Dienstvereinbarung über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz

Zwischen dem **Kirchenkreisrat des Ev.-Luth. Kirchenkreises Schleswig-Flensburg**

und der **Mitarbeitervertretung des Ev.-Luth. Kirchenkreises Schleswig-Flensburg**

wird die folgende Dienstvereinbarung über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz abgeschlossen:

1. Geltungsbereich und Zweckbestimmung

Diese Dienstvereinbarung regelt die Grundsätze für den Zugang und die Nutzung der Internet- und E-Mail-Dienste über die zentrale EDV. Dies betrifft den Standort Kirchenkreisverwaltung, die angebundenen Standorte (durch Router gekoppelt - ständige Verbindung), sowie die Einzel VPN Verbindungen (Telearbeit), die einen Zugriff auf von außen auf die Server der Verwaltung zulassen und gilt für alle Beschäftigte, die mit diesem System (Terminal-Server) arbeiten.

Des Weiteren regelt die Dienstvereinbarung die Nutzung von Telefongeräten, Faxgeräten und dienstlichen Mobiltelefonen im Kirchenkreis Schleswig-Flensburg und gilt für alle Beschäftigten der Kirchenkreisverwaltung.

2. Zielsetzung

Ziel dieser Vereinbarung ist es, die Nutzungsbedingungen sowie die Maßnahmen zur Protokollierung und Kontrolle transparent zu machen, die Persönlichkeitsrechte der Beschäftigten zu sichern und den Schutz ihrer personenbezogenen Daten zu gewährleisten.

3. Organisatorische Grundsätze

(1) Die elektronischen Kommunikationssysteme stehen den Beschäftigten als Arbeitsmittel im Rahmen der Aufgabenerfüllung zur Verfügung.

(2) Die Absicherung des Zuganges zum Internet wird durch eine Firewall sichergestellt. Die Installation und Konfiguration von Web-Browsern, die IT-fachliche Betreuung der Beschäftigten sowie die Administration ihrer Internetberechtigungen erfolgt durch IT Abteilung.

(3) Arbeitsplätze außerhalb der zentralen EDV müssen mit einem VPN- Internetzugang und durch Virenschutzprogramme vor Schadsoftware gesichert werden. Diese Programme dürfen durch Beschäftigte nicht eigenständig manipuliert oder deaktiviert werden. Gleiches gilt für den Einsatz von Filterprogrammen, die den Zugriff auf Angebote mit rechtswidrigen oder strafbaren Inhalten sperren, sowie für alle Sicherheitsprogramme und Sicherheitseinstellungen.

4. Nutzung

(1) Der Internetzugang, das E-Mail-System, die Festnetztelefonie, die Faxgeräte und ggf. Mobiltelefone werden nur für die dienstliche Nutzung zur Verfügung gestellt.

(2) Der Internetzugang steht den Beschäftigten als Arbeitsmittel im Rahmen der Aufgabenerfüllung zur Verfügung und dient insbesondere der Verbesserung der internen und externen Kommunikation, der Erzielung einer höheren Effizienz und der Beschleunigung der Informationsbeschaffung und der Arbeitsprozesse.

(3) Über die dienstlichen E-Mail-Adressen eingehende private E-Mails sind von den Beschäftigten sofort zu löschen.

(4) Emails mit Dokumentenanhängen, die personenbezogene oder andere sensible Daten beinhalten, dürfen nur verschlüsselt und mit Kennwortschutz übertragen werden.

(5) Das Abrufen und Ausführen von Dateien oder Programmen aus und im Internet; das Abrufen sowie die Installation von Treibern, Setup-Programmen oder ähnlicher systemeingreifender Software, ist nur von durch die IT-Abteilung bekanntzugebenden Anbietern gestattet. Urheberrechtlich geschützte Dateien, für die keine Lizenz vorhanden ist, dürfen nicht abgerufen und gespeichert werden. Das Ausführen von aktiven Inhalten (z.B. Makros) in heruntergeladenen Dokumenten ist nur bei als vertrauenswürdig gekennzeichneten Absendern gestattet. Die Einstellungen in den zugehörigen Anwendungen werden von der IT-Abteilung vorgenommen.

(6) Das Abrufen von für die Dienststelle kostenverursachenden Informationen oder Inhalten aus dem Internet bedarf der Zustimmung der zuständigen Abteilungsleitung.

(7) Das Anrufen von für die Dienststelle kostenverursachenden Rufnummern (z. B. Hotlines) bedarf der Zustimmung der zuständigen Abteilungsleitung.

(8) Ferngesteuerte Zugriffe oder Steuerungen von Rechnersystemen über sogenannte Remote-Anwendungen bzw. Terminal-Emulationen sind grundsätzlich nicht zugelassen. Ausnahmen bedürfen der Zustimmung der IT-Abteilung.

(9) Mit Beendigung des Beschäftigungsverhältnisses steht die E-Mail-Adresse nicht mehr zur Verfügung. Die Beschäftigten sind angehalten, ihre Kommunikationspartner über diesen Umstand zu informieren. Nach Beendigung des Beschäftigungsverhältnisses eingehende E-Mails werden an die zuständige Abteilungsleitung umgeleitet. Nach Ablauf von drei Monaten wird das Benutzerkonto von der IT-Abteilung gelöscht.

5. Protokollierung und Kontrolle

(1) Alle eingehenden E-Mails werden durch eine Firewall, einen Spam-Filter sowie Virenscanner geprüft.

(2) Die Verkehrsdaten für den Internetzugang werden mit Angaben von

- Datum / Uhrzeit,
- den Adressen von Absendern und Empfängern (IP-Adressen),
- der aufgerufenen Webseiten und
- der übertragenen Datenmenge

protokolliert.

(3) Die Protokolle nach Absatz 2 werden ausschließlich zu Zwecken der

- Analyse und Korrektur technischer Fehler,
- Gewährleistung der Systemsicherheit,
- Optimierung des Netzes,
- statistischen Feststellung des Gesamtnutzungsvolumens,
- Stichprobenkontrollen gemäß Absatz 4, und
- Auswertungen gemäß Ziffer 6 dieser Vereinbarung (Missbrauchskontrolle)

verwendet.

(4) Die Protokolle werden durch einen von der Dienststellenleitung schriftlich dazu beauftragten Beschäftigten halbjährlich - nicht personenbezogen - stichprobenhaft hinsichtlich der aufgerufenen Websites gesichtet und in aggregierter Form, also ohne Nennung von Namen und anderen Identifizierungsmerkmalen, ausgewertet. Die Auswertung der Übersicht des Gesamtdatenvolumens erfolgt halbjährlich ebenfalls durch den beauftragten Beschäftigten. Der/die Datenschutzbeauftragte und die Mitarbeitervertretung sind hierbei immer zu beteiligen.

(5) Der Zugriff auf die Protokolldateien gemäß Absatz 3 ist auf den von der Dienststellenleitung beauftragten Beschäftigten begrenzt.

(6) Die Protokolldaten werden nach 30 Tagen automatisch gelöscht.

6. Maßnahmen bei Verstößen / Missbrauchsregelung

(1) Bei Verdacht auf missbräuchliche oder unerlaubte Nutzung des Internetzugangs durch einen/eine oder mehrere Beschäftigte/n erfolgt auf Anordnung der Dienststellenleitung unter Beteiligung des Datenschutzbeauftragten des Kirchenkreises und der/des Vorsitzenden der Mitarbeitervertretung eine Überprüfung des Datenverkehrs durch die IT-Abteilung. Sind weitere Untersuchungsmaßnahmen (z.B. Offenlegung der IP-Adresse des benutzten Arbeitsplatzes) notwendig, werden diese von den in Satz 1 genannten Personen veranlasst.

Auf der Basis dieser Untersuchung wird ein Bericht erstellt, der dem Betroffenen ausgehändigt wird. Dieser ist anschließend dazu zu hören.

(2) Ist aufgrund der stichprobenhaften nicht-personenbezogenen Kontrollen bzw. der Auswertung der Übersicht des Datenvolumens eine nicht mehr tolerierbare Häufung von offensichtlich privater Nutzung des Internetzugangs zu erkennen, so werden innerhalb von einer zu setzenden Frist von zwei Wochen nach der Anhörung die Stichproben weiterhin nicht-personenbezogen durchgeführt. Ergeben diese Stichproben bzw. die Auswertung der Übersicht des Datenvolumens keine Änderung im Nutzungsverhalten, so werden die Protokolle der folgenden zwei Wochen durch die in Absatz 1 genannten Personen stichprobenhaft personenbezogen ausgewertet. Hierbei wird wie im Falle des Verdachts einer missbräuchlichen Nutzung (Abs. 1) vorgegangen. Zu den Verfahren nach Satz 1 und Satz 2 erfolgt eine entsprechende vorherige schriftliche Mitteilung an alle Beschäftigten, so dass deren Kenntnisnahme über die Maßnahmen gewährleistet werden kann.

(3) Ein Verstoß gegen diese Dienstvereinbarung kann neben den dienst- und arbeitsrechtlichen Folgen auch strafrechtliche Konsequenzen haben.

7. Änderungen und Erweiterungen

Geplante Änderungen und Erweiterungen an den elektronischen Kommunikationssystemen werden der Mitarbeitervertretung und dem/der Datenschutzbeauftragten durch die Dienststellenleitung mitgeteilt. Es ist dann zu prüfen, ob und inwieweit sie sich auf die Regelungen dieser Vereinbarung auswirken. Notwendige Änderungen oder Erweiterungen zu dieser Vereinbarung werden im Einvernehmen in einer ergänzenden schriftlichen Regelung vorgenommen.

8. Inkrafttreten

Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft. Gleichzeitig tritt die Dienstvereinbarung E-Mail-Intranet-Internet vom 1. Juli 2009 außer Kraft. Diese Dienstvereinbarung kann beiderseits mit einer Frist von drei Monaten zum Monatsschluss gekündigt werden. Eine Folgevereinbarung ist anzustreben.

Flensburg 19.04.2016
Ort, Datum

Mitarbeitervertretung

MITARBEITERVERTRETUNG
-MV-
EV.-LUTH. KIRCHENKREIS
SCHLESWIG-FLENSBURG

SL, 250416
Ort, Datum

Kirchenkreisrat

EV.-LUTH. KIRCHENKREIS SCHLESWIG - FLENSBURG

Beizufügende Anhänge

Artikel 10 Grundgesetz

(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, dass sie dem Betroffenen nicht mitgeteilt wird und dass an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

§ 88 Fernmeldegeheimnis

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Dienstanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 3 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

(4) Befindet sich die Telekommunikationsanlage an Bord eines Wasser- oder Luftfahrzeugs, so besteht die Pflicht zur Wahrung des Geheimnisses nicht gegenüber der Person, die das Fahrzeug führt oder gegenüber ihrer Stellvertretung.

Quelle: http://www.bfdi.bund.de/bfdi_wiki/index.php/Dienstvereinbarung_E-Mail_und_Internet_am_Arbeitsplatz