensdaten, wie eine Bilanz oder eine Statistik, ohne jeglichen Bezug zu natürlichen Personen, fallen nicht unter diese Kategorie. Es ist die unternehmensweite Vorgabe der *Muster GmbH*, dass in Zweifelsfällen davon ausgegangen werden soll, dass Daten personenbezogen sind.

Zentrale Vorschriften im Datenschutz sind in erster Linie die EU-Datenschutzgrundverordnung (DSGVO) sowie das Bundesdatenschutzgesetz (BDSG). Danach dürfen personenbezogene Daten nur verarbeitet werden, wenn die betroffene Person hierzu eingewilligt hat oder es eine Rechtsgrundlage gibt. Unter einer Verarbeitung wird jeder mit oder ohne Hilfe von EDV-Anlagen ausgeführte Vorgang im Zusammenhang mit personenbezogenen Daten verstanden, wie z.B. Erheben, Erfassen, Organisieren, Speichern, Verändern, Abfragen, Offenlegen, Löschen oder Vernichten.

Die Daten dürfen grundsätzlich nur zu den vorgesehenen Zwecken verwendet werden. Außerdem darf weder absichtlich noch unabsichtlich die Sicherheit der Datenverarbeitung verletzt werden, so dass es zu Veränderung, Vernichtung, Verlust der Daten oder zu Offenlegung bzw. Zugang durch unbefugte Dritte kommt.

Wenn Sie rund um das Thema Datenschutz Fragen haben oder sich unsicher sind, welche Regelungen zutreffen bzw. wie Sie sich verhalten sollen, können Sie sich jederzeit an Ihre/n Vorgesetzte/n wenden. [optional: „Außerdem steht Ihnen auch der Datenschutzbeauftragte der *Muster GmbH* jederzeit für Auskünfte zur Verfügung."]

Verstöße gegen das Datenschutzrecht können von Seiten der Aufsichtsbehörden bzw. Gerichte – je nach Verstoß – mit einer Geldbuße von bis zu 20 Mio. Euro, einer Geldstrafe oder gar einer Freiheitsstrafe geahndet werden. Im Falle eines materiellen oder immateriellen Schadens kann die von der unzulässigen Datenverarbeitung betroffene Person darüber hinaus ggf. einen Schadensersatzanspruch geltend machen. Sollte der *Muster GmbH* durch Ihr datenschutzwidriges Verhalten ein Schaden durch Bußgelder oder Schadenersatzansprüche Dritter entstehen, führt dies ggf. zu Regressansprüchen Ihnen gegenüber.

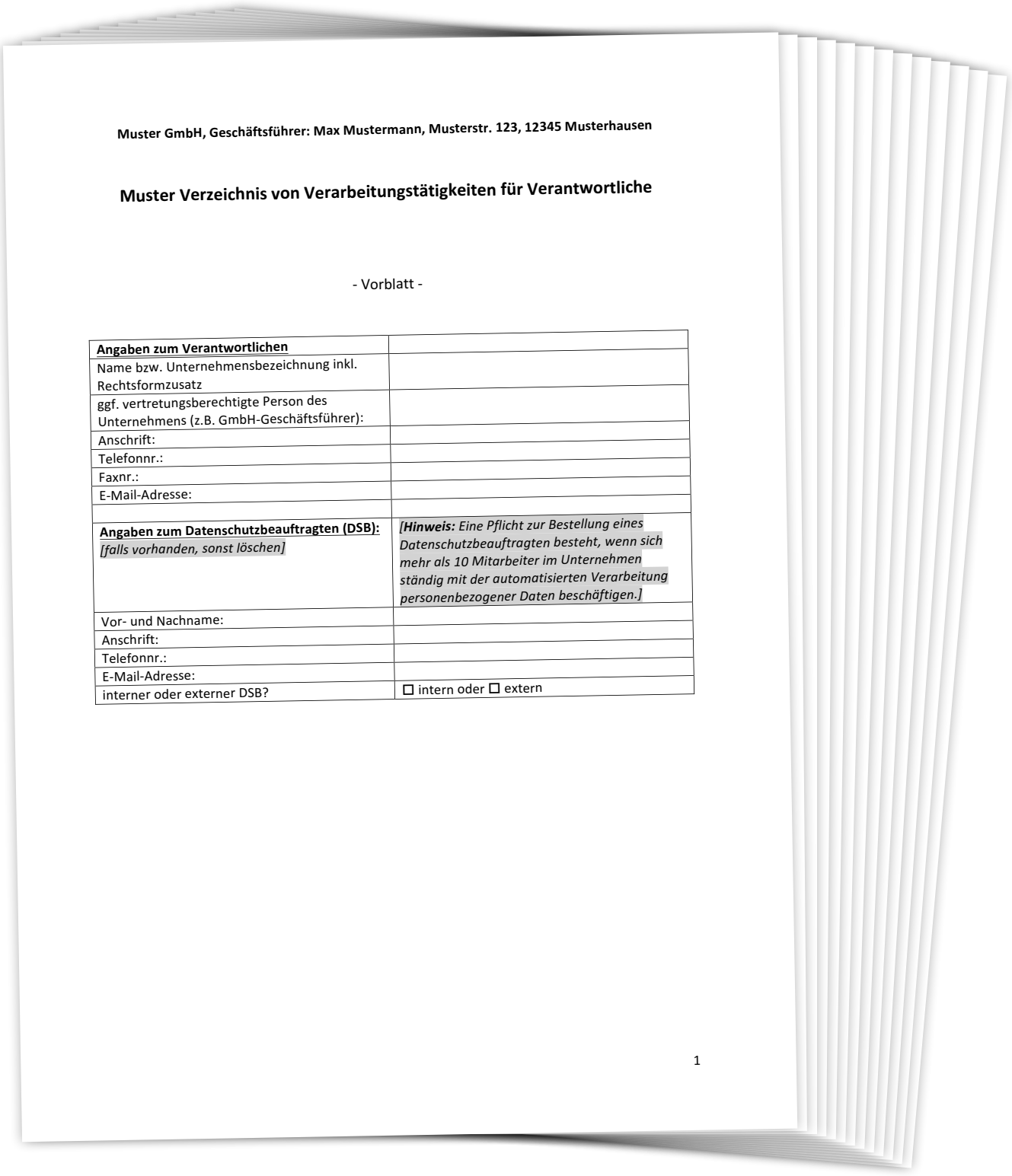
Ein Verstoß gegen Datenschutzvorschriften oder gegen diese Vertraulichkeitsverpflichtung stellt einen Verstoß gegen arbeitsvertragliche Pflichten dar, der entsprechend geahndet werden kann.

1

Muster Verzeichnis von Verarbeitungs-tätigkeiten für Verantwortliche

(13-seitiges Word Dokument)

Download: https://www.lexoffice.de/dsgvo-vorlage-2



Muster GmbH, Geschäftsführer: Max Mustermann, Musterstr. 123, 12345 Musterhausen

Muster Verzeichnis von Verarbeitungstätigkeiten für Verantwortliche

- Vorblatt -

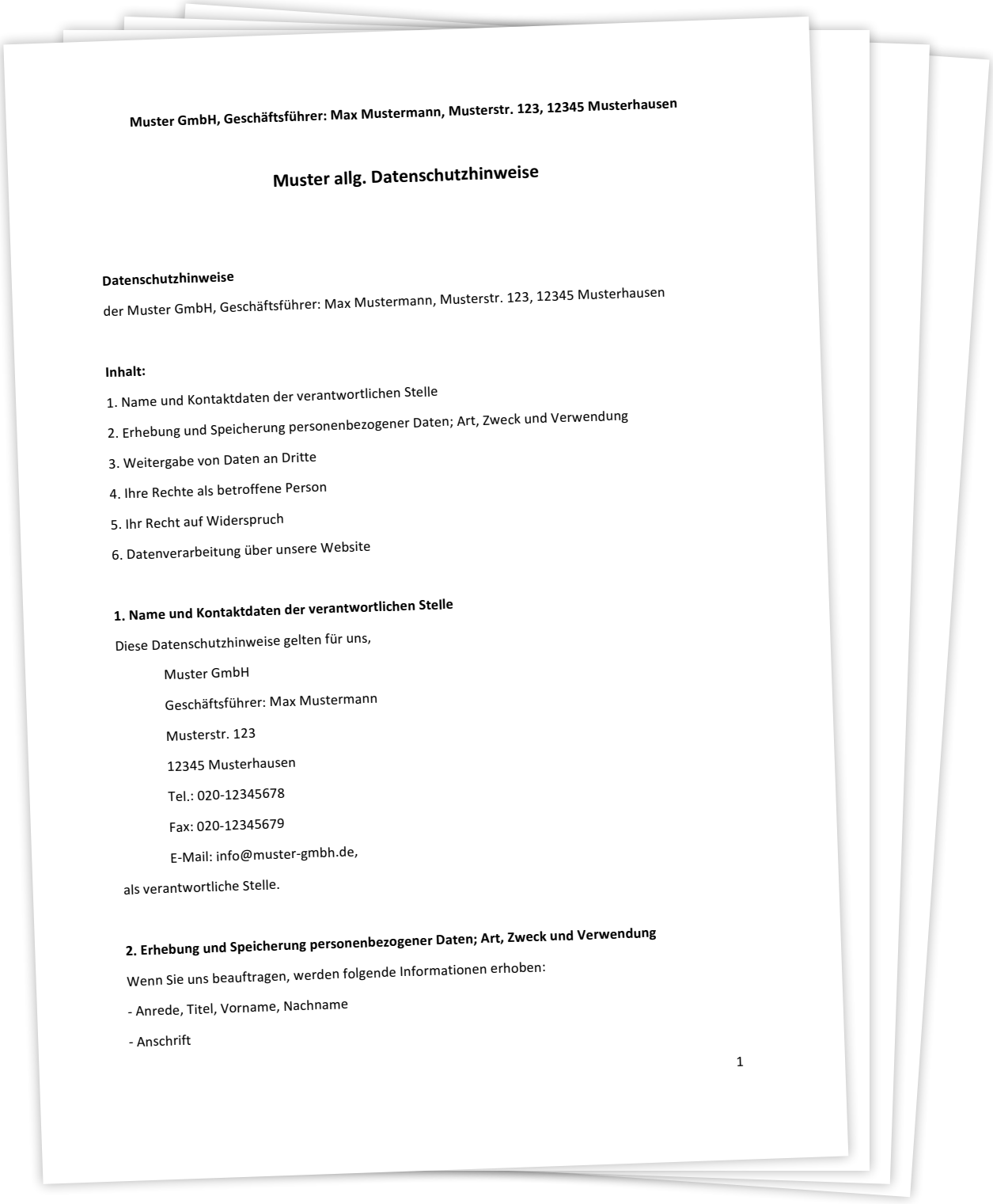
Angaben zum Verantwortlichen	
Name bzw. Unternehmensbezeichnung inkl. Rechtsformzusatz	
ggf. vertretungsberechtigte Person des Unternehmens (z.B. GmbH-Geschäftsführer):	
Anschrift:	
Telefonnr.:	
Faxnr.:	
E-Mail-Adresse:	
Angaben zum Datenschutzbeauftragten (DSB): *[falls vorhanden, sonst löschen]*	*[**Hinweis:** Eine Pflicht zur Bestellung eines Datenschutzbeauftragten besteht, wenn sich mehr als 10 Mitarbeiter im Unternehmen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.]*
Vor- und Nachname:	
Anschrift:	
Telefonnr.:	
E-Mail-Adresse:	
interner oder externer DSB?	☐ intern oder ☐ extern

1

Muster allg. Datenschutzhinweise

(4-seitiges Word Dokument)

Download: https://www.lexoffice.de/dsgvo-vorlage-3



Muster GmbH, Geschäftsführer: Max Mustermann, Musterstr. 123, 12345 Musterhausen

Muster allg. Datenschutzhinweise

Datenschutzhinweise

der Muster GmbH, Geschäftsführer: Max Mustermann, Musterstr. 123, 12345 Musterhausen

Inhalt:

1. Name und Kontaktdaten der verantwortlichen Stelle
2. Erhebung und Speicherung personenbezogener Daten; Art, Zweck und Verwendung
3. Weitergabe von Daten an Dritte
4. Ihre Rechte als betroffene Person
5. Ihr Recht auf Widerspruch
6. Datenverarbeitung über unsere Website

1. Name und Kontaktdaten der verantwortlichen Stelle

Diese Datenschutzhinweise gelten für uns,

Muster GmbH
Geschäftsführer: Max Mustermann
Musterstr. 123
12345 Musterhausen
Tel.: 020-12345678
Fax: 020-12345679
E-Mail: info@muster-gmbh.de,

als verantwortliche Stelle.

2. Erhebung und Speicherung personenbezogener Daten; Art, Zweck und Verwendung

Wenn Sie uns beauftragen, werden folgende Informationen erhoben:

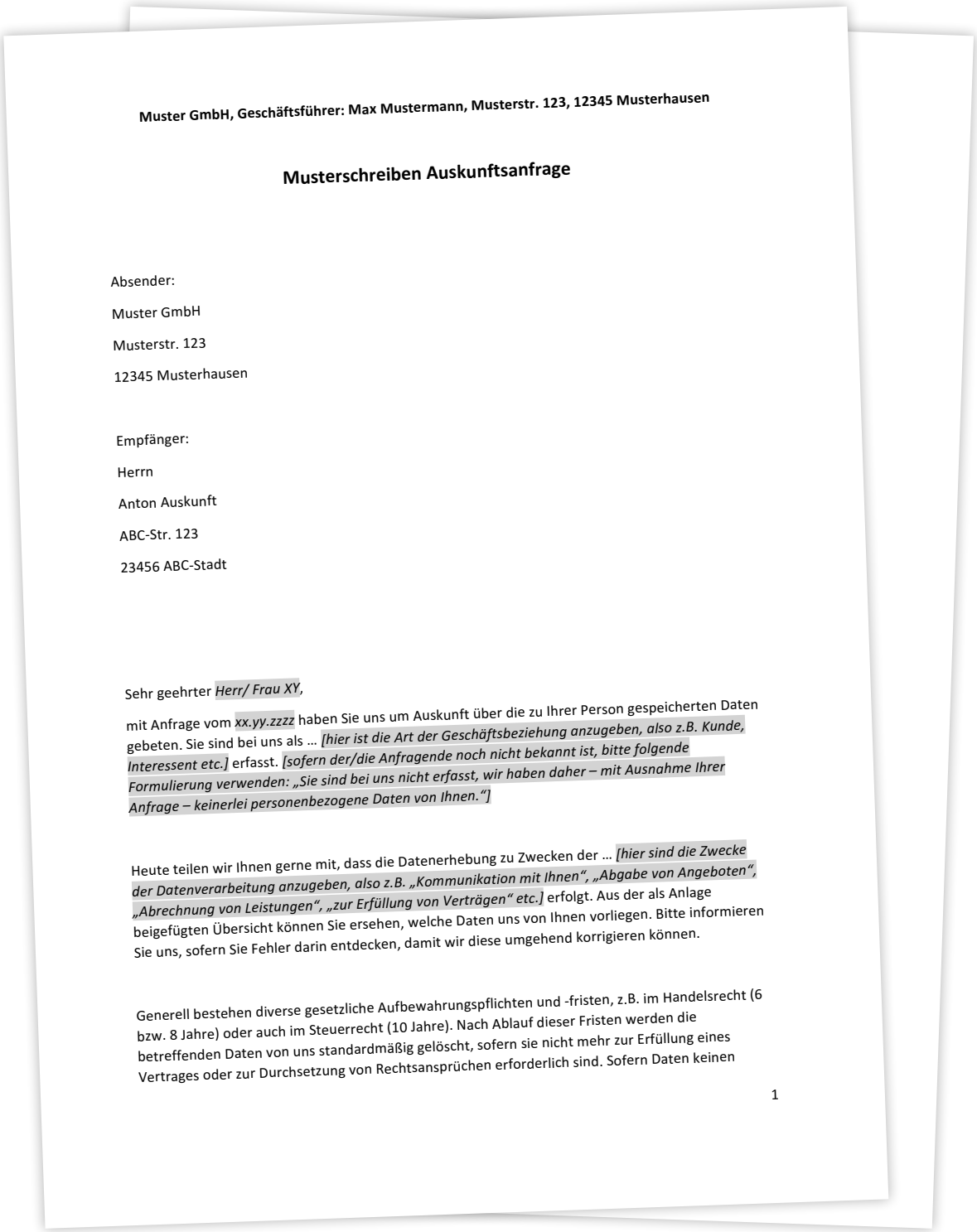
- Anrede, Titel, Vorname, Nachname
- Anschrift

1

Musterschreiben Auskunftsanfrage

(2-seitiges Word Dokument)

Download: https://www.lexoffice.de/dsgvo-vorlage-4



Muster GmbH, Geschäftsführer: Max Mustermann, Musterstr. 123, 12345 Musterhausen

Musterschreiben Auskunftsanfrage

Absender:

Muster GmbH

Musterstr. 123

12345 Musterhausen

Empfänger:

Herrn

Anton Auskunft

ABC-Str. 123

23456 ABC-Stadt

Sehr geehrter *Herr/ Frau XY*,

mit Anfrage vom *xx.yy.zzzz* haben Sie uns um Auskunft über die zu Ihrer Person gespeicherten Daten gebeten. Sie sind bei uns als … *[hier ist die Art der Geschäftsbeziehung anzugeben, also z.B. Kunde, Interessent etc.]* erfasst. *[sofern der/die Anfragende noch nicht bekannt ist, bitte folgende Formulierung verwenden: „Sie sind bei uns nicht erfasst, wir haben daher – mit Ausnahme Ihrer Anfrage – keinerlei personenbezogene Daten von Ihnen.“]*

Heute teilen wir Ihnen gerne mit, dass die Datenerhebung zu Zwecken der … *[hier sind die Zwecke der Datenverarbeitung anzugeben, also z.B. „Kommunikation mit Ihnen“, „Abgabe von Angeboten“, „Abrechnung von Leistungen“, „zur Erfüllung von Verträgen“ etc.]* erfolgt. Aus der als Anlage beigefügten Übersicht können Sie ersehen, welche Daten uns von Ihnen vorliegen. Bitte informieren Sie uns, sofern Sie Fehler darin entdecken, damit wir diese umgehend korrigieren können.

Generell bestehen diverse gesetzliche Aufbewahrungspflichten und -fristen, z.B. im Handelsrecht (6 bzw. 8 Jahre) oder auch im Steuerrecht (10 Jahre). Nach Ablauf dieser Fristen werden die betreffenden Daten von uns standardmäßig gelöscht, sofern sie nicht mehr zur Erfüllung eines Vertrages oder zur Durchsetzung von Rechtsansprüchen erforderlich sind. Sofern Daten keinen

1

lexoffice
just smile

Meine Buchhaltung ist DSGVO sicher!

Datenschutz-Grundverordnung
DSGVO konform

www.lexoffice.de