|  |
| --- |
| Anlage DatSch Ordner 2 Register 12  O2R12\_Anlage\_Vereinbarung Personal, Nutzung, Internet, E-Mail, Telefon |

**Vereinbarung über die Nutzung von**

**IT-Geräten, E-Mail, Internet, Telefon und Telefax für Beschäftigte**

zwischen

Unternehmen

Straße und Hausnummer

Postleitzahl und Ortsname

- im Folgenden „Arbeitgeber“ genannt -

und

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- im Folgenden „Mitarbeiter“ genannt -

**1. Allgemeines**

**1.1 Geltungsbereich**

Diese Vereinbarung gilt ab sofort für alle Benutzer der betrieblich zur Verfügung gestellten IT-Geräte und Ressourcen, sowie des Telefons und Telefax und des betrieblichen E-Mail- und Internet-Zugangs. Betrieblich genutzte IT-Geräte, im Sinne dieser Vereinbarung, sind alle Geräte die den Beschäftigten als Arbeitsmittel zur Verfügung gestellt werden, insbesondere Arbeitsplatz-PCs, Telefone, Faxgeräte, Notebooks, Smartphones, Tablets, externe Speichermedien (USB-Sticks, mobile Festplatten usw.). Sachlich gilt diese Vereinbarung für die Kommunikation der Berechtigten untereinander, sowie mit externen Stellen und für die Nutzung der Internet-Dienste zum Zwecke des Zugriffs auf weltweit verfügbare Informationen und Daten.

**1.2 Rechtscharakter**

Diese Vereinbarung ist Teil des bestehenden Arbeitsvertrages. Verstöße gegen diese Vereinbarung können zu arbeitsrechtlichen Konsequenzen führen.

**2. E-Mail**

**2.1 Verbot der Privatnutzung des betrieblichen E-Mail-Systems**

Dienstlich ist ausschließlich das firmeninterne E-Mail-System zu nutzen (Beschreibung Systeme hier eintragen.). Die zur Verfügung gestellten E-Mail-Adressen aus der Domain „\*adresse hier einfügen“ dürfen ausschließlich für betriebliche Zwecke genutzt werden. Eine private Nutzung des E-Mail-Systems ist untersagt.

Alle über die Firmendomäne ein- und ausgehenden E-Mails gelten somit als dienstliche E-Mails und werden entsprechend in Administration, Speicherung, SPAM-Abwehr, Weiterleitung, Archivierung und Protokollierung aber auch bei der Behandlung von Störfällen, die den Eingriff eines Administrators erfordern, behandelt und können von den IT-Verantwortlichen auch sporadisch im Bedarfsfall gelesen werden. Nicht zuletzt deshalb, dürfen private E-Mails grundsätzlich nicht über die Firmen-Domäne gesandt werden, um den Schutz der Privatsphäre der Mitarbeiterinnen und Mitarbeiter zu gewährleisten.

**2.2 Webmail**

Eine Nutzung von Webmailern (z.B. wie z.B. web.de, gmx, yahoo, msn) in Arbeitspausen ist unter Beachtung der Sicherheitsvorschriften und dieser Betriebsvereinbarung gestattet / untersagt. Für die Nutzung dieser Webmaildienste übernimmt die Unternehmername hier eintragen keine Haftung im Falle eines Datenverlusts.

Wenn Nutzung gestattet:

Für durch die private Nutzung von E-Mail-Diensten dem Arbeitgeber entstandene Schäden haftet der Mitarbeiter. Nach Ausscheiden eines Mitarbeiters werden sämtliche privaten Dateien (auch E-Mails) von PCs und mobilen Endgeräten des Arbeitgebers gelöscht. Das Anklicken und Verfolgen von Links, sowie das Öffnen von Dateianhängen in den Webmailern ist untersagt. Aus Sicherheitsgründen ist auf den betrieblichen Geräten nur das Lesen und Beantworten von privaten Emails in Webmailern gestattet.

**2.3 Ergreifen von Sicherheitsmaßnahmen**

Der Empfänger von E-Mails hat die üblichen Sicherheitsmaßnahmen (wie unter den Punkten 2.9, 2.10, 2.11, 2.12 genauer ausgeführt) zu beachten. Dies gilt insbesondere für Dateianhänge (Attachments) und bei unbekannten Absendern.

**2.4 Verantwortlichkeit**

Für die Zulässigkeit und Sicherheit beim Versenden von E-Mails, sowie die Einhaltung der betrieblichen Regelungen, ist grundsätzlich der Absender verantwortlich.

**2.5 Nutzungsbeschränkungen**

Das Versenden von E-Mails, deren Inhalt den Interessen der Gesellschaft oder deren Ansehen in der Öffentlichkeit schadet oder gegen geltende Gesetze und Verordnungen verstößt, ist verboten.

Folgende Nachrichtentypen dürfen insbesondere nicht per E-Mail gesendet werden:

• Nachrichten mit gesetzeswidrigem, beleidigendem, diskriminierendem, belästigendem, abfälligem, diffamierendem, drohendem oder obszönem Inhalt

• insbesondere Kopien von Dokumenten oder Computersoftware, die gegen die Copyright-Gesetze verstoßen

• Kettenbriefe oder Schneeballsysteme

• Nachrichten, bei denen die Identität des Senders geändert oder verborgen wurde (Spoofing)

**2.6 Manipulationen von E-Mails**

Die Manipulation von E-Mails (z. B. Verfälschung des Absenders oder des Inhaltes) ist verboten.

**2.7 Verbot des Versendens von ausführbaren Programmen**

Ausführbare Programme dürfen grundsätzlich nicht übermittelt werden (Dateiendung \*.exe, \*.pif, \*.com, \*.scr, \*.vbs, etc.).

**2.8 Beseitigung von Restinformationen**

Vor dem Versenden einer Datei per E-Mail ist diese daraufhin zu überprüfen, ob sie Restinformationen (z. B. verborgener Text, Kommentare, Änderungsmarkierungen, Emailadressen größerer Empfängergruppen) enthält, die nicht zur Weitergabe an Dritte bestimmt sind.

**2.9 Personenübergreifender Zugriff auf E-Mail-Postfächer**

Die Mitarbeiter haben bei Abwesenheit zur Information des Absenders den Abwesenheitsassistenten mit einer entsprechenden Benachrichtigung des Absenders einzuschalten. Der Zugriff auf einzelne Postfächer von anderen Mitarbeitern ist im Rahmen einer Weiterleitungs- oder Urlaubsregelung gestattet. Die Geschäftsleitung kann zur Wahrung des ordentlichen Betriebsablaufes auch bei ungeplanter Abwesenheit eines Mitarbeiters auf dessen Postfach Zugriff nehmen. E-Mails, die ungeöffnet im Postfach eines Mitarbeiters anhand von Absender oder Betreff als privat erkannt werden, dürfen bei einem Zugriff anderer Personen auf das Postfach des Mitarbeiters nicht geöffnet oder gelesen werden.

**2.10 Richtlinien für E-Mail-Zugriff bei Abwesenheit**

Eine automatische Weiterleitung an private E-Mail-Adressen ist unzulässig. Die Geschäftsleitung ist berechtigt, eine Vertretungsregelung für einen abwesenden Mitarbeiter einzurichten.

**2.11 Zugriffsschutzmaßnahmen**

Jeder Benutzer des E-Mail-Systems erhält eine Zugriffsberechtigung (Benutzerkennung und Passwort) und einen eigenen Datenbereich (Mailbox).

(Vorgaben prüfen) Persönliche Passwörter müssen aus mindestens acht Zeichen, davon mindestens einem Sonderzeichen bestehen. Die Benutzer haben ihre Passwörter sorgfältig auszuwählen, regelmäßig zu ändern und geheim zu halten. Persönliche Passwörter dürfen auch nicht an den Vertreter weitergegeben werden. Die Benutzer dürfen für betrieblich genutzte Authentifizierungen kein Passwort verwenden, das sie bereits privat verwenden.

Es ist nicht gestattet, die eigenen Zugriffsdaten an Dritte (auch nicht an Kolleginnen oder Kollegen) weiterzugeben oder diesen den Zugriff mit den eigenen Zugriffsdaten zu gewähren.

Jeder Nutzer muss bei Verlassen des Büros oder Arbeitsplatzes den PC und/oder das mobile Endgerät sperren.

Die E-Mails werden im Rahmen der täglichen Datensicherung gesichert.

**2.12 Virenschutz**

Es wird ein Virenschutzsystem im Netzwerk Unternehmensname betrieben. Alle eingehenden und ausgehenden Mails sowie Dateien und Daten werden umfassend auf Viren gescannt. Ein Virenschutz, der absolute Sicherheit bietet, kann jedoch aus technischen Gründen nicht gewährleistet werden. Deswegen ist jeder Nutzer aufgefordert, sorgsam mit E-Mail-Anhängen und aus dem Internet heruntergeladenen Dateien umzugehen und z. B. Dateien unbekannter Herkunft nicht zu öffnen oder auszuführen. Wird eine E-Mail mit Schadensfunktion entdeckt, sind unverzüglich die IT-Verantwortlichen und die Geschäftsleitung zu verständigen.

Ausführbare Dateianhänge (z. B. Dateien mit den Endungen .exe, .bat, .com, .vbs) dürfen nicht geöffnet werden. Beim Empfang verdächtiger Dateien ist ein IT-Verantwortlicher zu benachrichtigen.

**2.13 Rundmails**

Aus datenschutzrechtlicher Sicht stellt die Angabe aller E-Mail-Empfänger eine Übermittlung personenbezogener Daten dar, die nur zulässig ist, wenn der Betroffene eingewilligt hat oder die Übermittlung von einer gesetzlichen Grundlage abgedeckt ist. Daher ist darauf zu achten, dass bei Versendungen außerhalb des Unternehmens die E-Mail-Adressen einer Rundmail nicht einfach allen Empfängern offen bereitgestellt werden. Alle Rundmails und Newsletter sollten aus diesen Gründen immer mit der Funktion des BCC (Blind Carbon Copy) versendet werden.

**3. Internet**

**3.1 Nutzung von Internetdiensten**

Das Unternehmen untersagt die Nutzung von Internetdiensten für private Zwecke.

**3.2. Nicht tolerierte Aktivitäten im Internet**

Unzulässig ist jede Internet-Nutzung, die geeignet ist, den Interessen des Unternehmens oder dessen Ansehen in der Öffentlichkeit zu schaden, oder die gegen geltende Rechtsvorschriften verstößt; wie insbesondere das Abrufen oder Verbreiten von Inhalten, die gegen datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen.

Aktivitäten mit:

* rassistischen
* sexistischen
* diskriminierenden
* gewaltverherrlichenden

Inhalten werden nicht toleriert. Solche Aktivitäten können als Internet-Missbrauch am Arbeitsplatz gewertet werden und arbeitsrechtliche Konsequenzen nach sich ziehen.

Die private Nutzung von Audio- oder Videostreams ist untersagt.

Zu den nicht tolerierten Aktivitäten zählen außerdem solche, die potenziell dazu geeignet sind, das Unternehmen zu gefährden und/oder dessen Image zu schaden. Darunter fallen u. a. die Weitergabe vertraulicher Daten, Weitergabe von Betriebsdaten sowie das Herunterladen von urheberrechtlich geschützter Software und Dateien.

Entsteht dem Arbeitgeber durch die schuldhafte private Nutzung des Internetzugangs eines Mitarbeiters ein Schaden, wird die Haftung auf den Mitarbeiter übertragen.

**3.3 Verwendung von Toolbars und Messaging Software**

Das Herunterladen und Benutzen von sogenannten Toolbars (beispielsweise Yahoo, Google), Live Tickern jeder Art, Messaging Software (ICQ, MSN, Yahoo-Messenger, Facebook-Messenger, Twitter), insbesondere auch Nachrichtenapplikation für Smartphones (z. B. WhatsApp) ist nicht gestattet. Weiterhin ist das Benutzen und die Teilnahme an Tauschbörsen (BitTorrent, Rapidshare usw.) nicht gestattet.

**3.4 Betriebliche Nutzung von Internetangeboten**

Im Rahmen der notwendigen, betrieblichen Angelegenheiten darf das Internet genutzt werden. Bei Verstoß haftet der Mitarbeiter gegenüber der Firma. Bei Unklarheiten zur Nutzung der einzelnen Internetangebote für betriebliche Zwecke sollte die Geschäftsleitung konsultiert werden.

**3.5 Internetzugang**

Der Internetzugang darf ausschließlich über Kommunikationswege erfolgen, die durch die Geschäftsleitung oder die IT-Verantwortlichen genehmigt und freigegeben sind. Dazu sind die Hinweise in der der „Richtlinie IT-Sicherheit für Mitarbeiter“ zu beachten.

**3.6 Nutzung von Cloud-Storage-Diensten**

Cloud-Storage sind Dienste, die Speicherplatz auf einem Server zur Verfügung stellen, auf den über einen Webbrowser und/oder ein Zusatzprogramm zugegriffen werden kann und die teilweise Client-Software anbieten, um einen Datenbestand auf verschiedenen PCs oder mobilen Endgeräten synchron zu halten (z. B. Google Drive, etc.). Es ist nicht gestattet, betriebliche Daten auf Accounts solcher Dienste zu speichern und Konten zu erstellen, bei denen die betriebliche E-Mail-Adresse angegeben wird. Weiterhin ist das Einbinden privater Accounts auf firmeneigenen Geräten untersagt. Eine Freigabe erfolgt ausschließlich über die Unternehmensleitung.

**4. Telefon und Telefax**

Die private Nutzung der betrieblichen Telefon- und Faxanlage ist untersagt. Ausnahmen, etwa für Außendienstmitarbeiter, bedürfen der ausdrücklichen Vereinbarung. In dringenden Fällen wie Verspätungen, Erkrankung von Angehörigen, Unfällen oder Todesfällen darf der Mitarbeiter ohne weiteres private Telefonate auch während der Arbeitszeit über das betriebliche Telefon führen. Heimliches Mithören oder Mitschneiden von Telefonaten ist dem Arbeitgeber untersagt.

**5. Firewall und Protokollierung**

**5.1 Firewall Sicherheitssystem**

Zur Sicherstellung der Datenkommunikation Unternehmername ist eine IT-Sicherheitslösung in Form eines Firewall-Systems installiert. Durch dieses Sicherheitssystem soll eine Absicherung des zentralen Internetzugangs des Unternehmens erreicht werden. Das Internet darf nur in Verbindung mit dem Firewall-System genutzt werden.

**5.2 Protokollierung und Zweckbindung**

Alle ein- und ausgehenden E-Mails sowie der Internetverkehr und Datentransfer werden protokolliert und gespeichert und können zur Überprüfung von Kommunikationsverbindungen genutzt werden. Aufgezeichnet werden unter anderem Datum, Uhrzeit, Größe der Datei einschließlich Dateianhängen, Absenderadresse und Empfängeradresse sowie aufgerufene Internetwebseiten, abgerufene Daten und Verbindungsdaten. Eine Auswertung der Protokolle erfolgt im Bedarfsfall für Zwecke des Datenschutzes, zur Gewährleistung der System- und Datensicherheit und zur Sicherstellung und Optimierung des ordnungsgemäßen Betriebes und Verbindungsabläufe mit dem Internet sowie zur statistischen Feststellung des Gesamtnutzungsvolumens.

Der Arbeitgeber setzt eine Voice Over IP-Telefonanlage mit zugehöriger Software zur Verteilung und Entgegennahme von Anrufen ein. Die Software speichert insbesondere Anrufe mit Telefonnummer des externen Gesprächspartners, Weiterleitung und Entgegennahme des Anrufs, freie und belegte Telefonarbeitsplätze, Anschluss des Mitarbeiters, Zeitpunkt und Dauer eines Telefonats für die Dauer von 60 Tagen, um belegen zu können, dass Reklamanten zur Nachkontrolle kontaktiert wurden.

Eine weitergehende Protokollierung und Auswertung von benutzerspezifischen Aktivitäten erfolgt nur unter Einbindung der Geschäftsleitung (z. B. beim Verdacht einer missbräuchlichen Nutzung des E-Mail-Dienstes).

Die bei der Nutzung der Telefon-, Telefax-, E-Mail- und Internetdienste anfallenden personenbezogenen Daten (Protokoll- und Verbindungsdaten) dürfen nicht zur Leistungs- und Verhaltenskontrolle der Mitarbeiter verwendet werden. Personenbezogene Daten, die zur Sicherstellung des ordnungsgemäßen Betriebs des E-Mail-Systems sowie der Internetdienste erhoben und gespeichert werden, unterliegen der Zweckbindung nach Art. 6 DSGVO, sowie Art. 88 DSGVO i.v.m. § 26 BDSG-neu. Zugriffe auf das Internet können mit Datum, Uhrzeit, Zugriffsdauer, Transfervolumen und der genauen URL der aufgerufenen Internetseiten protokolliert werden. Diese Daten können gespeichert und zur Überprüfung von Kommunikationsverbindungen genutzt werden. Auch insoweit findet eine Verwendung der Protokolle zu Zwecken der Verhaltens- und Leistungskontrolle von Mitarbeitern grundsätzlich nicht statt.

Die Protokolle und die Protokolldateien werden nach dem „First-in-first-out“-Prinzip spätestens nach 30 Tagen gelöscht. Die Aufbewahrung der Protokolle richtet sich nach den jeweils aktuellen gesetzlichen Bestimmungen.

**6. IT-Equipment**

**6.1 Ordnungsgemäßer Umgang mit IT-Equipment**

Als selbstverständlich wird der bestimmungsgemäße Gebrauch und die pflegliche Behandlung der betrieblichen IT-Geräte vorausgesetzt. Für fahrlässig verschuldete Schäden an den betrieblichen IT-Geräten oder den Verlust der zum mobilen Gebrauch überlassenen Geräte (hierzu zählen insbesondere Notebooks und die Smartphones) haftet der Mitarbeiter, bzw. behält sich das Unternehmen eine Haftung vor. Endgeräte dürfen nicht Außenstehenden (z. B. Familienmitgliedern) zur Nutzung überlassen werden.

**6.2. Installation von Software**

Grundsätzlich darf auf den betrieblichen IT-Geräten keine Software von Mitarbeitern installiert werden. Die Administration ist hiervon ausgenommen.

**6.3 Verwendung privater Soft- und Hardware**

Das Einbringen von privater Soft- und Hardware ist nicht zulässig.

**6.4 Speicherung privater Dateien**

Das Speichern von privaten Dateien (z. B. Filmen, mp3, mp4, Musik-Dateien usw.) ist auf betrieblichen Datenträgern nicht gestattet. Für entstandene Schäden durch Speicherung privater Dateien haftet der verursachende Mitarbeiter.

**7. Überprüfung der Einwilligung**

**7.1 Kontrollen durch die Geschäftsleitung**

Die Einhaltung der vorliegenden Vereinbarung wird von der Geschäftsleitung stichprobenartig überprüft. Mit Kontrollen in unregelmäßigen Abständen ist zu rechnen. Der Arbeitgeber ist berechtigt, jede Nutzung von E-Mail, Telefon und Internet zu speichern, um die Einhaltung der obigen Bestimmungen anhand der gespeicherten Daten zu überprüfen.

**7.2 Wirksamkeit der Vereinbarung**

Sollte eine Bestimmung dieser Vereinbarung ganz oder teilweise nicht rechtswirksam sein oder ihre Rechtswirksamkeit später verlieren, so soll hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt werden. Anstelle der unwirksamen Bestimmung soll im Wege der Anpassung eine andere angemessene Regelung gelten, die dem am nächsten kommt, was die Vertragsparteien gewollt haben oder gewollt haben würden, wenn sie die Unwirksamkeit der Regelung bedacht hätten.

**7.3 Auswirkungen und Verstöße**

Die Geschäftsleitung ist unverzüglich über alle Missbräuche und Missbrauchsversuche bei der Nutzung von IT-Geräten und der Nutzung von Internet und E-Mail-Diensten zu unterrichten. Alle Mitarbeiter haben das Recht, vermutete oder tatsächliche Verstöße der Geschäftsleitung vorzutragen. Bei begründetem Verdacht auf missbräuchliche/unerlaubte Nutzung des Internetzugangs oder missbräuchliche/unerlaubte Nutzung von E-Maildiensten erfolgt eine gezielte personenbezogene Auswertung. Ggf. veranlasst die Geschäftsleitung weitere Untersuchungsmaßnahmen. In jedem Fall ist die Geschäftsleitung und der Datenschutzbeauftragte über diese Maßnahmen zu informieren. Die Geschäftsleitung entscheidet, ob der betroffene Beschäftigte informiert und ob diese dazu gehört, werden.

Der unberechtigte Zugriff auf personenbezogene Daten, die missbräuchliche/unerlaubte Nutzung des Internetzugangs oder missbräuchliche/unerlaubte Nutzung von E-Maildiensten hat arbeitsrechtliche Konsequenzen. Personenbezogene Daten, die entgegen dieser Vereinbarung erfasst oder gespeichert werden, dürfen nicht verwendet oder genutzt werden. Personelle Maßnahmen, die auf Informationen beruhen, die unter Verstoß gegen die Zweckbindung nach Ziffer 5.2 dieser Vereinbarung gewonnen wurden, sind unwirksam. Über den gemäß dieser Vereinbarung unbefugten Zugriff auf personenbezogene Daten ist die Geschäftsleitung zu informieren.

**7.4 Weiterentwicklung**

Die Mitarbeiter werden über geänderte Rahmenbedingungen, die sich aus der Schnelllebigkeit der Informationssysteme ergeben, fortlaufend unterrichtet. Sie bestätigen die Kenntnisnahme der Verfahrensweise, verpflichten sich zu deren Einhaltung und bestätigen durch Ihre Unterschrift den Erhalt einer Kopie der Vereinbarung.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ort und Datum

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Geschäftsleitung Arbeitgeber Mitarbeiter