Arbeitgeberverband Handwerk Bremen e.V.

IT-Nutzungsrichtlinie

Die Nutzungsrichtlinie bestimmt die Datenverwendung intern und klärt die Mitarbeiter über ihre Pflichten bei der Datenbearbeitung auf.

Auch hier sollte der Betrieb vorab prüfen, was konkret gewünscht und was umgesetzt wird.

Schwierig sind hier Ungleichbehandlungen, die entstehen, wenn dem einen Nutzungen gestattet werden, die anderen versagt sind, oder wenn Verstöße des einen bspw. arbeitsrechtliche Konsequenzen nach sich ziehen und die eines anderen nicht.

Die Nutzungsrichtlinie ist der Verpflichtungserklärung beizufügen.

IT-Nutzungsrichtlinie

Verantwortliche Stelle: … GmbH
….
…

Präambel

Stellt ein Unternehmer seinen Mitarbeitern einen Bildschirmarbeitsplatz zur Verfügung, dann ist es zwingend erforderlich für die Nutzung des Bildschirmarbeitsplatzes Verhaltensregeln vorzugeben und diese Regeln auch stichprobenmäßig zu prüfen. Andernfalls wird die individuelle Nutzung, z.B. privates Surfen im Internet, eine sogenannte „betriebliche Übung“ aus der sich ein Gewohnheitsrecht für den Mitarbeiter ableiten lässt. Nach aktueller Rechtsprechung1 wird ein Arbeitgeber nicht allein dadurch zum Dienstanbieter i. S. d. Telekommunikationsgesetzes, wenn er seinen Mitarbeitern einen Internetzugang einrichtet. Gleichgültig ob eine private Nutzung gestattet oder verboten ist. Der Zugriff des Arbeitgebers auf die individuellen E-Mail Postfächer der Mitarbeiter liegt im betrieblichen Interesse und ist zulässig, da er nicht den rechtlichen Beschränkungen des Fernmeldegeheimnisses unterliegt. Diese IT-Nutzungsrichtlinie ist Bestandteil der IT Security Policy im Unternehmen und beschreibt vorwiegend die Verantwortlichkeiten der Mitarbeiter.

§ 1 Gegenstand und Geltungsbereich

Diese Richtlinie regelt den Umgang mit der EDV-technischen Ausstattung am Arbeitsplatz, sowie die Grundsätze für die Internet- und E-Mail Nutzung.

§ 2 Zielsetzung

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

§ 3 Verarbeitung personenbezogener Daten

Die Vorschriften der Datenschutzgrundverordnung (DSGVO), insbesondere die Vorschriften nach Artikel 5 und 6 sind bei allen Tätigkeiten zu beachten. Danach ist es unzulässig nicht öffentlich zugängliche personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu erheben, zu verarbeiten, bekannt zu geben, zugänglich zu machen oder sonst zu nutzen. Demnach ist es untersagt firmeninterne Daten, dazu gehören auch Kontaktdaten von Kunden/Mandanten und sonstigen Geschäftspartnern ohne betriebliche Notwendigkeit auf externen Datenträgern zu speichern. Eine Speicherung firmeninterner Daten auf privaten Datenträgern, dazu gehören im Besonderen mobile Datenträger (USB-Sticks, SD-Speicherkarten etc.) und Smartphones ist grundsätzlich verboten.

§ 4 E-Mail

(1) Alle E-Mails, die über den dienstlichen E-Mail-Account empfangen und versendet werden, sind als dienstlich einzustufen und können damit auch aus betriebsorganisatorischen Gründen von den Kollegen eingesehen werden.

(2) Die private Nutzung des dienstlichen E-Mail-Accounts ist nicht gestattet.
(3) Alle ein- und ausgehenden E-Mails werden zu Revisionszwecken archiviert.

§ 5 Internet
(1) Der Internet-Zugang steht den Mitarbeitern ausschließlich 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.
(2) Das private Surfen im Internet ist nicht gestattet.

§ 6 Verhaltensgrundsätze für die Internetnutzung
Unzulässig ist jede absichtliche oder wissentliche Nutzung des Internet, die geeignet ist, den Interessen der **… GmbH** zu schaden oder deren Ansehen in der Öffentlichkeit zu schädigen, die Sicherheit des lokalen Netzwerkes zu beeinträchtigen oder die gegen geltende Rechtsvorschriften verstößt.

Dies gilt vor allem für:
(1) das Abrufen oder Verbreiten von Inhalten, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
(2) das Abrufen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen.
(3) das Abrufen kostenpflichtiger Seiten bzw. Downloads.

§ 7 Allgemeine Verhaltensgrundsätze für die EDV-Nutzung
(1) Bei Verlassen des Arbeitsplatzes ist der Computer gegen unbefugte Nutzung zu sichern, z.B. durch die Aktivierung eines Kennwort geschützten Bildschirmschoners, sofern kein automatischer Bildschirmschoner eingerichtet ist, der sich nach Ablauf einer Zeit selbst aktiviert.
(2) Alle eingehenden und ausgehenden Daten sind vor der Nutzung bzw. vor dem Versand mit dem installierten Antivirusprogramm zu prüfen, sofern eine automatisierte Prüfung nicht erfolgt.
(3) An den Bildschirmarbeitsplätzen mit Festplatte, die auch externe Daten (z.B. E-Mail Anhänge, USB-Sticks von Mandanten etc.) verarbeiten, sollte min. einmal pro Woche ein manueller Virenscan2 durchgeführt werden, z.B. während einer Arbeitspause, sofern eine automatisierte Überprüfung nicht eingerichtet ist.
(4) Bei Erkennung von Malware (Viren, Trojaner etc.) ist der Vorgesetzte umgehend zu informieren, auch wenn die Malware bereits durch das Virenschutzprogramm entfernt wurde.
(5) Der Anschluss privater Speichermedien, z.B. USB-Sticks, SD-Speicherkarten, CD’s/DVD’s und Smartphones u.a., am Arbeitsplatz oder im Firmennetzwerk ist nur nach ausdrücklicher Zustimmung der Geschäftsleitung erlaubt.
(6) E-Mails mit schutzwürdigen Inhalt (z.B. Daten die dem Berufsgeheimnis unterliegen) oder E-Mails mit sensitiven personenbezogenen Daten (z.B. Lohn- und Gehaltsdaten, Gesundheitsdaten etc.) sind mit Kennwort oder Zertifikat verschlüsselt zu übertragen. Solange kein standardisiertes Verschlüsselungsprogramm eingerichtet ist sind die vertraulichen Informationen als Anhang zu versenden, der mit einem Kennwort gegen unberechtigtes Lesen geschützt ist.

(7) Dateien und Dokumente dürfen nur dann mit einem Kennwort belegt werden, wenn die Geschäftsleitung darüber informiert wurde.
(8) Alle Anwendungsdaten müssen auf dem Server gespeichert werden, eine lokale Datenhaltung auf dem Arbeitsplatz ist zu vermeiden, sofern es dafür keine technische Begründung gibt. Diesbezügliche Ausnahmen müssen dem Administrator angezeigt werden. Mit Ausnahme der Datensicherung ist eine redundante Datenspeicherung (Kopien), d.h. Speicherung auf verschiedenen Medien, zu vermeiden.
(9) Die Weitergabe von personenbezogenen Daten oder ganzer Datenträger ist nur nach ausdrücklicher Zustimmung der Betroffenen zulässig, sofern keine gesetzliche Grundlage für die Weitergabe vorliegt.
(10) Auf den Arbeitsplätzen darf keine Software ohne ausdrückliche Zustimmung der Geschäftsleitung installiert werden; insbesondere dann nicht, wenn für diese Software kein Nutzungsrecht (Lizenz) vorliegt.
(11) Die Sicherheitseinstellungen (Browser, Virenschutz etc.) dürfen nicht verändert werden.
(12) Sofern Daten auf externen Datenträgern, z.B. auf Notebooks gespeichert werden, ist der Anwender verpflichtet die Daten täglich auf den Firmenserver zu übertragen und falls das nicht möglich ist oder einen unverhältnismäßig hohen Aufwand bedeuten würde, diese Daten täglich auf einem verschlüsselten Datenträger zu sichern.
(13) Vertrauliches bzw. schutzwürdiges Schriftgut, dazu gehören auch Fehldrucke, ist nur über Aktenvernichter oder über die bereitgestellten Sammelcontainer für die zentrale Aktenvernichtung zu entsorgen.
(14) E-Mails von unbekannten oder nicht vertrauenswürdigen Absendern dürfen nur im Textformat (Einstellung im E-Mail Client) geöffnet werden.
(15) E-Mail Anhänge dürfen nur vertrauenswürdigen Absendern geöffnet werden, wenn diese vorher vom Absender angekündigt wurden.
(16) In den Sicherheitseinstellungen der Office-Programme (MS-Word, MS-Excel, etc.) muss die automatische Ausführung von Makros deaktiviert werden.
(17) Die Geschäftsleitung oder eine von dieser beauftragten Person, z.B. der Administrator ist berechtigt stichprobenartig die Einhaltung der vorgenannten Verhaltensgrundsätze zu prüfen.

§ 8 Umgang mit Passwörtern

Alle Passwörter sind vertraulich und damit geheim zu halten. Für den Umgang mit den Passwörtern gelten folgende Regelungen:
(1) Passwörter sollten aus mindestens 10 Zeichen bestehen. Dabei sollte das Passwort Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten. In keinem Fall darf das Passwort von einem in einem Wörterbuch verzeichneten Wort hergeleitet werden können.
(2) Sofern bei der Einrichtung ein Standardpasswort vergeben wurde ist dieses bei der ersten Nutzung zu ändern.
(3) Ein Passwort-Sharing, d.h. gleiches Passwort für verschiedene Anwendungen ist zu vermeiden.
(4) Das Passwort sollte von Zeit zu Zeit geändert werden, spätestens jedoch dann, wenn die Vertraulichkeit des Passwortes nicht mehr gewährleistet werden kann.
(5) In den IT-Systemen darf keine Speicherung von Passwörtern im Klartext erfolgen
(6) Für Passwörter, die im Vertretungsfall bekannt sein müssen, beispielsweise Administrationspasswörter, gelten besondere Aufbewahrungspflichten (Safe, verschlossener Umschlag o.ä.)

§ 9 Information und Schulung der Mitarbeiter
Die Mitarbeiter werden durch den Datenschutzbeauftragten über die besonderen Datensicherheitsprobleme bei der Nutzung der elektronischen Kommunikationssysteme unterrichtet. Sie werden für den sicheren Umgang mit diesen Systemen und über die einschlägigen Rechtsvorschriften im Rahmen einer Datenschutzunterweisung informiert.

§ 10 Protokollierung und Kontrolle
Da die private Nutzung des Internetzugangs am Bildschirmarbeitsplatz untersagt ist, können zur Überprüfung der Regelungen dieser IT-Nutzungsrichtlinie sporadisch personenbezogene Stichproben in den Protokolldateien des Routers, der UTM oder im Proxy durchgeführt werden. Die Überprüfung erfolgt nach vorheriger Ankündigung oder nach dem 4-Augenprinzip bei dem der Zugriff auf die Protokolldateien nur durch die gleichzeitige Authentifizierung von zwei IT verantwortlichen Personen möglich ist. Eine automatisierte Vollkontrolle der Internet-, E-Mail und Telefonnutzung erfolgt nicht. Lediglich bei konkretem Missbrauchsverdacht im Einzelfall oder bei technischen Störungen wird eine Vollkontrolle durchgeführt. Die bei der Nutzung der Internetdienste anfallenden personenbezogenen Daten werden nicht zur Leistungs- und Verhaltenskontrolle verwendet. Sie unterliegen der Zweckbindung dieser Richtlinie und den einschlägigen datenschutzrechtlichen Vorschriften.

Die Protokolldateien enthalten folgende Informationen:

- Datum / Uhrzeit,
- IP-Adressen des Internetnutzers und der besuchten Webseiten und
- die übertragene Datenmenge.

Die Protokolle werden ausschließlich zu Zwecken der

- Analyse und Korrektur technischer Fehler
- Gewährleistung der Systemsicherheit
- Optimierung des Netzes
- statistischen Feststellung des Gesamtnutzungsvolumens
- Stichprobenkontrollen gemäß §§ 4-6
- Auswertungen gemäß § 11 dieser Vereinbarung (Missbrauchskontrolle) verwendet.

Aufbewahrungsfristen der Protokolldateien:

- max. 5 Tage für Web-Logs
- max. 3 Monate für System-Logs

Bei konkretem Missbrauchsverdacht kann die Aufbewahrungszeit für Web-Logs unter Einbeziehung des Datenschutzbeauftragten auf max. 30 Tage ausgedehnt werden. In diesen Fällen erfolgt die Auswertung personenbezogen und ohne Vorankündigung.

§ 11 Maßnahmen bei Verstößen / Missbrauchsregelung
(1) Bei Verdacht auf missbräuchliche/unerlaubte Nutzung des Internetzugangs gemäß §§ 4-6 dieser IT- Nutzungsrichtlinie durch einen Mitarbeiter erfolgt unter

Beteiligung des Administrators und des Datenschutzbeauftragten eine Überprüfung durch die Geschäftsleitung.
(2) Ein Verstoß gegen diese IT-Nutzungsrichtlinie kann neben den dienst- und arbeitsrechtlichen Folgen auch strafrechtliche Konsequenzen haben.
(3) Die Geschäftsleitung behält sich vor, bei Verstößen gegen diese IT-Nutzungsrichtlinie die Nutzung des Internetzugangs im Einzelfall zu untersagen.

_____
(Name des Mitarbeiters in Druckbuchstaben)

_____
(Datum, Unterschrift Mitarbeiter)