Der Diözesandatenschutzbeauftragte

des Erzbistums Hamburg
der Bistümer Hildesheim, Osnabrück und
des Bischöflich Münsterschen Offizialats in Vechta i.O.

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Dienstvereinbarung
über das DV-Verfahren Zeiterfassung, Fehlzeitenüberwachung und Zugangsberechtigung zum Dienstgebäude

(MV 601 - Stand: 07. April 2011)

Dienstvereinbarung

zwischen dem / der

_____

und

der Mitarbeitervertretung im _____

Das _____ und die Mitarbeitervertretung im _____

schließen nach § 38 Mitarbeitervertretungsordnung die folgende Dienstvereinbarung über das Datenverarbeitungsverfahren zur Zeiterfassung am Arbeitsplatz.

1. Geltungsbereich

Diese Dienstvereinbarung regelt den Einsatz eines DV-Verfahrens für Zwecke der Zeiterfassung, Fehlzeitenüberwachung und Zugangsberechtigung. Im übrigen gelten die Vorschriften der Anordnung über den kirchlichen Datenschutz - KDO -.

2. Eingesetzte Verfahren

2.1 Zeiterfassung/Fehlzeitenüberwachung

Das Verfahren ersetzt die bisherige mechanisch/manuelle Zeiterfassung durch Zeiterfassungskarte und Zeitstempler ("Stechkarte" und "Stechuhr") sowie die bisherige gesonderte automatisierte Urlaubs- und Krankheitsüberwachung.

Als Software wird - mit den nachfolgenden Einschränkungen bezüglich der verwendeten Datenarten und Auswertungen das Programm .....

der Firma. .....

eingesetzt. Zur Durchführung der Zeiterfassung werden Terminals "....."

der Firma. ..... verwendet,

die an folgenden Stellen angebracht werden:

_____

_____

_____

Hierdurch erfolgt auch eine Kontrolle der Zugangsberechtigung zur Dienstelle. Alle Mitarbeiter müssen sich durch Benutzung ihres Chips an ihrem Arbeitsplatz anmelden. Über seine Verwendung werden sie durch eine Informationsschrift unterrichtet. Bei Verlust oder Störungen haben sie unverzüglich die Dienststelle unter der Rufnummer ..... zu verständigen.

2.3 Zeiterfassung/Fehlzeitenüberwachung und Zugangsberechtigung

Die Zeiterfassung einschließlich der Fehlzeitenüberwachung und der Zugangsberechtigung erfolgt als "Online-Lösung" im Rahmen des vorhandenen Netzwerks. Hierbei werden die Daten auf dem Server der Dienstelle vorgehalten. Mitarbeiter haben nur im Rahmen ihrer Berechtigung Zugriff auf die Daten.

3. Gespeicherte Daten

Es dürfen nur die personenbezogenen Daten der Bediensteten aufgezeichnet werden, die für die Anwesenheitskontrolle und die Abrechnung der Arbeitszeit erforderlich sind. Dies sind:

- ❑ Name, Vorname
- ❑ Geburtsdatum
- ❑ Pers.Nr. (nicht identisch mit der "echten" Pers. Nr.)
- ❑ Ausweisnummer (Chip-Karte)
- ❑ Abteilung, Referat
- ❑ Abwesenheitskennzeichen (Urlaub, Krankheit, Dienstreise; Dienstbefreiung)
- ❑ Tages-, Wochen; Monatspläne
- ❑ Soll- und Ist-Arbeitszeit
- ❑ Gleitzeit-, Mehrarbeitszeitkonto, Möglichkeit weiterer Zeitkonten
- ❑ Urlaubsanspruch
- ❑ An- und Abwesenheitszeiten

Die gespeicherten Daten dürfen nicht mit anderen Personalverwaltungsverfahren verknüpft werden; sie werden nur für die in Nr. 1 genannten Zwecke verwendet. Die Daten dürfen nur in der Personalabteilung den mit der Durchführung des DV-Verfahrens beauftragten Bediensteten zugänglich sein.

4. Auswertungen

Folgende Auswertungen durch die Personalabteilung sind zugelassen:

a) Zeiterfassung:

- ❑ Personalübersicht (Liste aller teilnehmenden Personen)
- ❑ Tägliche An- und Abwesenheitsübersicht (Inhalt: Namen, Abteilung, Abwesenheits kennzeichen) für das Personalreferat
- ❑ Monatliche Resultatsliste für die Bediensteten bzw. bei Unstimmigkeiten für das Personalreferat
- ❑ Monatliche Summenübersicht für das Personalreferat

b) Urlaubs- und Fehlzeitenüberwachung:

- ❑ Urlaubsplan
- ❑ jährlicher/halbjährlicher Einzelausdruck der personenbezogenen Fehlzeiten für die Personalakte
- ❑ Personalausfallstatistik (Die Statistik selbst enthält keine personenbezogenen Daten).

Weitergehende Auswertungen dürfen nur nach schriftlicher Anordnung des zuständigen Referatsleiters und unter Beteiligung der Personalvertretung sowie der Frauenbeauftragten vorgenommen werden. Sie sind ausschließlich für Personalverwaltungszwecke zulässig. Nicht mehr zur Aufgabenerfüllung erforderliche Auswertungen sind unter Beachtung der entsprechenden Regeln zur Vernichtung von Schriftgut und sonstigen Datenträgern zu vernichten.

5. Datenlöschung

Die aufgezeichneten Daten über Urlaub und andere Fehlzeiten sind spätestens 1 Jahr nach Ablauf des Urlaubsjahres zu löschen. Die aufgezeichneten Zeiterfassungsdaten werden bereits nach 6 Monaten im System gelöscht; sie dürfen auf einem externen Datenträger für eine Dauer von längstens 6 weiteren Monaten gespeichert werden. Sofern die Daten länger gespeichert werden sollen, ist die Personalvertretung unter Angabe des Grundes zu unterrichten. Die Löschung der Daten ist zu protokollieren.

6. Technische und organisatorische Maßnahmen zum Schutz der Daten nach § 6 KDO und der hierzu erlassenen Anlage nach Nr. IV KDO-DVO

6.1 Besondere Sicherheitsmechanismen

- ❑ Sicherung des Systemzugangs bzw. der Betriebssystemebene durch "....."
- ❑ Datensicherheit durch Passwortsteuerung aller Dialoge im System, gegliedert nach Anwender- bzw. Prioritätsstufen
- ❑ Datenzugang nur für die mit der Administration und der Abrechnung betrauten Personen, das sind
  - der im Personalreferat für die Zeiterfassung und Urlaubs- und Krankheits-überwachung zuständige Bearbeiter

- der im Personalreferat für die Betreuung der Verfahrensanwendung zuständige Bearbeiter
- der im EDV-Referat für die Systembetreuung zuständige Bearbeiter.

Diese Personen werden namentlich benannt. Änderungen werden dem Personalrat mitgeteilt.

6.2 Raumzugang

Zu den Räumen, in denen die personenbezogenen Daten verarbeitet werden, dürfen nur Berechtigte Zugang haben. Außenstehende Personen (Publikumsverkehr, Wartungspersonal u.a.) dürfen sich nur in Begleitung eines Beauftragten der Dienststelle in diesen Räumen aufhalten. Unbesetzte Räume sind abzuschließen. Die Schlüssel sind so aufzubewahren, dass kein Zugriff Unbefugter erfolgen kann.

6.3 Datensicherung

Die auf dem Server gespeicherten Daten sind regelmäßig zu sichern. Das geschieht einmal wöchentlich auf einer hierfür eingesetzten externen und mit einem Schreibschutz versehenen WD-Festplatte. Sie wird zum Schutz vor Verlust und Beschädigung im Tresor der Systemverwaltung aufbewahrt und darf nur von hierzu berechtigten Personen befördert und genutzt werden. Von der Systemverwaltung ist eine Sicherungskopie anzulegen, die getrennt vom Originalbestand in Raum ..... aufzubewahren ist.

6.4 Speicher und Zugriff

Die Systemverwaltung ist für die Administration von Mehrplatzsystemen im lokalen Netzwerk verantwortlich. Die Rechte der Anwender für Dateien und Verzeichnisse werden von ihr in Absprache mit der Verwaltungsleitung vergeben und sind auf das unbedingt notwendige Maß zu beschränken. Die Rechtevergabe ist zu dokumentieren und fortzuschreiben.

Der Aufruf des Verfahrens ist den zugriffsberechtigten Anwender nur nach Eingabe ihrer jeweiligen Benutzerkennung und des Passwortes möglich. Die Benutzer sind verpflichtet, das Passwort spätestens nach Ablauf von ..... Tagen zu ändern. Kann nicht ausgeschlossen werden, dass eine Unbefugter Einblick in das Passwort erhalten hat, ist dieses sofort zu ändern.

Seitens der Systemverwaltung sind geeignete Maßnahmen zu treffen, die einen Zugriff auf die Betriebssystem-Ebene durch die Anwender ausschließen.

Die für den Zugriff auf das vorliegende Verfahren vergebenen Passworte werden in verschlossenen Umschlägen ..... (an einem gesicherten Ort) hinterlegt. Die Öffnung der Umschläge ist nur bei unabweisbarer Notwendigkeit (z.B. bei unvorhergesehener Abwesenheit des Zugriffsberechtigten und seiner Vertretung) und nur dann zulässig, wenn eine Neuvergabe des Passwortes an Dritte nicht in Betracht kommt.

Bei der Verarbeitung der personenbezogenen Daten ist zu verhindern, dass Unbefugte den Bildschirm einsehen. Hierzu ist beim Verlassen des Arbeitsplatzes der Bildschirm auf die Anmeldungsmaske/Begrüßungsbildschirm zu stellen bzw. eine Bildschirmdunkelschaltung sowie eine Maus- und Tastatursperre nach einer Zeitspanne ohne Eingabe einzustellen. Nach Abschluss der Arbeiten sind alle Ausdrucke aus dem Drucker zu entfernen und ggf. zu vernichten (s. Nr. 4).

6.5 Übermittlung/Transport von Daten

Durch das vorliegende Verfahren ist weder eine Übermittlung noch ein Transport von Daten vorgesehen. Es besteht daher kein Regelungsbedarf.

7. Einsichtnahme und Kontrolle

7.1 Einsicht durch die Bediensteten

Den Bediensteten wird im Rahmen der vorhandenen technischen und finanziellen Möglichkeiten Zug um Zug ein Lesezugriff auf die zu ihrer Person gespeicherten an ihrem Arbeitsplatzrechner ermöglicht. Soweit dies (noch) nicht möglich ist, wird jedem Bediensteten auf Anforderung monatlich eine Resultatsliste über die Zeiterfassung ausgedruckt und in verschlossenem Umschlag zugestellt. Darüber hinaus wird den Bediensteten das Recht eingeräumt, nach Abstimmung mit den zuständigen Bearbeitern in die sie betreffenden Daten Einsicht zu nehmen und entsprechende Ausdrucke zu erhalten; eine Zugriffsberechtigung ist damit nicht verbunden.

7.2 Einsicht durch die Personalvertretung

Die Personalvertretung ist berechtigt, die Einhaltung dieser Vereinbarung zu kontrollieren. Die Bearbeiter der Personalstelle haben einem im Einzelfall zu benennenden Vertreter des Personalrats nach Abstimmung mit der Referatsleitung auf Verlangen die Abläufe des Verfahrens zu demonstrieren und Einsichtnahme in die Ausdrucke zu gewähren. Eine Zugriffsberechtigung ist damit nicht verbunden.

7.3 Überwachung durch den betrieblichen Datenschutzbeauftragten

Der betriebliche Datenschutzbeauftragte ist befugt, im Rahmen der ihm übertragenen Aufgaben die Einhaltung dieser Vereinbarung zu überwachen. Er hat mindestens einmal jährlich eine Kontrolle durchzuführen.

8. Information der Bediensteten

Da mit dem Verfahren mobile personenbezogene Speicher- und Verarbeitungsmedien eingesetzt werden und zudem auch Personalaktendaten automatisiert verarbeitet werden (Urlaub, Fehlzeiten), besteht eine Informationspflicht gegenüber dem Betroffenen. Er ist bei erstmaliger Speicherung über die Funktionsweise des Mediums und die Art der über ihn erhobenen und gespeicherten Daten in verständlicher Form zu unterrichten, § 5b Abs. 1 Nr. 1 bis 3 KDO.

Ferner sind die Verarbeitungs- und Nutzungsformen automatisierter Personalverwaltungsverfahren nach § 3a Abs. 4 KDO zu dokumentieren und einschließlich des jeweiligen Verwendungszweckes sowie der regelmäßigen Empfänger und des Inhalts automatisierter Datenübermittlung allgemein bekannt zu geben. Zu diesem Zweck wird jedem Mitarbeiter ein Exemplar dieser Dienstvereinbarung zur Verfügung gestellt.

9. Systemänderungen/Systemerweiterungen

Jede Änderung oder Erweiterung des vorliegenden Verfahrens bedarf der Beteiligung der Personalvertretung. Diese Dienstvereinbarung ist ggf. entsprechend anzupassen.