Organisation

Name (verantwortliche Stelle gem. Art. 30 Abs. 1 Buchst. a DSGVO):
★★★★★★★★★★★★

Straße und Hausnummer:
★★★★★★★★★★★★

PLZ und Ort
95444 Bayreuth

Telefon: 0921-★★★★★★
Telefax: 0921-★★★★★★

E-Mail:
★★★★★★

Koordinator für den Datenschutz:
★★★★★★

Datenschutzbeauftragter

Name (gem. Art. 30 Abs. 1 Buchst. a DSGVO):
★★★★★★★★★★★★

Straße und Hausnummer:
★★★★★★★★★★★★

PLZ und Ort
95444 Bayreuth

Telefon: 0921-★★★★★★
Telefax: 0921-★★★★★★

E-Mail:
★★★★★★

Datum:
01.06.2020

B03 MITARBEITER UND DATENSCHUTZ

03.02 ARBEITSVERHÄLTNIS UND DATENSCHUTZ

01 Erläuterung

02 Formulare

F01 Datenschutzhinweise (Art. 13 DSGVO) für Mitarbeiter

F02 Verpflichtungserklärung für Mitarbeiter auf den Datenschutz

VERSIONSHISTORIE

VERSION	DATUM	AUTOR	BESCHREIBUNG
1.0	01.06.2020	[—]	Initiales Dokument

Firma

★★★★★★

Verpflichtungserklärung für Mitarbeiter

auf den Datenschutz

Vertraulichkeitsverpflichtung

Personenbezogene Daten, also alle Informationen, die sich auf einen benannten oder identifizierbaren Menschen beziehen, dürfen nicht unbefugt erhoben, genutzt, weitergegeben oder sonst verarbeitet werden.

Ich verpflichte mich, personenbezogene Daten vertraulich zu behandeln und ausschließlich auf Weisung der Firma ★★★★★★ zu verarbeiten. Soweit die Firma ★★★★★★ personenbezogene Daten im Auftrag eines Dritten verarbeitet, geht eine eventuelle Weisung dieses Dritten im Rahmen der Gesetze vor. Diese Vertraulichkeitsverpflichtung besteht auch nach Beendigung meiner Tätigkeit für die Firma ★★★★★★ fort.

Verstöße gegen meine Vertraulichkeitsverpflichtung können nach Art. 83 der Datenschutz-Grundverordnung (DSGVO), §§ 42 und 43 des Bundesdatenschutzgesetzes (BDSG) und anderen Gesetzen mit Geldbuße bis zu 20.000.000 EUR, Geld- oder Freiheitsstrafe geahndet werden. Eine Verletzung meiner Vertraulichkeitsverpflichtung kann zugleich eine Verletzung arbeitsvertraglicher Pflichten oder spezieller Geheimhaltungspflichten darstellen und beispielsweise zu Abmahnung, fristloser oder fristgerechter Kündigung und/oder Schadensersatzpflichten führen. Gesetzliche Folge von Verstößen gegen meine Vertraulichkeitsverpflichtung können auch Schadensersatzansprüche der Personen, auf die die Daten sich beziehen, gegen mich persönlich sein, für die ich unter Umständen unbeschränkt mit meinem gesamten Vermögen und ohne Möglichkeit einer Restschuldbefreiung in einem Insolvenzverfahren hafte. Sonstige Geheimhaltungsverpflichtungen, etwa aus dem Arbeitsvertrag, bestehen neben dieser Vertraulichkeitsverpflichtung.

_____ _____

Ort, Datum Unterschrift

Ich bestätige, dass ich heute über die Bedeutung meiner Verpflichtung zur Verschwiegenheit über personenbezogene Daten belehrt wurde. Ein Exemplar dieses Formulars sowie ein Merkblatt mit Erläuterungen und dem Text der Art. 29 DSGVO, Art. 83 Abs. 4–6 DSGVO, § 42 Abs. 1 und 2 BDSG und § 43 Abs. 1 und 2 BDSG habe ich erhalten.

_____ _____

Ort, Datum Unterschrift

Merkblatt zur Vertraulichkeitsverpflichtung

Sie werden heute über Ihre Pflichten im Umgang mit personenbezogenen Daten unterrichtet und unterzeichnen eine entsprechende Vertraulichkeitsverpflichtung. Dieses Merkblatt gibt Ihnen die Möglichkeit, das Wichtigste noch einmal nachzulesen. Sollten Sie Fragen haben – insbesondere wenn es darum geht, ob ein bestimmter Umgang mit personenbezogenen Daten erlaubt ist –, zögern Sie nicht, Ihren Vorgesetzten oder den betrieblichen Datenschutzbeauftragten zu fragen.

(1) Datenschutz schützt das Persönlichkeitsrecht

Ihre Vertraulichkeitsverpflichtung dient – wie das gesamte Datenschutzrecht – dem Schutz des Persönlichkeitsrechts derjenigen Menschen, auf die sich die Daten beziehen. Diese Menschen nennt das Gesetz "betroffene Personen". Das können unsere Kunden sein, Ihre Kollegen – oder auch Sie als unser Mitarbeiter.

Das Persönlichkeitsrecht gibt jedem Menschen das Recht, grundsätzlich selbst darüber zu entscheiden, wer was über ihn wissen darf. Beispielsweise darf jeder Kunde selbst entscheiden, wer seinen Wohnort erfahren soll, und Sie dürfen entscheiden, wer Ihren Gesundheitszustand kennen darf. Es ist Ihre Entscheidung, ob das geheim bleibt oder Sie es veröffentlichen.

Ausnahmen, in denen nicht nur der Wille des Betroffenen gilt, muss es natürlich geben – aber jede Ausnahme braucht nach dem Gesetz eine Rechtfertigung. Das kann nach der Regelung in Art. 6 Abs. 1 DSGVO eine Einwilligung der betroffenen Person oder eine gesetzliche Erlaubnis sein. Die wichtigste gesetzliche Erlaubnis gilt für diejenigen Daten, die unbedingt benötigt werden, um einen Vertrag mit der betroffenen Person zu erfüllen. Deshalb darf Ihr Vermieter beispielsweise Ihren Namen speichern, ohne dass Sie einwilligen müssten.

Neben der DSGVO, die in der gesamten Europäischen Union gilt, gibt es auch noch das Bundesdatenschutzgesetz (BDSG), das bestimmte Sonderfälle regelt, insbesondere den Beschäftigtendatenschutz.

(2) Ihre Vertraulichkeitspflichten

Sie müssen personenbezogene Daten nicht nur vertraulich behandeln, Sie dürfen sie zum Beispiel nicht an Dritte weitergeben oder offen herumliegen lassen. Das Gesetz verpflichtet Sie vielmehr dazu, nur dann mit personenbezogenen Daten zu arbeiten, wenn dies erlaubt ist – unabhängig davon, ob Sie diese Daten beispielsweise lesen, notieren, löschen oder weitergeben. Diese Erlaubnis muss einerseits [Unternehmen] als Unternehmen haben, andererseits aber auch Sie persönlich nach unserer unternehmensinternen Aufgabenverteilung. Die gesetzlichen Vertraulichkeitspflichten einzuhalten, ist also auch Ihre ganz persönliche Verpflichtung. Diese Pflicht ergibt sich übrigens bereits aus dem Gesetz (unter anderem Art. 29 DSGVO). Ihre heutige förmliche Verpflichtung zur Vertraulichkeit dient nur dazu, Ihnen deutlich zu machen, wie wichtig diese Pflicht ist.

Bitte beachten Sie: Ihre Vertraulichkeitsverpflichtung gilt zeitlich unbefristet, und zwar selbst dann, wenn Sie nicht mehr für uns tätig sind. Sie gilt gegenüber allen Personen, die nicht dienstlich für die jeweilige Sache zuständig sind – also auch gegenüber allen anderen Kollegen, Ihrer Familie und der Presse.

Wenn Sie mit personenbezogenen Daten arbeiten, müssen Sie sich dabei immer an die Weisungen Ihres Vorgesetzten halten. Die Firma ★★★★★★ verarbeitet ggfs. auch als sog. Auftragsverarbeiter personenbezogene Daten für unsere Kunden. Sollte im Fall von Auftragsverarbeitung Ihr Vorgesetzter Ihnen eine bestimmte Weisung erteilen, unser Kunde aber eine andere Weisung, geht die Weisung unseres Kunden vor, solange unser Kunde nichts Verbotenes verlangt. In ganz besonderen Fällen kann auch ein Gesetz vorschreiben, personenbezogene Daten z. B. an eine Behörde herauszugeben. Widersprüchliche Weisungen und gesetzliche Verarbeitungspflichten sind sehr selten, und die damit verbundenen komplizierten Rechtsfragen werden Sie kaum alleine entscheiden können. Wenden Sie sich daher bitte immer sofort an Ihren Vorgesetzten oder den betrieblichen Datenschutzbeauftragten.

(3) Der Begriff "personenbezogene Daten"

Das Datenschutzrecht gilt für alle "personenbezogenen Daten". Personenbezogene Daten sind Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person, also einen Menschen, beziehen (Art. 4 Nr. 1 DSGVO). Das kann die Angabe sein, dass jemand Mitglied in einem Verein ist, wo er wohnt oder wie viel Geld er auf dem Konto hat.

Personenbezogenes Datum kann aber auch die Angabe sein, dass die Kontonummer 123456 ihren Dispokredit überzogen hat. Denn obwohl hier kein Name genannt wird, ist einfach zu ermitteln, wer Inhaber dieses Kontos ist: Es handelt sich um Angaben zu einer "identifizierbaren" Person. Eine Person ist identifizierbar, wenn man – eigene und fremde – Informationen kombinieren kann und dadurch erfährt, um wen es sich handelt. Das geht sehr viel einfacher als man denkt: So konnten Forscher jeden einzelnen von 1,5 Millionen Menschen eindeutig identifizieren, wenn sie nur wussten, wo er sich zu elf beliebigen Zeitpunkten aufhielt (https://www.taz.de/!5070185/). Auch genügen Geburtsdatum, Postleitzahl und Geschlecht, um 87 Prozent der US-Amerikaner eindeutig zu identifizieren (http://www.chip.de/artikel/Re-Identifizierung-Die-neue-Kunst-der-Datenkraken-3_46575146.html).

Auch wenn Sie selbst denken, dass bestimmte Daten niemandem zuzuordnen sind, dürfen Sie diese deshalb nicht ohne Zustimmung Ihres Vorgesetzten und des betrieblichen Datenschutzbeauftragten an Dritte weitergeben oder veröffentlichen – abgesehen davon, dass es sich auch um Betriebsgeheimnisse handeln könnte, die Sie ebenfalls streng vertraulich behandeln müssen.

(4) Für welche Daten das Datenschutzrecht gilt

Das Datenschutzrecht gilt einerseits für Computer-Daten (wozu auch die Daten vieler technischer Geräte zählen). Wichtig ist aber zu wissen, dass es auch für "die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen" (Art. 2 Abs. 1 DSGVO) gilt, wobei unter Dateisystem jede geordnete Ablage zu verstehen ist (Art. 4 Nr. 6 DSGVO) – etwa eine Patientenkartei auf Papier oder eine alphabetische Sammlung ausgefüllter Formulare. Das Datenschutzrecht gilt zudem auch dann, wenn die Daten später in eine Datei gespeichert werden sollen oder aus einer Datei stammen – etwa eine ausgedruckte Liste mit Kundendaten. Daten von Mitarbeitern oder Bewerbern werden in jeder Form durch das deutsche BDSG geschützt, auch wenn es sich um einen unsortierten Stapel handschriftlicher Notizen handelt, der weggeworfen werden soll.

Die Telefonnummern Ihrer Kinder auf Ihrem Handy dürfen Sie übrigens weiterhin speichern, ohne dass Sie eine Rechtsgrundlage benötigen: solche rein persönlichen oder familiären Tätigkeiten sind von der Geltung des Datenschutzrechts ausgenommen (Art. 2 Abs. 2 lit. c DSGVO).

(5) Unsere und Ihre Pflichten

Wir als Unternehmen und Sie als unser Mitarbeiter dürfen personenbezogene Daten nur dann verarbeiten, wenn es dafür eine Rechtsgrundlage gibt. Art. 4 Nr. 2 DSGVO beschreibt den Begriff der Verarbeitung äußerst weit, so dass er letztlich jeden Kontakt mit personenbezogenen Daten umfasst: "jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung". Als mögliche Rechtsgrundlage nennt Art. 6 Abs. 1 DSGVO eine Einwilligung der betroffenen Person und verschiedene gesetzliche Erlaubnisse.

Für welche Daten es bei welchem Verfahren eine solche Rechtsgrundlage gibt, sagt Ihnen Ihr Vorgesetzter. Bitte beachten Sie: Andere Daten dürfen Sie nicht verwenden. Personenbezogene Daten dürfen zudem nur zu dem jeweils bestimmt festgelegten Zweck verwendet werden. Eine Zweckänderung braucht eine eigene Rechtsgrundlage. Das bedeutet, dass z. B. Kundendaten, die bisher nur für die Vertragsabwicklung verwendet wurden, nicht ohne Weiteres für Werbung genutzt werden dürfen. Auch hier sagt Ihnen Ihr Vorgesetzter, ob eine Zweckänderung erlaubt ist.

Als wichtigste Regel sollten Sie sich hier merken, dass Sie personenbezogene Daten nie aus eigener Entscheidung heraus weitergeben oder für sich selbst nutzen (beispielsweise außerhalb dienstlicher Notwendigkeit lesen) dürfen.

Außerdem müssen personenbezogene Daten geschützt werden, so dass Unbefugte keine Kenntnis von ihnen nehmen und dass sie auch nicht versehentlich verloren gehen können. Deshalb verschlüsseln wir personenbezogene Daten, wenn wir sie über das Internet übertragen müssen, und machen regelmäßig Sicherungskopien (Backups). Das Gesetz verpflichtet uns zu vielen weiteren Sicherheitsmaßnahmen. So dürfen z. B. Ausdrucke mit personenbezogenen Daten oder Datenträger wie CDs, USB-Sticks oder Festplatten keinesfalls einfach weggeworfen oder weggegeben werden, sondern müssen ordnungsgemäß geschreddert oder durch die EDV-Abteilung sicher gelöscht werden.

Dass Sie Ihr Passwort nicht an Kollegen oder Dritte weitergeben oder gar auf einem Zettel an den Computer kleben dürfen, sollte sich von selbst verstehen – es ist Ihr persönliches Passwort, und wenn es jemand missbraucht, sind Sie persönlich dafür verantwortlich (siehe "Folgen von Verstößen").

(6) Rechte der betroffenen Personen

Einer der wichtigsten Aspekte des Persönlichkeitsrechts ist es, zu wissen, was andere über einen wissen. Wenn ein Unternehmen Daten über jemanden sammelt, muss es daher fast immer die betroffene Person informieren. Jeder Mensch kann zudem von jedem Unternehmen eine Kopie der Daten verlangen, die das Unternehmen über ihn gespeichert hat (Art. 15 DSGVO). Dies bedeutet, dass alles, was Sie beispielsweise über einen Kunden notieren, auch schriftlich zu diesem Kunden gelangen kann. Achten Sie deshalb bitte darauf, dass Sie nur Angaben notieren, für die wir auch eine Erlaubnis zum Speichern haben – Ihr Vorgesetzter sagt Ihnen, welche Daten das in Ihrem konkreten Fall sind. Und achten Sie bitte auch darauf, wie Sie es aufschreiben: knapp, neutral und niemals beleidigend o. ä. Das Auskunftsrecht ist ein spezielles Recht des Betroffenen: An andere Personen und Stellen dürfen wir normalerweise keine Auskünfte geben – das wäre eine Übermittlung, für die wir eine Erlaubnis bräuchten.

Benötigen wir bestimmte Daten nicht mehr, müssen wir sie löschen (Art. 17 DSGVO); falsche Daten müssen wir berichtigen (Art. 16 DSGVO). Wenn Sie feststellen, dass nicht mehr benötigte Daten weiterhin gespeichert bleiben, sprechen Sie bitte Ihren Vorgesetzten darauf an. Denn die Speicherung von Daten, die eigentlich zu löschen wären, kann mit Geldbußen bis 20.000.000 EUR oder vier Prozent des weltweiten Jahresumsatzes des gesamten Konzerns – je nachdem, was höher ist – bestraft werden. Zusätzlich haben betroffene Personen einen Anspruch auf Schadensersatz einschließlich Schmerzensgeld für die Verletzung ihres Rechts auf Datenschutz.

Jede betroffene Person kann uns zudem verbieten, ihre Daten für Werbezwecke zu benutzen (Art. 21 Abs. 2, 3 und 5 DSGVO) und hat auch in bestimmten anderen Fällen ein Widerspruchsrecht (Art. 21 Abs. 1 DSGVO). Betroffene Personen haben zudem weitere Rechte, die aber für Sie als Mitarbeiter normalerweise nicht von Bedeutung sind.

Sollte ein Auskunftsersuchen, ein Widerspruch oder ein anderer Wunsch oder Hinweis mit Datenschutzbezug bei Ihnen eingehen, leiten Sie ihn bitte sofort an [den betrieblichen Datenschutzbeauftragten] weiter. Selbstständig dürfen Sie solche Dinge nur bearbeiten, wenn wir Ihnen diese Aufgabe ausdrücklich zugewiesen haben. In Zweifelsfällen fragen Sie den betrieblichen Datenschutzbeauftragten. Beachten Sie bitte, dass auch Behörden oder die Polizei nicht ohne Weiteres Daten von uns erhalten können. Wir benötigen hier einen förmlichen Beschlagnahmebeschluss. In bestimmten Fällen genügt ein förmliches Auskunftsersuchen. Wenn Sie von der Polizei oder einer anderen Behörde kontaktiert werden, informieren Sie bitte sofort Ihren Vorgesetzten und den betrieblichen Datenschutzbeauftragten.

(7) Folgen von Verstößen

Verstöße gegen das Datenschutzrecht können für die Firma ★★★★★★ schwerwiegende Folgen haben – aber auch für Sie persönlich.

Fast alle Verstöße gegen das Datenschutzrecht können mit Geldbuße bestraft werden (Art. 83 DSGVO). Diese Geldbuße kann bis zu 20.000.000 EUR pro Verstoß betragen oder für uns als Unternehmen bis zu vier Prozent des weltweiten Jahresumsatzes des gesamten Konzerns, je nachdem, was höher ist. Geldbußen können sogar gegen einzelne Mitarbeiter verhängt werden: Geben Sie beispielsweise ohne eine entsprechende Anweisung von der Firma ★★★★★★ personenbezogene Daten weiter oder nutzen Sie sie für Ihre eigenen Zwecke, können Sie persönlich mit einer Geldbuße bis zu 20.000.000 EUR bestraft werden. Zudem sind bestimmte Verstöße gegen das Datenschutzrecht Straftaten, die mit Gefängnis bestraft werden können (§ 42 BDSG): Beispiel: Jemand verkauft weisungswidrig eine Festplatte mit personenbezogenen Daten anstatt sie zu zerstören.

Verstöße gegen das Datenschutzrecht können zudem nach anderen Gesetzen strafbar sein, z. B. nach § 23 GeschGehG (Verletzung von Geschäftsgeheimnissen), § 202 a StGB (Ausspähen von Daten) oder § 263 a StGB (Computerbetrug).

Jede betroffene Person kann Schadensersatz für eine unzulässige Verarbeitung ihrer Daten verlangen, und zwar einschließlich Schmerzensgeld für die Persönlichkeitsrechtsverletzung (Art. 82 DSGVO, §§ 823 ff. BGB). Unter Umständen müssen Sie persönlich diesen Schadensersatz ganz oder teilweise bezahlen, wenn Sie mittlere oder schwere Verstöße begangen oder personenbezogene Daten weisungswidrig verarbeitet haben, etwa für Ihre eigenen Zwecke genutzt haben. Fragen Sie daher lieber einmal zu viel als zu wenig.

Schwere Schäden für die Firma ★★★★★★ kann es verursachen, wenn eine so genannte Datenpanne öffentlich bekannt wird. Kunden und Geschäftspartner verlieren das Vertrauen, wenn sie nicht sicher sein

können, dass ihre Daten bei uns in guten Händen sind. Hinzu kommt, dass wir nach Art. 34 Abs. 1 und Abs. 3 lit. c DSGVO verpflichtet sein können, eine Datenpanne allen Betroffenen mitzuteilen oder gar öffentlich bekanntzumachen. Bitte helfen Sie mit, dass es niemals dazu kommt.

Nicht zuletzt können wir arbeitsrechtliche Konsequenzen ziehen, wenn Sie gegen Ihre Vertraulichkeitspflichten verstoßen. Denkbar sind je nach Schwere Ihres Fehlverhaltens insbesondere eine Abmahnung, eine fristgerechte Kündigung oder sogar eine fristlose Kündigung ohne vorherige Verwarnung.

(8) Neue Verfahren mit personenbezogenen Daten

Sie sind an einem Projekt beteiligt, bei dem personenbezogene Daten eine Rolle spielen? Dann sorgen Sie bitte dafür, dass der betriebliche Datenschutzbeauftragte von Anfang an einbezogen wird. Er kann Ihnen sagen, ob es überhaupt rechtlich möglich ist, was Ihr Projektteam plant, und Tipps geben, was Sie verbessern könnten, insbesondere, welche Anforderungen wir zu "Privacy by Design" und "Privacy by Default" (Art. 25 DSGVO) oder zur Sicherheit (Art. 32 DSGVO) einhalten müssen. Wenn Sie diese Fragen rechtzeitig mit dem betrieblichen Datenschutzbeauftragten klären, können Sie von Anfang an das richtige Verfahren entwickeln. Wenn Sie ihn erst kurz vor Schluss einbeziehen, kann es sein, dass Ihr Projekt komplett scheitert, weil es rechtlich nicht oder nur unter aufwendigen Änderungen umzusetzen ist. Außerdem sind Sie nach Art. 38 Abs. 1 DSGVO verpflichtet, den betrieblichen Datenschutzbeauftragten ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden, unter Umständen eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchzuführen und das Verfahren zum Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO anzumelden. Werden Dritte eingeschaltet, etwa weil wir den Server nicht selbst betreiben, müssen besondere Verträge abgeschlossen werden (Art. 28 DSGVO). Wichtig ist, dass wir als Unternehmen jederzeit beweisen können, dass wir das Gesetz vollständig einhalten (Art. 5 und 24 DSGVO). Können wir diesen Nachweis nicht vollständig erbringen, haften wir auf Schadensersatz und Geldbußen – und auch Sie persönlich, wenn Sie das Verfahren ohne Genehmigung eingeführt haben.

(9) Besondere Hinweise für Nutzer von Internet und E-Mail

Internet und E-Mail sind sehr praktisch, weil man innerhalb von Sekunden Daten ans andere Ende der Welt schicken kann. Gerade diese Geschwindigkeit macht sie aber auch so risikoreich. Hinzu kommt, dass das Internet als Medium zur Kommunikation zwischen Wissenschaftlern erfunden wurde, die sich gegenseitig absolut vertrauen konnten. Deshalb gibt es standardmäßig keine Sicherheitsmaßnahmen. Das ist heute nicht mehr angemessen und eine große Gefahr für vertrauliche Daten. Denn eine E-Mail ist eigentlich nichts anderes als eine elektronische Postkarte, die vom Wind durch die Stadt getrieben und immer wieder von allen möglichen Leuten aufgehoben, angeschaut und wieder in die Luft geworfen wird. Deshalb beachten Sie bitte folgende Grundregeln:

Vertrauliche Daten dürfen Sie niemals per normaler E-Mail versenden. Wenn die EDV-Abteilung Ihren Computer mit einem Programm zur E-Mail-Verschlüsselung ausgestattet hat und der Empfänger der E-Mail ebenfalls solch ein Programm verwendet, können Sie ihm eine verschlüsselte Nachricht schicken, die gegen Abhören und Manipulation geschützt ist. Bitte prüfen Sie aber in jedem Fall vorher, ob Sie die Daten überhaupt an den Empfänger weitergeben dürfen!

Bevor Sie eine E-Mail versenden, achten Sie bitte unbedingt darauf, ob der richtige Empfänger im Adressfeld steht. Hier liegt eine große Fehlerquelle, wenn mehrere Leute einen ähnlichen Namen oder eine ähnliche E-Mail-Adresse haben. Schauen Sie vor dem Abschicken noch einmal genau darauf! Durch solche Verwechslungen sind schon extrem vertrauliche Informationen an die Öffentlichkeit gekommen.

Beachten Sie den Unterschied zwischen "To:/An:" (Empfänger), "CC:" (Kopie) und "BCC:" (Blindkopie): Jeder Empfänger der E-Mail sieht sämtliche anderen Empfänger, die im To:- bzw. CC:-Feld stehen. Soll ein Empfänger für die anderen nicht sichtbar sein, müssen Sie ihn ins BCC:-Feld schreiben. Die Daten aller To:-/CC:-Empfänger übermitteln Sie im rechtlichen Sinne an die anderen Empfänger. Und dafür benötigen Sie, wie Sie wissen, eine Erlaubnis. Wenn Sie Nachrichten an viele Empfänger senden müssen, sprechen Sie deshalb bitte mit der EDV-Abteilung, ob dafür eine Mailing-Liste o. ä. eingerichtet werden sollte, oder ob die Versendung über das BCC:-Feld ausreichend ist. Es wurden bereits Bußgelder gegen Mitarbeiter verhängt, die alle Empfänger ins To:-Feld geschrieben haben!

Sie dürfen niemals vertrauliche Daten an Ihren privaten E-Mail-Account weiterleiten oder woanders als auf unseren Servern speichern – insbesondere nicht in der "Cloud". Dies bedeutet unter anderem, dass Sie auch keinesfalls eine automatische Weiterleitung Ihres E-Mail-Accounts an Ihre private E-Mail-Adresse einrichten dürfen.

Sie werden möglicherweise E-Mails erhalten, die Sie im Namen der Firma ★★★★★★ oder einem anderen Unternehmen auffordern, auf einen Link in der E-Mail zu klicken oder eine bestimmte Seite aufzurufen und dort Ihr Passwort oder andere Daten einzugeben. Tun Sie dies niemals! Es handelt sich bei diesen Mails um gefälschte, sog. Phishing-Mails, die darauf abzielen, Ihre Passwörter, Zugangsdaten oder sonstige vertrauliche Informationen "abzufischen". Selbst wenn Sie in der E-Mail persönlich angesprochen werden oder gar Bezug auf bestimmte Personen oder Umstände genommen wird, hat dies nichts zu sagen – diese Daten wurden wahrscheinlich bereits zuvor gestohlen, im Zweifel durch einen erfolgreichen Phishing-Angriff auf einen Ihrer Kollegen. Melden Sie derartige E-Mails bitte immer sofort an die EDV-Abteilung per [Nachricht – Weiterleiten als Anhang].

Vertrauen Sie nicht zu sehr auf E-Mails. Absenderangaben von E-Mails lassen sich problemlos fälschen – vertrauen können Sie nur digital signierten und verschlüsselten E-Mails, falls Sie ein entsprechendes Programm von der EDV-Abteilung erhalten haben. Seien Sie daher bitte auch sehr vorsichtig, wenn Sie unaufgefordert E-Mails mit Anhängen (Attachments) erhalten: Oftmals enthalten diese Anhänge Schadprogramme (Viren). Wir versuchen, Viren so gut wie möglich auszufiltern, dass sie überhaupt nicht in Ihrem Postfach ankommen – aber die Kriminellen sind uns häufig ein Stück voraus. Bevor Sie einen solchen Anhang öffnen, fragen Sie bitte im Zweifel bei der EDV-Abteilung nach per [Nachricht – Weiterleiten als Anhang]. Seien Sie auch misstrauisch, wenn vermeintlich Ihr Vorgesetzter per E-Mail intern besondere Vertraulichkeit für ein angebliches besonderes Projekt verlangt. Fragen Sie lieber noch einmal auf einem anderen Kommunikationskanal – im Zweifel im persönlichen Gespräch – nach.

Bitte ändern Sie nicht die Einstellungen, insbesondere die Sicherheitseinstellungen, Ihrer Programme. Die EDV-Abteilung hat sich etwas bei der Konfiguration gedacht. Wenn Sie Änderungsvorschläge haben, sprechen Sie diese bitte mit der EDV-Abteilung ab – vielleicht können ja alle Mitarbeiter von Ihrer Idee profitieren.

Wortlaut der Gesetze

Art. 4 DSGVO Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

(1) "personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden "betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt der indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

(2) "Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

(3) […]

Artikel 5 DSGVO Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a. auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden ("Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz");

b. für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken ("Zweckbindung");

c. dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein ("Datenminimierung");

d. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden ("Richtigkeit");

e. in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden ("Speicherbegrenzung");

f. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen ("Integrität und Vertraulichkeit");

(2) […]

Artikel 32 Abs. 4 DSGVO Sicherheit der Verarbeitung

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

§ 42 BDSG neu

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht

und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.

§ 43 BDSG neu

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 30 Absatz 1 ein Auskunftsverlangen nicht richtig behandelt oder
2. entgegen § 30 Absatz 2 Satz 1 einen Verbraucher nicht, nicht richtig, nicht

vollständig oder nicht rechtzeitig unterrichtet.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

§ 202a Strafgesetzbuch (StGB) Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§202b StGB Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c StGB Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach ä 202a oder Q 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen,

oder

2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

§ 202d StGB Datenhehlerei

(1) Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

§ 23 GeschGehG Verletzung von Geschäftsgeheimnissen

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen,

1. entgegen § 4 Absatz 1 Nummer 1 ein Geschäftsgeheimnis erlangt,
2. entgegen § 4 Absatz 2 Nummer 1 Buchstabe a ein Geschäftsgeheimnis nutzt oder offenlegt oder
3. entgegen § 4 Absatz 2 Nummer 3 als eine bei einem Unternehmen beschäftigte Person ein Geschäftsgeheimnis, das ihr im Rahmen des Beschäftigungsverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Beschäftigungsverhältnisses offenlegt.

(2) Ebenso wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen, ein Geschäftsgeheimnis nutzt oder offenlegt, das er durch eine fremde Handlung nach Absatz 1 Nummer 2 oder Nummer 3 erlangt hat.

(3) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs oder aus Eigennutz entgegen § 4 Absatz 2 Nummer 2 oder Nummer 3 ein Geschäftsgeheimnis, das eine ihm im geschäftlichen Verkehr anvertraute geheime Vorlage oder Vorschrift technischer Art ist, nutzt oder offenlegt.

(4) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer

1. in den Fällen des Absatzes 1 oder des Absatzes 2 gewerbsmäßig handelt,
2. in den Fällen des Absatzes 1 Nummer 2 oder Nummer 3 oder des Absatzes 2 bei der Offenlegung weiß, dass das Geschäftsgeheimnis im Ausland genutzt werden soll, oder
3. in den Fällen des Absatzes 1 Nummer 2 oder des Absatzes 2 das Geschäftsgeheimnis im Ausland nutzt.

(5) Der Versuch ist strafbar.

(6) Beihilfehandlungen einer in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Person sind nicht rechtswidrig, wenn sie sich auf die Entgegennahme, Auswertung oder Veröffentlichung des Geschäftsgeheimnisses beschränken.

(7) § 5 Nummer 7 des Strafgesetzbuches gilt entsprechend. Die §§ 30 und 31 des Strafgesetzbuches gelten entsprechend, wenn der Täter zur Förderung des eigenen oder fremden Wettbewerbs oder aus Eigennutz handelt.

(8) Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

§ 2 Begriffsbestimmungen GeschGehG

Im Sinne dieses Gesetzes ist

1. Geschäftsgeheimnis

   eine Information

   a) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und

   b) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und

   c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht;

2. Inhaber eines Geschäftsgeheimnisses

   jede natürliche oder juristische Person, die die rechtmäßige Kontrolle über ein Geschäftsgeheimnis hat;

3. Rechtsverletzer

   jede natürliche oder juristische Person, die entgegen § 4 ein Geschäftsgeheimnis rechtswidrig erlangt, nutzt oder offenlegt; Rechtsverletzer ist nicht, wer sich auf eine Ausnahme nach § 5 berufen kann;

4. rechtsverletzendes Produkt

   ein Produkt, dessen Konzeption, Merkmale, Funktionsweise, Herstellungsprozess oder Marketing in erheblichem Umfang auf einem rechtswidrig erlangten, genutzten oder offengelegten Geschäftsgeheimnis beruht.

§ 4 GeschGehG Handlungsverbote

(1) Ein Geschäftsgeheimnis darf nicht erlangt werden durch

1. unbefugten Zugang zu, unbefugte Aneignung oder unbefugtes Kopieren von Dokumenten, Gegenständen, Materialien, Stoffen oder elektronischen Dateien, die der rechtmäßigen Kontrolle des Inhabers des Geschäftsgeheimnisses unterliegen und die das Geschäftsgeheimnis enthalten oder aus denen sich das Geschäftsgeheimnis ableiten lässt, oder
2. jedes sonstige Verhalten, das unter den jeweiligen Umständen nicht dem Grundsatz von Treu und Glauben unter Berücksichtigung der anständigen Marktgepflogenheit entspricht.

(2) Ein Geschäftsgeheimnis darf nicht nutzen oder offenlegen, wer

1. das Geschäftsgeheimnis durch eine eigene Handlung nach Absatz 1
   a) Nummer 1 oder
   b) Nummer 2
2. erlangt hat,
3. gegen eine Verpflichtung zur Beschränkung der Nutzung des Geschäftsgeheimnisses verstößt oder
4. gegen eine Verpflichtung verstößt, das Geschäftsgeheimnis nicht offenzulegen.

(3) Ein Geschäftsgeheimnis darf nicht erlangen, nutzen oder offenlegen, wer das Geschäftsgeheimnis über eine andere Person erlangt hat und zum Zeitpunkt der Erlangung, Nutzung oder Offenlegung weiß oder wissen müsste, dass diese das Geschäftsgeheimnis entgegen Absatz 2 genutzt oder offengelegt hat. Das gilt insbesondere, wenn die Nutzung in der Herstellung, dem Anbieten, dem Inverkehrbringen oder der Einfuhr, der Ausfuhr oder der Lagerung für diese Zwecke von rechtsverletzenden Produkten besteht.