IT-Richtlinie der FRISTO SE
Dienst-/Betriebsanweisung – IT

Stand: 01.07.2024

Präambel

Ziel dieser Richtlinie ist es, eine höchstmögliche Datensicherheit zu erreichen und die Nutzungsbedingungen sowie die Maßnahmen zur Protokollierung und Kontrolle transparent zu machen, die Persönlichkeitsrechte der Mitarbeiterinnen und Mitarbeiter (nachfolgend aus Gründen der leichteren Lesbarkeit „Mitarbeiter" genannt), die die elektronischen Kommunikationssysteme Internet, E-Mail, Intranet und Office 365 nutzen, zu sichern und den Schutz der personenbezogenen Daten zu gewährleisten.

1. Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiter der FRISTO SE

2. Nutzung von IT-Endgeräten und Diensten

Dienstliche IT-Endgeräte (z. B. PCs, Notebooks, internetfähige Mobiltelefone, Tablet-PCs) und zentrale Dienste (z. B. Internet-Zugang, E-Mail-Service, Netzlaufwerke, Office 365, Microsoft Teams, Webserver) stehen den Beschäftigten als Arbeitsmittel zur Aufgabenerfüllung zur Verfügung. Der unmittelbare Vorgesetzte kann die Nutzung dienstlicher IT-Endgeräte und zentraler Dienste anordnen, sofern und soweit dies zur Sicherstellung oder Vereinfachung der Arbeitsorganisation erforderlich ist.

Sofern die nachstehenden Regelungen nichts anderes bestimmen, ist eine Nutzung der in Absatz 1 bezeichneten Geräte und Dienste für private Zwecke nicht gestattet.

Private IT-Endgeräte (z.B. Handys, Tablets, Notebooks, Drucker, WLAN-Zugangspunkte) dürfen ausdrücklich nicht für dienstliche Zwecke genutzt oder mit den firmeneigenen Netzwerken verbunden werden. Ausnahmen hiervon müssen durch die IT-Leitung schriftlich freigegeben werden.

An USB-Schnittstellen dürfen nur firmeneigene Geräte angeschlossen werden, insbesondere keine Massenspeichergeräte, private Handys oder Kameras.

Jegliche, nicht autorisierte Veränderung bzw. Manipulation von Netzwerk Komponenten oder das Hinzufügen von fremden Geräten in das Unternehmensnetzwerk ist ausdrücklich verboten.

Alle Fremd-USB-Sticks müssen vor dem Einsatz durch die IT auf Viren geprüft werden.

Alle Warnmeldungen der Virenschutzprogramme sind umgehend per Mail oder telefonisch an die IT weiterzugeben.

Personenbezogene Daten (z.B. Personalakten, Abmahnungen usw.) dürfen nur verschlüsselt oder passwort-geschützt gespeichert und übermittelt werden.

Installation von Fremdsoftware darf nur nach Rücksprache / Freigabe durch IT erfolgen.

Das Kopieren von Firmendaten auf private Geräte und der Einsatz von privaten Geräten zu dienstlichen Zwecken sind untersagt, Ausnahmen können auf Antrag bei IT durch die IT-Leitung freigegeben werden.

Die Mitarbeiter sind verpflichtet, mit den zur Verfügung gestellten elektronischen Kommunikationsmitteln verantwortungsvoll umzugehen. Falls aufgrund der privaten Nutzung des Internets, wie z.B. der nicht genehmigten Installation von Software oder der Installation von Raubkopien, dem Unternehmen ein Schaden entsteht, wird dieser dem verantwortlichen Mitarbeiter in Rechnung gestellt werden. Arbeitsrechtliche Konsequenzen bleiben davon unberührt.

3. Nutzung des Internetzugangs

Der Internet- und Intranet-Zugang steht den Mitarbeitern zur dienstlichen Nutzung als Arbeitsmittel im Rahmen Ihrer Aufgabenerfüllung zur Verfügung und dient insbesondere der Verbesserung der internen und externen Kommunikation, der Beschleunigung der Informationsbeschaffung und der Arbeitsprozesse.

Die private Nutzung des Internetzugangs auf dienstlichen IT-Geräten ist grundsätzlich untersagt.

Zur Überprüfung der Einhaltung der Regelungen über die Nutzung des Internets, sowie zum Schutz des Unternehmens gegen Gefahren aus dem Internet setzt das Unternehmen ein System ein, welches bei einem Zugriff des Benutzers auf unsichere oder gesperrte Webseiten den Zugriff auf die Zieladresse im Internet blockiert. Dem Benutzer wird das Blockieren der Zieladresse im Internet-Browser angezeigt und es wird ein Eintrag in eine Protokolldatei erzeugt.

4. Nutzung des E-Mail-Dienstes

Das dienstliche E-Mail-Konto steht den Beschäftigten ausschließlich als Arbeitsmittel zur Aufgabenerfüllung zur Verfügung. Die private Nutzung des dienstlichen E-Mail-Kontos ist nicht gestattet. Unaufgefordert eingehende private E-Mails stellen keinen Verstoß gegen das Verbot der Privatnutzung dar und dürfen vor der Löschung an den privaten Account weitergeleitet werden.

Eingehende private E-Mails an die dienstliche E-Mail-Adresse sind nach inhaltlicher Kenntnisnahme grundsätzlich durch den Beschäftigten zu löschen. Die Beschäftigten sollen den Absender privater E-Mails, die auf dem dienstlichen E-Mail-Konto eingegangen sind, auf dessen ausschließlich dienstliche Zweckbestimmung hinweisen.

Öffnen Sie keine Mails von unbekannten Absendern oder mit verdächtigem Inhalt, insbesondere mit Links zu Webseiten oder mit Dateianhängen. (ggf. Informieren Sie bitte die IT und lassen verdächtige Mails prüfen)

Eine automatische Weiterleitung (sog. Forwarding) von E-Mails, die auf dem dienstlichen E-Mail-Account eingehen, an externe E-Mail-Konten (z.B. private E-Mail) sind grundsätzlich verboten und stellen einen datenschutzrechtlichen Verstoß dar.

Eine Weiterleitung von geschäftlichen E-Mails, Dateien oder Dokumenten an einen unbefugten Dritten oder die eigene private Mail Adresse ist untersagt.

Sofern Sie vertrauliche und/oder personenbezogene Daten aus dienstlichen Gründen per E-Mail versenden, darf dies an externe E-Mail-Empfänger grundsätzlich nur auf verschlüsseltem Wege oder passwortgeschützt geschehen. In Zweifelsfällen ist zuvor die IT-Abteilung zu Rate zu ziehen.

Der jeweilige Vorgesetzte kann verlangen, dass ihm der Arbeitnehmer die E-Mails bezüglich seiner geschäftlichen E-Mail-Adresse zugänglich macht, insbesondere weiterleitet oder ausdruckt. Sind der Arbeitnehmer und sein Vertreter nicht erreichbar und besteht ein dringendes betriebliches Bedürfnis die dienstliche Korrespondenz einzusehen, so ist der jeweilige Vorgesetzte sowie die Geschäftsführung zugriffsberechtigt. Der Arbeitnehmer ist vom Zugriff zu informieren. Nach dem Ausscheiden des Arbeitnehmers aus dem Arbeitsverhältnis (unabhängig aus welchem Grund), steht dem Unternehmen die dienstliche E-Mail-Adresse in dem Umfang zu, den der ordnungsgemäße Geschäftsgang oder betriebliche Ablauf erfordert.

5. Verhaltensgrundsätze

Grundsätzlich gelten die Regelungen dieser Richtlinie.

Unzulässig ist jede absichtliche oder wissentliche Nutzung der elektronischen Kommunikationssysteme, die geeignet ist, den Interessen des Unternehmens oder dessen Ansehen in der Öffentlichkeit zu schaden, die Sicherheit des IT-Systems zu beeinträchtigen oder die gegen geltende Rechtsvorschriften oder diese Richtlinie verstößt. Dies gilt vor allem für:

- das Abrufen und Verbreiten von Inhalten, die gegen Persönlichkeitsrechte, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen;
- das Abrufen und Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen;
- das Abrufen von kostenpflichtigen Informationen für den Privatgebrauch
- das unerlaubte Weiterleiten von internen Informationen, Dokumenten und E-Mails

Das Abrufen von Informationen für private Zwecke (z. B. durch Herunterladen, Streaming) auf Kosten von FRISTO ist unzulässig.

6. Kontrolle der IT-Richtlinie

Zur Sicherstellung und Wirksamkeit der IT-Richtlinie werden systemische und persönliche Überprüfungen auf Basis von Stichprobenkontrollen durchgeführt. Ergänzend kann eine Übersicht über das jeweilige Gesamtvolumen des ein- und ausgehenden Datenverkehrs erstellt werden.

7. Aktivierung von E-Mail-Abwesenheitsnachrichten

Bei Abwesenheit eines Beschäftigten (z. B. bei Urlaub oder Arbeits-/Dienstunfähigkeit) hat der Beschäftigte die automatische Abwesenheitsnachricht für dessen E-Mail-Konto zu aktivieren. Ist der Beschäftigte dazu (z.B. Unfall) nicht in der Lage, ist FRISTO berechtigt die automatische Abwesenheitsnachricht zur Sicherstellung des ordnungsgemäßen Arbeits- oder Dienstablaufs zu aktivieren.

Über die Aktivierung von Abwesenheitsnachrichten entscheidet der unmittelbare Vorgesetzte. Er beauftragt den zuständigen Systemadministrator schriftlich mit der Aktivierung einer im Wortlaut mitzuteilenden Abwesenheitsnachricht. Bei der Aktivierung einer Abwesenheitsnachricht hat eine Einsichtnahme in die Inhalte des betroffenen E-Mail-Kontos zu unterbleiben.

8. Einsichtnahme in E-Mails sowie in Daten auf dienstlichen Informations- und Kommunikationssystemen

Bei Abwesenheit eines Beschäftigten (z. B. bei Urlaub oder Arbeits-/Dienstunfähigkeit) ist das Unternehmen berechtigt, Einsicht in dessen E-Mail-Konto, einzelne E-Mails sowie auf dienstlichen IT-Endgeräten oder zentralen Diensten gespeicherte Daten zu nehmen, sofern und soweit dies zur Sicherstellung des ordnungsgemäßen Arbeits- oder Dienstablaufs im konkreten Fall notwendig ist. Dies gilt nicht für erkennbar private E-Mails oder Daten.

Über die geplante Einsichtnahme entscheidet der unmittelbare Vorgesetzte unter nötiger Freigabe durch die Geschäftsführung und die IT-Leitung im 4-Augen-Prinzip. Die Leitung der Personalabteilung ist in diesem Fall zu informieren."

9. Missbrauch der Internet- und Dienste-Nutzung

Bei einem Verdacht auf eine missbräuchliche oder unerlaubte Nutzung des Internet-Zugangs gemäß Ziffer 2, 3, 4 und 5 dieser Richtlinie erfolgt eine Überprüfung gemäß § 6 dieser Richtlinie. Die Leitung der Personalabteilung sowie die Geschäftsführung sind in diesem Fall zu informieren. Sie veranlassen gegebenenfalls weitere Untersuchungsmaßnahmen wie beispielsweise eine Protokollierung des gesamten Nutzungsverhaltens des betroffenen Nutzers für einen unbestimmten Zeitraum. Auf Basis dieser Untersuchung wird eine schriftliche Zusammenfassung der Ergebnisse erstellt, die dem jeweiligen Arbeitgeber ausgehändigt wird. Dem Arbeitnehmer ist die Möglichkeit einzuräumen, zu dem Bericht in angemessener Zeit Stellung zu nehmen.

Die Durchführung weiterer arbeitsrechtlicher Maßnahmen bleibt hiervon unberührt.

Ein Verstoß gegen diese Richtlinie kann neben den arbeitsrechtlichen Folgen auch, sofern ein Straftatbestand bekannt wird, strafrechtliche Konsequenzen haben.

10. Einsatz von Künstlicher Intelligenz bei der FRISTO SE

Die Nutzung von Künstlicher Intelligenz (KI) in unserer Organisation ist darauf ausgerichtet, Innovationen zu fördern, Prozesse zu optimieren und datengesteuerte Entscheidungen zu unterstützen. Um sicherzustellen, dass der Einsatz von KI den Geschäftszielen der FRISTO SE entspricht und im Einklang mit unseren ethischen Standards steht, gelten folgende Vorgehensweisen:

Zweckgebundener Einsatz: KI-Systeme dürfen ausschließlich für definierte Zwecke eingesetzt werden, die mit den Unternehmenszielen und den geltenden Gesetzen und Vorschriften vereinbar sind. Die Verwendung von KI sollte transparent und nachvollziehbar sein.

Datenschutz und Informationssicherheit: Beim Einsatz von KI ist sicherzustellen, dass die Grundsätze des Datenschutzes und der Informationssicherheit sowie gesetzliche Vorgaben eingehalten werden. Sensible Daten dürfen nur durch KI verarbeitet werden, wenn die Integrität und Vertraulichkeit der Daten gewährleistet ist. Vor dem Einsatz von KI ist der IT-Sicherheitsbeauftragte (ITSiBe) sowie der Datenschutzbeauftragte (DSB) in Projekten einzubinden, um die Ziele der Informationssicherheit und des Datenschutzes sicherzustellen.

Nutzung von öffentlichen KI-Systemen: Grundsätzlich ist die Eingabe von informationssicherheitsrelevanten Daten (Unternehmenszahlen, Kundendaten, Mitarbeiterdaten etc.) sowie von personenbezogenen Daten (Name, Vorname, Geburtsdatum etc.) in öffentliche KI-Systeme wie z.B. ChatGPT (oder andere) verboten. Es dürfen nur anonymisierte und nicht nachvollziehbare Daten eingegeben werden.

Überwachung und Governance: Es muss eine angemessene Überwachung und Governance für den Einsatz von KI implementiert werden, um sicherzustellen, dass die Systeme ordnungsgemäß funktionieren und die Richtlinien eingehalten werden. Jeder Einsatz von KI ist vor Inbetriebnahme dem Leiter IT mitzuteilen. Für die Überwachung und Governance ist eine Liste aller sich im Einsatz befindlicher KI-Systeme zu erstellen, die regelmäßig aktualisiert und kontrolliert wird.

11. Änderungen und Erweiterungen

Das Unternehmen behält sich vor, die Bestimmungen dieser Richtlinie über die Nutzung von Internet, E-Mail und Intranet an Änderungen in der Gesetzgebung, der Rechtsprechung sowie Stand der Technik anzupassen und entsprechend zu Ändern. Weiterhin behält sich das Unternehmen den jederzeitigen Widerruf dieser Richtlinie vor.

Um wesentlichen Anforderungen an die Verfügbarkeit und Sicherheit dienstlicher Informationen zu genügen, haben Sie die hierzu erlassenen Richtlinien zu beachten. Weil diese Anforderungen zusammen mit der technischen Entwicklung der Informationstechnik einem stetigen Wandel unterworfen sind, kann sich auch diese Richtlinie von Zeit zu Zeit ändern. Es gehört daher zu Ihren dienstlichen Pflichten, sich in regelmäßigen Abständen – wenigstens jedoch einmal jährlich – über etwaige Änderungen zu unterrichten.

12. Salvatorische Klausel

Sollten eine oder mehrere Bestimmungen dieser Dienstvereinbarung ungültig sein, so beeinträchtigt dies die Wirksamkeit der Dienstvereinbarung und der übrigen Bestimmungen nicht. Rechtsunwirksame Vorschriften werden die Parteien in vertrauensvoller Zusammenarbeit durch eine rechtskonforme Vorschrift ersetzen, die dem angestrebten Regelungsziel am nächsten kommt.

13. Schlussbestimmungen

Diese IT-Richtlinie (Dienst-/Betriebsanweisung – IT) tritt am 01.07.2024 in Kraft und ersetzt die bislang geltende Richtlinie vom 01.01.2015.

Buchloe, den 01.07.20224

Dennis Roth Vorstand	ppa. Ralf Bliem Leiter IT	ppa. Christian Hoffmann Leiter Personal