

Compliance im Umgang mit E-Mail

mag. iur. Maria Winkler

Agenda

- E-Mail im Business-Alltag
- Die Verbindlichkeit der E-Mail-Kommunikation
- E-Mail als Beweismittel
- E-Mail-Policy und Überwachung

E-Mail im Business-Alltag

E-Mail dient den Unternehmen als kostengünstiges, schnelles und effizientes Kommunikationsmittel, es dient

- als Ersatz für Telefon,
- als Ersatz für schriftliche Korrespondenz
- zur Abwicklung ihrer privaten Korrespondenz (auch in der Freizeit durch Zugriff auf das Firmen-E-Mail über mobile End-Geräte)
- In der Regel bestehen keine oder nur unzureichende Vorgaben, wie E-Mail in Unternehmen verwendet werden darf!

Herausforderungen

- Wie verbindlich ist die E-Mail-Kommunikation?
- Ist ein E-Mail ein gültiges Beweismittel?
- Welche Sorgfaltspflichten bestehen bei der Weiterleitung vertraulicher Informationen per E-Mail?
- Wie ist bei einem Verdacht auf eine strafbare Handlung eines Mitarbeitenden vorzugehen?
- Wie stellt man den jederzeitigen und vollständigen Zugriff auf die geschäftsrelevanten E-Mails sicher?

Verbindlichkeit der E-Mail-Kommunikation

- Rechtlich verbindliche Erklärungen bedürfen nur in seltenen Fällen einer bestimmten Form - sie können daher meist auch mit unsignierten E-Mails ausgetauscht werden.
- Eine der Handunterschrift gleichgestellte elektronische Signatur ist nur erforderlich, wenn das Gesetz die Schriftform verlangt oder die Parteien diese vereinbaren!
- E-Mail-Erklärungen sind daher in der Regel verbindlich!

E-Mail als Beweismittel

- In einem Rechtsstreit muss jede Partei die ihr günstigen Tatsachen beweisen - ein Beweis kann auch die Vorlage eines E-Mails erbracht werden.
- Die Problematik der Beweisführung mittels E-Mail liegt nicht in der Eignung des E-Mails als Beweismittel sondern in dessen Beweiskraft.
- Wird die **Beweiskraft des E-Mails** im Zivilprozess bestritten, dann scheitert unter Umständen der Beweis und das Unternehmen verliert den Prozess!

Erhöhung der Beweiskraft

- **Elektronische Signaturen** ermöglichen den Nachweis der Identität der signierenden Person und den Nachweis, dass das Dokument nicht verändert wurde.
- Elektronische Signaturen ermöglichen jedoch **nicht** den Nachweis, dass ein E-Mail versandt oder empfangen wurde oder die Wiederherstellung des ursprünglichen Dokuments!
- Die Integrität von E-Mails kann auch durch die Speicherung auf **unveränderbaren Datenträgern** oder eine Kombination von technischen und organisatorischen Massnahmen gesichert werden.

Empfehlung

- Anhand von Risikoüberlegungen ist zu entscheiden, welche Prozesse mittels E-Mail abgewickelt werden dürfen.
- Werden wichtige geschäftsrelevante Informationen mit E-Mail versandt und/oder empfangen, dann muss deren Beweiskraft gesichert werden.
- Dazu müssen E-Mails systematisch geordnet abgelegt und mit technischen und organisatorischen Massnahmen vor unbefugten Änderungen geschützt werden.
- Ist der Nachweis des Empfangs oder des Versands von E-Mails erforderlich, dann sind zusätzliche Massnahmen zu ergreifen!

Nutzung von E-Mail am Arbeitsplatz

- Im Rahmen seiner **Weisungsbefugnis** bestimmt der Arbeitgeber, wie E-Mail im Unternehmen verwendet werden darf. Er muss dabei die Persönlichkeit der Mitarbeitenden schützen.
- Die erlaubte Verwendung sollte in einem **Nutzungsreglement** festgehalten werden (fakultativ).
- Soll deren Einhaltung kontrolliert werden, dann muss zuvor ein **Überwachungsreglement** publiziert werden (obligatorisch).

E-Mail-Policy

- In der Praxis werden die erlaubte Nutzung und die Überwachung in **E-Mail-Policies** geregelt!
- E-Mail-Policies verschaffen Klarheit über die erlaubte Nutzung, geben Verhaltensregeln vor, regeln die Überwachung und mögliche Sanktionen bei Verstößen.
- Aus Gründen der Transparenz und der Rechtssicherheit sowie zur Erleichterung des Nachweises wird die schriftliche Abgabe mit Quittierung durch die Mitarbeitenden empfohlen!

Geschäftlich oder privat?

- Die private Verwendung des geschäftlichen E-Mails tangiert die Interessen des Unternehmens (z.B. Sicherheitsrisiken, Belastung der Speicherkapazitäten, Verletzung von Geschäfts- und Fabrikationsgeheimnissen, etc.)
- Die private Nutzung des geschäftlichen E-Mails kann daher verboten, eingeschränkt oder erlaubt werden.
- Auch wenn die private Nutzung erlaubt ist oder keine Regelung besteht, müssen die Mitarbeitenden die Interessen des Unternehmens schützen (**Treuepflicht**).

Vorbehalt der geschäftlichen Nutzung

Darf E-Mail nur geschäftlich genutzt werden, dann

- dürfen alle E-Mails automatisch protokolliert und gespeichert werden
- darf das Unternehmen auf alle E-Mails zugreifen.
- Auch wenn nur die geschäftliche Nutzung erlaubt ist, dürfen E-Mails, welche eindeutig als **private Korrespondenz** zu erkennen sind, durch den Arbeitgeber **nicht gelesen** werden!
- Eine vollständige Verhinderung eingehender privater E-Mails ist nicht möglich!

Erlaubte private Nutzung

- Private Post - dazu zählen auch E-Mails - genießt auch am Arbeitsplatz uneingeschränkten Schutz. Private Post ist ungeöffnet an die adressierte Person weiterzuleiten.
- Auch wenn die private Nutzung von E-Mail erlaubt ist, kann das Unternehmen von der geschäftlichen Natur eines E-Mails ausgehen, wenn **kein Unterscheidungsvermerk** besteht und die private Natur des E-Mails nicht erkennbar ist.
- Die Mitarbeitenden sind daher anzuhalten, private E-Mails als privat zu kennzeichnen und in separaten Ordnern oder auf separaten Datenträgern abzulegen.

Verhaltensregeln

- Zu empfehlen sind Regelungen über die Gestaltung von E-Mails, die Einhaltung von Sicherheitsvorgaben, die Ablage und Archivierung von E-Mails, etc.
- Zudem sollte verbindlich geregelt werden, dass vertrauliche Informationen wie z.B. sensible Personendaten oder **Geschäfts- und Fabrikationsgeheimnisse** nicht mit unverschlüsseltem E-Mail versandt werden dürfen!

Verhaltensregeln

- Verbindliche Vorgaben bei geplanten und ungeplanten Abwesenheiten der Mitarbeitenden sichern den Zugriff des Unternehmens auf geschäftsrelevante Informationen
- Die **Benennung von Stellvertretern** stellt den Zugriff auf die E-Mails bei Krankheit sicher. Der Stellvertreter sollte private E-Mails nicht lesen können.
- Vor dem **Austritt** aus dem Unternehmen müssen alle geschäftsrelevanten E-Mails übergeben und die privaten E-Mails gelöscht werden.

Überwachungsreglement

- Mit welchen Kontrollen ist zu rechnen (Kontrolle der technischen Ressourcen, Stichproben der Nutzungsreglemente)
- Gründe und Voraussetzungen der Kontrollen (Gewährleistung von Stabilität und Sicherheit der technischen Infrastruktur; Verdacht auf Missbrauch)
- Wer ordnet Kontrollen an
- Welche Daten werden protokolliert und wie lange werden diese aufbewahrt
- Wer erhält Einsicht in Auswertungen
- Welche Sanktionen sind möglich

Protokollierungen

- Eine Protokollierung ist eine fortlaufende Aufzeichnung der Randdaten wer was wann macht.
- Die E-Mail-Policy muss die Protokollierungen, ihren Zweck, den Inhalt und die Aufbewahrungsdauer angeben.
- Protokollierungen von privaten E-Mails dürfen nur die E-Mail-Adresse des Arbeitnehmers, den Vermerk „privat“, das Datum und die Zeitangaben enthalten.

Überwachungsmaßnahmen

- Die technische Prävention, die Sensibilisierung und die Mitwirkung der Mitarbeitenden hat Vorrang vor der Überwachung!
- Die technischen Schutzmassnahmen müssen regelmässig dem neuesten Stand der Technik angepasst werden.
- Eine Überwachung ist nur zulässig, wenn die Mitarbeitenden zuvor informiert wurden.
- Die Einhaltung der E-Mail-Policy darf zunächst nur durch die **anonyme oder pseudonyme Auswertung** von Protokollierungen überwacht werden.

Feststellung des Missbrauchs

- Eine personenbezogenen Auswertung von Protokollierungen setzt einen Verdacht auf Missbrauch voraus.
- Ein Missbrauch liegt vor, wenn gegen die E-Mail-Policy verstossen wird oder, wenn eine solche fehlt, wenn der Mitarbeitende die Treuepflicht verletzt.
- Ein Missbrauch kann im Rahmen einer Überwachung, bei der Gewährleistung der IT-Sicherheit oder durch andere Hinweise festgestellt werden.
- Die Daten, welche bei der Überwachung erhoben werden sind vor unberechtigtem Zugriff zu schützen!

Verdacht auf strafbare Handlung

- Bei Verdacht auf eine strafbare Handlung dürfen die Beweise wie z.B. Backups gesichert werden und Protokollierungen dürfen personenbezogen ausgewertet werden.
- Bei Vorliegen eines konkreten Verdachts auf eine strafbare Handlung und eines Rechtfertigungsgrundes (z.B. Einwilligung) darf das Unternehmen auch **direkt auf private E-Mails** zugreifen.
- Willigt der Mitarbeitende nicht ein, dann sollte der Zugriff auf die privaten E-Mails den **Untersuchungsbehörden** überlassen werden.

Sanktionen

- Die Mitarbeitenden haften gegenüber dem Unternehmen für die Schäden, welche sie diesem zufügen.
- In der E-Mail-Policy sollten die Sanktionen wie z.B. Abmahnungen, Lohnkürzungen, Schadenersatzforderungen, etc. bezeichnet werden.
- Die Sanktionen müssen durch die Vorgesetzten ausgesprochen werden und sie müssen der Schwere des Missbrauchs **angemessen** sein.

Leitfaden des EDÖB

- Auf der Website des EDÖB ist ein „Leitfaden über Internet- und E-Mail-Überwachung am Arbeitsplatz“ mit einem **Musterreglement** publiziert
- <http://www.edoeb.admin.ch/dokumentation/00445/00472/00532/index.html?lang=de>

Empfehlungen

- Um die Risiken, welche sich durch den Einsatz von E-Mail im Unternehmen ergeben angemessen zu reduzieren ist die erlaubte Verwendung verbindlich in einer E-Mail-Policy zu regeln.
- Die Einhaltung der Policy soll überwacht werden - dabei ist die Persönlichkeit der Mitarbeitenden zu schützen!
- Zusätzlich ist dafür zu sorgen, dass geschäftsrelevante E-Mails systematisch geordnet abgelegt werden und deren Beweiskraft erhalten bleibt.

Fragen und Antworten

mag. iur. Maria Winkler

im Auftrag der

Webgate Consulting AG

Seestrasse 202

8810 Horgen

www.webgate.biz