Dienstvereinbarung
Elektronische Kommunikationssysteme und informationstechnische Infrastruktur

Zwischen dem

Evangelischen Kirchenkreis Spandau,
vertreten durch den Vorsitzenden des
Kreiskirchenrats
(Arbeitgeber)

und der

Mitarbeitervertretung des Ev. Kirchenkreises Spandau
(Mitarbeitervertretung bzw. MAV)

wird die folgende Dienstvereinbarung abgeschlossen:

§ 1 Geltungsbereich, Zweckbestimmung und Zielsetzung

(1) Diese Dienstvereinbarung regelt die Grundsätze für den Zugang und die Nutzung des Email-Systems, des Internets sowie die Bereitstellung und Nutzung der Hardwarekomponenten im Kirchenkreis Spandau und gilt für alle von der Mitarbeitervertretung vertretenen Mitarbeiter*innen, mit Ausnahme der Beschäftigten im Kita-Bereich.

(2) Diese Vorschriften regeln die dienstliche und private Nutzung dienstlicher Kommunikationsmittel sowie die dienstliche Nutzung privater Kommunikationsmittel durch die Mitarbeiter*innen unter Wahrung der Vertraulichkeit des gesprochenen Wortes (§ 201 StGB).

(3) Der Arbeitgeber beauftragt und setzt Dritte, die Zugang zu dienstlichen Kommunikationsmitteln haben, nur so ein, dass die Vorgaben aus dieser Dienstvereinbarung eingehalten werden. Dritte sind insbesondere Mitarbeitende von Fremdfirmen, Ehrenamtliche, Honorarkräfte, Praktikanten ohne Mitarbeiterstatus und andere Personen. Zudem sind Dritte auf das EKD Datenschutzgesetz zu verpflichten.

(4) Ziel dieser Vereinbarung ist die Herstellung der Transparenz der Nutzungsbedingungen (nach § 2 Absatz 5), der Maßnahmen zur Protokollierung und Kontrolle, der Schutz der Persönlichkeitsrechte der Mitarbeiter*innen sowie die Gewährleistung des Schutzes ihrer personenbezogenen Daten.

(5) Ziel dieser Vereinbarung ist es zudem, den Einsatz einer leistungsfähigen und zeitgemäßen Technik mit dem Schutz der Persönlichkeitsrechte für die betroffenen Mitarbeiter*innen zu verbinden.

§ 2 Organisatorische Grundsätze

(1) Elektronische Kommunikationssysteme stehen den Mitarbeiter*innen als Arbeitsmittel im Rahmen der dienstlichen Aufgabenerfüllung nach Weisung des Arbeitgebers zur Verfügung.

(2) Elektronische Kommunikationsmittel im Sinne dieser Vereinbarung sind Betriebsmittel wie Telefon, Telefaxgerät, Personal Computer, Work Station, E-Mail und Internet-Anschlüsse und mobile Endgeräte wie Mobiltelefone, Smartphone, Tablets, Laptops, Notebooks, Thin-Clients, USB-Sticks, Smart Watches ebenso virtuelle Assistenten wie Smart Lautsprecher, sowie sämtliche Medien, die digitale Daten speichern, verarbeiten und übertragen können.

(3) Der Arbeitgeber entscheidet über die Bereitstellung der erforderlichen Kommunikationsmittel für die Mitarbeiter*innen der Dienststelle. Für einzelne Arbeitsbereiche kann eine Mindestausstattung festgelegt werden.

(4) Mobile Endgeräte werden bei Feststellung des dienstlichen Erfordernisses bereitgestellt. Für den Mobilfunk werden die Kosten direkt durch den externen Anbieter erhoben und der Dienststelle in Rechnung gestellt. **Die mobilen Endgeräte und deren Administration werden durch die Mitarbeiter*innen der internen IT-Abteilung verwaltet.** Dies betrifft insbesondere die Einrichtung des mobilen Endgerätes und die Erneuerung ggfs. notwendiger Zertifikate. Die interne IT-Abteilung kann unter Berücksichtigung der IT-Sicherheitsverordnung (ITSVO EKD) die Nutzung eines privaten mobilen Endgerätes zu dienstlichen Zwecken in Ausnahmefällen gestatten. Die Privatnutzung ist u. a. nur unter der Voraussetzung zu gestatten, dass eine Haftung des Arbeitgebers für Schäden am privaten Gerät bei dienstlicher Anwendung, insbesondere bei Verlust privater Daten, ausgeschlossen ist.

(5) Soweit ausnahmsweise die Nutzung eines privaten mobilen Endgerätes zu dienstlichen Zwecken gestattet wurde, obliegt die Wartung und Administration des mobilen Endgerätes dem Anwender. Die interne IT-Abteilung kann ggf. Zugangssoftware für den Zugriff auf das Firmennetzwerk installieren. Über die dienstliche Nutzung soll eine Nutzungsvereinbarung (Anlage 1 zur DV) abgeschlossen werden.

(6) Dienstliche Kommunikationsmittel werden im Namen und auf Rechnung des Arbeitgebers angeschafft.

(7) Privat genutzte Kommunikationsmittel bleiben Eigentum des Mitarbeiters bzw. der Mitarbeiterin. Eine Kostenübernahme ist grundsätzlich ausgeschlossen. Nur bei Vorliegen wichtiger Gründe kann der Arbeitgeber im Einzelfall ausnahmsweise eine Kostenübernahme gestatten.

(8) Die Absicherung des Zuganges zum Internet wird durch entsprechende technisch-organisatorische Maßnahmen seitens des Arbeitgebers sichergestellt. Die Installation und Konfiguration von Web-Browsern sowie die Administration der jeweiligen Berechtigungen der Mitarbeitenden erfolgt ausschließlich durch den Arbeitgeber bzw. den beauftragten IT-Dienstleister.

§ 3 Grundsätze der betrieblichen und /oder privaten Nutzung

Die vom Arbeitgeber zur Verfügung gestellten elektronischen Kommunikationssysteme und Endgeräte zur Nutzung vom Internet sind grundsätzlich nur zu betrieblichen Zwecken gestattet.

Das betriebliche E-Mail-Postfach darf ausschließlich zur betrieblichen Kommunikation genutzt werden.

§ 3 a Nutzung des dienstlichen Internetzugangs

(1) Die private Nutzung des dienstlichen Internetzugangs ist unter dem Vorbehalt des jederzeitigen Widerrufs in geringfügigem Umfang in den Pausenzeiten zulässig, soweit die dienstliche Aufgabenerfüllung sowie die Verfügbarkeit des IT-Systems für dienstliche Zwecke nicht beeinträchtigt werden und die private Nutzung keine negativen Auswirkungen auf die Bewältigung der Arbeitsaufgaben hat und zusätzliche Kosten nicht entstehen.
Die Gestattung der privaten Nutzung des Internetzugangs nach den Vorgaben dieser Vereinbarung erfolgt ausschließlich gegenüber den Mitarbeitenden, die zuvor eine Einwilligung gemäß dem Anhang 1 abgegeben haben. Sie ist insbesondere nur unter der Bedingung gestattet, dass der/die Mitarbeiter*in mit den in den §§ 7, 8 dieser Vereinbarung benannten Kontrollmaßnahmen einverstanden ist. Liegt eine Einwilligung vor, ist die private Nutzung im Umfang der Regelungen dieser Dienstvereinbarung zulässig.

Die Mitarbeitenden sind frei in der Entscheidung, ob sie eine solche Einwilligung abgeben. Die Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden. Soweit eine Einwilligung nicht erteilt oder widerrufen wird, ist ausschließlich eine betriebliche Nutzung zulässig.

(2) Das Abrufen und Ausführen von Dateien oder Programmen aus und im Internet ist nur von und bei der internen IT-Abteilung bekannt gegebenen Anbietern gestattet, soweit deren Inhalte für den dienstlichen Gebrauch benötigt werden.

Urheberrechtlich geschützte Dateien, für die keine Lizenz vorhanden ist, dürfen nicht abgerufen und gespeichert werden.

Das Abrufen und die Installation von Treibern, Setup-Programmen oder ähnlicher systemeingreifender Software sind nur durch die zuständige interne IT-Abteilung durchzuführen.

Das Ausführen von aktiven Inhalten (z.B. Makros) in heruntergeladenen Dokumenten ist nur bei als **vertrauenswürdig gekennzeichneten Anbietern** gestattet. Die Einstellungen in den zugehörigen Anwendungen werden von der internen IT-Abteilung vorgenommen.

(3) Ferngesteuerte Zugriffe oder Steuerungen von Rechnersystemen über sogenannte Remote-Anwendungen, mit Ausnahme von AnyDesk, bzw. Terminal-Emulationen sind grundsätzlich nicht zugelassen. Hierzu sind ausschließlich autorisierte Mitarbeiter der internen und externen IT-Abteilung befugt.

(4) Die Verwendung von Software für Internet- und Videotelefonie ist grundsätzlich nicht gestattet. Ausnahmen für den dienstlichen Gebrauch sind bei der internen IT Abteilung zu beantragen und nur mit der dafür zur Verfügung gestellten Hard- und Software zulässig.

(5) Das Abrufen von für den Arbeitgeber kostenverursachenden Informationen oder Inhalten aus dem Internet, ist nur mit Zustimmung des Arbeitgebers statthaft.

(6) Das Abrufen von Informationen oder Inhalten für den Privatgebrauch, die für den Arbeitgeber Kosten verursachen, ist unzulässig. Im Rahmen der privaten Nutzung dürfen keine politischen, kommerziellen, gewerblichen oder sonstigen geschäftlichen Zwecke verfolgt werden.

(7) Die Mitarbeitenden haben jede Nutzung des Internets zu unterlassen, die unserem kirchlichen Selbstverständnis zuwiderlaufen oder geeignet sind den Interessen des Arbeitgebers sowie dessen Ansehen in der Öffentlichkeit zu schaden.

Dies gilt vor allem für das aktive Abrufen oder Verbreiten von Inhalten im Internet oder in Chatrooms, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen, insbesondere das Verbreiten von ehrverletzenden, wahrheitswidrigen oder beleidigenden Behauptungen über den Arbeitgeber, sowie das Abrufen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, homophoben, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen.

Abrufen und Aufrufen heißt auf im Netz vorhandene Informationen mit dem vom Arbeitgeber zur Verfügung gestellten IT-Systemen insb. Internetbrowsern zuzugreifen.

Verbreiten heißt einer Person oder einem unbestimmten Personenkreis Ab- und Aufrufe über Internet-Dienste, unter Verwendung von IT-Systemen des Arbeitgebers, anzubieten.

Anbieten von z.B. Inhalten auf unserer eigenen Webseite, ist nur der für Presse- und Öffentlichkeitsarbeit zuständigen Stelle oder dem Arbeitgeber bzw. nur mit dessen Genehmigung gestattet.

(8) Eine Unterscheidung von dienstlicher und privater Nutzung auf technischem Weg erfolgt nicht. Die Protokollierung und Kontrolle gemäß §§ 7 und 8 dieser Vereinbarung erstrecken sich auch auf den Bereich der privaten Nutzung des Internetzugangs.

(9) Aus Wirtschaftlichkeits- oder IT-Sicherheitsgründen kann die Internetnutzung beschränkt werden. Dies kann beispielsweise folgendes beinhalten:
- Sperrung bestimmter Dienste der Internetnutzung
- Reduzierung auf bestimmte Internetanschlüsse,
- Beschränkung des Massendatentransfers oder des Speicherplatzes

§ 3 b Nutzung des betrieblichen E - Mail- Postfach

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

(2) Das betriebliche E-Mail-Postfach darf ausschließlich zur dienstlichen Kommunikation genutzt werden. Eine private Nutzung ist nicht gestattet. Die Weiterleitung, Zwischen - und Speicherung privater E-Mails sowie von Anhängen und sonstigen privaten Daten / Dateien auf dem dienstlichen E-Mail Account ist untersagt.

(3) Private E-Mails dürfen, soweit die private Nutzung des dienstlichen Internetzugangs gestattet ist, nur über die Nutzung von Webmail-Diensten versandt und empfangen werden. Private E-Mails, die im dienstlichen E-Mail-Postfach eingehen, sind von den Mitarbeitenden umgehend zu löschen.

(4) Dokumente, die personenbezogene oder andere sensible Daten beinhalten, dürfen nicht unverschlüsselt übertragen werden. Der Arbeitgeber informiert und schult die Mitarbeitenden über die Art und Weise der Verschlüsselung.

(5) Bei geplanter Abwesenheit des Mitarbeitenden ist durch den Mitarbeitenden unter Nutzung des Abwesenheitsassistenten ein automatischer Hinweis auf die Abwesenheit sowie die Vertretung einzurichten.

(6) Wurde eine Abwesenheitsnachricht entgegen von Absatz (5) nicht eingerichtet oder war dies aufgrund einer ungeplanten Abwesenheit nicht möglich, kann dies durch den Arbeitgeber erfolgen.

(7) Aufgrund dienstlicher Erfordernissen können dienstliche E-Mails zur Aufrechterhaltung des Dienstbetriebes, von der internen IT-Abteilung oder dem extern beauftragten IT-Dienstleister, bei längerer geplanter oder ungeplanter Abwesenheit an die zuständige Vertretungsperson, die von dem Arbeitgeber bestimmt werden, weitergeleitet werden. Hierbei ist die Mitarbeitervertretung von der internen IT-Abteilung zu informieren. Ist ein privater Charakter des Inhaltes dieser weitergeleiteten E-Mail ersichtlich, ist die E-Mail ohne weitere Kenntnisnahme des Inhaltes durch den Zugriffsberechtigten zu löschen. Eine Weiterleitung erfolgt nicht.

(8) Mit Beendigung des Beschäftigungsverhältnisses steht der dienstliche E-Mail Account nicht mehr zur Verfügung. Die Mitarbeitenden sind angehalten, wenn dies möglich ist, ihre außerbetrieblichen Kommunikationspartner über diesen Umstand zu informieren

§ 4 Verhaltensgrundsätze

(1) Zur Überprüfung der Einhaltung der Regelungen dieser Vereinbarung werden regelmäßige nicht namensbezogene Stichproben in den Protokolldateien durchgeführt. Ergänzend wird eine Übersicht über das jeweilige Gesamtvolumen des ein- und ausgehenden Datenverkehrs erstellt.

(2) Die bei der Nutzung der Internetdienste anfallenden personenbezogenen Daten werden nicht zur Leistungs- und Verhaltenskontrolle verwendet. Sie unterliegen der Zweckbindung dieser Vereinbarung und den einschlägigen datenschutzrechtlichen Vorschriften.

§ 5 Information der Mitarbeitenden

Die Mitarbeitenden werden durch die interne IT-Abteilung über die besonderen Datensicherheitsprobleme bei der Nutzung der elektronischen Kommunikationssysteme unterrichtet. Durch die/den externe/n Datenschutz-

beauftragte/n erfolgt die Information über den sicheren und wirtschaftlichen Umgang mit diesen Systemen und die zu beachtenden einschlägigen Rechtsvorschriften.

§ 6 Verantwortlichkeit

Die Verantwortung für die Beachtung der vorgenannten Festlegungen und Hinweise obliegt dem Arbeitgeber sowie den jeweiligen Mitarbeitenden. Die Mitarbeitenden haben insbesondere sicherzustellen, dass eine Nutzung der zur Verfügung gestellten oder eingebrachten Kommunikationsmittel durch Unbefugte sowie durch fahrlässige Handlungen ausgeschlossen ist. Dies betrifft alle dienstlich genutzten Peripherie- und Endgeräte.

Hinweis: Trotz des Einsatzes von Firewall oder Systemen und Software zum Schutz vor Schadsoftware ist das Ausspähen und Manipulieren von Daten durch Dritte nicht mit absoluter Sicherheit ausgeschlossen.

§ 7 Protokollierung und Kontrolle

(1) Die Verkehrsdaten für den Internetzugang werden mit Angaben von
- Datum/Uhrzeit,
- IP-Adressen
- der aufgerufenen Webseiten
- übertragener Datenmenge

protokolliert.

Ein- und ausgehende E-Mails werden mit folgenden Informationen protokolliert:
- Datum/Uhrzeit
- Absender- und Empfängeradresse
- Message ID
- Nachrichtengröße
- Betreff

(2) Die Protokolle nach (1) werden ausschließlich zu Zwecken der
- Analyse und Korrektur technischer Fehler
- Gewährleistung der Systemsicherheit
- Optimierung des Netzes
- Aktualisierung gesperrter Internetseiten (Black Lists)
- statistischen Feststellung des Gesamtnutzungsvolumens
- Stichprobenkontrollen hinsichtlich der §§ 3a und 3b
- Auswertungen gemäß § 8 dieser Vereinbarung (Missbrauchskontrolle)

verwendet.

(3) Die Protokolle werden durch die interne IT-Abteilung auf Weisung des Arbeitgebers anlassbezogen hinsichtlich der aufgerufenen Websites, aber nicht personenbezogen, gesichtet und in aggregierter Form, also ohne Nennung von Namen und anderen Identifizierungsmerkmalen, ausgewertet. Die interne IT-Abteilung unterrichtet den Arbeitgeber zeitnah über Regelwidrigkeiten.

(4) Der Zugriff auf die Protokolldateien gemäß § 7 (3) dieser Vereinbarung ist auf die interne IT-Abteilung und deren beauftragten externen IT-Dienstleister begrenzt. Dieser/diese ist auf die Einhaltung der datenschutzrechtlichen Anforderungen zu verpflichten. Darüber hinaus ist er/sie hinsichtlich der Einhaltung des Fernmeldegeheimnisses und des Datenschutzes auf die strafrechtlichen Konsequenzen bei Verstößen hingewiesen worden.

(5) Die Protokolldaten werden nach **30 Tagen** automatisch gelöscht.

(6) Die Kontrolle und Auswertung von personenbezogenen Protokollen können sich auch auf eine private Kommunikation auf einem dienstlichen Device erstrecken.

§ 8 Maßnahmen bei Verstößen / Missbrauchsregelung

(1) Entsteht durch eine Stichprobe der Verdacht, auf missbräuchliche oder unerlaubte Nutzung des Internetzugangs (hervorgerufen beispielsweise durch ein erhöhtes Gesamtdatenvolumen oder auch die Kenntnisnahme nicht zulässiger im Internet angebotener Inhalte) gemäß § 3 a dieser Vereinbarung durch Mitarbeitende, erfolgt auf Anweisung des Arbeitgebers und unter Beteiligung des/der örtlichen Datenschutzbeauftragten und der MAV eine Überprüfung des Datenverkehrs durch die nach § 7 (4) beauftragte IT-Abteilung.

(2) Sind weitere Untersuchungsmaßnahmen (z.B. Offenlegung der IP-Adresse des benutzten Arbeitsplatzes oder weitere Überprüfungen) notwendig, werden diese vom Arbeitgeber veranlasst. Auf der Basis dieser Untersuchung wird ein Bericht erstellt, der dem Betroffenen ausgehändigt wird. Dieser ist anschließend, auf Wunsch auch im Beisein der MAV, dazu zu hören.

(3) 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.

(4) 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 (1) genannte IT-Abteilung stichprobenhaft personenbezogen ausgewertet. Hierbei wird wie im Falle des Verdachts einer missbräuchlichen Nutzung vorgegangen. Zu den Verfahren nach Satz 1 und Satz

2 erfolgt eine entsprechende vorherige schriftliche Mitteilung an alle Mitarbeitenden, so dass deren Kenntnisnahme über die Maßnahmen gewährleistet werden kann.

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

(6) Der Arbeitgeber behält sich vor, bei Verstößen gegen diese Vereinbarung die private Nutzung des Internetzugangs im Einzelfall zu untersagen.

§ 9 Änderungen und Erweiterungen

(1) Geplante Änderungen und Erweiterungen an den elektronischen Kommunikationssystemen werden der MAV und dem/der Datenschutzbeauftragten mitgeteilt. Es wird dann geprüft, ob und inwieweit sie sich auf die Regelungen dieser Vereinbarung auswirken.

(2) Notwendige Änderungen oder Erweiterungen zu dieser Vereinbarung können im Einvernehmen mit der MAV in einer ergänzenden Regelung vorgenommen werden.

(3) Die Unwirksamkeit einzelner Bestimmungen dieser Vereinbarung führt nicht zur Unwirksamkeit der übrigen Regelungen. Im Falle der Unwirksamkeit einzelner Regelungen werden MAV und Arbeitgeber unverzüglich Verhandlungen über eine Neuregelung des jeweiligen Sachverhalts aufnehmen.

§ 10 Inkrafttreten

(1) Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft. Sie kann mit einer Frist von vier Wochen gekündigt werden.

(2) Im Falle einer Kündigung dieser Dienstvereinbarung ist jede private Nutzung des dienstlichen Internetzuganges bis zum Abschluss einer neuen Vereinbarung untersagt.

(3) Alle Mitarbeitenden bestätigen schriftlich die Kenntnisnahme. Ein Abdruck der Vereinbarung wird ihnen zusammen mit einer Kopie der Bestätigung ausgehändigt.

Berlin, den 19.12.2024

.....

KKR-Vorsitzender
Arbeitgebervertreter

Berlin, den 19.12.2024

.....

MAV
Mitarbeitervertretung

Mitarbeitervertretung (MAV)
des Kirchenkreises Spandau
Jüdenstraße 35-37 · 13597 Berlin
Tel.: 030 / 322 944-380
Fax: 030 / 322 944-381
E-Mail: mav@kirchenkreis-spandau.de

Einwilligung zur privaten Nutzung des dienstlichen Internetzugangs

Ich habe die „Dienstvereinbarung über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz" vom 19.12.2024 zur Kenntnis genommen.

Ich möchte den dienstlichen Internetzugang in dem in der Dienstvereinbarung erlaubten Umfang auch privat nutzen.
Bitte ankreuzen!

☐ JA ☐ NEIN

Ich bin mir insbesondere über die folgenden, mit der Privatnutzung des Internets verbundenen Nutzungsbedingungen bewusst:

Die private Nutzung ist nur in geringfügigem Umfang, das heißt täglich maximal 30 Minuten innerhalb der Pausenzeiten, gestattet und nur sofern und soweit dadurch die dienstliche Aufgabenerfüllung und die Verfügbarkeit der IT-Systeme für dienstliche Zwecke nicht beeinträchtigt werden.
Zum Schutz der IT-Systeme vor Viren, Trojanern und ähnlichen Bedrohungen sind der Download von Programmen aus dem Internet, sowie entsprechende Downloads von Dateianhängen im Rahmen der privaten Nutzung nicht gestattet.

Eine vorsätzliche Nutzung, welche geeignet ist, den Interessen des Arbeitgebers oder dessen Ansehen in der Öffentlichkeit zu schaden oder die gegen geltende Rechtsvorschriften verstößt, insbesondere der Abruf für den Arbeitgeber kostenpflichtigen Internetseiten, das Abrufen, Verbreiten oder Speichern von Inhalten, die gegen persönlichkeits, datenschutz, lizenz und urheberrechtliche oder strafrechtliche Bestimmungen verstoßen, Aktivitäten, die sich gegen die Sicherheit von IT-Systemen richten (z. B. Angriffe auf externe Webserver) oder Aktivitäten, die sich gegen den Arbeitgeber richten und/oder dem kirchlichen Selbstverständnis widersprechen unzulässig ist.
Der Arbeitgeber ist berechtigt, den Aufruf bestimmter Internet-Seiten durch den Einsatz geeigneter Filter-Programme zu verhindern. Es besteht kein Rechtsanspruch auf einen Zugriff auf gefilterte Internet-Inhalte.

Ich willige ein, dass auch meine privaten - also nicht nur die dienstlichen - Internetzugriffe im Rahmen der Dienstvereinbarung vom 19.12.2024 verarbeitet und unter den Voraussetzungen der §§ 7 und 8 der Dienstvereinbarung protokolliert sowie personenbezogen ausgewertet werden.

Mir ist bewusst, dass ich hierdurch auf den etwaigen Schutz des Fernmeldegeheimnisses gem. § 88 TKG verzichte. Ich bin mir darüber im Klaren, dass eine missbräuchliche oder unerlaubte Nutzung neben arbeitsrechtlichen Konsequenzen gegebenenfalls auch strafrechtliche Folgen haben kann und dass darüber hinaus ein Verstoß zivilrechtliche Schadensersatzpflichten auslösen kann.

Mir ist bekannt, dass ich diese Einwilligung jederzeit in Textform für die Zukunft widerrufen kann. Für den Fall des Widerrufs ist jegliche weitere Privatnutzung der dienstlichen IT untersagt.

Berlin, 06.01.2025 Berlin, 06.01.2025

Mitarbeiter*in Arbeitgeber

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 2 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.