Betriebsvereinbarung

über den Einsatz von Systemen zur IT- und Datensicherheit und die damit verbundene Verarbeitung personenbezogener Arbeitnehmer:innendaten

1. Anwendungsbereich

(1) Die Betriebsvereinbarung regelt gemäß §§ 96, 96a und 97 ArbVG die Einführung und Nutzung von Systemen zur IT- und Datensicherheit und die in diesem Zusammenhang stattfindende Verarbeitung personenbezogener Arbeitnehmer:innendaten.

(2) Diese Betriebsvereinbarung gilt für alle Arbeitnehmer:innen iSd § 36 ArbVG der <NAME>.

(3) Alle in dieser Betriebsvereinbarung angeführten Anhänge (Datenblätter, Zusatz-BV) bilden einen integrativen Bestandteil dieser Vereinbarung und werden im Zuge der Erweiterung der Systeme sukzessive ergänzt.

(4) [sofern zutreffend: Bestehende Betriebsvereinbarungen zu verschiedenen bereits im Einsatz befindlichen Systemen zur IT- und Datensicherheit, werden nach beiderseitiger Prüfung der Aktualität durch die Vertragsparteien in die Anlage aufgenommen bzw überarbeitet.]

(5) [sofern zutreffend: Die Regelungen der Rahmen-Betriebsvereinbarung zur personenbezogenen Datenverarbeitung gelten sinngemäß, sofern in dieser Vereinbarung nicht Abweichendes vereinbart wurde.]

2. Zielsetzung

(1) Der/die Arbeitgeber:in ist als datenschutzrechtliche/r Verantwortliche:r verpflichtet, die IT-Infrastruktur gegen Cyber-Angriffe zu schützen. Darüber hinaus sind aufgrund der rechtlichen Bestimmungen der Datenschutz-Grundverordnung (DSGVO) technische und organisatorischen Maßnahmen (TOMs) zur Sicherheit der Verarbeitung zu treffen und betriebliche Daten sowie Betriebs- und Geschäftsgeheimnisse nur vorab definierten Berechtigten zur Verfügung zu stellen.

(2) Die Vertragsparteien sind sich daher einig, dass zum Schutz der lokal oder über Cloudplattformen vom/von der Arbeitgeber:in[1] verarbeiteten (personenbezogenen und nicht-personenbezogenen) Daten und Dokumente des/der Arbeitgeber:in Maßnahmen ergriffen werden müssen. Daher werden zu diesem Zweck technische Systeme zur Gewährleistung der IT- und Datensicherheit sowie zur Netzwerkanalyse eingesetzt, sowie Regelungen für den sorgsamen Umgang mit entsprechenden Daten und Betriebs- und Geschäftsgeheimnissen erlassen. Zugleich besteht Einigkeit, dass die Persönlichkeitsrechte der Arbeitnehmer:innen gewahrt bleiben müssen und die Verarbeitung personenbezogener Daten der Arbeitnehmer:innen nach den Regelungen des Datenschutzrechts und dieser Betriebsvereinbarung zu erfolgen hat.

(3) Die Systeme zur Gewährleistung der IT- und Datensicherheit dienen der IT-Abteilung/Systemadministration zur Prüfung datensicherheitsrelevanter Aspekte und unterstützen die Etablierung eines Informationssicherheitsmanagementsystem (ISMS).

[1] In Unternehmen mit mehreren Standorten werden Maßnahmen zur IT- und Datensicherheit durch die Unternehmensleitung gesetzt. Die Vereinbarung sollte daher sinnvollerweise vom Zentralbetriebsrat abgeschlossen werden.

Die Erstellung dieses BV-Musters wurde durch den Digitalisierungsfonds Arbeit 4.0 der AK Wien gefördert.

(4) Darüber hinaus sollen Arbeitnehmer:innen in ihrer täglichen Arbeit unterstützt werden, indem mögliche Probleme an betrieblichen Endgeräten (Notebook, PC, Tablet, Smartphones, ...) und im betrieblichen Netzwerk frühzeitig erkannt und behoben werden.

3. Definitionen

Die folgenden Definitionen finden in dieser Betriebsvereinbarung Anwendung:

a) Daten werden nach der Daten-Governance Verordnung der EU als „jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material“ beschrieben.

b) Personenbezogene Daten sind nach Art 4 Z 1 DSGVO „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels 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.“

c) IT-Sicherheit beschreibt Maßnahmen zur Gewährleistung einer sicheren technischen Infrastruktur, darunter fallen alle eingesetzten Informationstechniken oder Informationstechnologien.

d) Datensicherheit (und Informationssicherheit) bezieht sich auf die sichere Verarbeitung von (personenbezogenen und nicht-personenbezogenen) Daten und Informationen. Diese Daten und Informationen müssen zum einen vor unberechtigtem Zugang und unberechtigter Verwendung (= Vertraulichkeit), zum anderen vor Verlust (insbesondere) bei technischen Problemen der eingesetzten Systeme geschützt werden (= Verfügbarkeit), wie auch die Sicherstellung der Korrektheit (= Integrität) von Daten und der korrekten Funktionsweise von Systemen sicherzustellen ist.

e) Cybersicherheit umfasst nach der Definition der NIS-Richtlinie der EU „alle Tätigkeiten, die notwendig sind um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen“.

f) Ein „System der künstlichen Intelligenz“ (KI-System) ist eine Software, die mit einer oder mehreren der im Folgenden aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren:
   - Konzepte des maschinellen Lernens, mit beaufsichtigtem, unbeaufsichtigtem und bestärkendem Lernen unter Verwendung einer breiten Palette von Methoden, einschließlich des tiefen Lernens (Deep Learning)
   - Logik- und wissensgestützte Konzepte, einschließlich Wissensrepräsentation, induktiver (logischer) Programmierung, Wissensgrundlagen, Inferenz- und Deduktionsmaschinen, (symbolischer) Schlussfolgerungs- und Expertensysteme
   - Statistische Ansätze, Bayessche Schätz-, Such- und Optimierungsmethoden.

g) E-Discovery bedeutet, dass für einen bestimmten Sachverhalt (zB eine datenforensische Suche aus einem bestimmten sicherheitsrelevanten Anlass) relevante Daten (meist aus den Inhalten von E-Mails und Dokumenten gewonnen) identifiziert, aufbereitet und bereitgestellt bzw an Dritte (zB Behörden) übergeben werden.

Die Erstellung dieses BV-Musters wurde durch den Digitalisierungsfonds Arbeit 4.0 der AK Wien gefördert.

4. Datenverarbeitung

(1) Die eingesetzten Systeme zur Gewährleistung der IT- und Datensicherheit werden, soweit sie personenbezogene (oder personenbeziehbare) Daten der Arbeitnehmer:innen verarbeiten, in **Anhang 1** angeführt und werden zumindest unter Beschreibung folgender Punkte mittels Datenblatt oder Zusatz-Betriebsvereinbarung dokumentiert:

- Bezeichnung System/Maßnahme und Anbieter
- Prüfziele/Zwecke der Datenverarbeitung
- Zuständige Abteilung (Stellen, Funktionen)
- Fokus der Datenverarbeitung: Person (Arbeitnehmer:in, Nutzer:in), Gerät/Endpoint (PC, Laptop, Smartphone, ...), Netzwerk, Anwendung (Applikation), Infrastruktur
- Ort der Datenhaltung: in eigener Infrastruktur lokal (on-prem), in eigen genutzter Cloudlösung, bei einem anderen Konzern-Unternehmen, bei einem Auftragsverarbeiter (insbesondere bei einem Cloud-Anbieter)
- verarbeitete Datenkategorien
- mittels Datenblatt oder (Zusatz-)Betriebsvereinbarung vereinbarte personenbezogene Auswertungen und Analysen
- berechtigte Empfängerkreise

(2) Zur Unterstützung der IT- und Datensicherheit werden auf den betrieblichen Endgeräten (Notebook, PC, Tablet, Smartphone) und Applikationen sowie bei der Nutzung dieser Endgeräte Systemparameter und technische Daten (diagnostische Daten, Protokoll-, Verkehrs- und Telemetriedaten, die im Hintergrund der Services/Komponenten anfallen) gesammelt und in Verbindung mit der/dem jeweiligen User:in/Endgerät ausgewertet. Die dabei gesammelten Informationen sind je System im jeweiligen Datenblatt in Anhang 1 beschrieben.

(3) Eine Analyse personenbezogener Informationen im Hinblick auf die Arbeitsleistung oder das (gegenwärtige oder zukünftige [„predictive analytics"]) Verhalten von Beschäftigten ist untersagt. Untersagt wird auch der Einsatz von KI-Systemen, deren Einsatz ist nur nach Abschluss einer speziellen Zusatz-Betriebsvereinbarung zulässig. Auch der Einsatz von E-Discovery-Tools und -Features bedarf zu seiner Zulässigkeit des vorangehenden Abschlusses einer speziellen Zusatz-Betriebsvereinbarung. Zur Aufrechterhaltung der betrieblichen System-Sicherheit dürfen personenbezogene Daten ausschließlich in den in dieser Vereinbarung angeführten Fällen und unter Einhaltung der in dieser Vereinbarung definierten Prozesse (Prinzip der [nur] „stufenweise Kontrollverdichtung") ausgewertet werden.

(4) Inhaltsdaten, wie zB der Text einer E-Mail oder eines Dokuments dürfen, sofern nicht in der Anlage ausdrücklich vereinbart, nicht ausgewertet werden, ebenso darf kein Keylogging (Erfassung aller Anschläge der Tastatur) stattfinden.

(5) Die erfassten Informationen dürfen auf verschiedene Bedrohungsszenarien und Verbesserungspotentiale hin zur Gewährleistung der IT- und Datensicherheit ausgewertet werden. Dazu stehen unterschiedliche Funktionalitäten (Alarmmeldungen, Standardauswertungen, Cockpitlösungen, Key Indikatoren, Dashboard) zur Verfügung. Die Darstellung der Auswertungsergebnisse darf in einem ersten Schritt nur in aggregierter Form ohne Bezug zu einzelnen Arbeitsplätzen/Beschäftigten (beispielsweise in Form von Dashboards) erfolgen. Die weiteren Auswertungsstufen und ihre Voraussetzungen finden sich im folgenden Absatz.

Die Erstellung dieses BV-Musters wurde durch den Digitalisierungsfonds Arbeit 4.0 der AK Wien gefördert.

(6) Bei konkret erkannten Gefährdungen oder Alarmmeldungen ist bei der Auswertung von Daten und der Darstellung der Datenverarbeitung einzelner Endgeräte und damit der Herstellung des Bezuges zu einzelnen Nutzer:innen von der IT-Abteilung/Systemadministration im Sinne des folgenden Prozesses wie folgt vorzugehen. Ausgenommen von den ersten beiden Stufen 1 und 2 sind nur die Fälle einer konkreten unmittelbaren Gefährdung für die IT-Infrastruktur oder für ihre korrekte Funktionsfähigkeit, welche von der IT-Abteilung/Systemadministration schriftlich zu dokumentieren bzw systemseitig zu protokollieren sind. Darüber hinaus für all diejenigen Fälle, in denen ein begründeter Verdacht eines schwerwiegenden Verstoßes gegen dienstrechtliche Bestimmungen vorliegt.

a) Stufe 1: Die Auswertung des Endgeräte- und Applikationsverhaltens erfolgt durch technische Systeme ohne Darstellung personenbezogener Einzeldaten (beispielsweise in Form von Dashboards).

b) Stufe 2: Bei konkret erkannten Störungen oder Alarmmeldungen findet die Auswertung des Endgeräte- und Applikationsverhaltens und die entsprechende Problembehebung durch die verantwortlichen Stellen in der IT-Abteilung/Systemadministration statt. Die von der Auswertung betroffene Person wird im 4-Augengespräch durch eine zuständige Person in der IT-Abteilung (unter möglicher Rückfrage bei der IT-Leitung) über den Sachverhalt informiert und gegebenenfalls zur Stellungnahme aufgefordert. Eine Meldung an die vorgesetzte Stelle der betroffenen Person darf nicht erfolgen.

c) Stufe 3: Im Fall des Weiterbestehens des regelwidrigen Verhaltens zu Lasten der betrieblichen IT-Infrastruktur oder einer hohen Wahrscheinlichkeit, dass ein tatsächlicher Schaden für das Unternehmen entstehen könnte (zB Datenverlust), ist die betroffene Person durch eine zuständige Person aus der IT-Abteilung auf den regelwidrigen Umgang und die erforderliche Verhaltensänderung hinzuweisen. Die Geschäftsführung und der Betriebsrat dürfen über den Vorfall, aber ohne Personenbezug, informiert werden. Eine allgemeine (nicht personenbeziehbare) Information an andere Arbeitnehmer:innenkreise kann erfolgen, um das regelkonforme IT-Verhalten zu veranschaulichen.

d) Stufe 4: Bei fortgesetzter pflichtwidriger und das IT-System gefährdender Nutzung darf eine personenbezogene Offenlegung des Vorfalls gegenüber der vorgesetzten Stelle der betroffenen Person unter Information an den Betriebsrat und sofern vorhanden an den Datenschutzbeauftragten und den Chief Information Security Officer (CISO) erfolgen.

e) Alle durchgeführten Verfahrensschritte, inklusive der dazu stattgefundenen datenforensischen Erhebungen und Auswertungen sind schriftlich zu dokumentieren und allen Betroffenen zur Verfügung zu stellen.

f) Nach Bereinigung der Gefährdungslage bzw Aufklärung des Vorfalles sind die zugrundeliegenden personenbezogenen Daten zu löschen bzw zu anonymisieren. Ausgenommen davon ist die allfällige Einleitung dienstrechtlicher Maßnahmen.

(7) In allfällig zu übermittelnden Auswertungsergebnissen an Dritte ist jedenfalls der Username zu pseudonymisieren, sodass ein Rückschluss auf einzelne Personen – mit Ausnahme der in dieser Betriebsvereinbarung getroffenen Regelung - ausgeschlossen ist.

(8) Auf Anfrage sind dem Betriebsrat je System die Berechtigungsrollen vorzulegen. Zugriffe durch die IT-Abteilung/Systemadministration sind zu protokollieren, damit tatsächlich durchgeführte Verarbeitungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können. Diese Protokolldaten sind in eine eigene Protokolldatenbank (mit einer jeweiligen Löschfrist von 2 Jahren) einzustellen, in die dem Betriebsrat Einsicht (vom BR-

Account aus) einzuräumen ist. Mit allen zugriffsberechtigten Personen sind Vereinbarungen zur Wahrung des Datengeheimnisses gemäß DSGVO bzw § 6 DSG abzuschließen und diese Personen sind – zusätzlich zu regelmäßigen Datenschutz-Schulungen – nachweislich von den Regelungen dieser Vereinbarung zu informieren.

(9) Werden die Berechtigungen durch externe (unternehmensfremde) Personen ausgefüllt, ist dies in den dazu notwendigen Verträgen mit Auftragsverarbeitern unter Einhaltung des jeweils geltenden Datenschutzrechts festzuhalten. Diese Auftragsverarbeiter sind nachweislich zur Einhaltung der Bestimmungen dieser Vereinbarung zu verpflichten. Diese rechtliche Überbindung und die arbeitnehmerrelevanten Inhalte der Verträge über eine Auftrags(daten)verarbeitung sind dem Betriebsrat auf Anforderung vorzulegen.

5. Informationssicherheitsmanagementsystem (ISMS)

(1) Die <NAME> evaluiert zur Sicherstellung der IT- und Datensicherheit regelmäßig die getroffenen Strategien, Konzepte sowie technischen und organisatorischen Maßnahmen (TOMs). In einem kontinuierlichen operativen Prozess werden die getroffenen Maßnahmen regelmäßig auf sich ändernde Rahmenbedingungen und aktuelle Bedrohungslagen überprüft.

(2) Dazu wird ein Informationssicherheitsmanagementsystem (ISMS) mit einem Informationssicherheits-Management-Team eingeführt.

(3) Zu den Mitgliedern des Informationssicherheits-Management-Teams gehört neben Personen aus den technischen und rechtlichen Fachabteilungen auch zumindest ein Mitglied des Betriebsrates.

(4) Die Entscheidungskompetenzen der Arbeitgeberin/des Arbeitgebers als Organ des Unternehmens und die des Betriebsrates als Organ der Belegschaft bleiben davon jedoch unberührt.

6. Beweismittel und -verwertungsverbot

(1) Eine Verarbeitung von personenbezogenen Daten der Arbeitnehmer:innen, die unter Zuhilfenahme der durch diese Betriebsvereinbarung erfassten Systeme und/oder gemäß der gegenständlichen Betriebsvereinbarung inklusive deren Anhänge in erlaubter oder unerlaubter Weise verarbeitet (erhoben/erfasst/ausgelesen/abgefragt) wurden, zur Leistungs- und Verhaltenskontrolle oder zur wie auch immer gearteten Beurteilung von Arbeitnehmer:innen ist untersagt und damit rechtwidrig.

(2) Es wird hiermit zur diesbezüglichen Bewehrung aus Gründen rechtlicher Vorsicht gemäß Art 88 Abs 1 DSGVO beschäftigtendatenschutzrechtlich ein entsprechendes außergerichtliches, gerichtliches und behördliches Beweismittel- und -verwertungsverbot, das sich an Jedermann (das sind insbesondere Arbeitgeber:in, Behörden und Gerichte) richtet, vereinbart, soferne von einem solchen Beweismittel- und -verwertungsverbot nicht sowieso schon eo ipso (europa-)rechtlich auszugehen ist.

(3) Erlangt der/die Arbeitgeber:in von derartigen Analysen Dritter Kenntnis (beispielsweise über eine entsprechende Verarbeitung im Konzern seitens eines anderen Konzernunternehmens oder seitens eines [Sub-]Auftragsverarbeiters eines Konzernunternehmens), sind der Betriebsrat und die davon betroffenen Arbeitnehmer:innen zu informieren. Darüber hinaus sind die Solches ausführenden Stellen von den Regelungen dieser Betriebsvereinbarung und ihren Anhängen zu informieren und sind diese Stellen sowie die entsprechenden Unternehmen nachweislich zur Unterlassung aufzufordern, welche Vorgehensweise dem Betriebsrat proaktiv zur Kenntnis zu bringen ist.

Die Erstellung dieses BV-Musters wurde durch den Digitalisierungsfonds Arbeit 4.0 der AK Wien gefördert.

7. Auftragsverarbeitung

(1) Bei allen zum Einsatz kommenden Auftragsverarbeitern gemäß Artikel 28 DSGVO hat der/die Arbeitgeber:in sicherzustellen, dass diese Auftragsverarbeiter neben den Bestimmungen des Datenschutzrechts auch die Regelungen dieser Betriebsvereinbarung einhalten. Die Auftragsverarbeiter sind deshalb nachweislich zur Einhaltung der Bestimmungen dieser Betriebsvereinbarung zu verpflichten. Diese rechtliche Überbindung und die arbeitnehmerrelevanten Inhalte der Verträge über die jeweilige Auftrags(daten)verarbeitung sind dem Betriebsrat auf Anforderung vorzulegen.

8. Mitwirkungsrechte des Betriebsrates

(1) Dem Betriebsrat sind alle geltenden Ordnungsvorschriften zur IT- und Datensicherheit nachweislich zur Kenntnis zu bringen und diese sind im Hinblick auf die Bestimmungen dieser Betriebsvereinbarung auf Konformität mit dieser hin zu prüfen.

(2) Der Betriebsrat hat zur Überprüfung dieser Betriebsvereinbarung das Recht in sämtliche technischen Protokolle und Funktionalitäten (Alarmmeldungen, Standardauswertungen, Cockpitlösungen, Key Indikatoren, Dashboard) nach Maßgabe des § 89 und § 91 Abs 2 ArbVG Einsicht zu nehmen. Zugang zu Hardware und Software ist ihm zu gewähren.

(3) Es ist dem Betriebsrat gestattet, externe Expert:innen zur Unterstützung und zur technischen Prüfung der Einhaltung dieser Betriebsvereinbarung hinzuzuziehen. Diese Expert:innen sind nachweislich zur Verschwiegenheit zu verpflichten. Sie sind bei ihrer Tätigkeit von den Fachabteilungen zu unterstützen. Die entsprechenden Kosten sind bis zur maximalen Höhe von € x.xxx pro Jahr vom Unternehmen zu tragen. Wird ein Verstoß gegen Bestimmungen dieser Betriebsvereinbarung festgestellt, sind die entsprechenden Kosten dieser Hinzuziehung vom Unternehmen ohne Anrechnung auf den Jahresmaximalbetrag zu tragen.

9. Sanktionen bei Verstößen

(1) Verstöße des/der Arbeitgeber:in gegen die gegenständliche Betriebsvereinbarung, gegen das DSG oder gegen die DSGVO berechtigen den Betriebsrat, schriftlich auf diese Missstände hinzuweisen und deren Beseitigung binnen vierzehn Tage nach der Beanstandung zu fordern.

(2) Im Falle der Nichtbeseitigung des Missstandes innerhalb dieser Frist trotz schriftlicher Aufforderung hat der Betriebsrat das Recht, die gegenständliche Betriebsvereinbarung, den betroffenen Anhang bzw die Zusatz-Betriebsvereinbarung mittels eingeschriebenen Briefes an den/die Arbeitgeber:in einseitig mit sofortiger Wirkung aufzulösen, wobei eine Nachwirkung ausgeschlossen ist, sodass die von der gegenständlichen Betriebsvereinbarung erfassten Datenverarbeitungen bzw die im Anhang geregelte betroffene Datenverarbeitung sofort zur Gänze einzustellen wären.

10. Rechte der ArbeitnehmerInnen

(1) Alle Arbeitnehmer:innen sind über ihre datenschutzrechtlichen Rechte und Pflichten, insbesondere geltende IT-Ordnungsvorschriften, nachweislich zu informieren.

(2) Alle Arbeitnehmer:innen sind in transparenter Form über die Verarbeitungen ihrer Daten zur Gewährleistung der IT- und Datensicherheit zu informieren.

Die Erstellung dieses BV-Musters wurde durch den Digitalisierungsfonds Arbeit 4.0 der AK Wien gefördert.

(3) Technische und organisatorische Maßnahmen zur IT- und Datensicherheit sind so zu erlassen und zur Verfügung zu halten, dass sich die Arbeitnehmer:innen über die für sie geltenden Regelungen jederzeit informieren können.

(4) Alle diese Informationen sind (auch) in deutscher Sprache bereit zu stellen.

11. Geltungsdauer der Betriebsvereinbarung

(1) Diese Betriebsvereinbarung tritt mit TT. MM. JJJJ in Kraft und gilt vorerst befristet für achtzehn Monate.

(2) Während dieser Zeit besteht eine Phase der beiderseitigen Prüfung ihrer praktikablen Anwendbarkeit, binnen derer – über Wunsch einer Vertragsseite – auch ergänzende Gespräche mit dem Ziel einer einvernehmlichen Abänderung geführt werden können.

(3) Sollte bis 3 Monate vor Ablauf der achtzehnmonatigen Befristung keine Vertragsseite gegenüber der anderen Partei ausdrücklich und schriftlich (maßgeblich für die Rechtzeitigkeit ist, wie für alle der Schriftform bedürftigen Veranlassungen gemäß dieser Betriebsvereinbarung, das Einlangen bei der anderen Partei, wobei auch Übermittlung per E-Mail akzeptiert wird) auf einem Auslaufen der Betriebsvereinbarung mit Fristende bestehen, so verlängert sich diese Betriebsvereinbarung befristet um jeweils 24 Monate unter Beibehaltung des vorbeschriebenen Procederes für eine allfällige Nichtverlängerungserklärung.

Die Erstellung dieses BV-Musters wurde durch den Digitalisierungsfonds Arbeit 4.0 der AK Wien gefördert.