IT-Sicherheitsrichtlinie UNTERNEHMEN/ORGANISATION

**Inhalt**

[1 Allgemeines 2](#_Toc195606551)

[1.1 Zielsetzung 2](#_Toc195606552)

[1.2 Zulässigkeit der Nutzung 2](#_Toc195606553)

[1.3 Verantwortlichkeit 2](#_Toc195606554)

[2 E-Mail-System 3](#_Toc195606555)

[2.1 Sichere Nutzung von E-Mails 3](#_Toc195606556)

[2.2 Betriebliche Nutzung von E-Mails 3](#_Toc195606557)

[3 Nutzung des Internets 4](#_Toc195606558)

[3.1 Sichere Nutzung des Internets 4](#_Toc195606559)

[3.2 Betriebliche Nutzung des Internet 4](#_Toc195606560)

[3.2.1 Grundsätze 4](#_Toc195606561)

[3.2.2 Fernzugriffe auf das System 5](#_Toc195606562)

[3.2.3 Verhaltensgrundsätze 5](#_Toc195606563)

[4 Mobiles Arbeiten 6](#_Toc195606564)

[5 Videomeetings, Videokonferenzen 6](#_Toc195606565)

[5.1 Organisation einer Videokonferenz durch Mitarbeiter:innen 6](#_Toc195606566)

[5.2 Teilnahme an einer Video-Konferenz auf Einladung 7](#_Toc195606567)

[6 Unternehmensinternes Netz 7](#_Toc195606568)

[6.1 Nutzung der Firmen-IT 7](#_Toc195606569)

[6.2 Regelung zur Speicherung von betrieblichen Daten und Dokumenten 7](#_Toc195606570)

[6.3 Nutzung von mobilen Geräten (Smartphones, Tablets, Laptops etc.) 8](#_Toc195606571)

[6.4 Passwort-Gebrauch Unternehmensnetz und Fachanwendungen 8](#_Toc195606572)

[6.5 Protokollierung und Kontrolle 9](#_Toc195606573)

[7 KI-Systeme 9](#_Toc195606574)

[8 Maßnahmen bei Verstößen / Missbrauchsregelung 13](#_Toc195606575)

[9 Änderungen und Inkrafttreten, Konsequenzen bei Nichteinhaltung 14](#_Toc195606576)

# Allgemeines

Diese Richtlinie regelt die Grundsätze für Einsatz und Anwendung elektronischer Kommunikationssysteme und den Betrieb und die Nutzung der informationstechnischen Infrastruktur bei der Firma und gilt für alle Beschäftigten, die mit solchen Systemen arbeiten. Diese Richtlinie umfasst unter anderem:

* das E-Mail-System
* Nutzung des Internet,
* Mobiles Arbeiten,
* Videokonferenzen, Video-Meetings,
* das geschäftliche Netz und die Informationstechnik des Unternehmens,
* die Nutzung von KI-Systemen. **NEU**

## Zielsetzung

Ziel dieser Richtlinie ist es, den Einsatz einer leistungsfähigen und zeitgemäßen Technik mit dem Schutz der Persönlichkeitsrechte für die betroffenen Mitarbeiterinnen und Mitarbeiter zu verbinden.

Die zur Verfügung gestellten Dienste dienen der Information und der Kommunikation im Interesse der Firma. Bei ihrer Nutzung muss die Sicherheit des IT-Systems bzw. Firmennetzes gewährleistet bleiben.

## Zulässigkeit der Nutzung

Das IT-System steht allein zu geschäftlichen Zwecken zur Verfügung. Jegliche private Nutzung bedarf der ausdrücklichen Erlaubnis durch die Geschäftsleitung.

## Verantwortlichkeit

Die Verantwortung für die Beachtung der vorgenannten Festlegungen und Hinweise obliegt der obersten Leitung sowie den Mitarbeiter:innen. Diese haben insbesondere auch sicherzustellen, dass eine Nutzung des Internets durch Unbefugte vom Arbeitsplatz aus nicht erfolgt.

# E-Mail-System

## Sichere Nutzung von E-Mails

1. **Vorsicht bei Anhängen und Links**: Öffnen Sie keine Anhänge und klicken Sie nicht auf Links in E-Mails von unbekannten Absendern. Diese könnten Phishing-Versuche oder Malware enthalten.
2. **Überprüfen Sie die Absenderadresse**: Phishing-E-Mails verwenden oft gefälschte Absenderadressen, die echten Adressen ähneln. Überprüfen Sie die Adresse sorgfältig, bevor Sie auf eine E-Mail reagieren.
3. **Vertrauliche Informationen schützen**: Geben Sie keine vertraulichen Informationen wie Passwörter oder Bankdaten per E-Mail weiter. Nutzen Sie sichere Kommunikationswege für solche Informationen.
4. **Verdächtige E-Mails melden**: Wenn Sie eine verdächtige E-Mail erhalten, melden Sie diese sofort der IT-Abteilung. Löschen Sie die E-Mail nicht, bevor sie überprüft wurde.

## Betriebliche Nutzung von E-Mails

Über geschäftliche E-Mail-Adressen eingehende private E-Mails sind wie private schriftliche Post zu behandeln. Eingehende private, aber fälschlich als Firmenpost behandelte E-Mails sind den betreffenden Beschäftigten unverzüglich nach Bekanntwerden ihres privaten Charakters zur alleinigen Kenntnis zu geben.

Die betreffenden Beschäftigten informieren nach Kenntnisnahme den Absender der privaten E- Mails, dass die geschäftlichen E-Mail-Adressen nicht für private Zwecke genutzt werden dürfen. Die privaten E-Mails sind danach unverzüglich zu löschen.

Dokumente, die personenbezogene oder andere sensible Daten beinhalten, dürfen nicht unverschlüsselt übertragen werden oder sollten zumindest kennwortgeschützt sein.

Für den Fall einer geschäftlichen Abwesenheit (Urlaub, Krankheit etc.) hat der Mitarbeiter eigenverantwortlich eine automatisierte Antwort an den Absender eingehender E-Mails einzurichten, die den Absender über die Abwesenheit informiert und einen Hinweis auf den zuständigen Vertreter und dessen Telefonnummer enthält. Gleichwohl wird eine Weiterleitung der E-Mail an die Vertretung eingerichtet!

Mit Beendigung des Beschäftigungsverhältnisses steht die E-Mail-Adresse dem jeweiligen Beschäftigten nicht mehr für diesen zur weiteren Nutzung zur Verfügung. Geschäftliche E-Mails werden zur Aufrechterhaltung des Geschäftsbetriebes an zuständige Beschäftigte weitergeleitet. Ist ein privater Charakter des Inhaltes dieser weitergeleiteten E-Mail ersichtlich, ist die E-Mail ohne weitere Kenntnisnahme des Inhaltes durch die jeweiligen Beschäftigten zu löschen. Eine Weiterleitung erfolgt nicht.

# Nutzung des Internets

## Sichere Nutzung des Internet

1. **Vermeiden Sie unsichere Websites**: Besuchen Sie nur vertrauenswürdige Websites. Achten Sie auf das Schloss-Symbol in der Adressleiste Ihres Browsers, das eine sichere Verbindung anzeigt.
2. **Downloads mit Vorsicht behandeln**: Laden Sie keine Dateien von unbekannten oder verdächtigen Websites herunter. Diese könnten Malware oder Viren enthalten.
3. **Nutzung öffentlicher WLAN-Netzwerke**: Nutzen Sie ausschließlich öffentliche WLAN-Netze, wenn diese verschlüsselt sind. Dieses wird Ihnen beim Verbindungsaufbau angezeigt.

## Betriebliche Nutzung des Internet

Die Internetnutzung dient grundsätzlich geschäftsmäßigen Zwecken. Soweit sich die Nutzung auf Einzelfälle beschränkt und eine ordnungsgemäße Erledigung der Aufgaben gewährleistet ist, dürfen auch Angebote zu privaten Zwecken im Internet genutzt werden.

### Grundsätze

Das Abrufen und Ausführen von Dateien oder Programmen aus und im Internet ist nur von und bei den von der Geschäftsführung bekannt gegebenen Anbietern gestattet, soweit deren Inhalte für den innerbetrieblichen Gebrauch benötigt werden. Urheberrechtlich geschützte Dateien, für die keine Lizenz vorhanden ist, dürfen nicht abgerufen und gespeichert werden. Ermöglicht die Berechtigung der Beschäftigten das Abrufen und die Installation von Treibern, Setup-Programmen oder ähnlicher systemeingreifender Software, muss dieses vorher von der Geschäftsführung genehmigt werden.

Das Ausführen von aktiven Inhalten (z.B. Makros) in heruntergeladenen Dokumenten ist nur bei als vertrauenswürdig gekennzeichneten Anbietern gestattet. Die Einstellungen in die zugehörigen Anwendungen werden von der Geschäftsführung durchgeführt oder beauftragt.

Das Abrufen von kostenverursachenden Informationen oder Inhalten aus dem Internet ist von der Geschäftsführung zu genehmigen. Das Anrufen von kostenverursachenden Sonder-, Service- oder ausländischen Rufnummern ist von der Geschäftsführung zu genehmigen.

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.

### Fernzugriffe auf das System

Ferngesteuerte Zugriffe oder Steuerungen von Rechnersystemen über sogenannte Remote- Anwendungen bzw. Terminal-Emulationen sind grundsätzlich nicht zugelassen. Sollte Bedarf für Remote-Zugriffe bzw. Terminal-Emulationen bestehen, sind diese bei

### Verhalten im Internet

Die Beschäftigten haben jede Nutzung des Internets zu unterlassen, die geeignet ist, den Interessen des Unternehmens oder dessen Ansehen in der Öffentlichkeit zu schaden, die Sicherheit des Unternehmensnetzes 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. die Nutzung des Internets zur Erledigung privater Rechtsgeschäfte, insbesondere die Nutzung von Zahlungsfunktionen (Onlinebanking, Internetversandhandel, eBay o.ä.) und
4. die Nutzung von Onlinespieleplattformen.

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.

# Mobiles Arbeiten

Die oberste Leistung gestattet mobiles Arbeiten grundsätzlich nur nach Vereinbarung mit den betreffenden Mitarbeiter:innen. Hierzu wird ausschließlich die Anlage 1 zu dieser Richtlinie genutzt. Mit allen Mitarbeiter:innen, die mobil arbeiten, werden die Regelungen festgelegt.

# Videomeetings, Videokonferenzen

Die Nutzung von Video- / Web-Konferenzen ist grundsätzlich zugelassen.

## Organisation einer Videokonferenz durch Mitarbeiter:innen

Die Einladung zur Teilnahme gegenüber internen wie externen Teilnehmer:innen erfolgt ausschließlich anhand der freigegebenen Software.

Die einladende Person trägt die Verantwortung dafür, dass die folgenden Regelungen eingehalten werden:

- Die Konferenz darf nicht aufgezeichnet werden.

- Es kann trotz entsprechender Sicherheitsmaßnahmen bei der Teilnahme externer Personen geschehen, dass diese Sitzungen aufzeichnen / mitfilmen. Die Mitarbeiterinnen und Mitarbeiter werden deshalb gebeten ihre Aussagen und Stellungnahmen daraufhin sorgsam und überlegt zu wählen.

Die Einladung zur Webkonferenz muss unter dem Hinweis erfolgen, dass die Konferenz vertraulich ist und die teilnehmenden Personen sicherzustellen haben, dass unberechtigte Personen nicht mithören oder mitsehen können.

## Teilnahme an einer Video-Konferenz auf Einladung

Sofern Mitarbeiter:innen auf Einladung einer dritten Person / Stelle an einer Video-Konferenz teilnehmen, ist dieses gestattet. Die bestehenden Regelungen zum Datenschutz sind weiter einzuhalten.

# Unternehmensinternes Netz

## Nutzung der Firmen-IT

Alle Mitarbeiter verpflichten sich die Firmen-IT (u.a. Workstations, Notebooks, Server, Drucker usw.) schonend und sorgfältig zu nutzen. Die Nutzung der Firmen-IT darf nur zu betrieblichen Zwecken erfolgen.

Das Einbringen von Software auf Firmen-IT ist nur nach vorheriger Genehmigung durch die Geschäftsführung zulässig. Die Nutzung privater Software auf Firmen-IT ist aus lizenzrechtlichen und sicherheitsbedingten Gründen untersagt.

Das Erstellen und Speichern privater Daten und Dokumente auf der Firmen-IT ist ebenfalls untersagt. Die Nutzung privater Hardware (u.a. Speichersticks, PDAs, Notebooks, externe Festplatten, Mobiltelefone usw.) mit der Firmen-IT ist nur nach vorheriger Genehmigung durch die Geschäftsführung zulässig.

## Regelung zur Speicherung von betrieblichen Daten und Dokumenten

Alle Mitarbeiter verpflichten sich alle Daten und Dokumente zentral auf dem Fileserver zu speichern. Nur so kann gewährleistet werden, dass alle Daten und Dokumente in den jeweils aktuellen Versionen gesichert werden können.  
Das Abspeichern von Dokumenten und Daten auf der lokalen Festplatte ist untersagt.  
Von der Geschäftsführung beauftragte IT-Fachkräfte werden bei Bedarf die lokalen Festplatten prüfen und darauf gespeicherte Daten und Dokumente löschen, um einen reibungslosen Betrieb zu gewährleisten.

## Nutzung von mobilen Geräten (Smartphones, Tablets, Laptops etc.)

Soweit nicht ausdrücklich eine Zustimmung der Geschäftsleitung erfolgt ist, darf die Nutzung von mobilen Geräten mit vom Unternehmen oder der IT freigegebenen Geräten ausschließlich für geschäftliche Zwecke erfolgen.  
Häufig tritt Datenverlust durch Diebstahl eines Geräts auf. Neben dem unmittelbaren Verlust des Geräts kommt hinzu, dass die Daten, die sich auf dem Gerät befunden haben, durch Fremde eingesehen und missbraucht werden können.

Um das Risiko eines (ungewollten) Datenverlustes zu verringern, sind nachfolgende Regeln zu beachten:

* Nutzeridentifikation: Soweit technisch möglich sind Maßnahmen wie Kennwortschutz, PIN, Tastensperren, etc. zu verwenden.
* Weitergabe: Die Weitergabe an Dritte ist nicht zulässig, Mobile Geräte dürfen nicht unbeaufsichtigt gelassen werden.
* Verlust: Der Verlust eines Geräts ist unverzüglich der Geschäftsleitung zu melden.
* Schnittstellen: Sämtliche Funk- (WLAN, Bluetooth etc.), Infrarot- und andere Kommunikationsschnittstellen sind zu deaktivieren, sofern diese nicht benutzt werden.
* Private mobile Geräte dürfen nicht an die IT Infrastruktur angeschlossen werden und es dürfen keine Server-Daten darauf gespeichert werden. Ausnahme bilden etwaige Gast-WLAN-Systeme, die das Unternehmen anbietet.

## Passwort-Gebrauch Unternehmensnetz und Fachanwendungen

Soweit technisch möglich, sind alle IT-Systeme und Applikationen erst nach hinreichender Authentifizierung des Nutzers nutzbar. Die Authentifizierung erfolgt in der Regel durch die Verwendung der Kombination Benutzername/Passwort. Die Geschäftsleitung wird, soweit keine betrieblichen oder technischen Gründe entgegen sprechen, jedem einzelnen berechtigten Nutzer einen Benutzernamen sowie ein Passwort zuweisen lassen.

Passwörter müssen eine Mindestlänge von 8 Zeichen haben. Das Passwort ist alphanumerisch (Buchstaben und Zahlen/Zeichen mit Sonderzeichen) zu gestalten.  
Soweit technisch möglich ist jeder Mitarbeiter verpflichtet, sein Initial-Passwort unverzüglich zu ändern.

Die Passwörter sind so zu wählen, dass sie nicht durch Dritte leicht zu erraten sind. Vor- und Familiennamen oder Geburtstage, sowie Namen von Angehörigen sind nicht zur Passwortwahl geeignet. Gleiches gilt für trivial angeordnete Zahlenkombinationen (z.B. 12345).

Um ein Erraten von Passworten zu unterbinden, erfolgt nach einer bestimmten Anzahl von Fehlversuchen die Deaktivierung des betreffenden Accounts.

## Protokollierung und Kontrolle

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

Die Verkehrsdaten für den Internetzugang werden mit Angaben von

1. Datum / Uhrzeit,
2. Adressen von Absender und Empfänger (z.B. IP-Adressen)
3. Benutzeridentifikation (z.B. bei der Verwendung eines Proxy-Servers)
4. der aufgerufenen Webseiten und
5. übertragener Datenmenge

protokolliert.

Die Protokolle nach Absatz 2 werden ausschließlich zu Zwecken der:

1. Analyse und Korrektur technischer Fehler
2. Gewährleistung der Systemsicherheit
3. Optimierung des Netzes
4. statischen Feststellung des Gesamtnutzungsvolumens
5. Stichprobenkontrolle gemäß Absatz 4 und
6. Auswertung gemäß Nr. 7 dieser Vereinbarung (Missbrauchskontrolle)

verwendet.

# KI-Systeme

In unserem Unternehmen werden KI-Systeme genutzt werden, um Geschäftsprozesse zu unterstützen. Dabei halten wir die rechtlichen Anforderungen der KI-Verordnung der EU (KI-VO) vollständig ein. Dabei werden KI-Systeme vor Ihrem Einsatz geprüft. Es werden ausschließlich KI-Systeme folgender Kriterien der KI-VO der EU eingesetzt:

* Allgemeine KI-Systeme
* Hoch-Risiko KI-Systeme (gem.- Art. 6 KI-VO EU)
  + Ausnahme: das System beeinflusst nicht wesentlich die Entscheidungsfindung
  + Biometrisches Ferinidentifizierungssystem
  + Kritische Infrastruktur (KRITIS)
  + Allgemeine und berufliche Bildung
    - KI-Systeme, die bestimmungsgemäß zur Feststellung des Zugangs oder der Zulassung oder zur Zuweisung natürlicher Personen zu Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung verwendet werden sollen;
    - KI-Systeme, die bestimmungsgemäß für die Bewertung von Lernergebnissen verwendet werden sollen, einschließlich des Falles, dass diese Ergebnisse dazu dienen, den Lernprozess natürlicher Personen in Einrichtungen oder Programmen aller Ebenen der allgemeinen und beruflichen Bildung zu steuern;
    - KI-Systeme, die bestimmungsgemäß zum Zweck der Bewertung des angemessenen Bildungsniveaus, das eine Person im Rahmen von oder innerhalb von Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung erhalten wird oder zu denen sie Zugang erhalten wird, verwendet werden sollen;
    - KI-Systeme, die bestimmungsgemäß zur Überwachung und Erkennung von verbotenem Verhalten von Schülern bei Prüfungen im Rahmen von oder innerhalb von Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung verwendet werden sollen.
  + Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit
    - KI-Systeme, die bestimmungsgemäß für die Einstellung oder Auswahl natürlicher Personen verwendet werden sollen, insbesondere um gezielte Stellenanzeigen zu schalten, Bewerbungen zu sichten oder zu filtern und Bewerber zu bewerten;
    - KI-Systeme, die bestimmungsgemäß für Entscheidungen, die die Bedingungen von Arbeitsverhältnissen, Beförderungen und Kündigungen von Arbeitsvertragsverhältnissen beeinflussen, für die Zuweisung von Aufgaben aufgrund des individuellen Verhaltens oder persönlicher Merkmale oder Eigenschaften oder für die Beobachtung und Bewertung der Leistung und des Verhaltens von Personen in solchen Beschäftigungsverhältnissen verwendet werden soll.

(Nichtzutreffendes bitte streichen).

In jedem Fall werden KI-Systeme so eingesetzt, dass keine unerlaubte Praktiken angewendet werden (gem. Art. 5 KI-VO EU). Insbesondere sind untersagt:

* das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins einer Person oder absichtlich manipulative oder täuschende Techniken mit dem Ziel oder der Wirkung einsetzt, das Verhalten einer Person oder einer Gruppe von Personen wesentlich zu verändern, indem ihre Fähigkeit, eine fundierte Entscheidung zu treffen, deutlich beeinträchtigt wird, wodurch sie veranlasst wird, eine Entscheidung zu treffen, die sie andernfalls nicht getroffen hätte, und zwar in einer Weise, die dieser Person, einer anderen Person oder einer Gruppe von Personen erheblichen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird.
* das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das eine Vulnerabilität oder Schutzbedürftigkeit einer natürlichen Person oder einer bestimmten Gruppe von Personen aufgrund ihres Alters, einer Behinderung oder einer bestimmten sozialen oder wirtschaftlichen Situation mit dem Ziel oder der Wirkung ausnutzt, das Verhalten dieser Person oder einer dieser Gruppe angehörenden Person in einer Weise wesentlich zu verändern, die dieser Person oder einer anderen Person erheblichen Schaden zufügt oder mit hinreichender
* Wahrscheinlichkeit zufügen wird;
* das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen zur Bewertung oder Einstufung von natürlichen Personen oder Gruppen von Personen über einen bestimmten Zeitraum auf der Grundlage ihres sozialen Verhaltens oder bekannter, abgeleiteter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale, wobei die soziale Bewertung zu einem oder beiden der folgenden Ergebnisse führt: Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder Gruppen von Personen in sozialen Zusammenhängen, die in keinem Zusammenhang zu den Umständen stehen unter denen die Daten ursprünglich erzeugt oder erhoben wurden und/oder Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder Gruppen von Personen in einer Weise, die im Hinblick auf ihr soziales Verhalten oder dessen Tragweite ungerechtfertigt oder unverhältnismäßig ist;
* das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung eines KI-Systems zur Durchführung von Risikobewertungen in Bezug auf natürliche Personen, um das Risiko, dass eine natürliche Person eine Straftat begeht, ausschließlich auf der Grundlage des Profiling einer natürlichen Person oder der Bewertung ihrer persönlichen Merkmale und Eigenschaften zu bewerten oder vorherzusagen; dieses Verbot gilt nicht für KI-Systeme, die dazu verwendet werden, die durch Menschen durchgeführte Bewertung der Beteiligung einer Person an einer kriminellen Aktivität, die sich bereits auf objektive und überprüfbare Tatsachen stützt, die in unmittelbarem Zusammenhang mit einer kriminellen Aktivität stehen, zu unterstützen;
* das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern;
* das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen zur Ableitung von Emotionen einer natürlichen Person am Arbeitsplatz und in Bildungseinrichtungen, es sei denn, die Verwendung des KI-Systems soll aus medizinischen Gründen oder Sicherheitsgründen eingeführt oder auf den Markt gebracht werden;
* das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von Systemen zur biometrischen Kategorisierung, mit denen natürliche Personen individuell auf der Grundlage ihrer biometrischen Daten kategorisiert werden, um ihre Rasse, ihre politischen Einstellungen, ihre Gewerkschaftszugehörigkeit, ihre religiösen oder weltanschaulichen Überzeugungen, ihr Sexualleben oder ihre sexuelle Ausrichtung zu erschließen oder abzuleiten; dieses Verbot gilt nicht für die Kennzeichnung oder Filterung rechtmäßig erworbener biometrischer Datensätze, wie z. B. Bilder auf der Grundlage biometrischer Daten oder die Kategorisierung biometrischer Daten im Bereich der Strafverfolgung;
* die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken.

Die Mitarbeiter:innen, die KI-Systeme dienstlich/ betrieblich nutzen, erhalten hierzu die notwendigen Schulungen zum sicheren Umgang mit den KI-Systemen im Hinblick auf den geplanten Nutzungsumfang.

Die KI-Nutzung wird durch den Datenschutzbeauftragten geprüft.

# Maßnahmen bei Verstößen / Missbrauchsregelung

Bei 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 dieser Vereinbarung durch Mitarbeiter:innen findet, unter Beteiligung des Datenschutzbeauftragten und bestellte IT-Fachkräfte eine Überprüfung des Datenverkehrs statt. Sind weitere Untersuchungsmaßnahmen (z.B. Offenlegung der IP-Adresse des benutzten Arbeitsplatzes oder weitere Überprüfungen) 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 anzuhören.

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, 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.

Zur Inventarführung der eingesetzten Hard- und Software sowie zur Netzwerkadministration und zur Benutzerunterstützung wird Software auf einem lokalen Server eingesetzt.

Aufzeichnungen und Auswertungen der System- oder systemnahen Software über Benutzeraktivitäten (Login/Logout, aufgerufene Programme, verbrauchte Systemressourcen, Zugang zu PC- Netzwerkservern usw.) dürfen ausschließlich zu den folgenden Zwecken benutzt werden:

1. Gewährleistung der Systemsicherheit,
2. Feststellung der Nutzungsdauer und -häufigkeit,
3. Analyse und Korrektur von technischen Fehlern im System,
4. Optimierung des Computersystems
5. statistische Auswertungen ohne individuelle Kennung über den Zugriff auf Ressourcen im Netz und
6. Missbrauchskontrolle (gem. Pkt. 7 dieser Richtlinie).

Der Zugriff auf die entsprechenden Funktionen ist auf diejenigen Personen begrenzt, die für die Wartung der Hard- und Software sowie die Netzwerkadministration zuständig sind.   
Die entsprechenden Dateien werden nur so lange gespeichert, wie dies zur Erfüllung der oben genannten Zwecke erforderlich ist.

Soweit mittels Software zur Unterstützung der Netzwerkverwaltung ein Zugriff auf die Arbeitsplatzrechner von Mitarbeitern/-innen möglich ist, so wird diese so installiert, dass nur die berechtigten Administratoren Zugriff auf die Endgeräte haben können.   
Der Einsatz von Softwareprodukten mit Eskalationsmanagement (automatische Erzeugung von Alarm- und Aufmerksamkeitsmeldungen) bleibt auf technische Fehlermeldungen der Server- und Systemsoftware begrenzt. Darüber hinaus können die Mitarbeiterinnen und Mitarbeiter Software mit solchen Leistungsmerkmalen einsetzen, um sich selbst auf die Einhaltung von Fristen oder die Durchführung termingebundener Arbeiten aufmerksam zu machen.

# Änderungen und Inkrafttreten, Konsequenzen bei Nichteinhaltung

Geplante Änderungen und Erweiterungen an den elektronischen Kommunikationssystemen werden möglichst frühzeitig dem Datenschutzbeauftragten mitgeteilt. Es wird dann geprüft, ob und inwieweit sie sich auf die Regelungen dieser Vereinbarung auswirken. Notwendige Änderungen oder Erweiterungen zu dieser Vereinbarung können in einer ergänzenden Regelung vorgenommen werden.

Ein Verstoß gegen diese Richtlinie kann neben arbeitsrechtlichen Folgen auch strafrechtliche Konsequenzen haben.

Diese Richtlinie tritt mit Unterzeichnung in Kraft.

Ort, Datum Oberste Leitung

**Anlage 1: Vereinbarung Mobiles Arbeiten zwischen Arbeitgeber und Mitarbeiter:in**

Der Arbeitgeber gewährt das mobile Arbeiten in folgendem Umfang:

- Tage, ggf. Uhrzeiten benennen.

Die Arbeitnehmerin / der Arbeitnehmer verpflichtet sich hiermit:

* Den Transport von dienstlichen Datenträgern / Arbeitsmitteln mit dem notwendigen Schutz und Fürsorge durchzuführen,
* Datenträger, Unterlagen und Arbeitsmittel bei Abwesenheit und nach Beendigung der Arbeit zu verschließen (abschließbare Möbel oder Büro),
* Keine privaten Datenträger und Geräte für die dienstliche Tätigkeit einzusetzen,
* ohne Weisung personenbezogene und unternehmensinterne Daten weder zu ändern, zu kopieren, zu lesen oder zu löschen und nicht an Dritte weiter zu geben,
* die Verarbeitung nur in Abwesenheit Dritter, dazu gehören auch im Haushalt lebende Personen, durchzuführen,
* personenbezogene und unternehmensinterne Daten nicht unbeaufsichtigt liegen zu lassen,
* Fenster und Türen bei Verlassen des Verarbeitungsbereiches zu schließen,
* Dritten keine Einsicht auf den Bildschirm zu gewähren und
* den Bildschirm beim Verlassen des Arbeitsplatzes zu sperren.

Die Verpflichtungserklärung zur Geheimhaltung bleibt hiervon unberührt.

Die Unternehmung wird den Arbeitnehmer/die Arbeitnehmerin mit allen notwendigen Arbeitsmitteln ausstatten, um ein geeignetes Schutzniveau der zu verarbeitenden personenbezogenen Daten herzustellen.

Bei Rückfragen steht Ihnen Abteilungsleiter/Führungskraft gerne zur Verfügung.

Der Arbeitnehmer/die Arbeitnehmerin bestätigt mit seiner/ihrer Unterschrift, dass er/sie die Anforderungen an den Schutz der zu verarbeitenden Daten bei seiner/ihrer Tätigkeit im mobilen Arbeiten verstanden hat und diese einhalten wird.

Ort, Datum:

………………………………………………………………………………………………….

Unterschrift Arbeitnehmer/in: ..……………………………………………………………………………..

Unterschrift Oberste Leitung: ..……………………………………………………………………………..