**Anlage 1: Verpflichtungserklärung gemäß § 5 des Bundesdatenschutzgesetzes (BDSG) (Datengeheimnis)**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Name und Anschrift der Firma)

Sehr geehrte(r) Frau/Herr \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Sie werden hiermit über die einschlägigen Vorschriften des Bundesdatenschutzgesetzes in Kenntnis gesetzt, über die sich daraus ergebenden besonderen Anforderungen an die Datensicherheit und den Datenschutz bei der Ausübung Ihrer Tätigkeit (insbesondere der Sorgfalts- und Geheimhaltungspflichten) vertraut gemacht sowie auf das Datengeheimnis (§ 5 BDSG) verpflichtet.

Sie werden insbesondere darüber belehrt, dass es Ihnen untersagt ist, geschützte personenbezogene Daten zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu erheben, zu verarbeiten oder zu nutzen. Die Weitergabe personenbezogener Daten an Dritte ist generell verboten. Alle Unterlagen mit personenbezogenen Daten sind so zu verwahren, dass sie vor dem Zugriff Unbefugter geschützt sind. Die Verpflichtung zur Wahrung des Datengeheimnisses bezieht sich auf alle zu natürlichen Personen gehörenden Angaben über deren persönliche und sachliche Verhältnisse und gilt ohne Rücksicht darauf, ob die personenbezogenen Daten in automatisierten oder in nicht automatisierten (manuellen) Verfahren verarbeitet werden. Diese Verpflichtung besteht auch nach Beendigung Ihrer Tätigkeit fort. Darüber hinaus haben Sie alle sonstigen in unserem Unternehmen erlassenen Datenschutz- und Datensicherheitsanweisungen zu befolgen. Verstöße gegen das Datengeheimnis können sowohl arbeitsrechtlich als auch gemäß §§ 44, 43 Abs. 2 BDSG und anderen Strafvorschriften mit Freiheits- oder Geldstrafe geahndet werden. Sie können auch Anlass zu einer außerordentlichen Kündigung sein. Ihre sich aus Arbeitsvertrag und -ordnung ergebende Geheimhaltungsverpflichtung wird durch diese Verpflichtung nicht berührt. Sie bestätigen mit Ihrer Unterschrift, dass Sie einen Abdruck dieser Verpflichtungserklärung, ein Merkblatt zum Datenschutz und Erläuterungen zu den Datenschutzgesetzen erhalten haben.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_

Ort, Datum

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Unterschrift Verpflichteter)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Unterschrift Verpflichtender)

**Merkblatt zur Verpflichtung auf das Datengeheimnis**

Sehr geehrte/r Frau/Herr \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

es ist sicher nicht in Ihrem Sinne, wenn Daten über Ihre Person und über Ihre persönlichen Verhältnisse Unbefugten zur Kenntnis gelangen würden. Davor schützen Sie das Bundesdatenschutzgesetz und andere bereichsspezifische Datenschutzregelungen.

Aber auch Sie sind im Rahmen Ihrer beruflichen Tätigkeit in unserem Unternehmen dazu verpflichtet, die personenbezogenen Daten anderer vertraulich und weisungsgerecht zu behandeln. Sie sind dafür verantwortlich, dass die Ihnen anvertrauten personenbezogenen Daten nur im Rahmen Ihrer Aufgabenstellung erhoben, verarbeitet (gespeichert, verändert, übermittelt, gesperrt, gelöscht) oder genutzt werden. Der Missbrauch dieser Daten und jede unbefugte Handlung sind unzulässig und strafbar.

Sie handeln unbefugt, wenn Sie personenbezogene Daten, entgegen dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck erheben, verarbeiten oder nutzen. Eine missbräuchliche Nutzung der anvertrauten Daten liegt auch dann vor, wenn die im beruflichen Bereich bekannt gewordenen Angaben zu privaten Zwecken verwendet werden. Insbesondere sind Sie persönlich dafür verantwortlich, dass die Ihnen anvertrauten Daten und Datenträger, wenn Sie nicht unmittelbar daran arbeiten, unter Verschluss gehalten werden, Ihr DV-Gerät, Ihre Anwendungen und Ihr Passwort keinem Unbefugten zugänglich werden, nicht mehr benötigte personenbezogene Datenträger datenschutzgerecht vernichtet werden, damit eine missbräuchliche Weiterverwendung nicht möglich ist, und die sonstigen angeordneten unternehmensinternen technischen und organisatorischen Datensicherungsmaßnahmen eingehalten werden.

Es ist Ihnen untersagt, unternehmenseigene DV-Geräte privat zu nutzen oder private Computer, Software oder Datenträger in die Firma einzubringen, da sonst eine wirksame Kontrolle des Datenschutzes nicht möglich ist. Erläuterungen zu den Datenschutzgesetzen enthält das Ihnen ebenfalls übergebene gleichnamige Informationsblatt. Auch nach Beendigung Ihrer Tätigkeit besteht das Datengeheimnis fort (§ 5 BDSG). Zum Datengeheimnis zählen alle personenbezogenen Informationen, die Ihnen während ihrer Tätigkeit zur Kenntnis gelangen. Bei Fragen zum Datenschutz oder in Zweifelsfragen wenden Sie sich bitte an Ihre Vorgesetzten oder – in besonderen Fällen – an den externen betrieblichen Datenschutzbeauftragten unseres Unternehmens.

**Merkblatt zum Datenschutz**

Hinweis: Der Übersichtlichkeit wegen werden im Folgenden nur die männlichen Formen verwendet!

Beim Umgang mit personenbezogenen Daten müssen neben anderen Gesetzen und Vorschriften hauptsächlich die Bestimmungen des Bundesdatenschutzgesetzes BDSG beachtet werden. Verantwortliches Handeln beim Umgang mit personenbezogenen Daten, aber auch die risikobewusste Nutzung von IT-Systemen und -Anwendungen sind die zentralen Zielsetzungen. Fehlverhalten kann zu großen materiellen und immateriellen Schäden mit teilweise beträchtlichen negativen Kundeneffekten führen.

Zweck des BDSG ist es, den Einzelnen davor zu schützen, dass durch den Umgang mit seinen personenbezogenen Daten seine Persönlichkeitsrechte beeinträchtigt werden.

**Kernaussagen des Bundesdatenschutzgesetzes (BDSG)**

**Gültigkeit**

Das Gesetz gilt u.a. für alle sogenannten „nicht-öffentlichen Stellen“. Das sind alle Unternehmen, Vereine oder sonstigen Vereinigungen, aber auch Niederlassungen ausländischer Unternehmen unabhängig von der Rechtsform. Die gesetzlichen Regelungen betreffen die Erhebung, Verarbeitung und Nutzung personenbezogener Daten.

**Begriff „Personenbezogene Daten“ (§ 3 Abs. 1 BDSG)**

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, gleichgültig ob Mitarbeiter, Kollege oder Kunde bzw. Lieferant oder deren Ansprechpartner [Betroffener]. Also alle Angaben, die zu einer identifizierbaren Person gehören, z.B. Adresse, Telefonnummer, Geburtsdatum, Foto, Arbeitgeber, Gehalt, Vermögen, Besitz, Urlaubsplanung, Arbeitsverhalten, Arbeitsergebnisse. Auch Daten ohne direkten Personenbezug (z.B. ohne Namensangabe) können personenbezogene Daten sein, wenn aus ihnen auf die zugehörigen Personen Bezug genommen werden kann (z.B. Personalnummer, PC-Benutzerkennung, maschinenbezogene Nutzungszeiten bei nur einem infrage kommenden Benutzer).

**Ausnahmen vom Verbot, mit personenbezogenen Daten umzugehen**

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Die Daten müssen für die Zwecke, für die sie erhoben und verarbeitet werden z.B. im Rahmen eines Vertrags, relevant sein, müssen sachlich richtig sein und dürfen nur so lange gespeichert werden, wie es der genannte Zweck erfordert. Unrichtige oder unvollständige Daten sind zu löschen oder zu berichtigen. Nur in gesetzlich bestimmten Fällen oder mit Einwilligung des Betroffenen ist eine anderweitige Verarbeitung zulässig.

**Einwilligung**

Die Einwilligung des Betroffenen ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf meistens der Schriftform, und ggf. ist eine optische Hervorhebung erforderlich. Für bestimmte Daten im Rahmen der Internet-Kommunikation ist auch eine elektronische Einwilligung zulässig. Die Einwilligung für besondere Kategorien personenbezogener Daten (besonders sensible Daten) ist gesondert erforderlich.

**Begriff Besondere Kategorien**

Besondere Kategorien personenbezogener Daten sind Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, das Sexualleben oder strafrechtliche Verurteilungen. Hier gelten besondere Vorschriften!

**Rechte des Betroffenen**

Jeder, dessen personenbezogene Daten verarbeitet werden, hat gegenüber der speichernden Stelle grundsätzlich das Recht auf Auskunft über gespeicherte Daten, Zweck und Rechtsgrundlage der Speicherung sowie Herkunft und Empfänger von Übermittlungen. Unzutreffende Daten sind zu berichtigen, unzulässig gespeicherte oder nicht mehr erforderliche Daten zu löschen.

Wenn jemandem durch eine unrechtmäßige automatisierte Verarbeitung seiner personenbezogenen Daten ein Schaden zugefügt wird, ist ihm Schadenersatz zu gewähren.

Jedermann hat das Recht, sich unmittelbar an die Datenschutzaufsichtsbehörde zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten in seinen Rechten verletzt zu sein; dies gilt auch für Beschäftigte in Unternehmen.

**Datensicherheit durch entsprechende technische und organisatorische Maßnahmen**

Das Gesetz verlangt die Umsetzung angemessener technischer und organisatorischer Maßnahmen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten. Obwohl üblicherweise Ihr Arbeitgeber die notwendigen Maßnahmen organisiert, ist jeder einzelne Mitarbeiter für die Umsetzung mitverantwortlich. Richtiges Verhalten gemäß Arbeitsvertrag und Arbeits-/Dienstanweisung ist unabdingbar. Einige ausgewählte Anforderungen sind im Folgenden dargestellt:

Zutritt: Unbefugten ist der Zutritt zu den Rechneranlagen, Servern und PCs, auf denen personenbezogene Daten verarbeitet werden, zu verwehren. Art und Umfang der notwendigen Sicherungsmaßnahmen zur Zutrittskontrolle richten sich nach der Sensibilität und der Menge der gespeicherten Daten.

Zugriff auf Daten und Informationen in einem Netzwerk oder auf EDV-Anlagen/PCs darf nur berechtigten Personen ermöglicht werden. Durch Benutzerkennung und Passwort werden die Systeme durch den Arbeitgeber entsprechend geschützt. In Ihrer Verantwortung liegt aber der vertrauliche und sorgfältige Umgang mit Ihren Zugangsberechtigungsdaten (Passwort).

Weitergabe von Daten und Informationen: Es ist sicherzustellen, dass Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Obwohl zahlreiche betriebliche Vorkehrungen getroffen sind, bleiben Sie als Mitarbeiter auch für die Umsetzung dieser Vorschrift mitverantwortlich dafür, Gefährdungen zu verhindern. Ein Beispiel ist die Weitergabe von USB-Sticks oder CD-ROMs mit Daten.

**Übermittlung in Nicht-EU/EWR-Staaten**

Die Übermittlung in Nicht-EU/EWR-Staaten ist nur bei sehr beschränkten Ausnahmen zulässig.

Verpflichtung zur Wahrung des Datengeheimnisses

Allen Mitarbeitern, die dienstlichen Zugang zu personenbezogenen Daten haben, ist es untersagt, solche Daten unbefugt zu verarbeiten oder zu nutzen; dies gilt auch nach Beendigung Ihrer Tätigkeit. Deshalb wurden Sie gemäß § 5 BDSG auf die zu beachtenden Vorschriften über den Datenschutz verpflichtet.

Zuwiderhandlungen gegen das BDSG sind mit Bußgeld, mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe belegt.

**Allgemeine Verhaltensregeln beim Umgang mit Daten:**

Es gelten vorrangig die Dienstanweisungen!

* Nur sichere Passwörter auswählen (z.B. mit Sonderzeichen, keine Namen) und regelmäßig wechseln.
* Bildschirme und PCs sind bei Abwesenheit vom Arbeitsplatz zu sperren.
* Laptops bei Reisen sorgfältig sichern, besonders im Auto, im Hotel und auf Flughäfen.
* Keine vertraulichen Informationen per Fax schicken, falls doch erforderlich, besondere Vorkehrungen treffen (z.B. telefonische Absprache wegen Anwesenheit des Empfängers, Doppelkontrolle der Richtigkeit der eingegebenen Fax-Nummer vor Versand).
* Nicht einfach mit Antwortfunktion auf E-Mail mit vertraulichem Inhalt reagieren, vorher Absenderlisten überprüfen! (Achtung: Vertrauliche Informationen über E-Mail grundsätzlich nicht versenden, wenn keine Verschlüsselung genutzt werden kann).
* Vertrauliche Telefonate nicht mit dem Handy in der Öffentlichkeit führen.

**Straftatbestände**

Bestimmte Handlungen, die einen Verstoß gegen das Datengeheimnis beinhalten, werden durch das Strafgesetzbuch mit Strafe bedroht. Insbesondere die Straftatbestände der §§ 303a („Datenveränderung“), 303b („Computersabotage“), 202a („Ausspähen von Daten“) und 263a StGB („Computerbetrug“) kommen hier infrage. Danach kann bestraft werden, wer rechtswidrig Daten verändert oder beseitigt, wer den Ablauf der Datenverarbeitung stört, wer sich oder einem Dritten unbefugt besonders gesicherte Daten aus fremden Datensystemen verschafft und wer fremdes Vermögen durch unbefugtes Einwirken auf einen Datenverarbeitungsvorgang schädigt.