**Dienstvereinbarung**

**zwischen …**

**, vertreten durch** …,

**und**

**der Mitarbeitervertretung des …, vertreten durch den Vorsitzenden**

Gemäß § 38 Abs. 1 Nr. 11 MAVO wird die nachfolgende Dienstvereinbarung über die Einführung und den Einsatz von EDV-Hard- und Software in einem Computernetzwerk, einer Telefonanlage sowie weiteren technischen Einrichtungen, die geeignet sind Mitarbeiter zu überwachen, geschlossen.

# Präambel

Die Dienstvereinbarung will gewährleisten, dass die EDV für Dienstgeber und Mitarbeiter[[1]](#footnote-1) nutzbar gemacht und die Anforde­rungen des Arbeits-, Gesundheits- und Datenschutzes sowie die Einhaltung der Bestimmungen der MAVO sicher­gestellt werden.

Die eingesetzte EDV-Anlage dient dem Zweck einer rationel­len und effizienten Abwicklung von Arbeitsprozessen und Ge­schäftsvorgängen in der Einrichtung.

Dienstgeber und Mitarbeitervertretung sind sich einig, dass die EDV-Anlage als Mittel zur Arbeitsunterstützung und nicht zur Leistungs- und Verhaltenskontrolle verwendet wird.

# § 1 Geltungsbereich

1. Diese Dienstvereinbarung bezieht sich auf den Einsatz von Anlagen zur elektronischen Datenverarbeitung in der Einrichtung, die mit Hilfe des Netzwerkes zusam­mengeschlossen sind. Diese sind im Folgenden als EDV-An­lage bezeichnet.

2. Sie bezieht sich weiterhin auf alle technischen Einrichtungen, welche Daten der Mitarbeiter automatisch erfassen und speichern.

Hierunter fallen insbesondere Telefonanlagen und die Protokollierungsfunktion von EDV-Programmen.

3. Sie gilt für alle Mitarbeiter, die in der Einrichtung arbeiten.

4. Diese Dienstvereinbarung gilt nicht für Arbeitszeiterfassungssysteme.

# § 2 Grundsätze

Die Datenverarbeitungs- und -erfassungsgeräte genügt folgenden Grundsätzen:

## 1. Grundsätze des Arbeits- und Gesundheitsschutzes

Sämtliche Arbeitsplatzsysteme (d.h. die Computer-Bildschirm-Einheiten) werden gemäß den gesetzlichen und berufsgenos­senschaftlichen Vorschriften ausgestattet und in regelmäßigen Abständen überprüft.

In regelmäßigen Abständen werden Augenuntersuchungen veranlasst.

## 2. Grundsätze des Datenschutzes

Die Nutzung der Datenverarbeitungs- und -erfassungsgeräte ist durch ein Passwort­systemvor Zugriffen nicht berechtigter Personen zu schützen. Näheres, auch den Schutz personenbezogener Daten, regelt die Datenschutz-Ordnung des Bistums Hildesheim.

## 3. Grundsätze im Zusammenhang mit möglichen Leistungs- und Verhaltenskontrollen

Eine Leistungs- und Verhaltenskontrolle durch Datenverarbei­tungs- und -erfassungssysteme findet nicht statt. Die eingesetzten Programme werden nicht darauf ausgerichtet, solche Kontrollen durchzu­führen.

Nutzungsdaten werden nur automatisiert erfasst und soweit es für die technische Betreuung und die Sicherheit des Systems unbedingt erforderlich ist.

Eine anderweitige Verwendung dieser Daten ist nur zur Verfolgung eines begründeten Verdachts einer Straftat mit Zustimmung der Mitarbeitervertretung zulässig.

# § 3 Systembeschreibung (Bestandsaufnahme der Anlage)

Sämtliche Systembestandteile des Hardwarebereiches, ein­schließlich aller Peripheriegeräte sind in der **Anlage1 "Einge­setzte Hardwarekomponenten"** beschrieben. Die Mitarbei­tervertretung erhält mindestens halbjährlich eine aktualisierte Anlage 1.

Eine Auflistung mit Kurzbeschreibung und arbeitsplatzmäßiger Zuordnung aller Softwaremodule ist in der **Anlage 2 "Einge­setzte Programme"** beigefügt. Die Mitarbeitervertretung er­hält mindestens halbjährlich eine aktualisierte Anlage 2.

# § 4 Beteiligungsrechte der MAV

Bei grundsätzlicher Erweiterung der Anlage und dem Einsatz neuer Systemkomponenten oder Programmen wird die Mit­arbeitervertretung beteiligt, wenn damit grundlegende Ände­rungen von Arbeitsmethoden oder Maßnahmen zur Hebung der Arbeitsleistung und zur Erleichterung des Arbeitsablaufes verbunden sind.

# § 5 Inhaltskontrollen und Protokolle

## 1. Schutzmaßnahmen

(a) Zum Schutz des internen Computernetzes vor Angriffen durch Hacker, vor Viren und anderen schädlichen Inhalten fin­den automatisiert Inhaltskontrollen (siehe 2.) und Protokol­lierungen (siehe 3.) des Datenverkehrs statt.

(b) Als Inhaltskontrollen werden ausschließlich durchgeführt:

* Die Kontrolle der empfangenen und zu versendenden E-Mails auf Viren,
* Kontrolle der eingehenden HTTP-Daten (HyperTextTrans­missionProtokoll) auf ActiveX-Controls und Java- Applets.

(c) Protokolliert wird ausschließlich der via Gateway über das Internet abgewickelte Datenverkehr. Die Nutzungen des inter­nen Netzwerks werden nicht protokolliert.

Es werden folgende Daten protokolliert:

1. Kennung des Benutzers und des Rechners, von dem aus zugegriffen wurde,

2. Datum und Uhrzeit des Zugriffs,

3. Menge der übertragenen Daten in Byte,

4. Adresse des Zielrechners, auf den zugegriffen wurde (URL).

Die Protokolldaten werden für einen Zeitraum von einem Mo­nat aufbewahrt und dann (wochenweise) von der EDV-Admi­nistration gelöscht.

(d) Weitere Kontrollmaßnahmen finden nicht statt. Insbeson­dere werden eingehende Informationen (E-Mails und www-Abrufe) nicht anhand von Suchwörtern auf bestimmte Inhalte geprüft.

## 2. Durchführung der Inhaltskontrollen

(a) Die Kontrolle der eingehenden und ausgehenden E-Mails erfolgt ausschließlich automatisiert. Finden sich in eingehen­den E-Mails Viren, wird der Empfänger informiert. Er kann ent­scheiden, ob die E-Mail von der EDV-Administration gelöscht, zurückgesandt oder geöffnet wird. Auf Wunsch wird er dabei hinzugezogen. Es wird ihm erlaubt, zunächst alleine vom In­halt der E-Mail Kenntnis zu erlangen. Nur wenn der Adressat dem zustimmt, darf die EDV-Administration die E-Mail öffnen. Hält der Adressat die E-Mail von Anfang an oder nach einerNachschau für zu persönlich, ist sie nach seiner Wahl ent­weder zurückzuschicken oder zu löschen.

(b) Die Benutzer werden darauf hingewiesen, dass ihnen be­stimmte Funktionen einiger Internetangebote nicht zur Verfü­gung stehen, weil aus Sicherheitsgründen manche ActiveX-Controls und Java-Applets ausgefiltert werden.

## 3. Auswertung der Protokolldaten

Die Protokolldaten dürfen ausschließlich für die im Folgenden aufgeführten Zwecke verwendet werden. Eine nachträgliche Änderung des Zwecks oder eine Verwendung zu anderen Zwecken ist unzulässig.

Für das Erkennen und Beseitigen technischer Probleme, für die Optimierung der Netzlastverteilung, zum Erkennen und zur Abwehr von Angriffen dürfen die oben in Punkt 1, Buchstabe c unter den Nummern 1 bis 4 genannten Protokolldaten verwen­det werden.

Der Zugriff auf diese Daten zu den genannten Zwecken ist nur den mit der Netzwerkadministration betrauten Mitarbeitern gestattet.

## 4. Verwertungsverbot

Wurden Informationen unter Nichtbeachtung der in den Punk­ten 1 bis 3 enthaltenen Bestimmungen gewonnen, dürfen diese nicht verwendet werden.

## 5. Internet-Anschluss für die Mitarbeitervertretung

Die Mitarbeitervertretung erhält einen eigenen E-Mail-An­schluss. Sie erhält die Möglichkeit, sich den Mitarbeiterinnen und Mitarbeitern im hausinternen Netz zu präsentieren.

# § 6 Inkrafttreten und Kündigung

Diese Dienstvereinbarung tritt mit Ablauf des Tages der Unter­zeichnung in Kraft. Sie kann von jeder Vertragspartei mit einer Frist von 6 Monaten zum Ende eines Kalenderjahres gekün­digt werden. Die Kündigung erfolgt schriftlich.

Nach Kündigung werden Verhandlungen über eine neue Dienstvereinbarung aufgenommen. Bis zu deren Abschluss wirkt die vorliegende Dienstvereinbarung im Sinne des § 38 Abs. 4, Satz 1 MAVO nach.

1. Soweit diese Dienstvereinbarung auf natürliche Personen Bezug nimmt, gilt sie für weibliche und männliche Personen in gleicher Weise. [↑](#footnote-ref-1)