# Vorschlag für eine schriftliche Verpflichtung der Mitarbeiter

## zur Datensicherheit und zur verantwortungs- und kostenbewussten Nutzung der Informationstechnologie des Unternehmens

Der Autor des nachfolgenden Formulierungsvorschlags war mit folgender Problematik konfrontiert:

- Er betreut mittelständige Unternehmen, die aufgrund ihrer Größe keinen professionellen Administrator beschäftigen können.
- Diese Unternehmen müssen E-Mail und das Internet von Monat zu Monat intensiver nutzen, die Unternehmensleiter scheuen andererseits die zunehmenden Risiken, die der Zugang zum Internet für ihre Informationstechnologie mit sich bringt, wie Computerviren, Spam-Mails, Spionage und Sabotage.
- Die Unternehmensleiter stehen vor der Frage, ob und wie weit sie den Mitarbeitern die Nutzung von E-Mails und Internet gestatten sollen. Insbesondere beschäftigt sie die Frage, welche zusätzlichen Aufwendungen die private Mitnutzung des Internets durch die Mitarbeiter verursacht werden und welche Grenzen gezogen werden sollen.

Als Hilfestellung bot der Autor den Entscheidungsträgern Muster-Betriebsvereinbarungen zur Nutzung von E-Mail und Internet an, wie man sie im Internet findet, z.B. auf den Internetforen von Gewerkschaften. Dieses führte jedoch nicht zu greifbaren Ergebnissen, da die angebotenen Muster-Betriebsvereinbarungen zu wenig auf mittelständische Unternehmen abgestimmt sind und selten konsequent ausformulierte Regelungen enthalten.

Der Autor stellte fest, dass nicht nur die Risiken des Internets für Unternehmen schwer kalkulierbar sind. Durch die zunehmende Digitalisierung von Zeichnungen (CAD), Schriftverkehr, Belegen aller Art, Fotos und Filmen steigt das Datenaufkommen auf den Servern immens an. Gleichzeitig sind die Mitarbeiter jedoch oft unzureichend darin geschult, die Daten auf den Servern strukturiert abzulegen. Als Folge werden Dokumente teils in persönlichen Verzeichnissen abgelegt, teils in chaotischen Verzeichnisstrukturen in den Gruppenverzeichnissen der Server, wobei sich in der Regel niemand um passende Zugriffsrechte kümmert.

Da sich niemand für das zunehmende Datenchaos auf den Servern verantwortlich fühlt, kommt es zu Wildwuchs, Redundanzen und Dateninkonsistenzen. Die zunehmende Datenmenge führt jedoch bei Speicherengpässen nicht dazu, dass konsequent auf den Servern aufgeräumt wird. Stattdessen wird das Problem vertagt, indem weitere oder größere Festplatten angeschafft werden. Als Folge muss bald in die Sicherungs- und Archivierungstechnologie investiert werden, um das Mehr an Speicherkapazität sichern zu können.

Der Autor erkannte, dass diese Unternehmen eine organisatorische Hilfestellung benötigen, die nicht nur die Risiken der Nutzung des Internets umfasst, sondern darüber hinaus den kostenbewussten und verantwortlichen Umgang der Mitarbeiter mit der gesamten Informationstechnik beinhaltet. Er formulierte daraufhin eine konsequente „Verpflichtung der Mitarbeiter zur Datensicherheit und zur verantwortungs- und kostenbewussten Nutzung der Informationstechnologie". Diese legt er den Entscheidungsträgern mit der Empfehlung vor, sie zu diskutieren und auf das Unternehmen anzupassen. Als Ergebnis sollte eine Verpflichtungserklärung verabschiedet werden, die später von allen Mitarbeitern zu unterschreiben sei und als Anlage zum Arbeitsvertrag abgeheftet werden würde.

Obwohl die vom Autor vorgeschlagene Verpflichtungserklärung äußerst konsequent formuliert

war (Sie beinhaltete z.B. ein prinzipielles Verbot von privaten E-Mails und privaten Dateibeständen auf den Servern.), wurde sie von den Entscheidungsträgern mit nur geringen Änderungen übernommen und im Betrieb umgesetzt. Der Autor führt das darauf zurück, dass die Entscheidungsträger mit der technischen Problematik überfordert waren und die vorgeschlagene Verpflichtungserklärung den Entscheidungsträgern geeignet erschien, die Ziele des Unternehmens schnell zu erreichen:

- produktive Nutzung des Internets bei kalkulierbaren Risiken
- Eindämmung des Daten-Wildwuchses auf den Servern
- eindeutige und überschaubare Datenstrukturen für alle Mitarbeiter
- klare Berechtigungsstrukturen
- kalkulierbarere Kosten bezüglich des Ausbaus und der Wartung der Informationstechnik

Eine Verpflichtungserklärung zum verantwortungs- und kostenbewussten Umgang mit der Informationstechnologie ersetzt kein technisches Sicherheitskonzept, welches die Einrichtung von Firewalls, die redundante Auslegung wichtiger Hardwarekomponenten, die Erstellung von Sicherheitsrichtlinien, ein Sicherungskonzept, einen Wiederanlaufplan und vieles mehr beinhaltet. Die als Muster zu verstehende Verpflichtungserklärung ist vielmehr eine flankierende Maßnahme, um die Mitarbeiter bezüglich der Probleme Datensicherheit, Datenschutz und Kosten der Informationstechnologie zu sensibilisieren. Die Zusammenstellung von Regelungen für eine Mitarbeiter-Verpflichtungserklärung und deren Ausformulierung erhebt nicht den Anspruch der Vollständigkeit oder Absolutät. Sie ist eher als Stoffsammlung zu verstehen, die auf den Betrieb zugeschnitten und erweitert werden muss.

Der Autor Ulrich Schlüter veröffentlichte beim Verlag Galileo Computing das Buch „Integrationshandbuch Microsoft-Netzwerk" (ISBN 3-89842-402-2).
➔ http://www.galileocomputing.de/katalog/buecher/titel/gp/titelID-634

Der Bundesverband Informationstechnologien, Telekommunikation und neue Medien (Bitkom) bietet eine Publikationen zum Thema "privaten Internetnutzung am Arbeitsplatz" unter www.bitkom.org an, die die rechtlichen Grundlagen erörtert und ebenfalls Musterformulierungen enthält.

## Motivationsgründe für eine Verpflichtungserklärung

Die Motivationsgründe sollten den Mitarbeitern zusammen mit der zu unterschreibenden Verpflichtungserklärung mündlich oder per Rundschreiben unterbreitet werden, damit die Notwendigkeit der Maßnahme durch die Mitarbeiter eingesehen und mitgetragen wird.

1. Die Gefahren der Lahmlegung der EDV durch Computerviren, Spam-Mails (Überschwemmung der Server mit nicht gewollter Werbung), „trojanische Pferde" (Spionage-Attacken) und Hackerangriffe sind in letzter Zeit drastisch gestiegen, wie man aus den öffentlichen Medien weiß. Die Antivirenhersteller als auch die Hersteller von Betriebssystemen, Anwendungssoftware und Dienstprogrammen wie z.B. Microsoft, Symantec oder NAI kommen im Wettlauf mit den Virenprogrammierern und Hackern kaum noch nach, die Software wirkungsvoll zu schützen. Ebenso sind IT-Verantwortliche kaum mehr in der

Lage, die ständig wachsenden Gefahrenpotentiale zu überblicken, das Ausmaß der Gefahren richtig einzuschätzen, frühzeitig geeignete Gegenmaßnahmen zu ergreifen oder im Falle eines gelungenen Angriffs den Schaden gezielt in Grenzen zu halten und zu beseitigen.

2. Diese Gefahren bedrohen nicht nur die informationstechnischen Einrichtungen, die EDV und Telefonanlagen, wobei die Telefonanlagen heute oft durch EDV gesteuert werden und von einem Ausfall der Software ebenfalls betroffen sind. Aufgrund der Bedeutung der Informationstechnologie (IT) für das Tagesgeschäft können diese Gefahren die Existenz des Unternehmens in Frage stellen. Ein Ausfall der IT zieht immense Kosten nach sich, da viele Mitarbeiter gar nicht oder nur eingeschränkt weiterarbeiten können, wenn die EDV oder die Telefonanlage nicht oder nur in begrenztem Umfang zur Verfügung stehen. Damit sind dann schnell Fertigstellungstermine gefährdet, was wiederum Konventionalstrafen nach sich ziehen kann und außerdem den Ruf des Unternehmens schädigt.
3. Der Schutz der EDV vor den Gefahren aus dem Internet und vor interner Spionage zieht immer größere Kosten nach sich: Firewall, Lizenzen für Antivirensoftware, notwendige Doppeltauslegung von Datenspeichern zur Ausfallsicherheit usw. Gleichzeitig steigen in vielen Unternehmen die elektronisch zu speichernden Datenmengen oft nicht linear, sondern exponentiell an. Leider verursachen wachsende digitale Datenmengen im Gegensatz zu wachsenden Auftragsvolumina vorwiegend Kosten und keine Erträge.
4. Die zu speichernden Datenmengen verursachen Mengenprobleme, Strukturierungsprobleme und Archivierungsprobleme und damit Kosten:
   - Wie können die beim einzelnen Sachbearbeiter anfallenden Daten so abgelegt werden, dass die Datenstruktur auch von Dritten schnell überblickt wird und einzelne Dokumente schnell wieder auffindbar sind?
   - Wie können verschiedene Versionsstände von Dokumenten oder CAD-Zeichnungen unterschieden werden, so dass jeder Zeit eindeutig ist, welcher Versionsstand zu welchem Zeitpunkt aktuell oder rechtsverbindlich war?
   - Wie können die Daten über Nacht komplett und kostengünstig auf Sicherungsbändern gesichert werden, damit beim Ausfall eines Servers die Daten auf einem Ersatzserver innerhalb akzeptabler Zeit wieder verfügbar gemacht werden können.
   - Welche Daten können wann auf externe Medien ausgelagert und archiviert werden, damit die verbleibenden Datenbestände bezüglich ihrer Menge wartbar bleiben (Kosten der Speicherung und der täglichen Sicherung) und die Gesamtdatenstruktur für die Mitarbeiter überschaubar bleibt.
5. Die Gründe für den exponentiellen Anstieg der EDV-Daten sind unter anderem folgende:
   - Es fallen immer mehr speicherintensive Daten in Form von Zeichnungen (CAD), digitalen Bildern, digitalen Filmen usw. an.
   - Die Betriebssysteme als auch die Anwendungssoftware werden immer aufwendiger und damit auch speicherintensiver.
   - Das E-Mail-Aufkommen wächst überproportional stark an, weil die Kommunikation mit Kunden, Lieferanten und natürlich mit Kollegen immer mehr über E-Mails abgewickelt wird. Mit E-Mails werden aber oft speicherintensive Dateianhänge verschickt.

Diese Dateianhänge werden von den Empfängern zwar in der Regel irgendwo auf dem Server abgespeichert und weiterverarbeitet. Jedoch wird die ursprüngliche E-Mail mitsamt dem ursprünglichen Dateianhang oft nicht gelöscht. Dadurch sind die Daten dann doppelt gespeichert: auf dem E-Mail-Server und auf dem Dateiserver.

- Faxe werden ebenfalls über Computer verschickt und sowohl die versendeten als auch die empfangenen Faxe auf Servern gespeichert.
- Mitarbeiter arbeiten intensiv mit dem Internet und speichern die dort gewonnenen Informationen auf den Servern ab. Diese im Internet gewonnenen Informationen sind oft reichlich illustriert und deshalb speicherintensiv.
- Hinzu kommt, dass es in der Regel für den einzelnen Benutzer keine Speicherbegrenzungen auf den Servern des Unternehmens gibt und die Kosten des belegten Speicherplatzes nicht den verursachenden Kostenstellen zugewiesen werden. Hatte früher ein Mitarbeiter eine beschränkte Raumgröße in seinem Büro zur Verfügung, um seinen in Papierform ein- und ausgehenden Schriftverkehr abzulegen, und war er für die Ordnung seiner Dokumentenablage selbst verantwortlich, so übergibt der Mitarbeiter heute seine elektronischen Akten dem Server, ohne sich Gedanken machen zu müssen, wie viel Platz und Kosten diese elektronischen Dokumente verursachen und wer sich um deren Sicherung und spätere Archivierung kümmert. Besonders in kleinen und mittelständigen Unternehmen gibt es aber oft keine Mitarbeiter, die sich hauptberuflich und professionell mit den Folgeproblemen dieser Verlagerung der Daten von Papier auf zentrale digitale Speicher kümmern können.

## Schlussfolgerung

Waren bis vor wenigen Jahren die Kosten für einen privaten Computer nebst Drucker, Scanner oder digitaler Kamera hoch und ein privater Internetzugang mit E-Mail nur für wenige EDV-Interessierte erschwinglich, so besitzt heute fast jeder private Haushalt einen Computer mit umfassender digitaler Peripherie sowie einen Internetzugang nebst E-Mail-Erreichbarkeit. Damit ist es aber zukünftig weder notwendig noch wünschenswert, dass Mitarbeiter ihre privaten Internetgeschäfte in die Arbeitszeit verlagern, private digitale Dokumente auf den Speicherplatten des Arbeitgebers speichern oder den Arbeitsplatzcomputer missbrauchen, um private Software oder Computerspiele aus dem Internet durchzutesten. Da die Gefahren des unkontrollierten Internetsurfens sowie privater, eventuell virenverseuchter E-Mails und die Kosten, die die Speicherung und Sicherung dieser zusätzlichen, nicht unternehmensrelevanten Daten verursachen, nicht tragbar sind, sollte aus Gründen der Gleichbehandlung aller Mitarbeiter die private Nutzung der Unternehmens-Informationstechnologie prinzipiell verboten werden.

Gleichzeitig müssen die Mitarbeiter jedoch auch angehalten werden, mit den Ressourcen der Informationstechnologie sparsam, kostenbewusst und sinnvoll umzugehen. Dabei handelt es sich weniger um eine technische Herausforderung, sondern um organisatorische Maßnahmen zur eindeutigen Bezeichnung und Strukturierung der Dateien und der Verzeichnisse. Unter anderem sollte sichergestellt werden, dass Redundanzen (mehrfache Speicherorte derselben Datenbestände) vermieden werden und im Vertretungsfall (Abwesenheit wegen Krankheit oder Kur) und beim Ausscheiden eines Mitarbeiters Dokumente auffindbar sind.

**Ergänzung zum Anstellungsvertrag vom** *(Datum)*

**Verpflichtung zur Datensicherheit und zur verantwortungs- und kostenbewussten Nutzung der informationstechnischen Einrichtungen des Unternehmens**

Die Sicherheit und der Fortbestand unseres Unternehmens sind in hohem Maße vom fehlerfreien Funktionieren der technischen Einrichtungen, speziell auch der informationstechnischen Einrichtungen abhängig. Dazu gehören die elektronische Datenverarbeitung (EDV) und die Telefonanlage. Durch Computerviren, Spionage und Sabotage sind diese Einrichtungen besonders gefährdet. Unsachgemäße Nutzung, bewusster und unbewusster Missbrauch der informationstechnischen Einrichtungen erhöhen nicht nur das Gefährdungspotential. Sie verursachen erhebliche Mehrkosten für Wartung und Reparatur, für die Speicherung der anfallenden digitalen Daten, deren tägliche Sicherung und Archivierung und für die ausfallsichere Auslegung der informationstechnischen Komponenten. Außerdem müssen laut Datenschutzgesetz personenbezogene Daten von Mitarbeitern, Kunden und Lieferanten besonders geschützt werden.

Um die Sicherheit und den Schutz der informationstechnischen Einrichtungen und der gespeicherten Daten zu gewährleisten und die Kosten der Informationstechnologie in akzeptablen Grenzen zu halten, ist es notwendig, dass alle Mitarbeiter unseres Unternehmens mit den informationstechnischen Einrichtungen verantwortungs- und kostenbewusst umgehen. Die nachfolgend aufgeführten Regelungen sind von allen Mitarbeitern einzuhalten. Mit seiner Unterschrift erkennt sie der Mitarbeiter an:

1. Im EDV-Netzwerk des Unternehmens und besonders auf allen Servern, Computern und Laptops dürfen nur Softwareprodukte installiert und genutzt werden, die von der Geschäftsleitung bzw. vom Leiter der Abteilung Informationstechnologie genehmigt wurden und die rechtmäßig lizenziert wurden. Ausnahmen von dieser Regelung (z.B. der Testbetrieb neuer Software oder aktualisierter Softwareversionen) bedürfen der Genehmigung des Leiters der EDV.
2. Die Installation von Software darf ausschließlich durch Personen erfolgen, die durch die Geschäftsführung damit beauftragt wurden. Insbesondere gelten folgende Regelungen:
   - Betriebssysteme, Anwendungsprogramme, Updates und Hotfixes dürfen nur von Beauftragten der Geschäftsleitung installiert werden.
   - Mitarbeiter dürfen ohne Befugnis keine fremde Software aus dem Internet herunterladen oder auf anderem Weg auf Computern des Unternehmens installieren. Dazu gehören auch Bildschirmschoner, Demoprogramme, Computerspiele oder Utilities.
   - Ohne besondere Genehmigung dürfen keine fremden Programme direkt aus dem Internet oder aus E-Mail-Anhängen gestartet werden.
   - Alle Datenbestände, die von außerhalb des Firmengeländes (z.B. auf externen Datenträgern wie Festplatten, Disketten, CDs, DVDs, Memory-Sticks etc.) kommen, müssen durch das aktuelle Antivirenprogramm des Unternehmens überprüft werden, bevor sie verwendet werden.
3. Unbefugten Personen dürfen weder von zugekaufter noch von im Unternehmen selbst erstellter Software Kopien erstellen. Die Lizenzbedingungen von Softwareherstellern sind einzuhalten.
4. Passwörter dürfen nicht offen einsehbar hinterlegt werden, weder als Notiz in den Büros der Mitarbeiter noch als Datei auf Computern oder Datenträgern. Wichtige administrative Passwörter müssen in einem versiegelten Umschlag im Tresor des Unternehmens hinterlegt werden. Passwörter dürfen unter keinen Umständen an Dritte weitergegeben werden.
5. Unternehmensinterne Daten dürfen nur mit Genehmigung der Geschäftsleitung das

Firmengelände verlassen oder außerhalb des Firmengeländes verwendet werden. Insbesondere dürfen ohne Zustimmung der Geschäftsleitung firmeninterne Datenbestände, speziell Adressbestände, Kundendaten oder Produktdaten, weder mittels E-Mail oder Fax noch mittels anderer Datenträger (Laptop, Diskette, CD, DVD, Memory-Stick, externe Festplatte etc.) oder in ausgedruckter Form außer Haus gebracht werden.

6. Der Mitarbeiter sichert zu, dass er alle ihm im Rahmen des Vertragsverhältnisses und seiner Tätigkeit bekannt gewordenen Daten, Informationen und Dokumente über die Angelegenheiten des Unternehmens, seiner Mitarbeiter, Lieferanten, Kunden und sonstigen Kontakte zeitlich unbegrenzt, insbesondere auch über die Dauer des Vertragsverhältnisses hinaus, streng vertraulich behandelt und geheim hält. Er versichert, dass er derartige Informationen Dritten nicht zugänglich machen oder sonst zum eigenen oder fremden Nutzen preisgeben wird, außer in Erfüllung seiner vertraglichen Pflichten. Zieht der Mitarbeiter im Auftrage des Unternehmens Dritte zur Mitarbeit hinzu, ist er verpflichtet, diesen die gleiche Verschwiegenheitspflicht aufzuerlegen.
7. Mitarbeiter dürfen nicht versuchen, auf Bereiche des LANs oder WANs vorzudringen, die nicht für den Mitarbeiter und sein Aufgabengebiet freigegeben oder vorgesehen sind, auch dann nicht, wenn es durch unzureichende Rechtevergabe oder technische Mängel möglich ist. Über derartige fehlerhafte Rechtevergabe oder technische Mängel ist der Vorgesetzte oder die EDV-Abteilung ohne Verzug zu informieren.
8. Bei Verdacht auf Virengefahr, Datenspionage oder anderer Umstände, die die Sicherheit der Informationstechnologie des Unternehmens betreffen, ist unverzüglich ein Vorgesetzter oder der EDV-Beauftragte des Unternehmens zu informieren.
9. Störungen und Defekte bei informationstechnischen Einrichtungen und auftretende Fehler in der Software sind unverzüglich den dafür verantwortlichen Personen zu berichten.
10. Mitarbeiter, die mit der Datensicherung beauftragt sind, haben diese Aufgaben mit besonderer Sorgfalt durchzuführen und müssen andere Vorgesetzte bzw. den EDV-Verantwortlichen unverzüglich informieren, wenn Probleme aufgetreten sind oder Gefahr im Verzug ist.
11. Jeder Mitarbeiter ist angehalten, die technischen Einrichtungen pfleglich zu behandeln und mit den informationstechnischen Ressourcen sparsam umzugehen. Das betrifft auch den Verbrauch von Speicherplatz auf den Servern und von Verbrauchmaterialien wie Druckerpapier, Druckfolien, Druckerpatronen usw.
12. Betriebsdaten müssen generell so gespeichert werden, dass bei Ausfall eines Mitarbeiters dessen Vertretung oder der Vorgesetzte auf diese Daten zugreifen kann. Für die Speicherung von Betriebsdaten ist das persönliche Verzeichnis, auf das nur der einzelne Mitarbeiter über sein Passwort zugreifen kann, nicht geeignet. Betriebsdaten wie Word- oder Exceldateien sollten vielmehr in Gruppenverzeichnissen abgelegt werden. Damit bei Ausfall eines Mitarbeiters diese Daten von anderen Mitarbeitern gefunden werden, muss die Ordnerstruktur im Gruppenverzeichnis auf dem/den Servern ständig mit den zuständigen Kollegen abgesprochen werden. Namen für Ordner oder Dokumente sollen eindeutig gewählt werden, damit Dokumente auch von Kollegen schnell geortet werden können.
13. Jeder Mitarbeiter ist angehalten, nicht mehr benötigte Dateien und E-Mails regelmäßig zu löschen und damit dazu beizutragen, dass die Datenbestände und deren Strukturen überschaubar bleiben und die Kosten der Datenhaltung und Datensicherung in vertretbaren Grenzen bleiben. Dazu gehört auch, dass sich die Mitarbeiter regelmäßig die EDV-Verantwortlichen informieren, welche Datenbestände auf externe Medien (CD-ROM, DVD usw.) ausgelagert werden können.
14. Verlässt ein Mitarbeiter/eine Mitarbeiterin befristet (Mutterschaftsurlaub, Kur) oder unbefristet

(Kündigung, Rente) das Unternehmen, so ist er/sie angehalten, nicht mehr benötigte Datenbestände und E-Mails zu löschen und die verbleibenden Datenbestände an einen Kollegen/eine Kollegin zu übergeben. Vorgesetzte sind angehalten, die ordnungsgemäße Übergabe von Datenbeständen sicherzustellen.

15. Die informationstechnischen Einrichtungen, besonders E-Mail und der Zugriff auf das Internet, dürfen prinzipiell nicht für private Zwecke gebraucht werden. Auf den Computern dürfen prinzipiell keine privaten Daten gespeichert werden.

    Alternativ kann folgende abgeschwächte Formulierung verwendet werden:
    Die Mitarbeiter und Mitarbeiter sind angehalten, nach Möglichkeit keine oder nur begrenzt private Daten (Dokumente, digitale Fotos etc.) auf den Computern zu speichern, da Speicherplatz und dessen Sicherung auf Sicherungsbändern kostenintensiv ist. Der Zugriff auf pornografische oder politisch radikale Internetinhalte ist generell verboten. Prinzipiell darf nur auf Internetinhalte zugegriffen werden, die zur Erledigung der Aufgaben nützlich sind. Das unnötige Surfen im Internet und Herunterladen von Internetinhalten, die nicht bereits im Netz vorhanden sind und/oder die für private Zwecke benötigt werden, ist verboten. Die Mitarbeiter sind verpflichtet, die durch die Nutzung des Internets auftretenden Kosten (Provider- und Leitungskosten) minimal zu halten und das Internet nach Durchsicht der für die Erfüllung der Aufgaben benötigten Internetinhalte zügig wieder zu verlassen, um unnötige Leitungskosten zu vermeiden. Ein Zuwiderhandeln wird wie die unnötige Verschwendung von Arbeitsmaterialien oder Betriebsmitteln betrachtet.

16. Da die Existenz des Unternehmens in hohem Maße von der Funktionsfähigkeit der informationstechnischen Einrichtungen abhängig ist, kann ein fahrlässiger Verstoß gegen eine oder mehrere der vorgenannten Regeln als Anlass für eine Beendigung des Beschäftigungsverhältnisses dienen, ohne dass es einer zusätzlichen Abmahnung bedarf.

17. Ferner haftet derjenige Mitarbeiter/diejenige Mitarbeiterin, welcher/welche gegen die genannten Regeln verstößt, zivilrechtlich für die dadurch entstehenden Schäden nach den gesetzlichen Regeln in unbegrenzter Höhe.

**Verpflichtung nach § 5 Bundesdatenschutzgesetz (BDSG) und § 2 Abs. 2 Datenschutzgesetz Nordrhein-Westfalen (DSG NW)**

Herr/Frau _____ *(Name)* _____ *(Vorname)*
ist nach § 5 BDSG/§ 2 Abs. 2 DSG NW auf das Datengeheimnis verpflichtet und auf die Strafbarkeit einer Geheimnisverletzung nach § 43 BDSG ausdrücklich hingewiesen worden.

Nach § 5 BDSG ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen. Die Verpflichtung bezieht sich auf alle zu einer natürlichen Person gehörenden Angaben über deren persönliche und sachliche Verhältnisse. Die Verpflichtung auf das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

Nach § 43 BDSG wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind

- speichert, verändert oder übermittelt,
- zum Abruf mittels automatisierten Verfahrens bereithält oder
- abruft oder sich oder einem anderen aus Dateien verschafft.

Ebenso wird bestraft, wer

- die Übermittlung von durch dieses Gesetz geschützten personenbezogenen Daten, die nicht offenkundig sind, durch unrichtige Angaben erschleicht,
- entgegen §§ 16 Abs. 4 Satz 1, 28 Abs. 4 Satz 1 BDSG, auch in Verbindung mit §§ 29 Abs. 3, 39 Abs. 1 Satz 1 oder 40 Abs. 1 BDSG die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder
- entgegen § 30 Abs. 1 Satz 2 BDSG die in § 30 Abs. 1 Satz 1 BDSG bezeichneten Merkmale oder entgegen § 40 Abs. 3 Satz 3 BDSG die in § 40 Abs. 3 Satz 2 BDSG bezeichneten Merkmale mit den Einzelangaben zusammenführt.

Handelt der Täter gegen Entgelt oder in der Absicht, einen anderen zu schädigen oder sich oder einen anderen zu bereichern, so ist die Strafe eine Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

Zum Schutz personenbezogener Daten ist im Rahmen der zugewiesenen Aufgabe die notwendige Sorgfalt anzuwenden. Bestehende Vorschriften über den Umgang bzw. die Sicherung personenbezogener Daten sind zu beachten. Festgestellte Mängel sind möglichst umgehend zu melden.

Sonstige Geheimhaltungspflichten bleiben durch diese Verpflichtung unberührt.

| | |
|---|---|
| *(Ort/Datum)* | *(Unterschrift des Verpflichteten)* |