E-MAIL

RICHTER

Version 1.0 • 08/2023

Richtlinie E-Mail

Warum diese Richtlinie?

Diese Richtlinie soll die berechtigten Interessen des Arbeitgebers mit den Interessen, Grundfreiheiten und Grundrechten der Arbeitnehmer bei der E-Mail-Nutzung in Einklang bringen.

Geltungsbereich

Für die dienstliche Nutzung des E-Mail-Systems durch alle Mitarbeiterinnen und Mitarbeiter unseres Unternehmens gilt diese Richtlinie.

Zielsetzung

Ziel dieser Richtlinie ist

- Transparenz zu schaffen, welche Regeln für die Nutzung des E-Mail-Systems gelten;
- die Aufrechterhaltung der Kommunikation im Krankheitsfall oder beim Ausscheiden eines Mitarbeiters zu gewährleisten;
- die Wahrung der Persönlichkeitsrechte der Beschäftigten und die Gewährleistung des Schutzes ihrer personenbezogenen Daten.

RICHTLINIE

Technische Grundsätze

- Den Beschäftigten steht zur Erfüllung ihrer Aufgaben einE-Mail-System als Arbeitsmittel zur Verfügung. Die technische Betreuung der Beschäftigten sowie die Verwaltung ihrer Zugangsberechtigungen erfolgt durch die IT-Beauftragten bzw. die IT-Abteilung. Es ist nicht zulässig, dass Beschäftigte das MailProgramm eigenständig manipulieren oder deaktivieren. Dies gilt insbesondere für alle Sicherheitseinstellungen.
- Im Rahmen der gesetzlichen Aufbewahrungsfristen werden alle ein- und ausgehenden E-Mails mindestens für diese Dauer (bis zu zehn Jahren) gespeichert.

Verhaltensgrundsätze

- Jeder Mitarbeiter hat die Persönlichkeits- und Datenschutzrechte von Vorgesetzten, Kollegen, Kunden und Vertragspartnern bei der dienstlichen Nutzung der E-Mail zu beachten.
- In der Kommunikation mit Vorgesetzten, Kollegen, Kunden und Vertragspartnern wird auf einen professionellen, höflichen und respektvollen Umgangston geachtet.
- Das E-Mail-System wird ausschließlich für dienstliche Zwecke zur Verfügung gestellt. **Jegliche private Nutzung ist untersagt.**
- Private E-Mails, die über dienstliche E-Mail-Adressen empfangen werden, müssen unverzüglich gelöscht werden. Aus Gründen des Datenschutzes dürfen sich keine privaten E-Mails in der dienstlichen E-Mail-Ablage befinden.

- Werden private E-Mails auf dem E-Mail-Account eines Mitarbeitenden festgestellt, können diese E-Mails von der IT gelöscht werden, ohne dass der Mitarbeitende darüber informiert werden muss.
- Mitarbeiterinnen und Mitarbeiter, die mindestens einen Arbeitstag abwesend sind, haben den Abwesenheitsassistenten zur Benachrichtigung des Absenders zu aktivieren.
- Es ist nicht erlaubt, während der Abwesenheit eingehende E-Mails an E-Mail-Adressen ausserhalb des Unternehmens weiterzuleiten. Dies schließt auch die Weiterleitung an eine private E-Mail-Adresse der Mitarbeiterin oder des Mitarbeiters ein.
- Versand an mehrere Empfänger
  - Der Kreis der Empfängerinnen und Empfänger ist so klein wie möglich zu halten.
  - Ein Versand an mehrere Empfänger (unter CC) ist aus Gründen des Datenschutzes nicht zulässig, da unter CC alle E-Mail-Adressen für alle Empfänger sichtbar sind. Darum ist beim Versand an mehrere Empfänger immer die Verwendung von BCC erforderlich.
  - Mehrfachversand ist nur zulässig, wenn die E-Mail für die ausgewählten Empfänger relevant ist.
- Geschäftliche E-Mails unterliegen der sogenannten Fußzeilenpflicht und müssen die offizielle E-Mail-Signatur des Mitarbeiters / Arbeitgebers enthalten.
- Dokumente, die personenbezogene Daten oder sonstige sensible Daten enthalten, dürfen nicht in unverschlüsselter Form übermittelt werden.

RICHTLINIE

- Eine Antwort "an alle" sollte bei der Beantwortung einer E-Mail stets vermieden werden. Stattdessen sollte bevorzugt an ausgewählte Absender geantwortet werden.
- Das Ausführen von aktiven Inhalten (z. B. Makros) in heruntergeladenen Dokumenten ist untersagt!
- Der Zugriff auf den dienstlichen E-Mail-Account ist nach Beendigung des Arbeitsverhältnisses nicht mehr möglich.
  - Zur Aufrechterhaltung des Dienstbetriebes werden die E-Mails des ausscheidenden Mitarbeiters an die zuständigen Mitarbeitenden weitergeleitet.
  - Wird festgestellt, dass der Inhalt einer weitergeleiteten E-Mail privaten Charakter hat, so wird die E-Mail gelöscht, ohne dass der betroffene Mitarbeitende den Inhalt zur Kenntnis nimmt. Es erfolgt weder eine Weiterleitung noch eine Benachrichtigung.
- Das Unternehmen ist jederzeit zur Einschränkung oder Sperrung des Mail-Zugangs berechtigt. Eine Verpflichtung, einen Mail-Zugang bereitzustellen, besteht nicht.

Netiquette

- Die Mitarbeiterinnen und Mitarbeiter haben die folgenden Regeln bei der Nutzung unseres E-Mail-Systems zu beachten:
- Überprüfen Sie jede E-Mail sorgfältig auf Rechtschreib-, Grammatik- und Formatierungsfehler, bevor Sie sie versenden.
- Lesen Sie den Text Ihrer E-Mail aus der Sicht des Empfängers noch einmal durch, bevor Sie die E-Mail versenden.

- Formulieren Sie klar und präzise. Vermeiden Sie Abkürzungen, Slangausdrücke oder unklare Formulierungen, die vom Empfänger missverstanden werden könnten.
- Verwenden Sie einen aussagekräftigen Betreff. Der Betreff sollte eine kurze Zusammenfassung des Inhalts der E-Mail enthalten. So kann der Empfänger schnell erkennen, worum es geht. Auch das Wiederfinden bereits abgelegter E-Mails wird durch einen aussagekräftigen Betreff erleichtert.
- Verwenden Sie beim Schreiben einer Nachricht zu einem neuen Thema NIEMALS die Funktion „Antworten“ einer alten E-Mail. In diesem Fall wird der Inhalt der alten Nachricht zitiert und der Betreff bleibt unverändert. Dies führt auf beiden Seiten zu Verwirrung und ist in höchstem Maße unhöflich. Hinzu kommt, dass die Mail im Zweifelsfall nicht mehr gefunden werden kann. Es gilt also: neues Thema, neue Mail, neuer Betreff.
- Verwenden Sie in der externen Kommunikation immer eine förmliche Anrede und Verabschiedung, wie sie im Geschäftsleben üblich sind.
- Prüfen Sie vor dem Versenden, ob die E-Mail-Adresse des Empfängers stimmt und nicht ein falscher Adressat angegeben wurde.
- Nur wenn es wirklich wichtig ist, sollten E-Mails als "wichtig” gekennzeichnet werden.
- Bleiben Sie Ihrerseits immer höflich und sachlich, wenn Sie unhöfliche oder beleidigende E-Mails erhalten.
- Vergewissern Sie sich, dass alle Anhänge vollständig und korrekt sind, bevor Sie die E-Mail versenden.

RICHTLINIE

- Vermeiden Sie es, Dateien anzuhängen, die für den Empfänger nicht von Interesse sind oder zu groß sind, um sie per E-Mail zu versenden.
- Verboten ist das Versenden von privaten Bildern oder lustigen Anhängen. Also darauf verzichten!
- Ein kurzes Telefongespräch kann in vielen Fällen schneller zur Lösung eines Kommunikationsproblems beitragen als der Austausch zahlreicher E-Mails.

Werbe-E-Mails

- Eingehende E-Mails werden nach unverlangter Werbung gefiltert und entsprechende Mails in einen getrennten Ordner (Spam) verschoben. Mitarbeitende müssen diesen Ordner regelmäßig (mindestens 1x täglich) sichten, da E-Mails falsch zugeordnet sein können.

Sicherheitsmaßnahmen gegen Phishing

Bei jeder E-Mail, die Sie erhalten, sollten Sie auf die folgenden Punkte prüfen:

Absender (from) beachten!

- Kennen Sie die Absenderadresse? Ist es eine Person, mit der Sie sonst in Kontakt oder in einer Geschäftsbeziehung sind?
- In jedem Fall ist Vorsicht geboten, wenn eine E-Mail von jemandem außerhalb unseres Unternehmens kommt und nichts mit Ihrem Aufgabenbereich zu tun hat.
- Wenn Sie E-Mails von Kunden, Lieferanten, Kollegen oder Mitarbeitern erhalten, die sehr ungewöhnlich oder untypisch für den Absender sind: Lassen Sie Vorsicht walten.

- Schauen Sie sich die Domain des Absenders an: Ist sie verdächtig? Um Vertrauen zu schaffen, werden oft scheinbar bekannte Domains wie paypal-helpdesk.com verwendet.
- Seien Sie vorsichtig, wenn Ihnen jemand, mit dem Sie lange nicht kommuniziert haben, unerwartet eine E-Mail mit einem Hyperlink oder einem Anhang schickt.

Adresse (to:) ansehen!

- Seien Sie vorsichtig bei E-Mails, die auch an Ihnen unbekannte Personen geschickt werden.
- Mails, die an eine Auswahl von Personen geschickt werden, die nichts miteinander zu tun haben, weil sie zum Beispiel in unterschiedlichen Abteilungen arbeiten, sind ein Indikator für Social Engineering.

Problematische Hyperlinks!

- Wenn die Adresse eines Hyperlinks in der Nachricht zu einer unbekannten Website führt (Sie erkennen dies, wenn Sie den Mauszeiger über den Link bewegen), klicken Sie besser nicht darauf.
- Da Links in E-Mails immer mit Vorsicht zu genießen sind, sollten Sie den angebotenen Link grundsätzlich manuell im Browser eingeben und nicht anklicken.
- Bitte beachten: Links in E-Mails enthalten oft die falsch geschriebene Adresse einer bekannten Website. In diesem Beispiel wurde bei PayPaI.com das kleine ”l” durch ein großes ”i” ersetzt. Bekannte Adressen können auch durch die Verwendung von Zeichen aus dem russischen oder griechischen Alphabet verfälscht werden.

- Eine ansonsten leere E-Mail, die nur ein paar Links enthält, sollten Sie sofort löschen. Klicken Sie auf keinen dieser Links.

Datum und Uhrzeit okay?

Wenn Sie eine E-Mail mitten in der Nacht und nicht wie üblich während der Geschäftszeiten erhalten, ist Misstrauen angebracht.

Passen Betreff und Thema?

Seien Sie vorsichtig, wenn die Betreffzeile einer E-Mail nicht aussagekräftig ist und nicht zum Inhalt der Nachricht passt oder wenn die E-Mail anscheinend eine Antwort auf eine E-Mail ist, die Sie nie gesendet haben.

Schädliche Anhänge!

Das Verstecken von Schadsoftware in Anhängen ist eine regelmäßige Praxis. Klicken Sie nicht auf einen Anhang, wenn Sie eine E-Mail mit einem nicht erwarteten Anhang erhalten. Auch dann nicht, wenn die E-Mail einen interessanten Inhalt verspricht oder wenn sie von einer bekannten E-Mail-Adresse kommt! Es gibt nur EINEN Dateityp, den Sie ohne Bedenken öffnen können: eine Datei mit der Endung .txt.

Verführerischer Inhalt!

- Social Engineers recherchieren ihre Zielpersonen bis ins kleinste Detail und wissen oft über Ihre Hobbys oder andere Anknüpfungspunkte Bescheid. Entsprechend wird der Inhalt der E-Mail gestaltet. Wenn Ihnen die Chance auf einen wertvollen Gewinn in Aussicht gestellt wird, wenn Sie wichtige Informationen über Ihr Hobby erhalten oder ein teures Gerät kostenlos testen können: Löschen Sie die

Mail UMGEHEND und vergessen Sie sie. Das gilt auch für Mails, in denen Druck ausgeübt und zur Eile gemahnt wird, um negative Konsequenzen zu vermeiden. **LÖSCHEN SIE DIE MAIL UMGEHEND!**

- Beachten Sie auf keinen Fall eine Mail, die schlechte Grammatik oder Rechtschreibfehler enthält.
- Oft wird in E-Mails behauptet, es seien kompromittierende Bilder von Ihnen oder Ihnen bekannten Personen im Umlauf, die Sie durch Anklicken eines Links sehen können. Das ist eine Falle. Beachten Sie die Mail nicht weiter und löschen Sie sie.
- Folgen Sie Ihrem Bauchgefühl. Klicken Sie auf keinen Link und öffnen Sie keine Datei, wenn Sie das Gefühl haben, dass etwas nicht stimmt. Im Umkehrschluss garantiert aber auch ein gutes Bauchgefühl keine Sicherheit.
- Denken Sie immer daran, dass es sich bei den Social Engineers um technisch und psychologisch gut ausgebildete Personen handelt, die ihre E-Mails und Strategien mittlerweile mithilfe von KI entwerfen. Das Erkennen von Fallen wird in Zukunft immer schwieriger werden.

Protokollierung und Kontrolle

- Die Nutzung von Internet und E-Mail wird protokolliert. Dabei werden die folgenden Daten erfasst:
    - Datum/Uhrzeit
    - Adressen von Absender und Empfänger
    - Dateiformate und übertragene Datenmenge
- Weiterhin werden Daten in den jeweiligen Server-, Netzwerkbetriebs- und Anwendungssystemen erfasst.

- Diese Daten werden nur aus Gründen der
  - - Daten- und Systemsicherheit
  - - Systemtechnik (z. B. zur Fehlerverfolgung) und
  - Betriebsorganisation (z. B. zur Feststellung von Art und Umfang der Nutzung und zur Missbrauchskontrolle)

  verarbeitet.
- Zusätzlich werden in regelmäßigen Abständen stichprobenartige Kontrollen der Log-Dateien durchgeführt, um die Einhaltung dieser Richtlinie zu überprüfen.
- Die Daten werden nicht zu Zwecken der Leistungs- und Verhaltenskontrolle verwendet und unterliegen der Zweckbindung dieser Richtlinie sowie den datenschutzrechtlichen Bestimmungen der Datenschutz-Grundverordnung (DSGVO).
- Eine inhaltliche Kontrolle findet grundsätzlich nicht statt. Ausnahmen sind z. B. die Überprüfung auf Schadsoftware oder auf eine missbräuchliche Nutzung unserer Systeme.
- Die Mitarbeiterinnen und Mitarbeiter, die Zugriff auf die Protokolldateien haben, wurden auf die Sensibilität der Daten hingewiesen und auf die Einhaltung des Datenschutzes verpflichtet.

Verschwiegenheitspflicht

- Auch bei der Nutzung unseres E-Mail-Systems gilt die Verschwiegenheitspflicht aller Mitarbeiterinnen und Mitarbeiter, insbesondere die Pflicht zur Wahrung von Betriebs- und Geschäftsgeheimnissen.

- **Es ist ausdrücklich untersagt, vertrauliche Informationen wie z. B. Geschäftspläne, Budgets, Kunden- und Lieferdaten über das Internet oder das E-Mail-System zu verbreiten.**

Verdacht auf Strafbarkeit

Besteht der Verdacht strafbarer Handlungen im Beschäftigungsverhältnis, entscheidet der Arbeitgeber unter Berücksichtigung des § 26 Abs. 1 Satz 2 BDSG (neu), wie vorzugehen ist und weitere Stellen, z. B. Ermittlungs- und Strafverfolgungsbehörden, einzuschalten sind. Soweit ein betrieblicher Datenschutzbeauftragter bestellt ist, ist dieser beratend hinzuzuziehen.

Arbeitsrechtliche Konsequenzen

Auf arbeitsrechtliche Konsequenzen bei Nichteinhaltung dieser Richtlinien bis hin zur ordentlichen oder außerordentlichen Kündigung wird ausdrücklich hingewiesen.