# Anhang 2 – Muster für ein Informationsblatt zur Verarbeitung von Beschäftigtendaten

**Information zur Verarbeitung Ihrer Beschäftigtendaten**

Hiermit informieren wir Sie über die Verarbeitung Ihrer personenbezogenen Daten durch die [Muster GmbH] und die Ihnen nach dem Datenschutzrecht zustehenden Rechte.

**Wer ist für die Datenverarbeitung verantwortlich und wer ist Datenschutzbeauftragter?**

**Verantwortlicher für die Datenverarbeitung ist Ihr Arbeitgeber** die

Arbeitgeber (Musterfirma)

Musterstraße

xxxxx Musterstadt

Telefon (allgemein)

Fax (allgemein)

E-Mail-Adresse (allgemein)

Unseren **Datenschutzbeauftragten** (Name, Abteilung) erreichen Sie unter der o.g. Adresse oder unter: E-Mail-Adresse (Datenschutzbeauftragter). Die Kontaktdaten sind darüber hinaus im Internet/Intranet unter \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ verfügbar.

**Welche Datenkategorien nutzen wir als Arbeitgeber und woher stammen diese?**

Zu den verarbeiteten Kategorien personenbezogener Daten gehören insbesondere Ihre Stammdaten (wie Vorname, Nachname, Namenszusätze, Staatsangehörigkeit und Personalnummer), Kontaktdaten (etwa private Anschrift, (Mobil-)Telefonnummer, E-Mail-Adresse), die bei der Nutzung der IT-Systeme anfallenden Protokolldaten sowie weitere Daten aus dem Beschäftigungsverhältnis (z. B. Zeiterfassungsdaten, Urlaubszeiten, Arbeitsunfähigkeitszeiten, Skill-Daten, ggf. Vorstrafen, Sozialdaten, Bankverbindung, Sozialversicherungsnummer, Rentenversicherungsnummer, Gehaltsdaten sowie die Steueridentifikationsnummer). Hierunter können auch besondere Kategorien personenbezogener Daten wie Gesundheitsdaten fallen.

Ihre personenbezogenen Daten werden in aller Regel direkt bei Ihnen im Rahmen des Einstellungsprozesses oder während des Beschäftigungsverhältnisses erhoben. In bestimmten Konstellationen werden aufgrund gesetzlicher Vorschriften Ihre personenbezogenen Daten auch bei anderen Stellen erhoben. Dazu gehören insbesondere anlassbezogene Abfragen von steuerrelevanten Informationen beim zuständigen Finanzamt sowie Informationen über Arbeitsunfähigkeitszeiten bei der jeweiligen Krankenkasse. Daneben können wir Daten von Dritten (z. B. Stellenvermittlung) erhalten haben.

*Optional: Zudem verarbeiten wir personenbezogene Daten, die wir aus öffentlich zugänglichen Quellen (z. B. beruflichen Netzwerken) zulässigerweise gewonnen haben.*

*Optional: Verarbeitung von tätigkeitsbezogenen Leistungsdaten*

**Für welche Zwecke und auf welcher Rechtsgrundlage werden Daten verarbeitet?**

Wir verarbeiten Ihre personenbezogenen Daten unter Beachtung der Bestimmungen der EU-Datenschutz-Grundverordnung (DS-GVO), des Bundesdatenschutzgesetzes (BDSG) sowie aller weiteren maßgeblichen Gesetze (z. B. BetrVG, ArbZG, etc.).

In erster Linie dient die Datenverarbeitung der Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses. Die vorrangige Rechtsgrundlage hierfür ist Art. 6 Abs. 1 b) DS-GVO i. V. m. § 26 Abs. 1 BDSG. Daneben können Kollektivvereinbarungen (Konzern-, Gesamt- und Betriebsvereinbarungen sowie tarifvertragliche Regelungen) gem. Art. 6 Abs. 1 b) i. V. m. Art. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 4 BDSG sowie ggf. Ihre gesonderten Einwilligungen gem. Art. 6 Abs. 1 a), 7 DS-GVO i. V. m. § 26 Abs. 2 BDSG (z. B. bei Videoaufnahmen) als datenschutzrechtliche Erlaubnisvorschrift herangezogen werden.

Ihre Daten verarbeiten wir auch, um unsere rechtlichen Pflichten als Arbeitgeber insbesondere im Bereich des Steuer- und Sozialversicherungsrechts erfüllen zu können. Dies erfolgt auf Grundlage von Art. 6 Abs. 1 c) DS-GVO i. V. m. § 26 BDSG.

Soweit erforderlich verarbeiten wir Ihre Daten zudem auf Grundlage von Art. 6 Abs. 1 f) DS-GVO, um berechtigte Interessen von uns oder von Dritten (z. B. Behörden) zu wahren. Dies gilt insbesondere bei der Aufklärung von Straftaten (Rechtsgrundlage § 26 Abs. 1 S. 2 BDSG) oder im Konzern zu Zwecken der Konzernsteuerung, der internen Kommunikation und sonstiger Verwaltungszwecke.

*Optional: Darüber hinaus sind wir aufgrund der europäischen Antiterrorverordnungen 2580/2001 und* *881/2002 verpflichtet, Ihre Daten gegen die sog. „EU-Terrorlisten“ abzugleichen, um sicherzustellen, dass keine Gelder oder sonstigen wirtschaftlichen Ressourcen für terroristische Zwecke bereitgestellt werden.*

*Optional: Datenverarbeitung zu statistischen Zwecken.*

Soweit besondere Kategorien personenbezogener Daten gem. Art. 9 Abs. 1 DS-GVO verarbeitet werden, dient dies im Rahmen des Beschäftigungsverhältnisses der Ausübung von Rechten oder der Erfüllung von rechtlichen Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und dem Sozialschutz (z. B. Angabe von Gesundheitsdaten gegenüber der Krankenkasse, Erfassung der Schwerbehinderung wegen Zusatzurlaub und Ermittlung der Schwerbehindertenabgabe). Dies erfolgt auf Grundlage von Art. 9 Abs. 2 b) DS-GVO i. V. m. § 26 Abs. 3 BDSG. Zudem kann die Verarbeitung von Gesundheitsdaten für die Beurteilung Ihrer Arbeitsfähigkeit gem. Art. 9 Abs. 2 h) i. V. m. § 22 Abs. 1 b) BDSG erforderlich sein.

Daneben kann die Verarbeitung besonderer Kategorien personenbezogener Daten auf einer Einwilligung nach Art. 9 Abs. 2 a) DS-GVO i. V. m. § 26 Abs. 2 BDSG beruhen (z. B. betriebliches Gesundheitsmanagement).

Sollten wir Ihre personenbezogenen Daten für einen oben nicht genannten Zweck verarbeiten wollen, werden wir Sie zuvor darüber informieren.

**Wer bekommt Ihre Daten?**

Innerhalb unseres Unternehmens erhalten nur die Personen und Stellen (z. B. Fachbereich, Betriebsrat, Schwerbehindertenvertretung) Ihre personenbezogenen Daten, die diese zur Erfüllung unserer vertraglichen und gesetzlichen Pflichten benötigen.

*Optional: Innerhalb unserer Unternehmensgruppe werden Ihre Daten an bestimmte Unternehmen übermittelt, wenn diese Datenverarbeitungsaufgaben für die in der Gruppe verbundenen Unternehmen zentral wahrnehmen (z. B. Gehaltsabrechnung, Entsorgung von Akten).*

Daneben bedienen wir uns zur Erfüllung unserer vertraglichen und gesetzlichen Pflichten zum Teil unterschiedlicher Dienstleister. Eine Auflistung der von uns eingesetzten Auftragnehmer und Dienstleister, zu denen nicht nur vorübergehende Geschäftsbeziehungen bestehen, können Sie der Übersicht im Anhang sowie im Intranet unter […] entnehmen.

Darüber hinaus können wir Ihre personenbezogenen Daten an weitere Empfänger außerhalb des Unternehmens übermitteln, soweit dies zur Erfüllung der vertraglichen und gesetzlichen Pflichten als Arbeitgeber erforderlich ist. Dies können z. B. sein:[[1]](#footnote-1)

* Behörden (z. B. Rentenversicherungsträger, berufsständische Versorgungseinrichtungen, Sozialversicherungsträger, Finanzbehörden, Gerichte)
* Bank des Mitarbeiters (SEPA-Zahlungsträger)
* Annahmestellen der Krankenkassen
* Stellen, um Ansprüche aus der betrieblichen Altersversorgung gewährleisten zu können
* Stellen, um die vermögenwirksamen Leistungen ausbezahlen zu können
* Im Falle einer Einstellung als Mitarbeiter im Versicherungsvertrieb prüfen wir, ob ein Eintrag bei der Auskunftsstelle über Versicherungs-/Bausparkassenaussendienst und Versicherungsmakler in Deutschland e.V. (AVAD) vorliegt.
* Drittschuldner im Falle von Lohn- und Gehaltspfändungen[[2]](#footnote-2)
* Insolvenzverwalter im Falle einer Privatinsolvenz

**Welche Datenschutzrechte können Sie als Betroffener geltend machen?**

Sie können unter der o.g. Adresse **Auskunft** über die zu Ihrer Person gespeicherten Daten verlangen. Darüber hinaus können Sie unter bestimmten Voraussetzungen die **Berichtigung** oder die **Löschung** Ihrer Daten verlangen. Ihnen kann weiterhin **ein Recht auf Einschränkung der Verarbeitung** Ihrer Daten sowie ein **Recht auf Herausgabe der von Ihnen bereitgestellten Daten** in einem strukturierten, gängigen und maschinenlesbaren Format zustehen.

**Widerspruchsrecht[[3]](#footnote-3)**

**Sie haben das Recht, einer Verarbeitung Ihrer personenbezogenen Daten zu Zwecken der Direktwerbung ohne Angabe von Gründen zu widersprechen. Verarbeiten wir Ihre Daten zur Wahrung berechtigter Interessen, können Sie dieser Verarbeitung aus Gründen, die sich aus Ihrer besonderen Situation ergeben, widersprechen. Wir verarbeiten Ihre personenbezogenen Daten dann nicht mehr, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.**

**Wo können Sie sich beschweren?**

Sie haben die Möglichkeit, sich mit einer Beschwerde an den oben genannten Datenschutz-beauftragten oder an eine Datenschutzaufsichtsbehörde zu wenden. Die für uns zuständige Datenschutzaufsichtsbehörde ist:[[4]](#footnote-4)

Musteraufsichtsbehörde

Musterstraße

xxxxx Musterstadt

**Wie lange werden Ihre Daten gespeichert?**

Wir löschen Ihre personenbezogenen Daten, sobald sie für die oben genannten Zwecke nicht mehr erforderlich sind. Nach Beendigung des Beschäftigungsverhältnisses werden Ihre personenbezogenen Daten gespeichert, solange wir dazu gesetzlich verpflichtet sind. Dies ergibt sich regelmäßig durch rechtliche Nachweis- und Aufbewahrungspflichten, die unter anderem im Handelsgesetzbuch und der Abgabenordnung geregelt sind. Die Speicherfristen betragen danach bis zu zehn Jahre. Außerdem kann es vorkommen, dass personenbezogene Daten für die Zeit aufbewahrt werden, in der Ansprüche gegen uns geltend gemacht werden können (gesetzliche Verjährungsfrist von drei oder bis zu dreißig Jahren).

**Werden Ihre Daten in ein Drittland übermittelt?[[5]](#footnote-5)**

Optional: Sollten wir personenbezogene Daten an Dienstleister oder Konzernunternehmen außerhalb des Europäischen Wirtschaftsraums (EWR) übermitteln, erfolgt die Übermittlung nur, soweit dem Drittland durch die EU-Kommission ein angemessenes Datenschutzniveau bestätigt wurde oder andere angemessene Datenschutzgarantien (z. B. verbindliche unternehmensinterne Datenschutzvorschriften oder EU-Standardvertragsklauseln) vorhanden sind. Detaillierte Information dazu sowie über das Datenschutzniveau bei unseren Dienstleistern in Drittländern finden Sie hier (Link zu den geeigneten Garantien). Sie können die Informationen auch unter den oben genannten Kontaktinformationen anfordern.

**Sind Sie verpflichtet, Ihre Daten bereitzustellen?**

Im Rahmen Ihrer Beschäftigung müssen Sie diejenigen personenbezogenen Daten bereitstellen, die für die Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses und der Erfüllung der damit verbundenen vertraglichen Pflichten erforderlich sind oder zu deren Erhebung wir gesetzlich verpflichtet sind. Ohne diese Daten werden wir nicht in der Lage sein, den Arbeitsvertrag mit Ihnen durchzuführen.

**Inwieweit finden automatisierte Einzelfallentscheidungen oder Maßnahmen zum Profiling statt?[[6]](#footnote-6)**

Optional:

Wir nutzen rein automatisierte Verarbeitungsprozesse zur Herbeiführung einer Entscheidung – einschließlich Profiling – über die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses in folgenden Fällen: (z. B. internes Bewerbermanagement etc.)[[7]](#footnote-7)

\*\*\*

# Anhang 3 – Muster für eine Rahmenbetriebsvereinbarung zur Anpassung des betrieblichen Datenschutzes an die DS-GVO und das BDSG

**Rahmenbetriebsvereinbarung zur Anpassung des betrieblichen Datenschutzes an die Europäische Datenschutz-Grundverordnung 2016/679 (DS-GVO) und das Bundesdatenschutzgesetz vom 30. Juni 2017 (BDSG)**

zwischen

[Name, gesetzliche Vertretung, Anschrift des Arbeitgebers]

nachstehend: **Arbeitgeber**

und

dem (Konzern-/Gesamt-) Betriebsrat des

[Name, gesetzliche Vertretung, Anschrift des Arbeitgebers]

nachstehend: **Betriebsrat**

nachstehend: **Betriebsparteien**

**Präambel**

Am 25.05.2018 wird die DS-GVO unmittelbar geltendes Recht in allen Mitgliedstaaten der Europäischen Union sein. Ziel der DS-GVO ist insbesondere der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Art. 1 Abs. 1 DS-GVO) sowie der freie Verkehr personenbezogener Daten (Art. 1 Abs. 3 DS-GVO). Daneben hat der deutsche Gesetzgeber, das bisherige BDSG a.F. durch ein neues abgelöst, um ein reibungsloses Zusammenspiel zwischen der DS-GVO und deutschem Datenschutzrecht sicherstellen zu können. In der Folge ergänzt das BDSG, soweit zulässig, die Vorgaben der DS-GVO und kommt parallel zur Anwendung.

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn sie auf einen gesetzlich geregelten Erlaubnistatbestand gestützt werden kann. Art. 6 Abs. 1 b) i. V. m. Art. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 4 BDSG sieht dabei vor, dass Betriebsvereinbarungen auch künftig spezifische Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorsehen können. Betriebsvereinbarungen können demnach weiterhin eine eigenständige Ausgestaltung für die Verarbeitung personenbezogener Arbeitnehmerdaten vorsehen.

Die Betriebsparteien haben bereits eine Vielzahl von Kollektivvereinbarungen, die datenschutzrelevante Regelungen und Anforderungen beinhalten (*z. B. Einführung von Zeiterfassungssystemen, Nutzung von E-Mail und Internet*) abgeschlossen, die beim Arbeitgeber zur Anwendung kommen. Um sicherzustellen, dass bis zur Anpassung der bestehenden Regelungswerke alle europa- und bundesrechtlichen Bestimmungen zum Datenschutzrecht transparent zur Anwendung kommen können, vereinbaren die Parteien die nachfolgende (Rahmen-)Regelung.

**1. Gegenstand und Zweck**

(1) Diese Betriebsvereinbarung regelt die Anwendung und Beachtung der für die Verarbeitung personenbezogener Beschäftigtendaten einschließlich besonderer Kategorien personenbezogener Beschäftigtendaten bestehenden gesetzlichen Regelungen auf der Grundlage der DS-GVO und des BDSG. Sie bildet eine Rahmenvereinbarung für alle mit (dem KBR, dem GBR und) den örtlichen Betriebsräten abgeschlossenen kollektiven Regelungen.

(2) Ziel dieser Betriebsvereinbarung ist die Umsetzung der in der DS-GVO und im BDSG geregelten Pflichten der Betriebsparteien und Rechte der Arbeitnehmer bei der Verarbeitung personenbezogener Beschäftigtendaten. Im Hinblick auf die Transparenz (Art. 88 Abs. 2 DS-GVO) der Datenverarbeitung werden die Arbeitnehmer über die geltenden Informationspflichten bei der Erhebung von personenbezogenen Daten und die ihnen zustehenden Betroffenenrechte nach der DS-GVO durch die vorliegende Rahmenregelung *[Optional: die zentral für alle Mitarbeiter im Intranet unter \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ abrufbar ist]* aufgeklärt, soweit keine spezielleren Regelungen in den bestehenden Betriebsvereinbarungen oder einzelvertraglichen Regelungen bestehen.

**2. Geltungsbereich**

(1) Diese Betriebsvereinbarung gilt in persönlicher Hinsicht für alle Arbeitnehmer des Innendienstes und des angestellten Außendienstes sowie für alle Auszubildenden des Arbeitgebers. *[Optional: Ausweitung auf leitende Angestellte und/oder Leiharbeitnehmer]*

(2) Der sachliche Geltungsbereich erfasst alle (Konzern-, Gesamt- und) Betriebsvereinbarungen, die im Sinne der DS-GVO und des BDSG datenschutzrelevante Inhalte aufweisen bzw. als Grundlage für eine Datenverarbeitung dienen.

(3) Soweit in dieser Betriebsvereinbarung die männliche Bezeichnung verwendet wird, so sind davon auch die Arbeitnehmerinnen umfasst. Eine volle Gleichberechtigung ist gewährleistet.

**3. Verpflichtung auf die Inhalte der DS-GVO und des BDSG-neu**

(1) Die Betriebsparteien verpflichten sich, die bereits bestehenden (Konzern-, Gesamt- und) Betriebsvereinbarungen mit datenschutzrelevanten Inhalten im Sinne der DS-GVO und des BDSG, insbesondere nach den Vorgaben von Art. 88 Abs. 2 DS-GVO, auszulegen und den dort geregelten Anforderungen und Verpflichtungen uneingeschränkt nachzukommen. Die Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 DS-GVO werden eingehalten.

(2) Die Betriebsparteien verpflichten sich ferner *[Optional: mit der gebotenen Eile sukzessiv]* die bestehenden Kollektivvereinbarungen den geänderten europa- und bundesrechtlichen Bestimmungen zum Datenschutzrecht, soweit erforderlich, anzupassen. *[Optional: Im Regelfall wird dies dann erfolgen, wenn die Parteien in Hinblick auf Änderungen an dem originären Regelungsgegenstand ohnehin in Verhandlungen miteinander eintreten.]* Der (Konzern-) Datenschutzbeauftragte ist so früh wie möglich zu beteiligen.

**4. Informationspflichten des Arbeitgebers**

(1) Der Arbeitgeber stellt sicher, dass die Arbeitnehmer in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und verständlichen Sprache darüber informiert werden, was mit ihren personenbezogenen Daten geschieht bzw. ob und auf welche Weise ihre personenbezogenen Daten verarbeitet werden.

(2) Werden durch bestehende (Konzern-, Gesamt- oder) Betriebsvereinbarungen personenbezogene Daten der Arbeitnehmer verarbeitet, wird für alle geltenden (Konzern‑, Gesamt- oder) Betriebsvereinbarungen folgendes mitgeteilt:

1. Verantwortlich für die Datenverarbeitung ist der Arbeitgeber bzw. das Unternehmen der *XY Gruppe,* bei dem der Arbeitnehmer angestellt ist. Die Arbeitnehmer können sich an die jeweilige Personalabteilung der *XY AG (Kontaktdaten; Adresse)* wenden. Der (Konzern-)Datenschutzbeauftragte ist unter der *Postanschrift\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* sowie *per E-Mail unter \_\_\_\_\_\_\_\_\_\_\_\_\_* erreichbar.

(b) Die Rechtsgrundlage der Datenverarbeitung ergibt sich direkt aus der jeweiligen Betriebsvereinbarung. Die Betriebsparteien sind sich darüber einig, dass die bestehenden (Konzern-, Gesamt- und) Betriebsvereinbarungen die Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis im Sinne von Art. 6 i. V. m. 88 Abs. 1 DS-GVO i. V. m. § 26 Abs. 4 BDSG näher ausgestalten können. Dem Arbeitgeber bleibt vorbehalten, personenbezogene Daten auch auf der Grundlage künftiger (Konzern-, Gesamt- oder) Betriebsvereinbarungen oder auf der Grundlage einschlägiger gesetzlicher Regelungen zu verarbeiten.

(c) Die Zwecke der Datenverarbeitung ergeben sich aus dem Regelungsgegenstand der jeweiligen Betriebsvereinbarung.

(d) Innerhalb des Unternehmens erhalten nur die Personen und Stellen (z. B. der Betriebsrat) die betroffenen Arbeitnehmerdaten, die zur Erfüllung der (kollektiv-)vertraglichen und gesetzlichen Pflichten erforderlich sind. Werden die Daten zu den oben genannten Zwecken an Auftragsverarbeiter (Art. 4 Nr. 8 DS-GVO) oder Dritte (Art. 4 Nr. 10 DS-GVO) übermittelt, wird hierauf in der jeweiligen (Konzern-, Gesamt- oder) Betriebsvereinbarung hingewiesen. Die fortlaufend aktualisierte Liste aller Dienstleister die im Auftrag des Arbeitgebers Datenverarbeitungen durchführen, kann im Intranet/Internet unter \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ jederzeit eingesehen bzw. heruntergeladen werden.

(e) Beabsichtigt der Arbeitgeber die Übermittlung personenbezogener Arbeitnehmerdaten in ein Drittland (Staaten außerhalb des Europäischen Wirtschaftsraums), wird dies in der jeweiligen (Konzern-, Gesamt- oder) Betriebsvereinbarung offengelegt. Es wird dargelegt, inwieweit die Übermittlung durch einen Angemessenheitsbeschluss der Kommission oder geeignete oder angemessene Garantien gem. Art. 46, 47, 49 DS-GVO gerechtfertigt ist. Der Arbeitnehmer hat die Möglichkeit, jene Garantie in Kopie *[optional: beim Datenschutzbeauftragten]* zu erhalten oder einzusehen.

(f) Die Speicherdauer oder die Kriterien für die Festlegung der Speicherdauer ergeben sich aus der jeweiligen (Konzern-, Gesamt- oder) Betriebsvereinbarung. Der (Konzern-, Gesamt- oder) Betriebsrat löscht die ihm übermittelten personenbezogenen Beschäftigtendaten, sofern sie nicht mehr zur Ausübung seiner Rechte und Pflichten erforderlich sind.

(g) Eröffnet eine (Konzern-, Gesamt- oder) Betriebsvereinbarung die Möglichkeit, in die Verarbeitung personenbezogener Daten einzuwilligen, hat der Arbeitnehmer jederzeit das Recht, die Einwilligung mit Wirkung für die Zukunft zu widerrufen.

(h) Der Arbeitnehmer hat nach Art. 77 DS-GVO ein Beschwerderecht bei der (Name der zuständigen Datenschutzaufsichtsbehörde).

(i) Die Bereitstellung personenbezogener Daten ist gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist. Im Rahmen von (Konzern-, Gesamt- oder) Betriebsvereinbarungen müssen personenbezogene Daten in der Regel für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses bereitgestellt werden. Die Nichtbereitstellung hätte zur Folge, dass das Beschäftigungsverhältnis nicht ordnungsgemäß begründet, durchgeführt oder beendet werden kann.

(j) *Variante 1:* Der Arbeitgeber nutzt keine automatisierten Verarbeitungsprozesse zur Herbeiführung einer Entscheidung – einschließlich Profiling – über die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses.

*Variante 2:* Der Arbeitgeber nutzt rein automatisierte Verarbeitungsprozesse zur Herbeiführung einer Entscheidung – einschließlich Profiling – über die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses in folgenden Fällen: ...

(k) *[Optional: Findet aufgrund einer (Konzern-, Gesamt- oder)* Betriebsvereinbarung *eine Datenerhebung nicht direkt beim betroffenen Arbeitnehmer statt, hat der Arbeitgeber die verarbeiteten Datenkategorien sowie die Herkunft der Daten mitzuteilen und anzugeben, ob sie aus öffentlichen Quellen stammen.]*

**5. Betroffenenrechte der Arbeitnehmer**

(1) Soweit einzelne (Konzern-, Gesamt- oder) Betriebsvereinbarungen die Verarbeitung von personenbezogenen Beschäftigtendaten gestatten, verpflichten sich die Betriebsparteien zur Umsetzung und Einhaltung der im Folgenden unter Abs. 2 dargestellten Betroffenenrechte.

(2) Erlauben bestehende (Konzern-, Gesamt- oder) Betriebsvereinbarungen die Verarbeitung von personenbezogenen Beschäftigtendaten, kann der Arbeitnehmer gegenüber dem Arbeitgeber folgende Betroffenenrechte geltend machen:

(a) Recht auf Auskunft (Art. 15 DS-GVO/ § 34 BDSG)

Auf Verlangen des Arbeitnehmers hat der Arbeitgeber mitzuteilen, ob personenbezogene Daten des Arbeitnehmers verarbeitet werden. Ist dies der Fall, richtet sich der Umfang des weiteren Auskunftsrechts nach Art. 15 DS-GVO und § 34 BDSG. *[Optional: Der Arbeitgeber stellt dem Arbeitnehmer in Papierform/elektronischem Format eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, unentgeltlich zur Verfügung. Für jede weitere Kopie, die der Arbeitnehmer beantragt, kann der Arbeitgeber ein Entgelt in Höhe von \_\_\_\_\_\_€ aufgrund der entstehenden Verwaltungskosten verlangen.]*

(b) Recht auf Berichtigung (Art. 16 DS-GVO)

Der Arbeitnehmer hat das Recht, unverzüglich Berichtung bzw. Vervollständigung ihn betreffender unrichtiger oder lückenhafter personenbezogener Daten zu verlangen. Die Verpflichtung des Arbeitgebers, unrichtige Daten von sich aus zu korrigieren, bleibt hiervon unberührt.

(c) Recht auf Löschung (Art. 17 Abs. 1 DS-GVO/ § 35 BDSG)

Der Arbeitnehmer hat das Recht, die Löschung personenbezogener Daten zu verlangen, sofern einer der in Art. 17 Abs. 1 DS-GVO aufgezählten Gründe einschlägig ist und sich der Arbeitgeber auf keine der in Art. 17 Abs. 3 DS-GVO und § 35 BDSG-neu genannten Ausnahmeregelungen berufen kann.

(d) Recht auf „Vergessenwerden“ (Art. 17 Abs. 2 DS-GVO)

Sofern der Arbeitgeber zu löschende personenbezogene Daten veröffentlicht hat, muss er im Rahmen der zur Verfügung stehenden Technologien die dazu angemessenen organisatorischen und technischen Maßnahmen ergreifen, damit alle Links zu diesen Daten oder Kopien oder Replikationen durch andere Verantwortliche gelöscht werden können.

(e) Recht auf Einschränkung der Datenverarbeitung (Art. 18 DS-GVO)

Auf Verlangen des Arbeitnehmers wird die Verarbeitung seiner personenbezogenen Daten eingeschränkt, wenn dies für ihn im Vergleich zur Löschung sinnvoller und eine der Voraussetzungen in Art. 18 DS-GVO gegeben ist. Dabei werden die betroffenen personenbezogenen Daten mit dem Ziel markiert, ihre künftige Verarbeitung einzuschränken.

(f) Recht auf Datenübertragbarkeit (Art. 20 DS-GVO)

Sofern eine (Konzern-, Gesamt- oder) Betriebsvereinbarung die Verarbeitung von Beschäftigtendaten mittels Einwilligungserklärung zulässt und die Verarbeitung mithilfe automatisierter Verfahren erfolgt, kann der Arbeitnehmer die von ihm selbst bereitgestellten personenbezogenen Daten (z. B. Skill-Daten) in einem strukturierten, gängigen und maschinenlesbaren Format herausverlangen, um diese entweder selbst oder – bei technischer Machbarkeit – durch den Arbeitgeber an einen Dritten übermitteln zu können.

*[Optional: (g) Widerspruchsrecht (Art. 21 DS-GVO)*

*Sofern Betriebsvereinbarungen die Nutzung von Social Media Diensten regeln, könnte ein Widerspruchsrecht gem. Art. 21 Abs. 5 DS-GVO bestehen.]*

(h) Rechte bei automatisierten Einzelfallentscheidungen einschließlich Profilingmaßnahmen (Art. 22 DS-GVO)

Sofern bestehende Betriebsvereinbarungen ausnahmsweise automatisierte Einzelfallentscheidungen – einschließlich Profiling (Art. 4 Nr. 4 DS-GVO) – gestatten, ist der Arbeitgeber nach Art. 22 DS-GVO verpflichtet, Vorkehrungen zu treffen, damit der Arbeitnehmer die Entscheidung beeinflussen kann. Hierzu zählt mindestens das Recht auf Erwirkung des Eingreifens einer natürlichen Person seitens des Arbeitgebers auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung.

(3) Die Ausübung der einzelnen Betroffenenrechte der Arbeitnehmer richtet sich nach der in Art. 12 Abs. 2 bis 6 DS-GVO beschriebenen Verfahrensweise *[Optional:* *sofern im Folgenden nichts anderes geregelt ist. Ist das Verlangen des Arbeitnehmers offenkundig unbegründet oder exzessiv, kann der Arbeitgeber entweder ein Entgelt in Höhe von \_\_\_\_\_\_€ verlangen, bei dem die Verwaltungskosten für die Durchführung der beantragten Maßnahme berücksichtigt werden, oder sich weigern, dem Verlangen des Arbeitnehmers nachzukommen. Ein exzessives Verlangen liegt vor, wenn der Arbeitnehmer innerhalb von \_\_\_\_\_\_\_\_\_\_\_\_\_(Zeitraum) seinen Antrag wiederholt.*

*[Optional:*

***6. Verpflichtung des (Konzern, Gesamt-, und) Betriebsrats auf Einhaltung des Datenschutzes***

*(1) Die Betriebsparteien sind sich einig, dass der (Konzern-, Gesamt- und) Betriebsrat als Teil der verantwortlichen Stelle selbst zur Einhaltung der gesetzlichen Datenschutzbestimmungen verpflichtet ist. Er hat eigenständig über Maßnahmen zu beschließen, die den Anforderungen der DS-GVO und des BDSG gerecht werden, um die Zulässigkeit eigenverantwortlicher Datenverarbeitungen sicherstellen zu können.*

*(2) Der (Konzern-, Gesamt- und) Betriebsrat untersteht der Kontrolle des (Konzern-) Datenschutzbeauftragten.*

*(3) Der (Konzern-, Gesamt- und) Betriebsrat hat in Ansehung seiner im BetrVG geregelten Beteiligungsrechte in jedem Fall zu prüfen, inwieweit der Zweck der Datenverarbeitung auch anhand von anonymisierten Beschäftigtendaten erreicht werden kann.*

*(4) Die Mitglieder und Ersatzmitglieder des (Konzern-, Gesamt- und) Betriebsrats verpflichten sich auf Einhaltung des Datengeheimnisses. Über personenbezogene Beschäftigtendaten, die im Rahmen der Amtstätigkeit verarbeitet worden sind, ist Stillschweigen zu bewahren.]*

**7. Inkrafttreten; Kündigung; Schlussbestimmungen**

(1) Diese Betriebsvereinbarung tritt zum 25.05.2018 in Kraft. Sie kann von beiden Seiten mit einer Frist von 6 Monaten zum Ende des Kalenderjahres gekündigt werden.

*[Optional:*

*(2) Die Betriebsvereinbarung entfaltet Nachwirkung bis zum Abschluss einer neuen Betriebsvereinbarung]*

(3) Sollte sich aufgrund von Entscheidungen des europäischen oder nationalen Gesetzgebers, der Datenschutzaufsichtsbehörden der Länder des Bundes sowie der EU oder in der europäischen oder nationalen Rechtsprechung konkret abzeichnen, dass die Praxis der sukzessiven Anpassung bestehender (Gesamt-, Konzern- und) Betriebsvereinbarungen nicht ausreichend ist, verpflichten sich die Parteien unverzüglich in Verhandlungen über Änderungen aus dieser Betriebsvereinbarung einzutreten. Können die Parteien sich nicht einigen, kann jede Partei die Einigungsstelle anrufen. Der Spruch der Einigungsstelle ersetzt die Einigung zwischen den Parteien. Die Einigungsstelle ist paritätisch besetzt durch je \_\_\_ Beisitzer des Arbeitgebers und des Betriebsrates unter Einbeziehung des Datenschutzbeauftragten als nichtstimmberechtigter Beteiligter. Die Beisitzer sind unverzüglich nach Aufrufung der Einigungsstelle zu benennen.

(4) Sollte eine Bestimmung dieser Vereinbarung ganz oder teilweise unwirksam sein oder werden, so wird hiervon die Wirksamkeit der übrigen Bestimmungen dieser Vereinbarung nicht berührt. Anstelle der unwirksamen Bestimmung werden die Parteien eine gesetzlich zulässige Bestimmung vereinbaren, die dem mit der unwirksamen Bestimmung Gewollten am nächsten kommt. Dasselbe gilt für den Fall einer vertraglichen Lücke.

\_\_\_\_\_\_\_[Ort]\_\_\_\_\_\_\_\_\_\_\_\_, den \_\_\_\_\_\_\_[Datum]\_\_\_\_\_\_\_\_\_

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

(Unterschrift Arbeitgeber) (Unterschrift Betriebsratsvorsitzende/r)

# Anhang 4 – Muster für eine Rahmenbetriebsvereinbarung im Hinblick auf die Vorgaben der DS-GVO und des BDSG

**Rahmenbetriebsvereinbarung zur Anpassung des betrieblichen Datenschutzes an die Europäische Datenschutz-Grundverordnung 2016/679 (DS-GVO) und das Bundesdatenschutzgesetz vom 30. Juni 2017 (BDSG)**

Die Betriebsparteien haben bereits eine Vielzahl von Kollektivvereinbarungen, die datenschutzrelevante Regelungen und Anforderungen beinhalten (z.B. Einführung von Zeiterfassungssystemen, Nutzung von E-Mail und Internet) abgeschlossen, die beim Arbeitgeber zur Anwendung kommen. Um sicherzustellen, dass bis zur Anpassung der bestehenden Regelungswerke alle europa- und bundesrechtlichen Bestimmungen zum Datenschutzrecht transparent zur Anwendung kommen können, vereinbaren die Parteien die nachfolgende (Rahmen-)Regelung.

Die Betriebsparteien verpflichten sich, die bereits bestehenden (Konzern-, Gesamt- und) Betriebsvereinbarungen mit datenschutzrelevanten Inhalten im Sinne der DS-GVO und des BDSG, insbesondere nach den Vorgaben von Art. 88 Abs.2 DS-GVO, auszulegen und den dort geregelten Anforderungen und Verpflichtungen uneingeschränkt nachzukommen. Die Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 DS-GVO werden eingehalten. Bei unterschiedlichen Auslegungsvarianten wird eine Alternative in einer Protokollnotiz festgehalten.

Die Betriebsparteien verpflichten sich ferner mit der gebotenen Eile sukzessiv die bestehenden Kollektivvereinbarungen den geänderten europa- und bundesrechtlichen Bestimmungen zum Datenschutzrecht, soweit erforderlich, anzupassen. Im Regelfall wird dies dann erfolgen, wenn die Parteien in Hinblick auf Änderungen an dem originären Regelungsgegenstand ohnehin in Verhandlungen miteinander eintreten. Der (Konzern-) Datenschutzbeauftragte ist so früh wie möglich zu beteiligen.

# Anhang 5 – Muster für eine Verpflichtung auf das Datengeheimnis und Merkblatt

**Verpflichtung auf das Datengeheimnis und Verschwiegenheitspflicht**

Herr Max Mustermann, Personal-Nr. 105640

wird wie folgt auf das Datengeheimnis verpflichtet und auf die Strafbarkeit von Verstößen hingewiesen:

Es ist Ihnen untersagt, personenbezogene Daten unbefugt zu verarbeiten.

Verstöße gegen das Datengeheimnis können nach Art. 83 DS-GVO i. V. m. §§ 41-43 BDSG mit Bußgeld, Geld- oder Freiheitsstrafe geahndet werden.

Darüber hinaus werden Sie auf die in Ihrem Arbeitsvertrag und der Arbeitsordnung enthaltene Verschwiegenheitspflicht hingewiesen, die durch die Verpflichtung auf das Datengeheimnis nicht berührt wird.

Beide Verpflichtungen bestehen auch nach Beendigung Ihres Beschäftigungsverhältnisses fort.

Zur Kenntnis genommen und bestätigt:

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

Ort, Datum Unterschrift der/des Beschäftigten

**Anlage: Merkblatt**

Original: Personalakte

Kopie: Beschäftigte(r)

**Für Ihre Unterlagen**

**Merkblatt**

**Verpflichtung auf das Datengeheimnis**

**1. Gesetzliche Grundlagen**

Neben den betrieblichen Geheimhaltungsvorschriften gelten für Sie aufgrund Ihrer Aufgabenstellung die Bestimmungen der Europäischen Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG).

Wir verpflichten Sie, das Datengeheimnis zu wahren. Hiernach ist es Ihnen untersagt, personenbezogene Daten unbefugt zu verarbeiten. Diese Verpflichtung ist Teil des Arbeitsvertrages und erlischt nicht, wenn Sie eine andere Aufgabe im Konzern übernehmen oder das Unternehmen verlassen.

Verstöße gegen das Datengeheimnis können nach Art. 83 DS-GVO i. V. m. §§ 41-43 BDSG mit Bußgeld, Geld- oder Freiheitsstrafe geahndet werden.

**2. Erläuterung der wichtigsten gesetzlichen Bestimmungen**

**2.1 Aufgabe des Datenschutzes**

ist es, Persönlichkeitsrechte des Menschen zu schützen: Seine individuellen Daten dürfen bei ganz oder teilweise automatisierter Verarbeitung sowie bei nichtautomatisierter Verarbeitung und Speicherung in einem Dateisystem nicht zweckentfremdet oder missbraucht werden. Im Rahmen eines Beschäftigungsverhältnisses gelten die gesetzlichen Regelungen zum Datenschutz auch für sonstige Unterlagen, die weder (teil-)automatisiert verarbeitet noch in einem Dateisystem gespeichert werden.

**2.2 Personenbezogene Daten**

sind „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere durch Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“.

Beispiele: Name, Anschrift, Geburtsdatum, Ausbildung, Gesundheitszustand, Kauf- und Zahlungsgewohnheiten, familiäre und finanzielle Verhältnisse von Mitarbeitern, Bewerbern, Kunden, Interessenten, Lieferanten, Fremdkräften.

**2.3.** **Verarbeitung**

„Verarbeitung“ meint jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

**2.4. Zulässigkeitsvoraussetzungen**

Eine Erlaubnis zum Verarbeiten personenbezogener Daten zur Erfüllung von Geschäftszwecken des Unternehmens besteht nur,

* wenn dies zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der das Unternehmen unterliegt, z. B. aufgrund von Steuer- und Sozialgesetzen, HGB, AktG, BetrVG, Tarifverträgen, Gerichtsbeschluss;
* wenn die betroffene Person vorab schriftlich eingewilligt hat;
* wenn dies für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist oder zur Durchführung einer vorvertraglichen Maßnahme, die auf Anfrage der betroffenen Person erfolgt, erforderlich ist (z. B. Arbeits-, Kauf-, Mietvertrag);
* soweit es zur Wahrung berechtigter Interessen der speichernden Stelle oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt (Interessenabwägung);
* wenn dies erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder eine anderen natürlichen Person zu schützen.

**2.5. Grundsätze für die Verarbeitung, insbesondere Zweckbindung**

Personenbezogene Daten müssen

* auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
* für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden;
* dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein;
* sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein;
* nach dem Wegfall des Zwecks der Speicherung gelöscht werden. Hierbei sind gesetzliche und interne Aufbewahrungsfristen zu beachten.

**2.6. Informationspflicht**

Die datenverarbeitende Stelle muss den Beauftragten für den Datenschutz über geplante Systeme und Datenverarbeitungsverfahren mit personenbezogenen Daten rechtzeitig informieren.

**2.7. Anfragen externer Stellen**

Bei einzelnen, im öffentlichen Interesse stehenden Ausnahmetatbeständen ist eine Datenweitergabe zusätzlich erlaubt (z. B. Erteilung von Auskünften an die Polizei bei Vorliegen einer staatsanwaltlichen Verfügung oder eines richterlichen Beschlusses, Flucht- oder Verdunkelungsgefahr). Anfragen von Banken, Versicherungen, Rechtsanwälten usw. dürfen – sofern sie nicht von einer in Punkt 2.4. aufgeführten Zulässigkeitsvoraussetzungen gedeckt sind - grundsätzlich nicht ohne Einwilligung der betroffenen Person beantwortet werden. In Zweifelsfällen sollte vor einer Datenübermittlung der Beauftragte für den Datenschutz eingeschaltet werden.

**2.8. Datensicherung**

Die personenbezogenen Daten sind in einer Weise zu verarbeiten, die ihre angemessene Sicherheit gewährleistet. Davon umfasst sind geeignete technische und organisatorische Maßnahmen zum Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

**3. Datenschutz als permanente Aufgabe**

Es liegt in Ihrem und in unserem Interesse, sowohl die gesetzlichen Verpflichtungen nach dem BDSG als auch die betrieblichen Geheimhaltungsvorschriften strikt einzuhalten. Die Verantwortung hierfür und für die zu treffenden internen Maßnahmen und Regelungen zum Umgang mit personenbezogenen Daten liegt in den Fachabteilungen.

Aus diesem Grunde sollten Sie zusätzlich zu dieser Verpflichtung auf das Datengeheimnis ein Datenschutzseminar besuchen, das Sie im ständigen Angebot der Weiterbildungsstellen finden.

Da der betriebliche Datenschutz im Wesentlichen auf Grundsätzen und weniger auf gesetzlichen Detailregelungen beruht, muss bei der Verarbeitung personenbezogener Daten in jedem Einzelfall eine sorgfältige Abwägung zwischen unterschiedlichen Interessen vorgenommen werden. Daher ist es unerlässlich, Verantwortungsbewusstsein und Sensibilität in Datenschutzfragen zu entwickeln.

Sollten Sie Mängel hinsichtlich Datenschutz, Datensicherung und Ordnungsmäßigkeit der Datenverarbeitung feststellen, werden Auskünfte über personenbezogene Daten von Ihnen gefordert oder haben Sie Fragen zum Thema Datenschutz, so wenden Sie sich bitte an Ihre Führungskraft oder direkt an den Beauftragten für den Datenschutz.

# Anhang 7 – Muster für eine Rahmenbetriebsvereinbarung über die Einführung und Nutzung von DVM

**Inhalt**

[§ 1 Geltungsbereich 20](#_Toc501049416)

[§ 2 Definitionen und Verzeichnis der DVM 20](#_Toc501049417)

[2.1 Definition 20](#_Toc501049418)

[2.2 Verzeichnis der DVM (VdDVM) 21](#_Toc501049419)

[2.3 Zugriffsrechte für Beschäftigte 22](#_Toc501049420)

[§ 3 Umgang mit DVM und Zusammenarbeit der Betriebsparteien 22](#_Toc501049421)

[3.1 Bestehende DVM 22](#_Toc501049422)

[3.2 Änderungen/Anpassungen bestehender DVM 22](#_Toc501049423)

[3.3 Einführungen neuer DVM 23](#_Toc501049424)

[3.4 Zugriffsrechte des Betriebsrats 23](#_Toc501049425)

[3.5 Sachverständige 23](#_Toc501049426)

[§ 4 Umgang mit Beschäftigtendaten 23](#_Toc501049427)

[4.1 Zweckbestimmungen 24](#_Toc501049428)

[4.2 Weitergabe von Beschäftigtendaten an konzerninterne und externe Empfänger 25](#_Toc501049429)

[4.3 Rechte der betroffenen Personen 25](#_Toc501049430)

[§ 5 Verhaltensgrundsätze bei der Verarbeitung mit Hilfe von DVM 25](#_Toc501049431)

[§ 6 Missbrauchskontrolle 26](#_Toc501049432)

[§ 7 Zuwiderhandlungen und Konfliktlösungsmechanismus 26](#_Toc501049433)

[§ 8 Sonstiges 27](#_Toc501049434)

ANLAGE 1

[Verzeichnis der Datenverarbeitungsmethoden (VdDVM) 28](#_Toc501049436)

**Rahmenbetriebsvereinbarung über die Einführung und Nutzung von DVM**

zwischen der „XYZ GmbH“ –

**Arbeitgeber einerseits**

und

dem Gesamt-Betriebsrat der XYZ GmbH

– nachfolgend „GBR“ genannt –

gleichzeitig auch im Auftrag und mit Vollmacht nach § 50 Abs. 2 BetrVG handelnd für

**GBR andererseits**

**Präambel**

Die Betriebsparteien stimmen darin überein, dass die Anwendung von Systemen und Verfahren zum Umgang mit Beschäftigtendaten (Datenverarbeitungsmethoden; Abkürzung: DVM) zur wirtschaftlichen und ordnungsgemäßen Erledigung von Aufgaben sinnvoll und notwendig ist. Vor diesem Hintergrund ist es wichtig, dass die Beschäftigten vor missbräuchlichem Umgang mit ihren personenbezogenen Daten geschützt werden, die Persönlichkeitsrechte der Beschäftigten beachtet und die Beschäftigtendaten entsprechend dem Datenschutzrecht behandelt werden.

Mit der nachfolgenden Vereinbarung werden Rahmenregelungen für alle DVM festgelegt. Nähere Einzelheiten können auf Wunsch einer Betriebspartei in ergänzenden Betriebsvereinbarungen von den jeweiligen Betriebsparteien festgelegt werden. Sofern Zuständigkeiten nicht beim GBR liegen, empfehlen die Parteien dieser GBV den jeweils zuständigen Gremien dennoch, die Grundsätze dieser GBV einzuhalten und auf diese Bezug zu nehmen.

**§ 1 Geltungsbereich**

Die Inhalte dieser Betriebsvereinbarung finden Anwendung auf Arbeitnehmer i. S. d. des § 5 BetrVG und alle DVM.

**§ 2 Definitionen und Verzeichnis der DVM**

**2.1 Definition**

Unter dem Begriff **DVM (Datenverarbeitungsmethoden)** werden technische Einrichtungen und deren Anwendungen verstanden, die über Verarbeitungs-, Speicherungs- oder Auswertungsmöglichkeiten von Beschäftigtendaten verfügen und andere technische Einrichtungen, die geeignet sind, Verhalten oder Leistung von Beschäftigten zu überwachen. Insbesondere sind hier sowohl Hardware, z. B. Computer und Telefone, als auch Software, z. B. Anwendungen und Programme wie Smartphone-Apps, SAP und SMS-Dienste und Daten, wie z. B. Bilder Sprache, Grafik, Video, Ton, Zeichnungen und Texte gemeint. DVM werden von den Betriebsparteien in folgende Kategorien eingeteilt und das Ergebnis dokumentiert:

**Kategorie 1:** Solche DVM, die auch oder ausschließlich dazu genutzt werden sollen, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen (z. B. Personalmanagement, Zielvereinbarungsgespräche, Zutrittskontrolle, Zeitkontrolle);

**Kategorie 2:** Solche DVM, die zwar dazu geeignet sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, zu diesem Zweck aber nicht genutzt werden sollen (z. B. das GPS-Navigationssystem in Dienstwagen *oder Handy*, *Videoüberwachung*); und

**Kategorie 3:** Solche DVM, die nicht dazu geeignet sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen (z. B. die Rechnerfunktion im Smartphone, Google Maps).

**Anpassungen** sind sogenannte Updates oder ein Hardwareaustausch ohne Funktionsänderung. Der Begriff Update umfasst die Aktualisierung von Software, Daten oder Datenbanken. Es enthält in der Regel kleinere Verbesserungen wie etwa Optimierungen in der Programmausführungsgeschwindigkeit und beseitigt Fehler oder Sicherheitslücken innerhalb eines bestimmten Programms oder Softwarestands, was auch als Service Release, Patch oder Hotfix bezeichnet wird.

**Änderungen** sind sogenannte Upgrades oder ein Hardwareaustausch mit Funktionsänderung. Der Begriff Upgrade bezeichnet dabei die Änderung eines Produkts auf eine höherwertige Konfiguration oder Version mit deutlich neuen Funktionen. Regelmäßig wird es sich dabei um Hard-/ Software Produkte handeln, die sodann durch eine Änderung der Versionsnummer gekennzeichnet sind.

**2.2 Verzeichnis der DVM (VdDVM)**

Zur korrekten und einheitlichen Dokumentation werden die zuständigen Betriebsparteien die nachfolgend aufgeführten Informationen für einzelne oder zusammengefasste DVM (*z. B. einzelne SAP-Module oder zusammengefasst MS Office*), in ein Verzeichnis (VdDVM) aufnehmen, das den geltenden Datenschutzbestimmungen genügt (Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DS-GVO); [**Anlage**](#_ANLAGE_1) **1.**

* + Verantwortliche Stelle (Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten)
  + Zweckbestimmung (Zweck der Verarbeitung)
  + Betroffene Personengruppen und Daten oder Datenkategorien (Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten)
  + Empfänger oder Kategorien von Empfängern (Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen)
  + Zugriffsberechtigungen (funktionsbezogen, auch internationaler Bezug)
  + Geplante Datenübermittlung in Drittstaaten ohne anerkanntes EU-Datenschutzniveau (Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie, falls nach den datenschutzrechtlichen Vorschriften erforderlich – die Dokumentierung geeigneter Garantien (Art. 49 Abs. 1 Unterpunkt 2 DS-GVO))
  + Regelfristen für die Löschung bzw. Sperrung der Daten (evtl. Fristen für die Löschung der verschiedenen Datenkategorien)
  + Beurteilung der Angemessenheit getroffener Sicherheitsmaßnahmen
  + Nachweis/Dokumentation Prozess der unabdingbaren Rechte der Betroffenen
  + Beschreibung der technischen und organisatorischen Maßnahmen

**Optional:**

* + ggf. mitgeltende Unterlagen, wie bspw. Arbeits-/ Verfahrensanweisungen o. ä.
  + Zeitpunkt der Aufnahme und geplante Dauer des Verfahrens
  + Ergebnis der Datenschutz-Folgenabschätzung (falls erforderlich)

Die Betriebsparteien sind sich darüber einig, dass es für solche DVM, deren Zwecke in den §§ 4–6 aufgeführt sind und deren Beschreibung gemäß dieser Ziffer 2.2 bereits erfolgt ist, keiner gesonderten Betriebsvereinbarung bedarf.

Das Verzeichnis wird regelmäßig überprüft und gepflegt.

**2.3 Zugriffsrechte für Beschäftigte**

Berechtigung für den Zugriff auf DVM bzw. auf die sich hierin befindlichen Daten werden entsprechend der jeweiligen dienstlichen Tätigkeit der Mitarbeiter vergeben und ggf. auch wieder entzogen und sind auf das zur jeweiligen fachbezogenen Aufgabenerfüllung erforderliche Maß zu beschränken.

Jedes Zugriffskonzept muss den gesetzlichen Vorgaben des Datenschutzes und den jeweils gültigen Richtlinien und Standards des Arbeitgebers entsprechen. Dem zuständigen Betriebsrat wird auf Wunsch Einblick in das jeweilige Zugriffskonzept gegeben.

**§ 3 Umgang mit DVM und Zusammenarbeit der Betriebsparteien**

**3.1 Bestehende DVM**

Diejenigen DVM, die bei Inkrafttreten dieser Betriebsvereinbarung bereits eingeführt sind, gelten bis zur nächsten Änderung als legitimiert.

**3.2 Änderungen/Anpassungen bestehender DVM**

Ein neues Mitbestimmungsrecht entsteht nur bei Änderungen von DVM bzw. bei Upgrades bereits eingeführter DVM mit neuen wesentlichen Änderungen der Überwachungsmöglichkeiten von Beschäftigtendaten, nicht dagegen bei Anpassungen. Bei solchen Änderungen ist gemäß Ziff. 3.3 vorzugehen.

Einspielen von Patches und Updates(einschl. Ersatz von Hardware), die der Fehlerbehebung dienen oder vom Hersteller/Lizenzgeber standardmäßig vorgesehen sind, sind Anpassungen und keine Änderungen im Sinne dieser Betriebsvereinbarung, sofern dadurch der Funktionsumfang nicht geändert wird und sich keine Änderungen der DVM ergeben. Ein Mitbestimmungsrecht beim Hardwareaustausch besteht nicht, sofern dadurch die DVM nicht wesentlich verändert wird und keine neuen, über die bisherigen DVM hinausreichenden Funktionen genutzt werden. Auf Nachfrage ist der Betriebsrat über solche Anpassungen zu unterrichten.

**3.3 Einführungen neuer DVM**

Wenn eine neue DVM eingeführt werden soll, ist wie folgt vorzugehen:

a) Bei einer DVM der Kategorie 1 wird der Betriebsrat rechtzeitig vor der Einführung informiert. Die Nutzung der DVM zur Verhaltens- oder Leistungskontrolle ist nur zu den unter §§ 5 und 6 aufgeführten Zwecken zulässig oder wenn diese gesetzlich erlaubt oder mit dem Betriebsrat abgestimmt ist.

b) Bei einer DVM der Kategorie 2 ist die Einführung zulässig, wenn der zuständige Betriebsrat vorher das VdDVM erhalten hat. Eine Leistungs- und Verhaltenskontrolle findet nicht statt, außer in den Fällen des § 6 (Missbrauch).

c) Bei einer DVM der Kategorie 3 wird der Betriebsrat auf Nachfrage über die Einführung informiert, sofern dem Arbeitgeber dies bekannt ist.

**3.4 Zugriffsrechte des Betriebsrats**

Der Betriebsrat hat das Recht die Einhaltung der Regelungen dieser Betriebsvereinbarung im Rahmen seiner betriebsverfassungsrechtlichen Überwachungsaufgaben zu prüfen. Die hierzu notwendigen Angaben werden ihm auf Anfrage zur Verfügung gestellt.

Ein eingeschränktes, zweckgebundenes Zugriffsrecht kann ihm im Rahmen seiner betriebsverfassungsrechtlichen Aufgaben gewährt werden, sofern er dem Datenschutzbeauftragten den Nachweis seiner datenschutzkonformen Betriebsratsarbeit und die Selbstverpflichtungen auf das **Datengeheimnis** (i. S. d. des § 53 BDSG) und weiterer betrieblicher Geheimhaltungspflichten erbringt.

**3.5 Sachverständige**

Der Betriebsrat hat im Rahmen seiner Aufgaben bei technischen Fragen zur Funktion und betrieblichen Arbeitsweise von DVM und Fragen zum Datenschutz zunächst innerbetriebliche Informationsquellen (z. B. den Datenschutzbeauftragten) zu nutzen.

**§ 4 Umgang mit Beschäftigtendaten**

Im Zusammenhang mit DVM dürfen nur so viele personenbezogene Daten der Beschäftigten verarbeitet werden, wie zur Erfüllung der mit den DVM verfolgten betrieblichen Aufgaben erforderlich sind. Daten, die für die Erreichung der mit den DVM verfolgten Zwecken nicht mehr erforderlich sind, sind zu löschen oder zu sperren. Gesetzliche Aufbewahrungspflichten sind zu beachten.

**4.1 Zweckbestimmungen**

Der Einsatz von DVM kann dazu führen, dass Rückschlüsse auf das Verhalten und/oder die Leistung einzelner Beschäftigter möglich werden (z. B. durch Log-Dateien, die Aktivitäten der Beschäftigten aufzeichnen oder protokollieren). Die Durchführung von DVM zu nachfolgenden Zwecken ist grundsätzlich zulässig, ohne dass für diese Zweckbestimmungen eine gesonderte Betriebsvereinbarung erforderlich ist:

* + zur Erfüllung gesetzlicher oder gesetzesgleicher Vorschriften (z. B. steuerliche Belange, amtliche Statistiken, Sozialversicherung usw.);
  + für die Durchführung und Dokumentation gesetzlich oder betrieblich notwendiger rechtlicher, technischer oder wirtschaftlicher Prüfungen (z. B. Wirtschaftsprüfer, Innenrevision);
  + zur Sicherstellung ordnungsgemäßer Datenverarbeitung gemäß IT-sicherheitstechnischer und datenschutzrechtlicher Anforderungen (z. B. Anmeldedaten bei DVM, Protokolldateien);
  + zum Zwecke der Identifikation von Ansprechpartnern (z. B. Name, Telefonnummern, E-Mail-Adressen) und Durchführung betrieblicher Kommunikation
  + zur Durchführung von Mitarbeiterbefragungen auf freiwilliger Basis
  + Analyse und Korrektur technischer Fehler
  + Gewährleistung der Systemsicherheit und -verfügbarkeit
  + Optimierung und Steuerung der Systeme
    - Aktualisierung der Liste gesperrter Internetseiten
    - Optimierung der Netzdienste
  + Datenschutzkontrolle/Datenschutzzwecke
  + Gesetzliche Auskunftspflichten
  + zur Maschinen- und Anlagensteuerung (z. B. Betriebs-/ Maschinendatenerfassung (BDE/MDE))
  + zur Lohn- und Gehaltsabrechnung sowie zur Reisekostenerstattung
  + zur Personalaktenführung;
  + zur Personaleinsatzplanung und Disposition;
  + zur Erfassung von An- und Abwesenheitszeiten;
  + zur Durchführung eines betrieblichen Eingliederungsmanagements (BEM)
  + zur Entgeltabrechnung per E-Mail
  + zur Personalverwaltung (z. B. Darlehensabwicklung, Dienstwagenabwicklung, Versicherungen, betriebliche Altersversorgung);
  + zur Personalplanung und Personalcontrolling;
  + zur Personalentwicklung (insbesondere Nachwuchssicherung, Personalaustausch, Aus- und Fortbildung, gezielte Stellenbesetzung);
  + zur Speicherung von Wiedervorlagedaten (z. B. Ablauf der Probezeit, Befristung, Dauer des Mutterschutzes usw.).
  + zur Zugangs-/Zutrittskontrolle
  + zur Erfassung der Lenk- und Ruhezeiten mittels digitalem Tachograph/Fahrerkarte
  + zur Mautabrechnung
  + zur automatisierten Durchführung der Führerscheinkontrolle i. R. der Halterhaftung

…

Für alle vorgenannten DVM gilt: Es findet keine Verhaltens- und Leistungskontrolle statt, es sei denn, dieser Zweck ist in dem VdDVM ausdrücklich beschrieben oder gemäß § 6 (Missbrauch) erlaubt.

Weitere Zweckbestimmungen können zwischen Arbeitgeber und dem jeweils zuständigen Betriebsratsgremium vereinbart werden.

**4.2 Weitergabe von Beschäftigtendaten an konzerninterne und externe Empfänger**

Zu den vorgenannten Zwecken kann die Datenverarbeitung gemeinsam mit oder durch andere Datenverarbeiter erfolgen, soweit die Vorschriften dieser Betriebsvereinbarung eingehalten werden.

Insbesondere können Beschäftigtendaten bei berechtigtem Interesse i. S. d. DS-GVO (ErwGr. 48) innerhalb der Unternehmensgruppe übermittelt werden. Dieses berechtigte Interesse liegt bei allen durch diese Betriebsvereinbarung geregelten DVM vor.

**4.3 Rechte der betroffenen Personen**

Den Beschäftigten stehen die Betroffenenrechte nach §§ 32–37 BDSG n. F. / Artikel 12 ff. DS-GVO zu. Die Informationspflichten des Arbeitgebers entfallen unter anderem wenn die Speicherung oder Offenlegung der personenbezogenen Daten ausdrücklich durch Rechtsvorschriften geregelt ist oder wenn sich die Unterrichtung als unmöglich erweist oder mit unverhältnismäßig hohem Aufwand verbunden ist

**§ 5 Verhaltensgrundsätze bei der Verarbeitung mit Hilfe von DVM**

Die Nutzung der vom Arbeitgeber als Arbeitsmittel zur Verfügung gestellten DVM ist grundsätzlich nur zu betrieblichen Zwecken mit einem verantwortungsvollen Umgang zulässig. Die damit erzeugten Daten sind grundsätzlich Eigentum des Unternehmens.

Jede Verarbeitung mit Hilfe von DVM ist unzulässig, die

* + gegen geltende Rechtsvorschriften (z. B. der Verrat von Betriebs- oder Geschäftsgeheimnissen) und/oder
  + lizenz- und urheberrechtliche Bestimmungen verstößt oder
  + die geeignet ist, den Interessen des Arbeitgebers oder dessen Ansehen in der Öffentlichkeit zu schaden oder
  + die Sicherheit und Funktionsfähigkeit des Firmennetzes und/oder
  + der daraus zu erreichenden Dienste zu beeinträchtigen.

Dabei ist insbesondere folgende Verarbeitung untersagt:

* + Die Verarbeitung von Informationen, die gegen Gesetze verstößt oder die geeignet ist, den Betriebsfrieden zu stören. Hierzu gehören insbesondere Inhalte, die sich gegen die Würde des Menschen richten, vor allem pornographische, sexistische, pädophile, gewaltverherrlichende, fremdenfeindliche, nazistische, rassistische, politisch-radikale oder sittenwidrige Inhalte.
  + Das Herunterladen von Programmen (z. B. komprimierte .exe; .bat; .com-Dateien, DVD’s etc.) und die Installation dieser Programme auf dem Arbeitsplatzrechner oder dem geschäftlichen Laptop. Auf diesem dürfen nur Programme installiert werden, die durch die IT-Abteilung autorisiert wurden. In Zweifelsfällen ist die IT-Fachabteilung anzusprechen.
  + Das Herunterladen von Radioprogrammen, Filmen, MP3-Dateien, Spielen oder Ähnlichem.
  + Das Aufsuchen von Chatrooms aus privaten Gründen sowie die Teilnahme an interaktiven Spielen.
  + Die Werbung, das Starten oder Weiterleiten von Kettenmails, die beispielsweise Warnungen vor Gefahren (Viren oder ähnlichem) zum Inhalt haben.
  + Die Nutzung von kostenpflichtigen Internetseiten.
  + Das Abrufen von bestimmten gesperrten Internetseiten/-diensten (black-list)
  + Jegliche Art von Tausch- und Versteigerungsplattformen (z. B. ebay), sowie von Shoppingangeboten
  + Die Nutzung sogenannter Instantmassaging-Dienste und sozialer Netzwerke (z. B. WhatsApp/Facebook)

Spezifischere Regelungen zum Umgang mit DVM sind in den entsprechenden Betriebsvereinbarungen, Richtlinien oder Arbeitsordnungen geregelt.

**§ 6 Missbrauchskontrolle**

Kontrollen der Leistung und des Verhaltens des Beschäftigten, die in dieser Betriebsvereinbarung nicht ausdrücklich vorgesehen sind, sind nur zulässig, wenn die schutzwürdigen Interessen des Arbeitgebers diejenigen des Beschäftigten überwiegen.

Schutzwürdige Interessen des Arbeitgebers sind die Vermeidung von Gefährdungen der Systemsicherheit sowie die Verhinderung und die Aufdeckung von Straftaten, Missbrauch oder Verstoß gegen die in den Betriebsvereinbarungen aufgestellten Nutzungsregeln. Der begründete, konkrete und dokumentierte Verdacht auf einen Verstoß berechtigt den Arbeitgeber unter Wahrung des Verhältnismäßigkeitsgrundsatzes zur Einleitung von Kontrollmaßnahmen und ggf. auch zur Durchführung personenbezogener Auswertungen.

Der Betriebsrat und der Datenschutzbeauftragte sind unverzüglich zu informieren. Sollte der Betriebsrat oder eines seiner Mitglieder selbst Gegenstand einer Maßnahme sein, ist der Datenschutzbeauftragte im Voraus einzubeziehen.

Bei unerlaubter bzw. missbräuchlicher Nutzung von DVM sind arbeitsrechtliche Konsequenzen möglich.

**§ 7 Zuwiderhandlungen und Konfliktlösungsmechanismus**

Die Verarbeitung von personenbezogenen Daten und die Nutzung von DVM sind unzulässig, wenn sie gegen gesetzliche Bestimmungen oder gegen diese oder eine andere Betriebsvereinbarung verstoßen. Vermutet eine Betriebspartei eine unzulässige Nutzung, hat sie dies der jeweils anderen Partei unverzüglich anzuzeigen.

Meinungsverschiedenheiten im Zusammenhang mit dieser GBV oder einer ergänzenden Betriebsvereinbarung gem. der Präambel sowie allgemein im Zusammenhang mit DVM, insbesondere ihrer Einführung, Nutzung oder Änderung, sollen einvernehmlich zwischen den zuständigen Betriebsparteien gelöst werden.

Sollte dies in Fällen der Zuständigkeit des Betriebsrats nicht möglich sein, kann von jeder Seite ein paritätischer Ausschuss einberufen werden, der aus vier unternehmensangehörigen Personen zusammengesetzt ist, von denen jeweils zwei vom Arbeitgeber und vom Betriebsrat zu bestimmen sind. Er soll innerhalb von sechs Wochen nach Zugang des Einberufungsschreibens mit einfacher Mehrheit eine Lösung herbeiführen. Das entsprechende Verfahren soll möglichst auch von den Betriebsparteien in anderen Zuständigkeitsbereichen durchgeführt werden.

Im Falle einer Nichteinigung innerhalb dieser Frist über mitbestimmungspflichtige Tatbestände kann jede Seite die Einigungsstelle gem. § 76 BetrVG anrufen, die im Rahmen der Zielsetzung dieser BV verbindlich entscheidet. Sie soll innerhalb weiterer sechs Wochen entscheiden.

**§ 8 Sonstiges**

Diese Betriebsvereinbarung tritt zum 1. Januar 2017 in Kraft. Sie gilt unbefristet und kann mit einer Frist von sechs Monaten zum Jahresende schriftlich gekündigt werden. Im Falle der Kündigung entfaltet sie Nachwirkung.

Die Betriebsparteien sind sich darüber einig, dass Betriebsvereinbarungen als datenschutzrechtliche Erlaubnis zum Umgang mit personenbezogenen Daten wirken und als Erlaubnisvorschrift im Sinne des Art. 6 i. V. m. Art. 88 DS-GVO i. V. m. § 26 BDSG gelten.

Sie regeln den Umgang mit personenbezogenen Daten nicht abschließend. Dem Arbeitgeber bleibt vorbehalten, personenbezogene Daten auch auf der Grundlage einschlägiger gesetzlicher Regelungen oder auf der Grundlage sonstiger Betriebsvereinbarungen zu verarbeiten.

Diese Betriebsvereinbarung ersetzt die Betriebsvereinbarung(en) … (evtl. auflisten).

|  |  |  |  |
| --- | --- | --- | --- |
| , den / / | |  | |
| Ort, Datum |  | |  | |  | |
|  |  |  | |  | |
|  |  |  | |  | |
|  |  |  | |  | |
|  |  |  | |  | |
| Geschäftsführung |  | Betriebsrat | |  | |

**ANLAGE 1**

**Verzeichnis der Datenverarbeitungsmethoden (VdDVM)**

Die nachfolgende Aufstellung gibt einen Überblick über die von der Betriebsvereinbarung \_\_\_\_\_\_ geregelten Datenverarbeitungsmetoden (DVM). Die Aufstellung ist nicht abschließend und wird von den Betriebsparteien entsprechend fortgeschrieben.

1. Tabelle aller DVM [Inhaltsverzeichnis]
2. Template der Aufsichtsbehörden (noch in der Entwicklung) |Muster für Anlage 1, gem. Art. 30 DS-GVO (*weitere detailliertere Informationen werden unter … geführt*)

# Anhang 8 – Betriebsvereinbarung zur privaten und betrieblichen Nutzung einzelner DVM

[§ 1 Geltungsbereich 30](#_Toc501052103)

[§ 2 Betriebliche/private Nutzung 30](#_Toc501052104)

[2.1 Private Nutzung des betrieblichen Internetzugangs 31](#_Toc501052105)

[2.2 Verbot privater Nutzung betrieblicher E-Mail Adressen 32](#_Toc501052106)

[2.3 Nutzung der betrieblichen E-Mail-Adressen 32](#_Toc501052107)

[2.4 Ausscheiden eines Beschäftigten 33](#_Toc501052108)

[§ 3 Technikgestaltung und Missbrauchskontrolle 33](#_Toc501052109)

[3.1 Technische Schutzmaßnahmen/Spamfilter/Virenschutz 33](#_Toc501052110)

[3.2 Auswertungen der Protokolldaten 33](#_Toc501052111)

[3.3 Kontrollen der E-Mail-Postfächer besonderer Personengruppen 34](#_Toc501052112)

[§ 4 Bring your own device (BYOD) 34](#_Toc501052113)

[4.1 Grundsätze 34](#_Toc501052114)

[4.2 Rechte und Pflichten 35](#_Toc501052115)

[§ 5 Skype for Business 36](#_Toc501052116)

[5.1 Grundsätze 36](#_Toc501052117)

[5.2 Übersicht Dienste 36](#_Toc501052118)

[5.3 private Nutzung der Skype-Funktionen 38](#_Toc501052119)

[5.4 Skype für besondere Personengruppen 38](#_Toc501052120)

[§ 6 Voice over IP (VoIP) Telefonanlage 39](#_Toc501052121)

[6.1 Grundsätze 39](#_Toc501052122)

[6.2 Nutzung und Aufzeichnung 39](#_Toc501052123)

[6.3 Private Nutzung 40](#_Toc501052124)

[6.4 Besondere Personengruppen 40](#_Toc501052125)

[§ 7 Social Media 40](#_Toc501052126)

[7.1 Gestattung der Nutzung 40](#_Toc501052127)

[7.2 Äußerungen 41](#_Toc501052128)

[7.3 Ende des Arbeitsverhältnisses 41](#_Toc501052129)

[§ 8 Schlussbestimmungen 41](#_Toc501052130)

[Anlage 1 zur BV zur Internet- und E-Mail-Nutzung 42](#_Toc501052131)

[Anlage 2 zur BV zur Internet- und E-Mail-Nutzung 43](#_Toc501052132)

[Anlage 3 | BV zur Internet- und E-Mail-Nutzung | BYOD 44](#_Toc501052133)

[Anlage 4 | BV zur Internet- und E-Mail-Nutzung | Social Media Guideline 45](#_Toc501052134)

**Betriebsvereinbarung**

**zur privaten und betrieblichen Nutzung einzelner DVM**

Ergänzung zur Rahmenbetriebsvereinbarung über die „Einführung und Nutzung von DVM – Datenverarbeitungs-Methoden“

zwischen dem Unternehmen

und dem Betriebsrat

**Präambel**

Auf Basis der Rahmenbetriebsvereinbarung über die Einführung und Nutzung von DVM vom \_\_\_\_/\_\_\_\_/\_\_\_\_\_\_ wird folgende Betriebsvereinbarung zur Nutzung und dem Umgang mit Informations- und Kommunikationsmedien, wie **Internet**, **Intranet**, **eMail** und den **sozialen Medien** sowie mit den hierfür zur Verfügung gestellten Ressourcen (IT-Arbeitsplätze, Internetzugang sowie die zugelassenen mobilen und stationären Endgeräte (Desktop PC, Laptop/ Notebook etc. Handy/Smartphone …)) abgeschlossen. Dabei werden die berechtigten Interessen des Arbeitgebers und die Rechte und Freiheiten der Beschäftigten gewahrt.

**§ 1 Geltungsbereich**

Diese Betriebsvereinbarung gilt für Arbeitnehmer i. S. d. § 5 BetrVG.

Vorbehaltlich eventueller Regelungen eines Sprecherausschusses sind Leitende Angestellte zwar vom Geltungsbereich des BetrVG nicht erfasst und der Betriebsrat kann sie im Rahmen des BetrVG nicht wirksam vertreten jedoch gelten die Inhalte dieser Betriebsvereinbarung auch für diese Gruppe von Betroffenen.

**§ 2 Betriebliche/private Nutzung**

Die Nutzung der vom Arbeitgeber als Arbeitsmittel zur Verfügung gestellten DVM (siehe Ziff. 2.1 RahmenBV DVM) ist grundsätzlich nur zu betrieblichen Zwecken gestattet.

Die betriebliche(n) E-Mail-Adresse(n) und Nutzeridentifikation(en) dürfen ausschließlich zur betrieblichen Kommunikation genutzt werden. Private E-Mail-Adresse(n) und Nutzeridentifikation(en) dürfen nicht zu betrieblichen Zwecken genutzt werden.

Grundsätzlich gelten die im § 5 der RahmenBV DVM aufgestellten Verhaltensgrundsätze bei der Nutzung von DVM. Ergänzend gelten nachfolgende Regelungen, wobei insbesondere das Aufrufen und Verbreiten von Internetseiten oder E-Mails mit Inhalten unzulässig ist, die sich gegen die Würde des Menschen richten, vor allem pornographische, sexistische, pädophile, gewaltverherrlichende, fremdenfeindliche, nazistische, rassistische, politisch-radikale oder sittenwidrige Inhalte. Dies gilt auch bei der Nutzung von sozialen Netzwerken (wie bspw. Facebook, Twitter, etc.).

**2.1 Private Nutzung des betrieblichen Internetzugangs**

2.1.1 Den Beschäftigten ist die private Nutzung des für sie als Arbeitsmittel eingerichteten, betrieblichen Internetzugangs im geringfügigen Umfang nur gestattet, wenn die vorgenannten und nachfolgenden Verhaltensgrundsätze beachtet werden.

Eine Nutzung des betrieblichen Internetzugangs und des E-Mail-Systems zu kommerziellen, aber nicht betrieblichen Zwecken ist untersagt.

Die Privatnutzung darf die Erfüllung arbeitsvertraglicher Pflichten und die Betriebsabläufe nicht stören und neben den Gerätebetriebskosten keine zusätzlichen Kosten für das Unternehmen verursachen.

Die Zeit der Privatnutzung zählt nicht als Arbeitszeit. In Bereichen, in denen feste Arbeitszeiten vorgegeben sind, ist die Nutzung ausschließlich in den Pausenzeiten oder außerhalb der Arbeitszeit zulässig.

Die private Nutzung des betrieblichen Internetzugangs ist den Beschäftigten darüber hinaus nur dann gestattet, wenn sie einwilligen, dass die Daten über die näheren Umstände ihrer Internetnutzung **(Anlage 1)** zu Zwecken der Missbrauchskontrolle im Sinne dieser Vereinbarung erhoben, verarbeitet und genutzt werden dürfen. Die **Einwilligungserklärung** ist als **Anlage 2** beigefügt. Sie kann auch elektronisch erfolgen. Die Einwilligungen werden dokumentiert.

Die private Nutzung unterliegt der gleichen Überwachung und Kontrolle wie die betriebliche Nutzung, im Rahmen der gesetzlichen Bestimmungen und auf der Grundlage der vom Beschäftigten erteilten Einwilligung.

Es ist nicht zulässig, Dateien, die im Rahmen der privaten Internetnutzung heruntergeladen wurden (Downloads), auf betrieblichen Speichermedien (z. B. Festplatte des genutzten PC, Serverlaufwerken etc.) oder privaten Speichermedien (z. B. USB-Stick) zu speichern.

2.1.2 Die private Nutzung kann auch bei erteilter Einwilligung des Arbeitnehmers ganz oder teilweise durch den Arbeitgeber ausgeschlossen werden. Die Erlaubnis zur privaten Nutzung betrieblicher DVM kann gegenüber dem einzelnen Arbeitnehmer jederzeit bei Missbrauchsverdacht gem. § 6 der RahmenBV DVM sofort mit Wirkung für die Zukunft verboten werden.

2.1.3 Der Arbeitgeber übernimmt keine Haftung für die ordnungsgemäße Funktionsweise des betrieblichen Internetanschlusses und/oder darüber angebotener Dienste. Gleiches gilt für die Inhalte der über den betrieblichen Internetanschluss erreichbaren Seiten.

Die Privatnutzung begründet für den Beschäftigten keine Rechte gegenüber dem Arbeitgeber auf eine bestimmte Behandlung (Speicherung, Kenntlichmachung, Sicherung usw.) seiner privaten Daten. Er kann auch keinen Schadensersatz bei Verlust der Daten verlangen. Insoweit werden seine privaten Daten wie betriebliche Daten behandelt.

**2.2 Verbot privater Nutzung betrieblicher E-Mail Adressen**

Die Beschäftigten dürfen die betrieblichen E-Mail-Adressen nicht zu privaten Zwecken nutzen. Die Nutzung vom Arbeitgeber freigegebener Webmail-Dienste zur Nutzung privater E-Mail über den betrieblichen Internetzugang ist zulässig. Das Lesen bzw. Herunterladen (Download) von Anhängen (Attachments) von Webmails sowie das Hinzufügen (Upload) von Anhängen an Web-Mails sind jedoch nicht zulässig.

Über die private Webmail-Adresse dürfen keine betrieblichen Daten versendet oder empfangen werden. Betrieblich begründete Ausnahmefälle sind in Abstimmung mit dem jeweiligen Vorgesetzten unter Einbeziehung des zuständigen Systemadministrators zulässig. Die private Webmail-Adresse darf nicht zur Abwicklung von Geschäftsvorgängen genutzt werden.

Private E-Mails, die an betriebliche E-Mail-Adressen gesendet wurden, sind vom Beschäftigten zu löschen. Den Absendern von privaten E-Mails soll mitgeteilt werden, dass es sich um eine betriebliche E-Mail-Adresse handelt und der Empfang von privaten E-Mails nicht erlaubt ist. Dies gilt nicht für Spam-Mails, auf die niemals geantwortet werden darf.

**2.3 Nutzung der betrieblichen E-Mail-Adressen**

Auf personenbezogene E-Mail-Postfächer haben grundsätzlich nur die jeweiligen Beschäftigten Zugriff. Die Beschäftigten haben die zur Erfüllung ihrer arbeitsvertraglichen Pflichten erforderliche Kenntnisnahme ihrer E-Mail-Eingänge zu gewährleisten. Unabhängig davon kann der Arbeitgeber sog. Funktionspostfächer einrichten, die nicht einer bestimmten Person zugeordnet sind.

2.3.1 Bei *geplanter Abwesenheit* (z. B. Urlaub/Dienstreise) eines Beschäftigten ist durch den Beschäftigten ein automatisierter Hinweis auf die Abwesenheit des Beschäftigten sowie auf seine Vertretung einzurichten. Soweit dies für betriebliche Zwecke erforderlich ist, kann ein Vertretungsassistent eingerichtet werden bzw. können eingehende E-Mails automatisiert an einen Vertreter weitergeleitet werden.

Wurde eine Abwesenheitsnachricht nicht wie zuvor beschrieben eingerichtet oder war dies aufgrund einer *ungeplanten Abwesenheit* (z. B. Arbeitsunfähigkeit) nicht möglich, kann dies durch den Arbeitgeber erfolgen.

Eine automatisierte Weiterleitung wird nur in dringend erforderlichen Fällen eingerichtet, insb. soweit eine Abwesenheitsnachricht allein den betrieblichen Erfordernissen nicht gerecht wird.

2.3.2 Um gesetzlich vorgegebenen Aufbewahrungspflichten (z. B. gem. § 257 HGB, § 147 AO) gerecht zu werden und zur Sicherstellung der Funktionsfähigkeit des Systems, werden die eingehenden und ausgehenden E-Mails des betrieblichen E-Mail Postfachs nach Ablauf von (*bspw*. 3) Tagen archiviert. Die archivierten Daten werden für maximal (*bspw*. 10) Jahre aufbewahrt.

2.3.3 Bei E-Mail-Postfächern von Beschäftigten, die einen besonderen gesetzlichen Vertraulichkeitsschutz genießen (wie z. B. Betriebsräte, Werksärzte, Schwerbehindertenvertreter, Datenschutzbeauftragter) wird dieser gewahrt. Die Kommunikation mit derartigen Vertrauenspositionen sollte verschlüsselt erfolgen.

**2.4 Ausscheiden eines Beschäftigten**

Vor Ausscheiden eines Beschäftigten ist dafür Sorge zu tragen, dass dem Unternehmen alle betrieblichen Informationen (z. B. E-Mails, Termine, Kontakte, Kontaktlisten etc.) weiterhin zur Verfügung stehen.

Mit dem Ende des Arbeitsverhältnisses wird die Abwesenheitsnotiz vom Arbeitgeber aktiviert und eine Leseberechtigung für den Vertreter/Nachfolger eingerichtet. Die E-Mailadresse wird nach spätestens (*bspw*. 2)Wochen/Monaten gelöscht.

**§ 3 Technikgestaltung und Missbrauchskontrolle**

Der Arbeitgeber trifft unter Berücksichtigung des Stands der Technik Maßnahmen zur Gewährleistung eines ordnungsgemäßen und sicheren IT-Betriebs.

**3.1 Technische Schutzmaßnahmen/Spamfilter/Virenschutz**

Der Arbeitgeber wird Verfahren nutzen, die geeignet sind, die missbräuchlichen Nutzungsmöglichkeiten im Sinne dieser Vereinbarung auf technischem Weg zu reduzieren. Durch diese Verfahren wird insbesondere das Aufrufen bestimmter Inhalte/Seiten im Internet verhindert. Gesperrt werden insbesondere solche Inhalte/Seiten, deren Inhalt gegen § 2 dieser BV und § 5 der RahmenBV DVM verstößt.

Weiterhin kommen so genannte Content-Filterprogramme zum Einsatz, mit denen E-Mail Inhalte oder Internetseiten gefiltert werden, die gegen diese Vereinbarung verstoßen. Für eingehende E-Mails wird außerdem ein Filter eingesetzt, der Spam-Mails von außerhalb filtert. Der Nutzer erhält jeweils am darauf folgenden Tag eine Übersicht über die für seinen E-Mail Account gefilterten E-Mails. Er hat sodann die Möglichkeit, die Freigabe einzelner E-Mails bei der IT-Abteilung zu beantragen, die gegebenenfalls fälschlicherweise ausgefiltert wurden. Eine Auswertung erfolgt nicht.

**3.2 Auswertungen der Protokolldaten**

Der Arbeitgeber kann die Einhaltung dieser Vereinbarung sowie der RahmenBV DVM unter Beachtung der jeweils anwendbaren Multimedia- und Datenschutzgesetze und -bestimmungen in Hinblick auf die Funktionsfähigkeit der Systeme, sowie möglichen Missbrauch (§ 6 RahmenBV DVM) auswerten. Dazu nimmt der Arbeitgeber zunächst pseudonymisierte Auswertungen der Internetaktivitäten vor. Hierbei werden die in Anlage 2 aufgeführten Daten ohne die Angaben zur Identität des Benutzers ausgewertet und dokumentiert.

Der Datenschutzbeauftragte wird generell beteiligt, wenn er dies wünscht.

Treten bei diesen pseudonymisierten Auswertungen Auffälligkeiten auf, die auf eine im Sinne dieser Vereinbarung missbräuchliche Nutzung des betrieblichen Internetzugangs hindeuten, werden die Daten des Benutzers entpseudonymisiert, d.h. es werden auch die Angaben zur Identität des Benutzers ausgewertet.

Zudem kann der Arbeitgeber unter Einbeziehung des Betriebsrates oder des Datenschutzbeauftragten die betrieblichen E-Mail-Postfächer der Beschäftigten hinsichtlich einer missbräuchlichen Nutzung kontrollieren, nachdem zuvor eine pseudonymisierte Auswertung des Datenvolumens und der E-Mail-Domain erfolgt ist.

Die Protokolldaten werden nach drei (3) Monaten automatisch gelöscht, sofern keine weitere Nutzung erforderlich ist.

**3.3 Kontrollen der E-Mail-Postfächer besonderer Personengruppen**

E-Mail-Postfächer von Beschäftigten, die einen besonderen gesetzlichen Vertraulichkeitsschutz genießen (wie z. B. Betriebsräte, Werksärzte, Schwerbehindertenvertreter, Datenschutzbeauftragter) werden grundsätzlich keiner Kontrolle durch den Arbeitgeber unterzogen, es gilt § 6 der RahmenBV DVM.

**§ 4 Bring your own device (BYOD)**

Der Begriff Bring Your Own Device (BYOD) bezeichnet die Integration privater mobiler Endgeräte wie Smartphones, Tablets oder Laptops in die Netzwerke des Arbeitgebers.

**4.1 Grundsätze**

Es besteht generell kein Anspruch auf BYOD.

Werden private Endgeräte auch betrieblich genutzt, sind folgende Bestimmungen zum Schutz der betrieblichen Daten und der Rechte und Freiheiten der Beschäftigten zu beachten:

Private und betriebliche Daten sind technisch getrennt zu halten. Um dies gewährleisten zu können, behält sich der Arbeitgeber vor, entsprechende technische Vorgaben für die Endgeräte festzulegen, hierzu gehören insbesondere Regelungen zur Nutzung sog. Container-Apps sowie zur Nutzung von Cloud-Diensten. Die Nutzung eines Endgerätes, das dem Beschäftigten gehört, zugleich aber den Zugriff auf IT-Ressourcen des Arbeitgebers erhält, bedarf der ausdrücklichen Erlaubnis durch den Arbeitgeber und ist durch eine gesonderte gegenseitige Vereinbarung mit Einwilligung des Beschäftigten zu regeln ([**Anlage 3**](#_Anlage_3_|)).

**4.2 Rechte und Pflichten**

4.2.1 Eigene Endgeräte des Beschäftigten dürfen zu betrieblichen Zwecken nur eingesetzt werden, wenn das Gerät zuvor vom Arbeitgeber (Systemadministrator/IT-Abt.) technisch freigegeben ist.

4.2.2 Auf dem privaten Endgerät des Beschäftigten sind für betriebliche und private Zwecke getrennte Accounts vom Arbeitgeber einzurichten, um ihm die Zugriffskontrolle auf den betrieblich genutzten Account einzuräumen, so dass insbesondere Funktionen der Fernlöschung und -sperrung vom Arbeitgeber (i.d.R. Systemadministrator/IT-Abt.) benutzt werden können.

Die Sperrung des Handys und/oder Fernlöschung ist insbesondere in folgenden Fällen möglich:

* Beschädigung, Zerstörung oder Verlust des Endgeräts;
* Das Passwort wird zu häufig falsch eingegeben;
* Wenn der Arbeitnehmer aus dem BYOD-Programm austritt;
* Wenn das BYOD-Programm beendet wird;
* Wenn das Arbeitsverhältnis beendet oder der Beschäftigte freigestellt wird.

4.2.3 Der Arbeitgeber nimmt keinen Zugriff auf private Daten, die auf dem Endgerät gespeichert sind, bzw. wird er auch im Falle der technischen Möglichkeit ohne Einwilligung des Beschäftigten keinen Zugriff auf diese privaten Daten nehmen.

4.2.4 Der Beschäftigte verpflichtet sich, regelmäßige Sicherheitsupdates des Betriebssystems sowie aller vorhandenen Apps zeitnah durchzuführen. Die vom Arbeitgeber zur Verfügung gestellte Container-App, die die betrieblichen Daten enthält, darf vom Beschäftigten nicht in der Cloud gesichert werden. Es dürfen keine Softwareinstallationen vorgenommen werden, die das Betriebssystem verändern, um bspw. die Leistung des Endgeräts zu erhöhen (sog. Jailbreaking) und/oder die gegen § 5 der RahmenBV DVM verstoßen.

4.2.5 Der Beschäftigte ist verpflichtet, die betrieblichen Informationen auf dem mobilen Endgerät durch geeignete Maßnahmen vor unberechtigter Kenntnisnahme zu schützen.

4.2.6 Der Beschäftigte ist verpflichtet, den Verlust seines betrieblich genutzten Endgerätes dem Arbeitgeber unverzüglich zu melden und mit ihm Folgemaßnahmen abzustimmen, insbesondere die Löschung zu veranlassen und/oder Meldung von Datenverlusten.

4.2.7 Hinsichtlich der Missbrauchskontrolle wird auf § 3 dieser BV sowie § 5 der RahmenBV DVM verwiesen.

4.2.8 Der Beschäftigte trägt alle in Zusammenhang mit dem Betrieb des Endgeräts anfallenden Kosten. Der Arbeitgeber übernimmt die Kosten für die technische Einrichtung und eventuelle Lizenzgebühren. Ferner haftet der Arbeitgeber nicht im Falle von Verlust oder Zerstörung des Endgerätes, hierzu gehört u.a. auch der Verlust privater Daten und Software (bspw. Apps).

4.2.9 Im Fall der Beendigung des Arbeitsverhältnisses oder der Freistellung von den Arbeitspflichten sind betriebliche Daten durch den Beschäftigten unverzüglich auf den Server des Arbeitgebers zu übertragen. Nach Prüfung und Bestätigung des Übertragungsvorgangs durch den Arbeitgeber hat der Beschäftigte die betrieblichen Daten auf dem Endgerät restlos und rückinformationssicher zu löschen. Die Löschung ist von dem Beschäftigten in Textform zu bestätigen.

4.2.10 Entsteht dem Arbeitgeber durch die Missachtung dieser Regelungen ein Schaden, so kann er diesen vom Arbeitnehmer ersetzt verlangen.

**§ 5 Skype for Business**

Skype for Business (i.F. Skype) ist ein Kollaborationsdienst mit folgenden Kernfunktionen:

1. Anwesenheitsstatus
2. Videoanruf/Webconferencing
3. Desktop-Sharing
4. Telefonate
5. Chat/Instant Messaging

**5.1 Grundsätze**

Die Entscheidung zur Aktivierung und Freigabe vorgenannter Funktionen ist dem Arbeitgeber vorbehalten.

Die Nutzung aller Funktionen ist grundsätzlich nur zu betrieblichen Zwecken nach Maßgabe des § 5 der RahmenBV DVM und § 2 dieser BV gestattet. Der Arbeitgeber behält sich vor, eine Missbrauchskontrolle i. S. d. § 6 der RahmenBV durchzuführen.

Alle Kommunikationsvorgänge sind technisch so abgesichert (z. B. durch Verschlüsselung), dass ein an der Kommunikation nicht Beteiligter diese Kommunikation nicht abhören oder beeinflussen kann.

Den Beschäftigten wird die Möglichkeit zu einem Training bzw. Informationsmaterial für Skype angeboten. Hierin werden insbesondere die in dieser BV erwähnten Einstellungsmöglichkeiten erläutert.

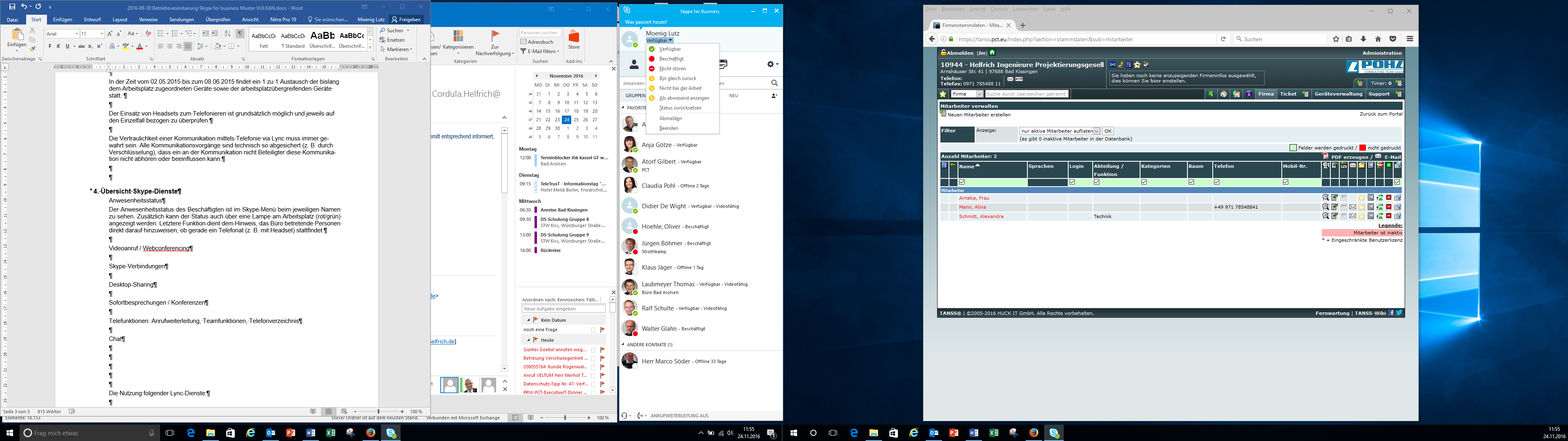
**5.2 Übersicht Dienste**

1. **Anwesenheitsstatus**

Anwesenheitsstatus ist eine Funktion, bei der anderen Nutzern angezeigt wird, welchen Status der Einzelne gerade eingestellt hat. Mögliche Einstellungen sind: verfügbar, beschäftigt, nicht stören, bin gleich zurück, nicht bei der Arbeit, abwesend (seit).

Die Statusanzeige ist individuell vom Beschäftigten selbst einstellbar. Die *Standortanzeige* kann sowohl individuell aktiviert oder auch eingestellt werden. Die *Abwesenheitsanzeige* kann individuell von dem Beschäftigten aktiviert oder deaktiviert werden.

Die Nutzung dieser Funktion ist rein freiwillig und hat keine arbeitsrechtlichen Konsequenzen.



1. **Videoanruf/Webconferencing**

Webconferencing oder auch Online-Meeting bezeichnet ein „virtuelles“ Treffen verschiedener Teilnehmer, bei dem die Inhalte über den Computer ausgetauscht oder betrachtet werden.

Bei der Nutzung sind die üblichen Grundsätze der Transparenz und Vertraulichkeit in der Kommunikation zu beachten. Die Vertraulichkeit kann insbesondere durch den Einsatz technischer Hilfsmittel (z. B. Headsets) gewahrt werden.

Es werden keine Aufzeichnungen ohne ausdrückliche Einwilligung aller Teilnehmer der Videokonferenzen vorgenommen. Im Falle der Aufzeichnung sind Zweck und Speicherfrist konkret zu definieren.

1. **Desktop-Sharing**

Desktop-Sharing (oder auch Screen-Sharing) bezeichnet die Übertragung des Bildschirminhaltes eines Computers an einen oder mehrere andere Computer.

Die Funktion erfordert die individuelle Freigabe des Nutzers, der seine Inhalte überträgt.

Es werden keine Aufzeichnungen ohne ausdrückliche Einwilligung der Teilnehmer vorgenommen, die ihren Bildschirminhalt teilen. Hierbei sind Zweck und Speicherfrist konkret zu definieren.

1. **Telefonate**

Die aus Telefonanlagen bekannten Funktionalitäten (Rufweiterleitung, Wahlwiederholung, Freisprechanlage, Konferenzschaltungen, Anrufbeantworter etc.) stehen auch mit der Skype-Technologie zur Verfügung. Daten zu Verbindungen, Teilnehmern, Zeitpunkten und zur Dauer von Telefonaten werden aufgezeichnet, gespeichert und ausschließlich gemäß der Beschreibung dieser DVM verwendet (RahmenBV DVM § 2.2). Alle Kommunikationsvorgänge sind technisch so abgesichert (z. B. durch Verschlüsselung), dass ein an der Kommunikation nicht Beteiligter diese Kommunikation nicht abhören oder beeinflussen kann.

Es ist möglichst die kostengünstigste Variante der Telefonie zu wählen. Die Nutzung von Skype ist freiwillig, solange der Arbeitgeber alternative Möglichkeiten zur Telekommunikation (z. B. Festnetz oder Mobiltelefon) bereitstellt. Die Nutzung von Skype zu anderen Festnetzanschlüssen ist technisch unterbunden, sofern Kosten verursacht würden.

Bei der Nutzung sind die üblichen Grundsätze der Transparenz und Vertraulichkeit in der Kommunikation zu beachten. Die Vertraulichkeit kann insbesondere durch den Einsatz technischer Hilfsmittel (z. B. Headsets) gewahrt werden.

Es werden keine Aufzeichnungen der Gesprächsinhalte ohne ausdrückliche Einwilligung aller Teilnehmer des Telefonats vorgenommen. Im Falle der Aufzeichnung sind Zweck und Speicherfrist konkret zu definieren. Die Aufzeichnung von Anruflisten und das Führen eigener Kontaktlisten kann jeder Skype-Nutzer für seinen Skype-Account selber einstellen.

[*optional*: Der Arbeitgeber ist berechtigt, alle Anrufe an Notfallrufnummern (110/112/betriebliche Notfallnummern) aufzuzeichnen. Die Erreichbarkeit von Notfallnummern ist sichergestellt].

1. **Chat/Instant Massaging**

Chat/Instant Messaging ist eine Kommunikationsmethode, bei der sich zwei oder mehr Teilnehmer per Textnachrichten unterhalten. Dabei löst der Absender die Übermittlung aus (sogenanntes Push-Verfahren), so dass die Nachrichten möglichst unmittelbar (englisch „instant“) beim Empfänger ankommen. Diese Funktion ist nützlich, wenn man nur eine kurze Frage hat oder schnell ein paar Informationen senden möchte, für die sich das Starten eines Videoanrufs oder einer Videokonferenz nicht lohnt. In der Regel können Nachrichten auch abgeschickt werden, wenn der Gesprächspartner gerade nicht online/empfangsbereit ist. Dabei ist nicht sichergestellt, dass die Nachricht dann später an den Empfänger ausgeliefert wird, da der Empfänger dies in seinen Einstellungen ausschließen kann.

Die Nutzung dieser Kommunikationsmethode darf nur zu betrieblichem, aber nicht rechtsverbindlichem Informationsaustausch verwendet werden.

Die Nutzung dieser Funktion ist rein freiwillig.

Die Chat-Nachrichten werden auf einem eigens dafür installierten Chat-Server gespeichert. Die nutzerseitige Archivierung erfolgt grundsätzlich in Outlook unter „Aufgezeichnete Unterhaltungen“ Die nutzerseitige Speicherung kann benutzerbezogen unterbunden werden.

**5.3 private Nutzung der Skype-Funktionen**

Hinsichtlich der privaten Nutzung gelten die unter § 2.1 und § 2.4 aufgeführten Regelungen sinngemäß. Die Einwilligung ist entsprechend zu ergänzen.

**5.4 Skype für besondere Personengruppen**

Bei der Nutzung von Skype Diensten von Beschäftigten, die einen besonderen gesetzlichen Vertraulichkeitsschutz genießen (wie z. B. Betriebsräte, Werksärzte, Schwerbehindertenvertreter, Datenschutzbeauftragter) können diese auf Wunsch einen eigenen Skype-Account erhalten. Dieser wird grundsätzlich keiner Kontrolle durch den Arbeitgeber unterzogen, es gilt § 6 der RahmenBV DVM.

**§ 6 Voice over IP (VoIP) Telefonanlage**

In Abhängigkeit zur TK-Anlage

Beschreibung der TK-Anlage

1. Gesprächsaufzeichnungen
2. Kopplung Telefonie, Fax/SMS und Mobiltelefon (unified Massaging)
3. Makeln, Anrufe heranholen, übernehmen und durchstellen, Weiterleitung
4. Anrufbeantworter
5. Telefonkonferenzen
6. Unerwünschte Anrufe sperren
7. Anruferlisten einsehen
8. Telefonbuch
9. …

**6.1 Grundsätze**

Die Entscheidung zur Aktivierung und Freigabe möglicher Funktionen ist dem Arbeitgeber vorbehalten.

Die Nutzung aller Funktionen ist grundsätzlich nur zu betrieblichen Zwecken nach Maßgabe des § 5 der RahmenBV und § 2 dieser BV gestattet. Der Arbeitgeber behält sich vor, eine Missbrauchskontrolle i. S. d. § 6 der RahmenBV durchzuführen.

Alle Kommunikationsvorgänge sind technisch so abgesichert (z. B. durch Verschlüsselung), dass ein an der Kommunikation nicht Beteiligter diese Kommunikation nicht abhören oder beeinflussen kann.

Den Beschäftigten wird die Möglichkeit zu einem Training bzw. Informationsmaterial angeboten, in dem insbesondere die in dieser BV erwähnten Einstellungsmöglichkeiten erläutert werden.

**6.2 Nutzung und Aufzeichnung**

Die bei Telefonanlagen üblichen Funktionalitäten (Rufweiterleitung, Wahlwiederholung, Freisprechanlage, Konferenzschaltungen, Anrufbeantworter etc.) stehen auch mit der VoIP-Technologie zur Verfügung. Daten zu Verbindungen, Teilnehmern, Zeitpunkten und zur Dauer von Telefonaten werden aufgezeichnet, gespeichert und ausschließlich gemäß der Beschreibung dieser DVM verwendet (RahmenBV DVM § 2.2). Alle Kommunikationsvorgänge sind technisch so abgesichert (z. B. durch Verschlüsselung), dass ein an der Kommunikation nicht Beteiligter diese Kommunikation nicht abhören oder beeinflussen kann.

Bei der Nutzung sind die üblichen Grundsätze der Transparenz und Vertraulichkeit in der Kommunikation zu beachten.

Es werden keine Aufzeichnungen der Gesprächsinhalte ohne ausdrückliche Einwilligung aller Teilnehmer des Telefonats vorgenommen. Im Falle der Aufzeichnung sind Zweck und Speicherfrist konkret zu definieren. Die Aufzeichnung von Anruflisten und das Führen eigener Kontaktlisten kann jeder Nutzer für seine Nebenstelle selber einstellen.

[optional: Der Arbeitgeber ist berechtigt, alle Anrufe an Notfallrufnummern (110/112/betriebliche Notfallnummern) aufzuzeichnen. Die Erreichbarkeit von Notfallnummern ist sichergestellt].

**6.3 Private Nutzung**

Hinsichtlich der privaten Nutzung gelten die unter § 2.1 und 2.4 aufgeführten Regelungen sinngemäß. Die Einwilligung (**Anlage 2**) ist entsprechend zu ergänzen.

**6.4 Besondere Personengruppen**

Bei der Nutzung durch Beschäftigte, die einen besonderen gesetzlichen Vertraulichkeitsschutz genießen (wie z. B. Betriebsräte, Werksärzte, Schwerbehindertenvertreter, Datenschutzbeauftragter) erhalten diese eine eigene Nebenstelle. Diese wird grundsätzlich keiner Kontrolle durch den Arbeitgeber unterzogen, es gilt § 6 der RahmenBV DVM.

**§ 7 Social Media**

Social Media sind alle externen Medien (Plattformen), die die Nutzer der Plattformen über externe digitale Kanäle in der gegenseitigen Kommunikation und dem interaktiven Austausch von Informationen unterstützen. Dieses betrifft alle Arten von Medien bspw. XING, YouTube, Facebook, Twitter, Threema, WhatsApp, Instagram, SnapChat, Pinterest, etc.

**7.1 Gestattung der Nutzung**

Die betriebliche Nutzung von Social Media Kanälen erfolgt über Firmen-Accounts, auf die verschiedene Funktionsträger Zugriff erhalten: … (z. B. Pressestelle, Marketing, Vertrieb, Personalwesen, Social-Media-Referent ).

Betriebliche Nutzung ist jede Nutzung durch den Beschäftigten, die in unmittelbarem Zusammenhang mit der Tätigkeit des Arbeitgebers bzw. mit der Tätigkeit des Beschäftigten für den Arbeitgeber steht.

Die private Nutzung von Social Media während der Arbeitszeit richtet sich nach den Regelungen zur privaten Nutzung von Internet und E-Mail § 2 dieser Betriebsvereinbarung.

Die ausschließlich private Nutzung unterliegt nicht der Regelungsbefugnis der Betriebsparteien. Dennoch sind die Verhaltensgrundsätze des § 5 der Rahmen BV DVM zu beachten. Darüber hinaus wird empfohlen, die als [**Anlage 4**](#_Anlage_4_|) beigefügte Social Media Guideline zu beachten.

**7.2 Äußerungen**

Werden Beschäftigte im Internet auf sachliche oder unsachliche Kritik oder auf Beschwerden oder sonstige Probleme von Kunden aufmerksam, so sind das Beschwerdemanagement (Alternative: die Kundenbetreuung) und die Pressestelle zu informieren.

Der Arbeitgeber ist berechtigt, bei Internetauftritten (bspw. Facebook) Posting- und Kommentarfunktionen zuzulassen und auszuwerten. Sofern Beschäftigte namentlich benannt werden, ist Rücksprache mit dem Betriebsrat zu halten, ob die Namensnennung unkenntlich gemacht wird, der Post gelöscht wird, eine Stellungnahme dazu erfolgen soll oder wie dem zu begegnen ist. Dabei sind die Fürsorgepflicht des Arbeitgebers gegenüber seinen Beschäftigten, sowie die Meinungsfreiheit zu beachten.

**7.3 Ende des Arbeitsverhältnisses**

Soweit der Arbeitnehmer Social Media zu betrieblichen Zwecken genutzt hat, hat er nach Ende des Arbeitsverhältnisses dem Arbeitgeber sowohl die im betrieblichen Rahmen angefallenen Kontakte als auch die berufliche Korrespondenz zur Verfügung zu stellen.

**§ 8 Schlussbestimmungen**

Diese Betriebsvereinbarung tritt zum \_\_\_\_\_\_\_\_\_\_\_\_\_ in Kraft.

Sie gilt unbefristet und kann von den Betriebsparteien mit einer Frist von drei Monaten zum Quartalsende schriftlich gekündigt werden. Im Falle ihrer Kündigung wirkt sie nach.

Die Teilkündigung einzelner Paragraphen ist zulässig. Die übrigen Paragraphen bleiben davon unberührt. Soweit an anderer Stelle auf die gekündigten Paragraphen Bezug genommen wird, bleiben diese Regelungen für die ungekündigten Paragraphen gültig.

ANLAGE 1 Übersicht der Log-File Datenfelder

Anlage 2 Einwilligungserklärung

Anlage 3 BYOD

Anlage 4 Social Media Guideline

**Anlage 1 zur BV zur Internet- und E-Mail-Nutzung**

Übersicht der Log-File Datenfelder:

Angaben zur Identität des Benutzers [bei Pseudonymisierung sind diese Daten ausgeblendet]

• Benutzer Anmeldename/CompanyID (C-ID) (domain/user)

• Benutzername (user)

• Quell-IP-Adresse (source IP)

• Gruppenzugehörigkeit (group)

• Rechner/Device

Angaben zu Zeit und Dauer der Internetnutzung

• Datum (date)

• Uhrzeit (time)

• Proxyserver und Zugriffsweg (externe IP)

• Dauer des Seitenaufrufes (browse time)

• Übertragene Datenmenge (bytes transferred)

• Dauer der Datenübertragung (duration time)

Angaben zum verwendeten Protokoll und zur URL

• URL-Name (domain name)

• Ziel-IP-Adresse (destination IP)

• Aufgerufene Seiten/Objekte (hits)

• Heruntergeladene Dateien und Dateitypen

• Verwendetes Protokoll/Methode (z. B. http) ggfs. den Port (protocol)

**Anlage 2 zur BV zur Internet- und E-Mail-Nutzung**

**Erklärung und Einwilligung zur Privatnutzung von DVM**

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

Name, Vorname Personal-Nr.

Ich bestätige hiermit, dass ich die Rahmen-Betriebsvereinbarung DVM und die Ergänzungsbetriebsvereinbarung zur privaten und betrieblichen Nutzung einzelner DVM zur Kenntnis genommen und verstanden habe.

Die mir überlassenen DVM dürfen grundsätzlich nur betrieblich genutzt werden. Abweichend von diesem Grundsatz dürfen die DVM nur im Rahmen der Betriebsvereinbarung privat genutzt werden.

Vor diesem Hintergrund erkläre ich hiermit, dass ich von der Möglichkeit einer solchen Privatnutzung Gebrauch machen möchte. Ich bestätige, dass ich die o. g. Bedingungen einhalten werde. Mir ist bewusst, dass mir bei einem Verstoß gegen diese Bedingungen rechtliche Sanktionen drohen, z. B. arbeitsrechtliche Maßnahmen, Schadensersatzpflichten oder sogar strafrechtliche Sanktionen.

Weiterhin nehme ich zur Kenntnis, dass mir im Zusammenhang mit der Privatnutzung keine Rechte oder Schadensersatzansprüche gegen das Unternehmen, z. B. wegen Datenverlust, zustehen. Mir ist auch bewusst, dass meine Privatnutzung durch das Unternehmen in gleicher Weise kontrolliert und überwacht werden kann, wie die betriebliche Nutzung, und ich willige darin ein.

Diese Erklärung ist freiwillig. Ich kann sie jederzeit durch Erklärung in Textform gegenüber dem Arbeitgeber für die Zukunft widerrufen. Nach einem solchen Widerruf werde ich die mir überlassenen DVM nur noch für betriebliche Zwecke nutzen.

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

Verteiler:

Original: Personalakte

Kopie: Mitarbeiter

Datum Unterschrift

**Anlage 3 | BV zur Internet- und E-Mail-Nutzung | BYOD**

**Vereinbarung und Einwilligung zur Nutzung privater Endgeräte (Own Device)**

zwischen und der

<<Anrede>> <<Firma>>

<<Vor-/Name>> <<Personal-Nr.>> <<Anschrift>>

(im Folgenden Beschäftigte(r)) (im Folgenden Arbeitgeber)

Der Arbeitgeber erlaubt <<Herrn/Frau>> <<Vor->> <<Name>> die Nutzung privater Mobiltelefone, Laptops und Tablets (Mobil Device) im Rahmen des Arbeitsverhältnisses (BYOD) bis auf Widerruf und unter den Bedingungen des § 4 der „Betriebsvereinbarung zur privaten und betrieblichen Nutzung einzelner DVM“ unter der Voraussetzung dass <<er/sie>> mit diesen Bedingungen einverstanden ist.

Antrag und Einwilligung der/des Beschäftigten

Ich <<Vor-/Name>> möchte meine unten aufgeführten mobilen Endgeräte auch im Rahmen meines Arbeitsverhältnisses nutzen (BYOD). Der damit einhergehenden Verantwortung bin ich mir bewusst und verpflichte mich hiermit zur Einhaltung der in der „Betriebsvereinbarung zur privaten und betrieblichen Nutzung einzelner DVM“ (insb. § 4) beschriebenen Rechte und Pflichten. Die Betriebsvereinbarung habe ich zur Kenntnis genommen und ist im Intranet jederzeit abrufbar unter … . Zudem bin ich damit einverstanden, dass der Arbeitgeber ein Programm installiert, mit dem eine Sperrung der mobilen Endgeräte und/oder Fernlöschung von Daten möglich ist.

Diese Einwilligung kann jederzeit ohne Angabe von Gründen widerrufen werden. Der Widerruf ist in Textform gegenüber der IT-Abteilung zu erklären.

Mit dem Widerruf verpflichte ich mich, sämtliche betriebliche Information (insb. Kontaktdaten, E-Mails und Kalendereinträge) umgehend auf einen Server des Arbeitgebers zu übertragen, diese von meinen privaten Geräte zu löschen und meine privaten Geräte sodann nicht länger im Rahmen des BYOD zu nutzen. Die weitere Nutzung nach Widerruf kann mit arbeitsrechtlichen Konsequenzen verbunden sein.

Verifikation mobiler Endgeräte (Laptop, Handy, Tablet)

|  |  |  |  |
| --- | --- | --- | --- |
| Hersteller | Modell | Serien-Nr. | Freigabe IT |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Ort, Datum |  | | Ort, Datum |
|  | |  |  | |
|  | |  |  | |
| Unterschrift Beschäftigte(r) | |  | Unterschrift (Arbeitgeber) | |

**Anlage 4 | BV zur Internet- und E-Mail-Nutzung | Social Media Guideline**

**Social Media Guideline**

Social-Media-Portale wie Facebook, YouTube oder Twitter bieten neue Möglichkeiten, um Meinungen, Gedanken und Erfahrungen mit anderen Nutzern, Freunden, Kollegen oder Kunden auszutauschen – und das weltweit.

Auch über unser Unternehmen wird im Web diskutiert. Jeder, der sich online über unser Unternehmen äußert, prägt damit auch das Bild des Unternehmens in der Öffentlichkeit. Bitte unterlassen Sie unsachliche Kritik gegenüber unserem und anderen Unternehmen/Personen.

Wenn auch Sie sich über uns in Blogs, Foren oder sozialen Netzwerken austauschen, möchten wir Sie bitten, die folgenden Punkte zu beachten:

1. Respektieren Sie die Netiquette

Respektieren Sie die Internetgemeinschaft. Halten Sie sich an geltendes Recht, informieren Sie sich über die Regeln von Communitys oder anderen sozialen Plattformen, und achten Sie die üblichen Gebote von Anstand und Respekt.

2. Respektieren Sie geistiges Eigentum

Häufig haben Autoren schöpferische Kraft in die Entwicklung ihrer Ideen gesteckt und ein Urheberrecht erworben. Veröffentlichen Sie also nichts, bei dem Sie unsicher sind, ob es Urheberrechte verletzen könnte. Ändern Sie Inhalte anderer nur, falls dies ausdrücklich zugelassen ist. Gehen Sie dabei respektvoll vor, und weisen Sie die Änderung aus. Sollte Ihnen auffallen, dass jemand rechtlich geschützte Informationen oder die Marke unseres Unternehmens ohne Zustimmung verwendet, wenden Sie sich bitte an das Social-Media-Team (E-Mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_).

3. Internes bleibt intern

Wo immer Sie in sozialen Netzwerken über Ihren Arbeitgeber oder berufliche Belange reden, gilt: Internes bleibt intern. Wahren Sie Betriebsgeheimnisse und Verschwiegenheitsverpflichtungen.

4. Sprechen Sie für sich selbst

Wenn Sie im Internet agieren, sagen Sie offen, wer Sie sind, und halten Sie Ihren Hintergrund transparent. Wenn Sie als Mitarbeiter Ihre Haltung zum Unternehmen privat zum Ausdruck bringen, schreiben Sie bitte ausschließlich in der ersten Person, und machen Sie deutlich, dass es sich um Ihre persönliche Meinung handelt.

5. Respektieren Sie Wettbewerber

Seien Sie sich bewusst, dass Kritik, die Sie an Wettbewerbern unseres Unternehmens und ihren Produkten äußern, gegebenenfalls als Statement von uns oder versteckte Werbung missverstanden werden kann. Bleiben Sie deswegen sachlich, und machen Sie klar, dass es sich um Ihre persönliche Erfahrung beziehungsweise Meinung handelt.

6. Beachten Sie Zuständigkeiten

Verlautbarungen, die das Unternehmen betreffen, werden nur von offiziellen Vertretern veröffentlicht. Bitte beachten Sie, dass Sie persönlich für die von Ihnen publizierten Inhalte haften.

7. Halten Sie uns im Bilde

Wenn Sie im Internet auf Lob, Kritik oder andere Informationen stoßen, von denen Sie meinen, sie könnten für unser Unternehmen relevant sein, teilen Sie diese bitte dem Social-Media-Team mit.

8. Behandeln Sie Kritik konstruktiv

Achten Sie darauf, ob Kritik gerechtfertigt ist, fair erscheint und ob es sich lohnt, darauf zu antworten. Nehmen Sie berechtigte Kritik ernst, und reagieren Sie darauf konstruktiv. Lassen Sie sich auf offensichtlich emotionale, unsachliche Beiträge gar nicht erst ein.

9. Handeln Sie verantwortlich

Verlassen Sie sich auf Ihren gesunden Menschenverstand. Beginnen Sie keine Streitigkeiten, und versuchen Sie, eigene Fehler als Erster zu korrigieren. Tragen Sie dazu bei, wann immer möglich, Probleme zu erkennen und bei ihrer Lösung zu helfen. Bei alldem gilt der Grundsatz: erst nachdenken, dann veröffentlichen. In Zweifelsfällen hilft Ihnen das Social-Media-Team gerne weiter.

Bitte beachten Sie, dass sich im Internet gepostete Beiträge (sowohl Texte als auch Bilder) schnell verbreiten, zeitlich unbegrenzt und für einen nicht eingrenzbaren Benutzerkreis abrufbar sind. Sie sollten daher stets überlegen, ob Sie hinter diesen Äußerungen auch Jahre später noch stehen würden.

1. Baustein kann von den Unternehmen verwendet und individuell ergänzt bzw. angepasst werden, wenn sie an weitere oben nicht genannte Empfänger Daten übermitteln, die keine Dienstleister oder Auftragsverarbeiter sind. [↑](#footnote-ref-1)
2. Über derartige Datenübermittlungen könnte auch im konkreten Einzelfall informiert werden. Gleiches gilt für den folgenden Fall der Privatinsolvenz. [↑](#footnote-ref-2)
3. Nach Art. 21 Abs. 4 DSGVO muss auf das Widerspruchsrecht nach Art. 21 Abs. 1 und 2 DSGVO ausdrücklich und in einer von anderen Informationen getrennten Form hingewiesen werden. [↑](#footnote-ref-3)
4. Es besteht keine Notwendigkeit eine bestimmte Behörde zu benennen. Es könnte allerdings vorteilhaft sein, durch Benennung der für den Verantwortlichen zuständigen Behörde, den Betroffenen gleich in diese Richtung zu lenken. Sollte das Muster konzernweit für mehrere Verantwortliche genutzt werden, ist die Angabe einer bestimmten Behörde demgegenüber nicht sinnvoll. Hier müsste das Muster dann entsprechend den eigenen Bedürfnissen angepasst werden. [↑](#footnote-ref-4)
5. Baustein kann vollständig gestrichen werden, wenn keine Übermittlung in Drittländer durchgeführt wird. [↑](#footnote-ref-5)
6. Baustein kann vollständig gestrichen werden, wenn keine automatisierte Einzelfallentscheidung getroffen wird. [↑](#footnote-ref-6)
7. Findet eine automatisierte Einzelfallentscheidung statt, muss über die involvierte Logik, die Tragweite und die angestrebten Auswirkungen für Beschäftigte informiert werden. Denkbar ist hier, etwa über die Kategorien der in die Entscheidung einfließenden Daten sowie über deren Gewichtung zu informieren. [↑](#footnote-ref-7)