- Anlage 3 -

Verpflichtungserklärung zum Datengeheimnis

Aufgrund Ihrer Aufgabenstellung in unserem Unternehmen gilt für Sie die Verpflichtung zur Vertraulichkeit nach dem neuen Bundesdatenschutzgesetz bzw. der Datenschutzgrundverordnung. Die einschlägigen gesetzlichen Vorschriften verlangen, dass personenbezogene Daten so verarbeitet werden, dass die Rechte der durch die Verarbeitung betroffenen Personen auf Vertraulichkeit und Integrität ihrer Daten gewährleistet werden.

(1) Daher ist es Ihnen nur gestattet, personenbezogene Daten in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der Ihnen übertragenen Aufgaben erforderlich ist. Nach diesen Vorschriften ist es untersagt, personenbezogene Daten unbefugt oder unrechtmäßig zu verarbeiten oder absichtlich oder unabsichtlich die Sicherheit der Verarbeitung in einer Weise zu verletzen, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder zum unbefugtem Zugang führt.

(2) Mit dieser Erklärung verpflichten Sie sich, personenbezogene Daten vertraulich zu behandeln und ausschließlich auf Weisung zu verarbeiten.

(3) Diese Vertraulichkeitserklärung besteht auch über das Ende Ihrer Tätigkeit in unserem Unternehmen hinaus.

(4) Die afm Datenschutzrichtlinie in der aktuellsten Fassung, verfügbar über das afm BeraterPortal, findet unmittelbar Anwendung und ist integraler Bestandteil der vorliegenden Verpflichtungserklärung.

(5) Eine Verletzung Ihrer Vertraulichkeitsverpflichtung kann zugleich eine Verletzung arbeitsvertraglicher Pflichten oder spezieller Geheimhaltungspflichten darstellen und beispielsweise zu Abmahnung, fristloser oder fristgerechter Kündigung und/oder Schadensersatzpflichten führen.

(6) Sonstige Geheimhaltungsverpflichtungen, etwa aus dem Arbeitsvertrag, bestehen neben dieser Vertraulichkeitsverpflichtung.

(7) Verstöße gegen diese Verpflichtungserklärung auf Vertraulichkeit bzw. die Datenschutzvorschriften können ggf. mit Geldbuße, Geldstrafe oder Freiheitsstrafe geahndet werden. Entsteht der betroffenen Person durch eine unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden, kann ein Schadenersatzanspruch entstehen. Abschriften der einschlägigen Vorschriften der DSGVO bzw. des BDSG n.F. im Anhang zur afm Datenschutzrichtlinie.

Ihre Verpflichtung auf Vertraulichkeit haben Sie hiermit zur Kenntnis genommen. Mit Ihrer Unterschrift bestätigen Sie zugleich, dass Sie eine Kopie der Verpflichtungserklärung sowie das Merkblatt zur Verpflichtungserklärung erhalten haben.

Ort, Datum	Arbeitnehmer

Merkblatt zur Verpflichtungsvereinbarung

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.

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 DS-GVO 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.

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 müssen einerseits die Unternehmen der afm Unternehmensgruppe 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). Die 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.

In ganz besonderen Fällen kann auch ein Gesetz vorschreiben, personenbezogene Daten z. B. an eine Behörde herauszugeben.

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.

Ein 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.

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 DS-GVO).

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 oder sich auf mobilen Datenträgern befinden, 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 vernichtet 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“).

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. 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 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 Datenschutzbeauftragten weiter. Selbstständig dürfen Sie solche Dinge nur bearbeiten, wenn wir Ihnen diese Aufgabe ausdrücklich zugewiesen haben. 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 oder den Datenschutzbeauftragten.

Folgen von Verstößen
Verstöße gegen das Datenschutzrecht können für unser Unternehmen 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 vom Arbeitgeber personenbezogene Daten weiter oder nutzen Sie sie für Ihre eigenen Zwecke, können Sie persönlich mit einer Geldbuße 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 § 17 UWG (Verrat von Geschäfts- und Betriebsgeheimnissen), § 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 unser Unternehmen kann es verursachen, wenn eine so genannte Datenpanne öffentlich bekannt wird. Kunden verlieren das Vertrauen und kaufen nicht mehr bei uns, 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.

Besondere Hinweise
Beachten Sie bitte unsere afm Datenschutzrichtlinie nebst Anlagen sowie die Social-Media-Guideline. All diese Richtlinien enthalten auch Regelungen zur Sicherheit und sind für Sie verbindlich.

Datenschutz | Bestätigung

Die Daten der Kunden und Partner sind ein wichtiger Wettbewerbsfaktor und tragen in großem Umfang zur Wertschöpfung der afm Gruppe bei. Diese Daten sind gegen Gefährdungen eines unzulässigen Zugriffs zu schützen. Neben diesem technischen Schutz erwarten die Kunden und Partner aber auch generell einen sorgsamen Umgang mit ihren Daten. Ohne eine vertrauensvolle Beziehung zu den Kunden und Partnern sind dauerhafte Geschäftsbeziehungen nicht realisierbar.

afm bekennt sich zu seiner Verantwortung im Umgang mit den Daten und gibt sich mit diversen Richtlinien einen einheitlichen Datensicherheitsstandard für die Verarbeitung personenbezogener Daten von Kunden und Partnern. Diese unterstützen die Wettbewerbsfähigkeit des Konzerns und stellt eine Basis für eine dauerhafte und vertrauensvolle Geschäftsbeziehung dar. So ist gewährleistet, dass das von der Europäischen Datenschutzrichtlinie (DSGVO) und den nationalen Gesetzen (bspw. BDSG n.F.) ausgehende und verlangte Schutzniveau gewahrt bleibt.

Name, Vorname	Anschrift

Hiermit bestätige ich, dass ich:

- ☐ die afm Richtlinien (u. a. Datenschutzrichtlinie, Verhaltensregeln zum Datenschutz, SocialMedia Guideline) zur Kenntnis genommen habe und diese in meinem täglichen Arbeitsprozess Anwendung finden.
- ☐ die Regeln zur Verschlüsselung mobiler Datenträger/Endgeräte umgesetzt und alle meine im Geschäftsprozess genutzten Geräte nach aktuellem Stand der Technik verschlüsselt (Datenverschlüsselung) sowie mit einem Zugangscode/Passwort (bei Smartphones mindestens Zahlencode) versehen habe.
- ☐ meine Mitarbeiter auf die Einhaltung der Richtlinien zum Datenschutz hingewiesen habe.
- ☐ von mir beauftragte externe Unternehmen (z. B. Hausmeister- oder Putzservice), sofern diese Zutritt zu den Büroräumlichkeiten haben, zur Wahrung des Datenschutzes verpflichtet habe.

Ort, Datum

Unterschrift