Datenschutzkonzept

Inhalt

1. Leitlinie zu Datenschutz und Informationssicherheit

Einleitung

BeWo Durchblick verabschiedet hiermit diese Leitlinie zu Datenschutz und Informationssicherheit in unserem Unternehmen.
Als Unternehmen verarbeiten wir eine Vielzahl von personenbezogenen Daten, um unsere Aufgaben und Pflichten gegenüber unseren Kund*innen (nachfolgend Leistungsberechtigte genannt), Vertragspartnern, Dienstleistern, öffentlichen Stellen und sonstigen Dritten zu erfüllen.
Dabei verarbeiten wir Daten mit unterschiedlichem Schutzbedarf. Die Sicherheit der Informationsverarbeitung und der Schutz von personenbezogenen Daten spielt eine wesentliche Rolle in unserem Unternehmen. Diese Leitlinie soll die Strategie, die Organisation und Ziele von Datenschutz und Informationssicherheit in unserem Unternehmen in übersichtlicher Form darstellen.

Geltungsbereich

Die Leitlinie gilt für BeWo Durchblick. Diese Leitlinie verpflichtet alle Beschäftigten von BeWo Durchblick zur Einhaltung der hier festgelegten Pflichten.

Ziele

Ziel dieser Leitlinie ist es, Datenschutz und Informationssicherheit im Unternehmen zu gewährleisten. Für diesen Zweck wird BeWo Durchblick bei der Planung, Einführung und während des Ablaufs von Prozessen nachfolgende Ziele berücksichtigen:

- Rechtmäßigkeit
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Verfügbarkeit, Integrität und Vertraulichkeit
- Intervenierbarkeit und Verarbeitung nach Treu und Glauben („Fairness“)
- Rechenschaftspflicht („Accountability-Prinzip“)

Die Berücksichtigung dieser Ziele wird durch gesonderte Richtlinien konkretisiert.
Bei der konkreten Umsetzung der Ziele müssen die getroffenen Schutzmaßnahmen in einem wirtschaftlich vertretbaren Verhältnis zum Schutzbedarf der verarbeiteten Daten und Informationen stehen.

Organisation von Datenschutz und Informationssicherheit

Verantwortlich für die Sicherheitsorganisation ist die Geschäftsführung von BeWo Durchblick, vertreten durch die Geschäftsführerin.

Maßnahmen

Die Maßnahmen zur Umsetzung dieser Leitlinien können in Form von technischen und organisatorischen Maßnahmen erfolgen. Dazu gehören auch Richtlinien, betriebliche Regelungen oder betriebliche Anweisungen. Diese sind von den Beschäftigten zu befolgen.

Verantwortlichkeiten

Die Geschäftsführung übernimmt die Gesamtverantwortung für die Informationssicherheit und den Datenschutz im Unternehmen.
Sie hat auch die Aufgabe der Initiierung, Planung, Umsetzung und Steuerung des Informationssicherheitsprozesses im Unternehmen. Sie ist Ansprechpartnerin für Informationssicherheit im Unternehmen. Sie wird dabei beraten durch die Geschäftsleitung und den*die Administrator*in. Die Geschäftsführerin kann Umsetzungs- und Verantwortungsbereiche an Personen delegieren.

Der*die Administrator*in führt die technischen Maßnahmen in Abstimmung mit der Geschäftsführerin durch und trägt durch Verbesserungsvorschläge zur Optimierung der Informationssicherheit bei.

Vorgesetzte mit Personalverantwortung haben die Aufgabe, sicherzustellen, dass die getroffenen technischen und organisatorischen Maßnahmen zur Informationssicherheit in Bezug auf die in ihrem Verantwortungsbereich tätigen Personen umgesetzt werden.

Jede*r Mitarbeiter*in trägt durch sein*ihr Verhalten zur Gewährleistung von Datenschutz und Informationssicherheit bei. Alle Beschäftigten sind verpflichtet, diese Leitlinie und die Richtlinien zu Datenschutz und Informationssicherheit einzuhalten. Um Datenschutz und Informationssicherheit im Unternehmen zu gewährleisten, ist jede*r Mitarbeiter*in verpflichtet, Störungen, Sicherheitsvorfälle und Notfälle im Bereich der Informationssicherheit unverzüglich und direkt an die Geschäftsführung zu melden. Vorfälle im Bereich des Datenschutzes sind von allen Beschäftigten unverzüglich nach Kenntnisnahme an die Geschäftsführung zu melden.

Externe Dienstleistende und sonstige Auftragnehmende sind durch gesonderte Vereinbarungen zu verpflichten, die sie betreffenden Vorgaben zu Datenschutz und Informationssicherheit einzuhalten, wenn diese Daten im Auftrag verarbeiten oder die Möglichkeit der Kenntnisnahme von personenbezogenen Daten oder als nicht öffentlich klassifizierten Informationen des Unternehmens haben.

Sanktionen

Ein Verstoß gegen diese Leitlinie kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

2. IT-Richtlinie für Nutzer*innen

Einleitung

BeWo Durchblick verfügt über eine IT-Infrastruktur, die den Beschäftigten im Zusammenhang mit ihrer Tätigkeit für BeWo Durchblick als Arbeitsmittel zur Verfügung steht. Die IT-Infrastruktur ist unerlässlich für den Geschäftsbetrieb von BeWo Durchblick.

Geltungsbereich

Diese IT-Richtlinien gelten für BeWo Durchblick. Sie gelten für alle Standorte von BeWo Durchblick. Diese IT-Richtlinien sind von allen Beschäftigten von BeWo Durchblick einzuhalten.

Ziele

Um die Integrität, Verfügbarkeit und Vertraulichkeit der IT-Systeme auf Dauer zu gewährleisten, sind die nachfolgenden IT-Richtlinien von allen Beschäftigten einzuhalten.

Allgemeine Nutzungsrichtlinien für IT-Systeme

Sofern nachfolgend von IT-Systemen die Rede ist, sind darunter ausnahmslos alle Geräte oder Anwendungen (Hard- und Software) zu verstehen, mit denen Informationen elektronisch verarbeitet oder übertragen werden können. Dazu gehören insbesondere PCs, Notebooks/Laptops, Tablet PCs (z.B. iPad), Telefone, Mobiltelefone, Server, Speichermedien, Netzwerktechnologie, Softwareprodukte und Drucker.

Die Nutzung der IT-Systeme und Applikationen (Apps) im Unternehmen ist ausschließlich zu dienstlichen Zwecken und in jeweils erlaubten Umfang zur Aufgabenerledigung zulässig. Abweichungen hiervon bedürfen der Erlaubnis des Arbeitgebers. Es darf nur die Software auf IT-Systemen des Unternehmens installiert werden, die vom Arbeitgeber freigegeben worden ist. Applikationen (Apps) dürfen nur aus dem Google Playstore auf das dienstliche Smartphone heruntergeladen werden, um eine vorherige Sicherheitsüberprüfung der Applikation zu gewährleisten.

Die Benutzung privater Hard- und Software zu dienstlichen Zwecken ist zulässig und unterliegt folgenden Regelungen:

1. Passwörter und Zugangsdaten dürfen nicht aufgeschrieben, gespeichert oder weitergegeben werden. Selbst vergebene Passwörter müssen sicher sein (BSI - Sichere Passwörter erstellen).
2. Für die Tätigkeit benötigte und gespeicherte Daten müssen nach der Aktivität sofort gelöscht werden, sowohl aus Hauptordnern als auch aus dem Zwischenspeicher.
3. Die privaten Endgeräte und IT-Systeme müssen mit aktueller Sicherheitssoftware ausgestattet sein, um die Daten vor Angriffen von Schadsoftware zu schützen.
4. Betriebssysteme auf den IT-Systemen müssen auf dem jeweils aktuellen Stand von Sicherheitsupdates des jeweiligen Betriebssystemanbieters sein.
5. Es muss sichergestellt sein, dass Dritte keinen Zugang zu dienstlichen Daten bekommen.

Die Nutzung von IT-Systemen bei BeWo Durchblick erfolgt grundsätzlich nur für berufliche Zwecke. Eine private Nutzung von IT-Systemen von BeWo Durchblick ist zulässig unter folgenden Bedingungen:

1. Umfang der privaten Nutzung: Die dienstlichen Endgeräte dürfen für die Nutzung von Social-Media-Plattformen, E-Mails oder das Surfen im Internet (“ClearWeb”) genutzt werden. Illegale und unsichere Aktivitäten sind untersagt (BSI - Darknet und Deep Web).
2. Verantwortungsbewusste Nutzung: Vermeidung von illegalen Aktivitäten, die Einhaltung der IT-Richtlinien von BeWo Durchblick und der Schutz von vertraulichen Daten muss jederzeit gewährleistet sein.

3. Sicherheitsmaßnahmen: Zur Sicherung des Endgerätes vergebene Passwörter dürfen nicht aufgeschrieben, gespeichert oder weitergegeben werden.

Sanktionen

Ein Verstoß gegen diese Richtlinie kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

3. Richtlinie Regelungen für externe Dienstleistende und sonstige Auftragnehmende

Einleitung

Bei BeWo Durchblick können auch externe Dienstleistende oder sonstige Auftragnehmende für die Durchführung von Leistungen beauftragt werden. Um die Verfügbarkeit, Integrität und Vertraulichkeit von Daten zu gewährleisten, macht diese Richtlinie Vorgaben für Beschäftigte von BeWo Durchblick, aus denen sich ergibt, ob und wie externe Dienstleistende oder sonstige Auftragnehmende im Hinblick auf die Wahrung der Vertraulichkeit und des Datenschutzes beauftragt werden können.

Geltungsbereich

Diese Richtlinie gilt für die Beauftragung von externen Dienstleistern oder sonstigen Auftragnehmern durch BeWo Durchblick. Diese Richtlinie gilt für alle Standorte von BeWo Durchblick. Diese Richtlinie verpflichtet alle Beschäftigten von BeWo Durchblick zur Einhaltung der hier festgelegten Pflichten und Vorgaben.

Ziele

Diese Richtlinie soll dazu beitragen, dass die Integrität, Verfügbarkeit und Vertraulichkeit von Informationen bei Erbringung von Leistungen durch externe Dienstleistende oder sonstige Auftragnehmende gewährleistet wird.

Grundsätze der Inanspruchnahme von externe Dienstleistende oder sonstigen Auftragnehmenden

Wenn externe Dienstleistende oder sonstige Auftragnehmende mit Ihrer Tätigkeit für BeWo Durchblick Zugriff auf Informationen des Unternehmens und/oder personenbezogene Daten, die vom Unternehmen verarbeitet werden, erhalten, ist die Beauftragung vorher von dem*der Vorgesetzen zu genehmigen. Der*die Vorgesetzte wird sich mit der Geschäftsführerin des Unternehmens in Verbindung setzen, um die datenschutzrechtliche Zulässigkeit und rechtliche Absicherung der Inanspruchnahme der externen Dienstleistenden oder sonstigen Auftragnehmenden zu prüfen und zu klären.
Wenn eine Kenntnisnahme von personenbezogenen Daten durch externe Dienstleistende oder sonstige Auftragnehmende nicht möglich ist, so sollte gleichwohl eine Geheimhaltungsverpflichtung mit den jeweiligen Auftragnehmenden abgeschlossen werden. Eine entsprechende Vorlage für eine solche Erklärung ist bei der Geschäftsführung zu erhalten.
Alle Mitarbeitenden sollten beachten, dass für den Fall, dass externe Dienstleistende oder sonstige Auftragnehmende personenbezogene Daten im Auftrag verarbeiten und/oder eine Wartung oder Pflege von IT-Systemen durchgeführt wird, bei der eine Kenntnisnahme von personenbezogenen Daten theoretisch möglich ist, zwingend ein sogenannter Auftragsdatenverarbeitungsvertrag abzuschließen ist.

Regelungen für externe Dienstleistende und sonstige Auftragnehmende

Um die IT-Infrastruktur vor Störungen zu schützen und die Sicherheit der in ihr verarbeiteten, gespeicherten und übertragenen Informationen zu gewährleisten, sind externe Dienstleistende oder sonstige Auftragnehmende, die Zugriff auf IT-Systeme von BeWo Durchblick haben, zwingend auf nachfolgende Regelungen zu verpflichten:

- Das unrechtmäßige Abrufen oder Verbreiten von Inhalten, die urheberrechtlich geschützt sind, ist untersagt.
- Ebenfalls untersagt ist das Abrufen oder Verbreiten von strafrechtlich relevanten oder sittenwidrigen Inhalten.
- Zugangskennungen für die Nutzung der IT-Infrastruktur (wie z. B. Passwörter) sind von einem externen Dienstleistenden oder sonstigen Auftragnehmenden geheimzuhalten und dürfen grundsätzlich nicht an Dritte weitergegeben werden. Auch innerhalb der jeweiligen Organisation der externen Dienstleistenden oder sonstigen Auftragnehmenden sind diese verpflichtet, die Daten vor anderen Beschäftigten des Auftragnehmers geheim zu halten. Ausnahmen hiervon können gemacht werden, wenn die Leistungen des*der Auftragnehmenden von einem Team von Personen für BeWo Durchblick durchgeführt werden.
- Die private Nutzung von IT-Systemen von BeWo Durchblick ist jedem externen Dienstleistenden oder sonstigen Auftragnehmenden untersagt.
- Bei einem Einsatz von IT-Dienstleistenden sind stets folgende Punkte zu berücksichtigen: IT-Systeme des Dienstleistenden müssen über grundlegende Sicherheitsmaßnahmen verfügen:
    - Das IT-System muss ausreichend vor Schadsoftware gesichert sein.
    - Betriebssysteme auf den IT-Systemen müssen auf dem jeweils aktuellen Stand von Sicherheitsupdates des jeweiligen Betriebssystemanbieters sein. Es sind nur Betriebssysteme zu verwenden, die vom Hersteller noch unterstützt und gepflegt werden („Support“).
- Es gelten des Weiteren die allgemeinen Nutzungsrichtlinien für IT-Systeme aus der IT-Richtlinie für Nutzer*innen (siehe S. 3).

Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

Die Verträge mit externen Dienstleistenden oder sonstigen Auftragnehmenden sollten ebenfalls Sanktionsmöglichkeiten für Verstöße der Auftragnehmenden gegen die jeweils vereinbarten Pflichten im Zusammenhang mit Datenschutz und Informationssicherheit vorsehen.

4. Richtlinie für mobile IT-Systeme

Einleitung

BeWo Durchblick verfügt über eine IT-Infrastruktur, die den Beschäftigten im Zusammenhang mit ihrer Tätigkeit für BeWo Durchblick als Arbeitsmittel zur Verfügung steht. Bei BeWo Durchblick sind auch mobile IT-Systeme im Einsatz. Um den besonderen Risiken aus der Nutzung von mobilen IT-Systemen Rechnung zu tragen, wird die Nutzung dieser Systeme durch diese Richtlinie gesondert geregelt.

Geltungsbereich

Diese Richtlinie gilt für die Nutzung von mobilen IT-Systemen von BeWo Durchblick. Zu mobilen Endgeräten gehören insbesondere Laptops/Notebooks, Tablets und Smartphones. Diese Richtlinie gilt für alle Standorte von BeWo Durchblick.

Diese Richtlinie verpflichtet alle Beschäftigten von BeWo Durchblick zur Einhaltung der hier festgelegten Pflichten und Vorgaben.

Ziele

Diese Richtlinie soll dazu beitragen, dass die Integrität, Verfügbarkeit und Vertraulichkeit von Informationen auf mobilen IT-Systemen gewährleistet ist.

Grundsätze der Nutzung von mobilen IT-Systemen

Mobile IT-Systeme bergen das Risiko, dass unbefugte Dritte in Besitz von Informationen von BeWo Durchblick oder Leistungsberechtigten und/oder Geschäftspartnern von BeWo Durchblick kommen können.

Daher sind mobile IT-Systeme grundsätzlich nur von den Mitarbeitenden einzusetzen, die aufgrund ihrer Tätigkeit bei BeWo Durchblick auf die Nutzung eines mobilen IT-Systems angewiesen sind.

Grundsätzlich sind auf mobilen IT-Systemen nur dann Daten zu speichern, wenn dies für die Aufgabenerfüllung der Nutzenden im Zusammenhang mit ihrer Tätigkeit für BeWo Durchblick oder für Zwecke von BeWo Durchblick erforderlich ist.

Grundsätzlich gilt, dass alle Daten und Dokumente, die auf mobilen Endgeräten gespeichert werden, schnellstmöglich (spätestens jedoch nach 5 Werktagen) in den Dateimanager der Software von BeWo Durchblick hochgeladen werden müssen, um dann auf dem mobilen Endgerät dauerhaft entfernt zu werden.

Auf dienstlichen Smartphones dürfen folgende Kontaktdaten gespeichert werden und verbleiben: Vor- und Nachname, Telefonnummer, Email-Adresse.

Der*die Nutzer*in darf das ihm zur Verfügung gestellte mobile IT-System nicht anderen Personen zur Nutzung überlassen.

Im Hinblick auf die Installation von Software auf den mobilen IT-Systemen gilt die „IT-Richtlinie für Nutzer*innen“.

Verwendung von mobilen IT-Systemen außerhalb des Betriebsgeländes

Werden mobile IT-Systeme außerhalb des Betriebsgeländes von BeWo Durchblick verwendet, hat der*die Nutzer*in in besonderem Maße Sorge dafür zu tragen, dass Dritte keine Kenntnis von Informationen erhalten können, die mit dem mobilen IT-System verarbeitet werden.
Besonders schutzbedürftige Informationen sollten nach Möglichkeit nur an Orten verarbeitet werden, die von Dritten nicht einzusehen sind.
Sollte dies nicht möglich sein, muss der*die Nutzer*in einen Ort bzw. Platz zur Verarbeitung von Daten wählen, der gewährleistet, dass der Bildschirm nicht von Dritten eingesehen werden kann.

Datensicherung

Der*die Nutzer*in hat Sorge dafür zu tragen, dass Daten ausschließlich auf https://app.bewo-durchblick.de/ gespeichert werden. Bei Fragen zur Vorgehensweise der Übertragung der Daten hat sich der*die Nutzer*in an die Geschäftsführerin zu wenden.

Diebstahl und Verlust (ggf. Meldepflicht)

Sollte ein mobiles IT-System gestohlen werden oder verloren gehen, hat der*die Nutzer*in dies unverzüglich nach Kenntnisnahme an die Geschäftsführerin von BeWo Durchblick zu melden. Die Meldung muss so schnell wie möglich erfolgen, da in diesen Fällen gesetzliche Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen bestehen können, die im Falle einer zu späten Meldung Bußgelder in erheblicher Höhe nach sich ziehen können.
Die Geschäftsführung entscheidet, ob eine Meldung an die Aufsichtsbehörde erforderlich ist. Falls ja, muss die Meldung spätestens innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls erfolgen.

Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

5. Richtlinie für mobile Datenträger

Einleitung

Bei BeWo Durchblick können zum Teil auch mobile Datenträger verwendet werden. Diese Richtlinie regelt die Nutzung von mobilen Datenträgern durch Beschäftigte von BeWo Durchblick.

Geltungsbereich

Diese Richtlinie gilt für die Nutzung von mobilen Datenträgern von BeWo Durchblick. Mobile Datenträger sind alle leicht transportablen Geräte, auf denen Daten gespeichert werden können. Dazu gehören insbesondere USB-Sticks, externe Festplatten, Speicherkarten, CD-ROMs und DVDs.
Diese Richtlinie gilt für alle Standorte von BeWo Durchblick.
Diese Richtlinie verpflichtet alle Beschäftigten von BeWo Durchblick zur Einhaltung der hier festgelegten Pflichten und Vorgaben.

Ziele

Diese Richtlinie soll dazu beitragen, dass die Integrität, Verfügbarkeit und Vertraulichkeit von Informationen auf mobilen Datenträgern gewährleistet ist.

Grundsätze der Nutzung von mobilen Datenträgern

Mobile Datenträger bergen das Risiko, dass unbefugte Dritte in Besitz von Informationen von BeWo Durchblick oder Leistungsberechtigten und/oder Geschäftspartnern von BeWo Durchblick kommen können.
Daher sind mobile Datenträger grundsätzlich nur von den Mitarbeitenden einzusetzen, die aufgrund ihrer Tätigkeit bei BeWo Durchblick auf die Nutzung von mobilen Datenträgern angewiesen sind.

Daten auf mobilen Datenträgern sind, sofern diese für die dauerhafte Speicherung bei BeWo Durchblick vorgesehen sind, unverzüglich in die Software von BeWo Durchblick zu übertragen, sofern sie dort nicht schon vorhanden sind. Bei der Übertragung der Daten ist in besonderer Weise darauf zu achten, dass eine Prüfung der Inhalte auf dem Datenträger im Hinblick auf Schadsoftware erfolgt. Der*die Mitarbeitende kann sich bei Fragen der Umsetzung an die Geschäftsführerin wenden.
Der*die Nutzer*in darf das ihm zur Verfügung gestellte mobile IT-System nicht anderen Personen zur Nutzung überlassen.
Im Hinblick auf die Installation von Software auf den mobilen IT-Systemen gilt die „IT-Richtlinie für Nutzer*innen“.

Verwendung von mobilen IT-Systemen außerhalb des Betriebsgeländes

Werden mobile IT-Datenträger außerhalb des Betriebsgeländes von BeWo Durchblick verwendet, hat der*die Nutzer*in in besonderem Maße Sorge dafür zu tragen, dass Dritte keine Kenntnis von Informationen erhalten können. Dies beinhaltet insbesondere die sorgfältige und sichere Verwahrung des mobilen Datenträgers, um diesen vor Diebstahl und Verlust zu schützen.

Mobile Datenträger von Dritten

Sollten Beschäftigte einen mobilen Datenträger auf dem Betriebsgelände oder an sonstiger Stelle auffinden oder von Dritten mitgebrachte Datenträger erhalten, so dürfen solche Datenträger niemals an IT-Systeme von BeWo Durchblick angeschlossen werden. Es ist nicht auszuschließen, dass sich auf dem Datenträger Schad- oder Spionagesoftware befindet. Gefundene Datenträger sind der Geschäftsführerin zu melden und von dieser sorgfältig im Hinblick auf schädliche Inhalte zu inspizieren oder zu vernichten.

Diebstahl und Verlust

Sollte ein mobiler Datenträger gestohlen werden oder verloren gehen, hat der Nutzer dies unverzüglich nach Kenntnisnahme an die Geschäftsführerin von BeWo Durchblick zu melden. Die Meldung muss so schnell wie möglich erfolgen, da in diesen Fällen gesetzliche Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen bestehen können, die im Falle einer zu späten Meldung Bußgelder in erheblicher Höhe nach sich ziehen können.

Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

6. Richtlinie Speicherorte

Einleitung

Bei BeWo Durchblick können Daten auf verschiedenen IT-Systemen gespeichert werden („Speicherorte“). Um die Verfügbarkeit, Integrität und Vertraulichkeit von Daten zu gewährleisten, macht diese Richtlinie Vorgaben für Beschäftigte von BeWo Durchblick, aus denen sich ergibt, wo Daten zu speichern sind.

Geltungsbereich

Diese Richtlinie gilt für die Speicherung von Daten im Zusammenhang mit der Tätigkeit für BeWo Durchblick.
Diese Richtlinie gilt für alle Standorte von BeWo Durchblick.
Diese Richtlinie verpflichtet alle Beschäftigten von BeWo Durchblick zur Einhaltung der hier festgelegten Pflichten und Vorgaben.

Ziele

Diese Richtlinie soll dazu beitragen, dass die Integrität, Verfügbarkeit und Vertraulichkeit von Informationen durch eine Vorgabe von Speicherorten gewährleistet wird.

Grundsätze der Speicherung von Daten

Grundsätzlich sind Daten nicht auf lokalen Festplatten oder Datenspeichern von Endgeräten zu speichern. Hintergrund ist neben der fehlenden Verfügbarkeit der Daten vor allem auch, dass eine Sicherung der Daten auf den lokalen Datenspeichern nicht erfolgt.
Die Speicherung von Daten hat grundsätzlich im Dateimanager der von BeWo Durchblick genutzten Software zu erfolgen, in den jeweiligen Ordnern, die für den*die Nutzer*in freigegeben sind. Sollte eine Zuordnung zu einem bestimmten Gruppen-, Personen- oder Projektordner nicht möglich sein, sind Daten zunächst im persönlichen Ordner zu speichern, bis die Freigabe erfolgt ist. Ansonsten sind Daten stets in den jeweils einschlägigen Gruppen-, Personen- oder Projektordnern zu speichern.

Bei der Verwendung von mobilen IT-Systemen und mobilen Datenträgern sind die insoweit geltenden Richtlinien zu beachten.

Datensicherung

BeWo Durchblick nutzt eine eigene Dokumentations- und Abrechnungssoftware. Die Software ist onlinebasiert und wird von der STRATO GmbH gehostet. Alle gespeicherten Date werden auf deutschen Servern hinterlegt und unterliegen dem geltenden deutschen Datenschutz und den Datenschutzrichtlinien der STRATO GmbH. Weitere Informationen befinden sich hier: STRATO | Gedacht. Gemacht.

Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

7. Richtlinie für Störungen und Ausfälle

Einleitung

Diese Richtlinie regelt den Umgang mit Störungen und Ausfällen von IT-Systemen bei BeWo Durchblick.

Geltungsbereich

Diese Richtlinie gilt für die gesamte IT-Infrastruktur von BeWo Durchblick und gilt für alle Standorte von BeWo Durchblick.
Diese Richtlinie verpflichtet alle Beschäftigten der BeWo Durchblick zur Einhaltung der hier festgelegten Pflichten und Vorgaben.

Ziele

Diese Richtlinie soll dazu beitragen, dass die Integrität, Verfügbarkeit und Vertraulichkeit von Informationen der IT-Infrastruktur der BeWo Durchblick gewährleistet ist.

Grundsätze

Die IT-Infrastruktur von BeWo Durchblick umfasst ausnahmslos alle Geräte, die auf elektronischem Wege Informationen verarbeiten, übertragen oder speichern wie z.B. Arbeitsplatz-PCs, Server, Drucker, Speichermedien, Telefone, Fax-Geräte, mobile Telefone, Smartphones, Tablet-PCs u.ä.
Eine **Störung** ist eine Situation, in der Prozesse oder Ressourcen von BeWo Durchblick nicht wie vorgesehen funktionieren. Die dadurch entstehenden Schäden sind als *gering* einzustufen. Die Beseitigung einer Störung kann im allgemeinen Tagesgeschäft vorgenommen werden.
Ein **Ausfall** liegt vor, wenn ein Teil oder Teile der IT-Infrastruktur ihre Funktionsfähigkeit verloren haben.

Meldung

Störungen und Ausfälle beeinträchtigen die Funktionsfähigkeit des Unternehmens und können zu Kosten und weiteren Schäden führen. Wenn Störungen und Ausfälle nicht oder zu spät gemeldet werden, kann dies zu Folgeschäden führen, die zu vermeiden sind.
Um Störungen und Ausfälle schnell beheben zu können, ist eine unverzügliche Meldung entsprechender Vorfälle notwendig.
Jede*r Mitarbeitende meldet mögliche Störungen und Ausfälle an die Geschäftsführung.
Bei gravierenden Ausfällen wird die Geschäftsleitung ebenfalls sofort von den Mitarbeitenden informiert. Ein Ausfall gilt als gravierend, wenn eines der folgenden Merkmale zutreffend ist:

- Verletzung von Leib oder Leben von Menschen
- Störung der Software
- Störung des Internets
- Es besteht ein Verstoß gegen Gesetze, Verträge oder Normen und es sind Haftungsrisiken entstanden, die für das Unternehmen oder für einzelne Verantwortliche beträchtlich sind, insbesondere mögliche Verstöße im Bereich des Datenschutzes.

Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

8. Richtlinie für Sicherheitsvorfälle

Einleitung

Diese Richtlinie regelt den Umgang mit Sicherheitsvorfällen bei BeWo Durchblick.

Geltungsbereich

Diese Richtlinie gilt für die gesamte IT-Infrastruktur von BeWo Durchblick und gilt für alle Standorte von BeWo Durchblick.
Diese Richtlinie verpflichtet alle Beschäftigten von BeWo Durchblick zur Einhaltung der hier festgelegten Pflichten und Vorgaben.

Ziele

Diese Richtlinie soll dazu beitragen, dass die Integrität, Verfügbarkeit und Vertraulichkeit von Informationen der IT-Infrastruktur von BeWo Durchblick gewährleistet ist.

Grundsätze

Die IT-Infrastruktur von BeWo Durchblick umfasst ausnahmslos alle Geräte, die auf elektronischem Wege Informationen verarbeiten, übertragen oder speichern wie z.B. Arbeitsplatz-PCs, Server, Drucker, Speichermedien, Telefone, Fax-Geräte, mobile Telefone, Smartphones, Tablet-PCs u.ä.
Ein **Sicherheitsvorfall** ist ein unerwünschtes Ereignis, das Auswirkungen auf die Informationssicherheit und/oder den Schutz von personenbezogenen Daten hat und in der Folge große Schäden nach sich ziehen kann.

Meldung

Sicherheitsvorfälle können erhebliche, negative Konsequenzen für das Unternehmen haben. Schon bei einem Verdacht eines Sicherheitsvorfalles muss sofort eine Meldung durch Mitarbeitende erfolgen, die den Sicherheitsvorfall bemerken.
Ausnahmen hierzu gibt es nur, wenn dem*r jeweiligen Mitarbeitenden sicher bekannt ist, dass der Sicherheitsvorfall bereits von einem*r anderen Mitarbeitenden gemeldet worden ist. Im Zweifel muss eine Meldung erfolgen.

Sicherheitsvorfälle sind **vorrangig**. Das bedeutet, dass die Meldung von Sicherheitsvorfällen stets dem Tagesgeschäft oder sonstigen aktuellen Arbeiten vorgeht.
Die Meldung erfolgt an die Geschäftsführung des Unternehmens.

Behandlung des Sicherheitsvorfalls

Die Geschäftsführerin wird den Sicherheitsvorfall unverzüglich analysieren und – soweit erforderlich – alle Sofortmaßnahmen treffen, die zur Gewährleistung der Integrität, Verfügbarkeit und Vertraulichkeit der Informationen erforderlich sind.

Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

9. Notfallplan

Definition Notfall

Ein Notfall ist ein unerwünschtes, zeitlich nicht vorhersehbares Ereignis, das den Geschäftsbetrieb nachhaltig gefährden kann. Im Falle eines Notfalls gelten die nachfolgenden Richtlinien mit dem Zweck, den Geschäftsbetrieb aufrechtzuerhalten bzw. unverzüglich wieder einen Zustand einer funktionsfähigen IT-Infrastruktur herzustellen.

Generelles Verhalten

Beim Auftreten eines Notfalles ist ein besonnenes Vorgehen besonders geboten. Vorrangig ist, in einem Notfall Ruhe zu bewahren. Die Situation ist unverzüglich zu analysieren, und der Meldeplan ist unbedingt einzuhalten.

Bei einem reinen Verdacht auf Unregelmäßigkeiten, die auf einen Notfall oder sich ankündigenden Notfall hindeuten, ist in jedem Fall die Geschäftsführerin zu informieren.

Feuer

In allen Räumen, in denen sich IT-Systeme befinden, die für den laufenden Geschäftsbetrieb zwingend erforderlich oder kritisch sind, sind Rauchmelder und/oder Brandmeldeanlagen in Betrieb.
Darüber hinaus befinden sich in allen Gebäuden an mehreren Stellen die erforderlichen Feuerlöscher. Diese sind gut sichtbar angebracht und im Bedarfsfall zu nutzen. Im Falle eines Brandes ist zudem unverzüglich die Feuerwehr zu informieren. Ferner sind Vorgesetzte und die Geschäftsführerin sofort zu informieren.
Im Falle eines größeren Brandereignisses werden die Mitarbeitenden an den jeweiligen Betriebsstätten umgehend evakuiert. Fluchtwegepläne hängen in jedem Gebäude an gut sichtbarer Stelle aus.

Wasser

Größere Wasserschäden, die die für den Geschäftsbetrieb erforderlichen, kritischen IT-Systeme negativ beeinträchtigen könnten, stellen an allen Betriebsstätten aufgrund der Lage nur ein sehr geringes Risiko dar. Es ist regelmäßig nicht damit zu rechnen, dass ein Wasserschaden zu einer Beeinträchtigung der kritischen IT-Systeme führt. Die IT-Systeme befinden sich an Orten, an denen kein Hochwasser zu befürchten ist. Auch Schäden durch Wasserleitungen sind aufgrund der räumlichen Gegebenheiten äußerst unwahrscheinlich. Sollte dennoch ein Wasserschaden auftreten, der eine Gefahr für die kritischen IT-Systeme oder andere IT-Systeme darstellen könnte, sind sofort die Vorgesetzten und die Geschäftsführerin zu informieren. Diese werden dann nach Sichtung der Lage eine Risikobewertung und die weiteren erforderlichen Maßnahmen vornehmen.

Stromausfall

Es gibt bei BeWo Durchblick keine kritischen IT-Systeme, die über eine unterbrechungsfreie Stromversorgung (USV) verfügen. Im Falle eines Stromausfalls ist die Geschäftsführerin zu informieren, die weitere Schritte einleitet.

Angriffe von außen

Alle Server-IT-Systeme und alle kritischen IT-Systeme sollen durch Firewall-Technologie gesichert und überwacht werden. Ein Zugriff unbefugter Dritter von außen wird auf diese Weise wesentlich erschwert. Die Firewall-Technologie wird regelmäßig gewartet und aktualisiert, um eine Anpassung an neue Gefahrenlagen zu gewährleisten.
Die Installation einer Firewall-Technologie und eines Virenschutzprogramms ist, basierend auf dem aktuellen Stand der Bedrohungslage in Bezug auf Schadsoftware für Linux, unter Debian/Ubuntu nicht notwendig. (Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)). Dieser Stand wird regelmäßig überprüft und dem aktuellen Sicherheitsstand angepasst.

Einbruch und Diebstahl

Alle Büro- und Geschäftsräume sind vor dem Zutritt unbefugter Dritter gesichert. Dies gilt insbesondere für den Zutritt zu Gebäuden außerhalb der Büro- und Geschäftszeiten.
Für den Fall, dass ein Einbruch und/oder ein Diebstahl von IT-Systemen bemerkt wird, hat der*die jeweilige Mitarbeitende unverzüglich die Vorgesetzten sowie die Geschäftsführerin zu informieren.

Ausfall von IT-Administratoren

Im Unternehmen verfügen nur wenige Personen über Administrator-Rechte. Diese Personen sind entsprechend geschult und ausgebildet. Im Falle eines Ausfalls eines IT-Administrators (z.B. durch Krankheit) ist Sorge dafür getragen worden, dass mindestens ein*e weitere*r Mitarbeiter*in mit Administrator-Rechten sofort erreichbar ist, um ggf. erforderliche Administrator-Handlungen durchzuführen.

Notfall-Verantwortlicher

Im Unternehmen gibt es einen Notfall-Verantwortlichen, der bei Vorliegen eines Notfalles für die Veranlassung der jeweils vorgesehenen und gebotenen Maßnahmen verantwortlich ist.
Hierbei handelt es sich um die Geschäftsführerin.

Im Falle eines Funktionsausfalles eines IT-Systems wird die Ursache des Vorfalls unverzüglich untersucht. Parallel dazu werden sofort Maßnahmen in die Wege geleitet, um einen Wiederanlauf des IT-Systems oder eines Alternativsystems kurzfristig zu ermöglichen.
In der IT-Abteilung werden alle verantwortlichen Personen dahingehend geschult, Funktionsausfälle zu untersuchen und ein Wiederanlaufen der kritischen IT-Systeme schnellstmöglich vorzunehmen. Dabei ist in besonderer Weise dafür Sorge zu tragen, dass die Integrität der Daten gewährleistet ist.

10. Richtlinie: Konzept zur Löschung personenbezogener Daten

Inhalt

1. Präambel

Die Regelungen des Datenschutzes gehen auf das grundrechtlich geschützte informationelle Selbstbestimmungsrecht zurück, wonach Betroffene grundsätzlich selbst über die Preisgabe und die Verwendung von personenbezogenen Daten bestimmen können. Ausfluss dieses Rechts ist unter anderem der datenschutzrechtliche Grundsatz des Verbots mit Erlaubnisvorbehalt, wonach die Verarbeitung und auch die Speicherung personenbezogener Daten lediglich dann zulässig ist, wenn hierfür ein Rechtsgrund besteht. Daraus folgt, dass diese Daten nicht pauschal für unbestimmte Zeit gespeichert und verwendet werden dürfen, sondern nach Wegfall des Rechtsgrundes gelöscht werden müssen. Angesichts der immensen Datenmengen, die in der heutigen Zeit verarbeitet werden, ist es für Unternehmen, Vereine und sonstige Gesellschaften unumgänglich, eine konzeptionelle Grundlage für die Löschung von Daten zu schaffen. Dieses Konzept soll eine solche konzeptionelle Grundlage bieten, indem es eine exemplarische Übersicht über die bestehenden gesetzlichen Aufbewahrungsfristen gibt und gleichzeitig Vorgaben für die Umsetzung der Löschung von personenbezogenen Daten definiert.

2. Allgemeines

Da die Löschung von personenbezogenen Daten aus Effizienzgründen nicht in jedem Einzelfall individuell rechtlich geprüft werden kann, ist es sinnvoll, eine Standardisierung der Datenlöschung zu erreichen. Entsprechend richtet sich das nachfolgende Konzept nach den Vorgaben der DIN-Norm 66398 „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“, die dem Prinzip folgt, dass diverse sogenannte Standardlöschfristen definiert werden, denen sodann die einzelnen Datenarten entsprechend zugeordnet werden können. Dieses Vorgehen kann zur Folge haben, dass die Löschung nicht in jedem Einzelfall unverzüglich nach Zweckerreichung erfolgt, sondern gegebenenfalls erst nach einer gewissen Umsetzungsfrist. Jedoch ist zu berücksichtigen, dass nur durch eine Standardisierung der Löschprozesse sichergestellt werden kann, dass die Löschung dauerhaft und zuverlässig über die gesamte IT-Landschaft hinweg durchgeführt wird und sämtliche Daten von der Löschung erfasst werden, sodass geringfügige Verzögerungen bei der Löschung in Kauf genommen werden müssen.

3. Anwendungsbereich

Dieses Konzept gilt für sämtliche Daten in Systemen und auf Dokumenten, die bei BeWo Durchblick im Rahmen einer elektronischen Verarbeitung vorgehalten werden. Es gilt darüber hinaus auch für sämtliche Personaldaten, selbst wenn diese keiner elektronischen Verarbeitung unterliegen.
Ausdrücklich ausgenommen vom Anwendungsbereich dieses Konzepts sind hingegen solche Daten, die sich abseits der Produktivsysteme in Backups sowie in Archivsystemen befinden. Diese Daten werden zur Nachvollziehbarkeit vergangener Geschäftsvorfälle sowie zur Gewährleistung der Systemsicherheit vorgehalten, weshalb das informationelle Selbstbestimmungsrecht der Betroffenen für diese Systeme hinter den legitimen Zwecken der BeWo Durchblick zurücksteht.

4. Definitionen

Die nachfolgenden Definitionen werden diesem Konzept zugrunde gelegt:

Personenbezogene Daten

Als personenbezogene Daten gelten 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.

Löschen
Daten gelten als gelöscht im Sinne dieses Konzepts, wenn sie in einer solchen Art verändert werden, dass sie nach dem Vorgang nicht mehr vorhanden oder unkenntlich sind und nicht mehr verwendet werden können.

Einschränkung der Verarbeitung
Unter Verarbeitungseinschränkung im Sinne dieses Konzepts wird die Markierung mit dem Ziel, die künftige Verarbeitung einzuschränken, verstanden. Die Einschränkung kann durch Übertragung der Daten auf ein Parallelsystem geschehen. Entscheidend ist dabei, dass die Daten von der produktiven Nutzung ausgenommen werden können.

5. Grundsatz der Verarbeitung
Für den Umgang mit personenbezogenen Daten gilt stets der sogenannte Zweckbindungsgrundsatz. Diesem Grundsatz zufolge dürfen Daten immer nur für einen bestimmten, vorab festzulegenden Zweck verarbeitet werden, da sämtliche datenschutzrechtlichen Erlaubnistatbestände sich stets nur auf einen bestimmten Verarbeitungszweck beziehen. Ist dieser Zweck erreicht beziehungsweise weggefallen, sind die Daten entsprechend des Gebots der Datensparsamkeit unverzüglich zu löschen, da in diesem Fall keine Rechtsgrundlage für die Verarbeitung mehr besteht. Eine Ausnahme besteht lediglich in den beiden folgenden Fällen:

Es besteht eine gesetzliche, vertragliche oder satzungsmäßige Aufbewahrungsfrist, die fordert, dass die Daten für einen bestimmten Zeitraum vorzuhalten sind, oder es liegt eine Einwilligung des Betroffenen vor, die die weitere Aufbewahrung nach Erreichung des Hauptzweckes explizit gestattet (zum Beispiel das Vorhalten von Bewerbungsunterlagen für künftige Stellenausschreibungen). In diesen Fällen kann von einer Löschung nach Zweckerreichung abgesehen werden.

6. Aufbewahrungsfristen
Aus Gründen der Prüfbarkeit und Nachvollziehbarkeit vergangener Geschäftstätigkeiten hat der Gesetzgeber eine Reihe von gesetzlichen Aufbewahrungsfristen definiert. Diese Aufbewahrungsfristen legen jeweils einen bestimmten Zeitraum fest, innerhalb dessen die Daten vorgehalten werden müssen, auch wenn sie für den laufenden Geschäftsbetrieb nicht mehr benötigt werden. Diese Aufbewahrungsfristen verfolgen das Ziel, vergangene Geschäftsvorfälle auch im Nachhinein noch nachvollziehen oder prüfen zu können, beispielsweise zur steuerlichen Veranlagung. Da diese Aufbewahrungsfristen in vielen verschiedenen Gesetzen, Verordnungen oder anderen statuiert sind, werden wichtige Aufbewahrungsfristen nachfolgend kurz exemplarisch dargestellt.

6.1 Handelsgesetzbuch (HGB)
Das Handelsgesetzbuch gibt in § 257 HGB zwei unterschiedliche Fristen vor. Für Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Einzelabschlüsse nach § 325 Abs. 2a HGB, Lageberichte, Konzernabschlüsse, Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen und für Buchungsbelege nach § 238 Abs. 1 HGB gilt eine Frist von zehn Jahren, für empfangene Handelsbriefe sowie die Wiedergaben der Abgesandten Handelsbriefe gelten sechs Jahre. Der Beginn der jeweiligen Frist richtet sich nach §257 Abs. 5 HGB und beginnt demnach mit dem Schluss des Kalenderjahres, in dem die letzte Eintragung ins Handelsbuch gemacht, das Inventar aufgestellt, die Eröffnungsbilanz oder der Jahresabschluss festgestellt, der Einzelabschluss nach § 325 Abs. 2a HGB oder der Konzernabschluss aufgestellt, der Handelsbrief empfangen oder abgesandt worden oder der Buchungsbeleg entstanden ist.

6.2 Abgabenordnung (AO)
Im Bereich des Steuerrechts regelt § 147 AO ebenfalls verschiedene Aufbewahrungsfristen. Die AO gilt für sämtliche Steuerschuldner. Die Aufbewahrungsfrist für Bücher und Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, die Eröffnungsbilanz sowie deren zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen, Buchungsbelege sowie Unterlagen nach Artikel 15 Abs. 1 und Artikel 163 des Zollkodexes der Union beträgt zehn Jahre analog zum HGB. Die

Aufbewahrungsfrist für die empfangenen Handels- und Geschäftsbriefe sowie Wiedergaben der abgesandten Handels- und Geschäftsbriefe und sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind, beträgt sechs Jahre. Aufbewahrungsfristen für steuerrelevante Unterlagen können erst ablaufen, wenn die Festsetzungsfrist für die entsprechende Steuer abgelaufen ist. Die Frist beginnt mit Beendigung der Geschäftsbeziehung.

6.3 Bürgerliches Gesetzbuch (BGB)

Das Bürgerliche Gesetzbuch enthält zwar keine gesetzlichen Aufbewahrungsfristen, jedoch sind dort diverse Verjährungsfristen festgelegt. Der Ablauf einer Verjährungsfrist bewirkt, dass ein rechtlicher Anspruch nicht mehr durchsetzbar ist. Hieraus kann das berechtigte Interesse des „Verantwortlichen“ (BeWo Durchblick) abgeleitet werden, Daten bis zum Ablauf dieser Frist aufzubewahren, um sich gegen möglicherweise noch auftretende Rechtsstreitigkeiten zu verteidigen. Neben den Aufbewahrungsfristen können daher auch Verjährungsfristen bei der Erstellung eines Löschkonzepts berücksichtigt werden. Die Regelverjährungsfrist beträgt grundsätzlich drei Jahre; gegebenenfalls besteht auch eine zehn- oder dreißigjährige Verjährungsfrist.

Verwendete Standardlöschfristen

In der Praxis ist es kaum möglich, für jedes gespeicherte Datum die zugehörige Aufbewahrungsdauer und somit auch den konkreten Löschzeitpunkt individuell zu definieren. Dies liegt zum einen an der Vielzahl der gesetzlich vorgeschriebenen Aufbewahrungsfristen, die noch dazu jeweils einen individuellen Fristbeginn haben. Zum anderen fordert der Datenschutz eine Löschung der Daten nach Zweckerreichung, sofern keine gesetzliche Aufbewahrungsfrist besteht. Wann der mit der jeweiligen Verarbeitung verfolgte Zweck erreicht ist, kann allerdings ebenfalls von einer Vielzahl verschiedener Gesichtspunkte abhängen. Dies lässt sich am Beispiel von Interessentendaten illustrieren. Lehnt ein Interessent ein von BeWo Durchblick erstelltes individuelles Angebot ab, sind die Daten unmittelbar nach der Absage zu löschen. Unterbleibt hingegen eine Rückmeldung des Interessenten, ist für den Zeitpunkt des Zweckfortfalls abzuwägen, ab welchem Zeitpunkt nicht mehr mit einer Rückmeldung des Interessenten zu rechnen ist.

Um dieser Vielzahl an verschiedenen Löschanforderungen Herr zu werden, werden von BeWo Durchblick sogenannte Standardlöschfristen bestimmt. Dies sind von BeWo Durchblick festgelegte Fristen, die sowohl aus gesetzlichen als auch betrieblichen Anforderungen abgeleitet wurden, und dazu dienen, die unzähligen Löschanforderungen auf ein handhabbares Maß zu reduzieren. Hierbei ist darauf zu achten, dass die festgelegten Standardlöschfristen eine praktikable Anzahl nicht übersteigen, andererseits aber für jede gesetzliche Löschanforderung eine Standardlöschfrist besteht, die der gesetzlich vorgegebenen Frist in etwa entspricht.

Ziel ist es, eine Standardisierung der Löschprozesse in der Form zu erreichen, dass sämtliche Daten von BeWo Durchblick einer der nachfolgend definierten Standardlöschfristen zugeordnet werden, sodass für jedes Datum ein konkreter Löschzeitpunk definiert wird.

Eine Standardlöschfrist setzt sich unter anderem aus gesetzlicher Aufbewahrungsfrist und dem Zeitraum für die Umsetzung der Löschung zusammen.

Folgende Standardlöschfrist wird bei BeWo Durchblick genutzt:

Standardlöschfrist
11 Jahre

Bei der Festlegung der Standardlöschfristen ist der Tatsache Rechnung zu tragen, dass gesetzliche Fristen oftmals einen starren Fristbeginn haben. So beginnt beispielsweise die Aufbewahrungsfrist nach § 147 AO stets mit dem Schluss des Jahres, in dem die letzte Veränderung in den Büchern getätigt wurde, unabhängig davon, ob diese Änderung am Anfang, in der Mitte oder gegen Ende des Jahres vorgenommen wurde. Die Aufbewahrungsfrist von zehn Jahren kann also wegen des starren Fristbeginns mitunter auch zehn Jahre und

364 Tage betragen, sofern ein Datum am 01.01. gespeichert wurde. Aus diesem Grunde ist es sinnvoll, die Standardlöschfrist insoweit pauschal auf elf Jahre festzulegen, da nur so eine Unterschreitung der gesetzlichen Vorgabe ausgeschlossen werden kann.

Verwendete Datenarten

Aus Effizienzgründen ist es nicht sinnvoll, jedes einzelne Datenfeld gesondert einer der obigen Standardlöschfristen zuzuordnen. Denn der Löschzeitpunkt von personenbezogenen Daten hängt im Regelfall von deren Verwendungszweck ab. So gestattet der Datenschutz die Nutzung von Daten grundsätzlich jedenfalls so lange, wie dies zur Erfüllung eines legitimen Zwecks erforderlich ist. Daher sind die bei BeWo Durchblick genutzten Daten entsprechend ihres Verwendungszwecks zu typisieren und zu gruppieren. Sämtliche Einzeldaten sind somit einer der nachfolgenden Datenarten zuzuordnen. Die Datenarten werden jeweils einer bestimmten Standardlöschfrist zugeordnet.

Folgende Datenarten werden bei BeWo Durchblick definiert:

Datenart	Beschreibung	Beispiele
Bewerberdaten	Daten, die im Rahmen des Bewerbungsprozesses über Bewerber*innen erhoben werden	Lebenslauf, Motivationsschreiben, Zeugnisse etc.
Kundenstammdaten	Stammdaten von Leistungsberechtigten	Name, Adresse, Kontaktdaten, Telefonnummer, E-Mail-Adresse
Kundeninhaltsdaten	Sensible Daten von Leistungs-berechtigten, die über Stammdaten hinausgehen.	Diagnosen, finanzielle Situation, Ärzt*innen etc.
Personalstammdaten	Stammdaten über das Personal	Name, Adresse, Kontaktdaten, Personalnummer
Personalinhaltsdaten	Personaldaten, die über Stammdaten hinausgehen, wie z. B. die Inhalte der Personalakte	Beurteilungen, Zeugnisse, Abmahnungen, Bescheinigungen
Authentifikationsdaten	Daten, die zur Anmeldung und Authentifikation an IT-Systemen genutzt werden	Benutzerkennungen, biometrische Zugangsdaten, Passwörter
Interessentendaten	Stamm- und Inhaltsdaten von Interessierten, mit denen es nicht zum Geschäftsabschluss kommt	Name, Adresse, Kontaktdaten, Angebote, Unterlagen über persönliche Verhältnisse
Kontoauszugsdaten	Daten über laufende Kontostände und Kontobewegungen	Kontoauszüge, Kontomitteilungen, Kontoeröffnungsanträge
Fachliche Protokolldaten / Logdaten	Fachliche Protokollierungen, die zum Nachweis von Geschäftsvorfällen dienen	Dokumentation von Assistenzleistungen etc.
E-Mails	Elektronische Geschäftsbriefe	Mails mit Kostenträgern, sonstigen Personen, Einrichtungen etc.
Technische Hilfsdaten	Daten, die zur Übertragung in andere Systeme benötigt werden, sollen nach Übertragung gelöscht werden.	
Legitimationsdaten	Daten, die zur Legitimation von Kunden erhoben werden	Ausweiskopien

Zuordnung der Datenarten zu den Standardlöschfristen
Die genannten Datenarten sind anschließend den unter 7. definierten Standardlöschfristen zuzuordnen. Hierbei ist darauf zu achten, wann genau eine Löschfrist zu laufen beginnt. So kommen in der Praxis durchaus unterschiedliche Startzeitpunkte für den Anlauf der Standardlöschfristen in Betracht, es ist nicht zwangsläufig stets auf die Erhebung der Daten abzustellen. Insbesondere bei bestehenden Dauerschuldverhältnissen wäre es nicht sinnvoll, die Kundenstammdaten fortwährend zehn Jahre nach Erhebung zu löschen. Hier ist somit ein anderer Zeitpunkt für den Anlauf der Löschfrist notwendig, nämlich das Ende der Geschäftsbeziehung.

Um an dieser Stelle eine Standardisierung zu erreichen, werden die nachfolgenden Ereignisse als einzig mögliche Anknüpfungspunkte für den Fristbeginn definiert.

Startzeitpunkt	Beschreibung
Datenerhebung	Zeitpunkt, in dem die Daten vom Verantwortlichen (BeWo Durchblick) erstmals erhoben werden. Im Regelfall fällt dieser Zeitpunkt mit der Speicherung zusammen.
Ende eines Vorgangs	Hier wird auf das Ende eines speziellen Vorgangs abgestellt, beispielsweise die Kündigung eines einzelnen Geldanlageprodukts.
Ende der Beziehung	Dieser Zeitpunkt bezieht sich auf das Ende der gesamten Beziehung, beispielsweise in Form der Kündigung eines Mitarbeiters oder der Aufkündigung der gesamten Geschäftsbeziehung durch einen Kunden.

Durch Zuordnung der Datenarten zu den jeweiligen Standardlöschfristen sowie der Zugrundelegung des richtigen Fristbeginns ergibt sich sodann ein konkretes Datum, an dem die Daten tatsächlich gelöscht werden müssen.

Löschen in Sondersituationen
In manchen Fällen kann der Bedarf bestehen, von den Standardlöschfristen abzuweichen. Dies liegt unter anderem daran, dass es sich bei den Standardlöschfristen um abstrakte Regeln handelt, deren Zweck es ist, die praktische Umsetzung der rechtlichen Anforderungen zu erleichtern. Naturgemäß können abstrakte Löschregeln nicht alle Sondersituationen abdecken, die im Rahmen der Datenverarbeitungsprozesse vorkommen. Daher gelten im Einzelfall die nachfolgenden Regeln für die Abweichung.

Unterschreiten der Löschfristen
Im Falle der geplanten Unterschreitung der Standardlöschfristen ist vorab zu prüfen, ob durch die vorzeitige Löschung möglicherweise gesetzliche Aufbewahrungsfristen verletzt werden. Sofern dies der Fall wäre, dürfen die Daten nicht gelöscht werden. Wird die gesetzliche Aufbewahrungsfrist hingegen nicht unterschritten, dürfen die Daten auch vor Ablauf der Standardlöschfrist gelöscht werden.

Abgesehen davon gibt es auch Situationen, in denen eine Unterschreitung der Standardlöschfristen zwingend geboten ist. Dies gilt insbesondere für folgende Situationen:

es liegt ein berechtigtes Löschverlangen des Betroffenen vor;
der Betroffene hat seine Einwilligung, auf deren Basis die Daten verarbeitet wurden, widerrufen;
personenbezogene Daten wurden unberechtigt erhoben und gespeichert;
Außerbetriebnahme eines IT-Systems.

In diesen Fällen ist jeweils eine individuelle Beurteilung des Sachverhalts durch BeWo Durchblick erforderlich, bei der zu entscheiden ist, ob von den Standardlöschfristen abgewichen wird oder nicht.

Überschreiten der Löschfristen

Sollen Löschfristen überschritten werden, so ist grundsätzlich die Vereinbarkeit der Überschreitung mit dem Datenschutz zu prüfen, insbesondere mit dem Gebot der Datensparsamkeit. Daher müssen Überschreitungen stets mit dem Datenschutzbeauftragten bzw. der Geschäftsführerin abgestimmt werden.

Bestehen für einen Datensatz unterschiedliche Vorgaben bezüglich der technischen Löschung (etwa weil der Datensatz verschiedenen Datenkategorien unterfällt), dann gilt die längere Löschfrist für diesen Datensatz.

Einschränkung der Verarbeitung
Gemäß den Regelungen der Datenschutz-Grundverordnung ist die Verarbeitung personenbezogener Daten einzuschränken, wenn die Löschung der Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Durch die Verarbeitungseinschränkung soll dem Grundsatz der Datensparsamkeit Rechnung getragen werden. Dies kann wahlweise durch das Setzen einer Markierung oder sonstigen Hervorhebung geschehen, die Auskunft darüber gibt, dass die Daten fortan von der produktiven Verarbeitung ausgenommen sind. Zudem ist darauf zu achten, dass die Zugriffsberechtigungen auf die gesperrten Daten entsprechend auf das notwendige Maß beschränkt werden, sofern dies innerhalb der technischen Möglichkeiten liegt.

Anonymisierung
Anstelle einer Löschung von Daten können diese auch anonymisiert werden. Hierdurch entfällt der Personenbezug und die Daten unterfallen nicht länger den datenschutzrechtlichen Vorgaben. Das vorliegende Löschkonzept findet auf anonymisierte Daten keine Anwendung.

Durchführung von Löschläufen
Die Durchführung von Löschläufen soll nach Möglichkeit in automatisierter und standardisierter Form erfolgen. Sofern Löschläufe nicht routinemäßig gefahren werden, ist die jeweilige Fachabteilung für die Initiierung zuständig. Diese hat sodann eigenständig dafür Sorge zu tragen, dass regelmäßige (manuelle) Datenlöschungen stattfinden.

Um Schäden durch ungewollten Datenverlust vorzubeugen, sind die automatisierten und auch manuell angestoßenen Löschläufe stets durch den jeweiligen Anwendungseigentümer (falls vorhanden ggf. auch Dateneigentümer) „Owner“ zu genehmigen. Sofern Zweifel bestehen, ob eine Datenlöschung rechtmäßig ist oder eine gesetzliche Löschpflicht besteht, kann der Datenschutzbeauftragte als beratende Instanz hinzugezogen werden.

Datenhaltung bei Dienstleistern
In vielen Fällen sind Systeme externer Dienstleister in die Datenverarbeitung eingebunden. Hierbei ist zu beachten, dass auch im Falle einer Auftragsverarbeitung BeWo Durchblick weiterhin der für die Datenverarbeitung „Verantwortliche“ ist: Sie hat damit auch für die fristgerechte Löschung der Daten Sorge zu tragen – unabhängig davon, ob die Daten unternehmensintern oder auf den Systemen des Dienstleisters gespeichert sind. Dies kann beispielsweise dadurch geschehen, dass sich der Dienstleister vertraglich verpflichtet, die von BeWo Durchblick definierten Löschfristen umzusetzen. Hat ein Dienstleister über ein eigenes Löschkonzept Löschroutinen festgelegt, muss BeWo Durchblick die Rechtmäßigkeit und Angemessenheit der Löschfristen prüfen, wobei insbesondere bestehende gesetzliche Aufbewahrungsfristen zu berücksichtigen sind. Soll die Löschung durch den Dienstleister erfolgen, sind zudem entsprechende Regelungen in den Auftragsverarbeitungsvertrag aufzunehmen, um eine Verbindlichkeit der Löschregelungen zu erreichen.

11. Richtlinie Betroffenenrechte

Einleitung

Die Datenschutz-Grundverordnung (DSGVO) sieht in den Art. 12 ff. DSGVO Rechte der von einer Verarbeitung personenbezogener Daten betroffenen Personen vor, die von BeWo Durchblick einzuhalten sind. Dies bedarf der Umsetzung von Maßnahmen bei BeWo Durchblick.

Geltungsbereich

Diese Richtlinie gilt für alle Standorte von BeWo Durchblick.
Diese Richtlinie verpflichtet alle Beschäftigten von BeWo Durchblick zur Einhaltung der hier festgelegten Pflichten und Vorgaben.

Ziele

Diese Richtlinie soll dazu beitragen, dass die Rechtsvorschriften für die Wahrung der Rechte der betroffenen Personen eingehalten werden.

Informationspflichten

Die Geschäftsführerin trägt Sorge dafür, dass für jede Verarbeitung seitens der „Owner/Eigentümer“ der Verarbeitung Sorge dafür getragen wurde, dass Datenschutzinformationen für die betroffenen Personen im erforderlichen Umfang vorliegen und auch den betroffenen Personen in geeigneter Weise zur Verfügung gestellt werden. Die Informationen sind auch bei Änderungen der Verarbeitung auf ihre Aktualität vom „Owner/Eigentümer“ zu prüfen.
Art und Umfang der Informationserteilung sind mit der Geschäftsführerin abzusprechen.

Rechte auf Auskunft, Löschung, Widerspruch und weitere Betroffenenrechte aus den Art. 15-22 DSGVO

Jede Person kann seine*ihre Betroffenenrechte nach den Art. 15-22 DSGVO gegenüber BeWo Durchblick geltend machen.
Dies beinhaltet insbesondere das Recht auf **Auskunft, Berichtigung und Löschung** von personenbezogenen Daten sowie einen **Widerspruch** gegen die Verarbeitung von Daten (z.B. auch gegen die Verwendung von Daten für Werbezwecke).
Alle Beschäftigten von BeWo Durchblick sind verpflichtet, einen von einem Betroffenen geltend gemachten Anspruch auf Auskunft, Berichtigung, Löschung oder einen Widerspruch unverzüglich nach Zugang der Mitteilung an die Geschäftsführerin weiterzuleiten.
Die Geschäftsführerin wird die Anfrage dokumentieren und unverzüglich, spätestens aber binnen eines Monats nach Eingang der Mitteilung des Betroffenen bei BeWo Durchblick gegenüber dem Betroffenen beantworten.
Die Geschäftsführerin hat bei der Beantwortung von Anfragen von Betroffenen sicherzustellen, dass vor der Erteilung von Informationen an Betroffenen sichergestellt wurde, dass die Person diejenige ist, für die sie sich ausgibt, um zu verhindern, dass personenbezogene Daten an Unbefugte gelangen. Im Fall einer Auskunftserteilung per E-Mail ist von dem Betroffenen vorab die Zustimmung einzuholen, dass die Informationen per E-Mail zur Verfügung gestellt werden. Bei Fehlen einer Zustimmung ist die Auskunft schriftlich zu erteilen.

Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

12. Richtlinie Datenschutz (für Beschäftigte)

Einleitung

Bei BeWo Durchblick werden personenbezogene Daten verarbeitet. BeWo Durchblick ist gesetzlich verpflichtet, personenbezogene Daten unter Einhaltung der jeweils geltenden datenschutzrechtlichen Vorschriften einzuhalten.
Einschlägige Rechtsvorschriften sind dabei die Datenschutz-Grundverordnung (DSGVO), das Bundesdatenschutzgesetz sowie ggf. bereichsspezifische Rechtsvorschriften.
Jeder Geschäftsprozess, der mit einer Verarbeitung personenbezogener Daten einhergeht, ist von BeWo Durchblick auf die Einhaltung der rechtlichen Vorgaben zu prüfen.
Zudem ist die Geschäftsführerin von BeWo Durchblick für die Überprüfung der Einhaltung der gesetzlichen Aufgaben zuständig.
Um eine rechtskonforme Verarbeitung von personenbezogenen Daten zu gewährleisten, sind auch grundsätzliche Verhaltensanweisungen für die Beschäftigten erforderlich.
Diese sind Gegenstand dieser Richtlinie. Die Verhaltensanweisungen dieser Richtlinie können durch spezifische Anweisungen für den Umgang mit personenbezogenen Daten in besonderen Fällen (z.B. in spezifischen Projekten) ergänzt oder konkretisiert werden.

Geltungsbereich

Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten durch Beschäftigte von BeWo Durchblick.
Diese Richtlinie gilt für alle Standorte von BeWo Durchblick.
Diese Richtlinie verpflichtet alle Beschäftigten von BeWo Durchblick zur Einhaltung der hier festgelegten Pflichten und Vorgaben.

Ziele

Diese Richtlinie soll dazu beitragen, dass die Rechtsvorschriften zur Verarbeitung personenbezogener Daten eingehalten werden.

Grundsätze für den Umgang mit personenbezogenen Daten

Die nachfolgenden Grundsätze sind von allen **Beschäftigten** von BeWo Durchblick einzuhalten:
Personenbezogene Daten werden nicht eigenmächtig verarbeitet. Es wird ausschließlich die von BeWo Durchblick bereitgestellte oder genehmigte Software genutzt. Private Hardware kann bei Einhaltung entsprechender Sicherheitsvorkehrungen (siehe IT-Richtlinie für Nutzer*innen in diesem Konzept) genutzt werden.
Sollten zusätzliche Verarbeitungsprozesse für die Geschäftsprozesse erforderlich werden, werden diese beim Vorgesetzten gemeldet. Der Vorgesetzte wird die Erforderlichkeit prüfen. Im Falle einer Erforderlichkeit wird der Vorgesetzte den gewünschten Verarbeitungsprozess prüfen und ggf. freigeben. Beschäftigte der BeWo Durchblick sind verpflichtet, alle sie oder ihre Tätigkeit betreffenden Richtlinienvorgaben oder Anweisungen im Umgang mit personenbezogenen Daten einzuhalten. Dies gilt insbesondere für Vorgaben, die die Sicherheit personenbezogener Daten betreffen.
Beschäftigte melden mögliche Datenschutzvorfälle unverzüglich an die Geschäftsführerin.

Ausnahmen

BeWo Durchblick kann Ausnahmen von den unter Ziff. 4 genannten Grundsätzen in begründeten Einzelfällen erlauben. Ausnahmen sind von der Geschäftsführerin zu prüfen. Genehmigte Ausnahmen sind inklusive einer Begründung zu dokumentieren.

Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

13. Richtlinie Datenschutzmaßnahmen

Einleitung

Bei BeWo Durchblick werden personenbezogene Daten verarbeitet. BeWo Durchblick ist gesetzlich verpflichtet, personenbezogene Daten unter Einhaltung der jeweils geltenden datenschutzrechtlichen Vorschriften zu verarbeiten.
Einschlägige Rechtsvorschriften sind dabei die Datenschutz-Grundverordnung (DSGVO), das Bundesdatenschutzgesetz sowie ggf. bereichsspezifische Rechtsvorschriften.
Jeder Geschäftsprozess, der mit der Verarbeitung personenbezogener Daten einhergeht, ist von BeWo Durchblick auf die Einhaltung der rechtlichen Vorgaben zu prüfen.
Zudem ist die Geschäftsführerin für die Überprüfung der Einhaltung der gesetzlichen Aufgaben zuständig.
Um die Rechtskonformität von Datenverarbeitungen im Unternehmen zu gewährleisten, macht BeWo Durchblick durch diese Richtlinie Vorgaben für die Einrichtung und Durchführung von Datenverarbeitungsprozessen.

Geltungsbereich

Diese Richtlinie gilt für die Beschäftigten, die für die Einrichtung oder Durchführung von Verarbeitungen personenbezogener Daten bei BeWo Durchblick oder für eine Verarbeitung selbst als „Owner“/Eigentümer” verantwortlich sind.
Diese Richtlinie gilt für alle Standorte von BeWo Durchblick.

Ziele

Diese Richtlinie soll dazu beitragen, dass die Rechtsvorschriften zur Verarbeitung personenbezogener Daten eingehalten werden.

Grundsätze für die Einrichtung oder Änderung von Verarbeitungen personenbezogener Daten

Bei der Verarbeitung personenbezogener Daten und auch bei der Einrichtung oder Änderung von den damit zusammenhängenden Prozessen sind folgende Grundsätze der Datenverarbeitung i.S.d. Art. 5 DSGVO einzuhalten:

Personenbezogene Daten müssen

1 auf Basis einer Rechtsgrundlage oder Einwilligung, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
2 für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“);

3 dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
4 sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
5 in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung“);
6 in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);
7 für jeden Geschäftsprozess, der die Verarbeitung personenbezogener Daten beinhaltet, muss es einen Verantwortlichen bei BeWo Durchblick geben („Owner/Eigentümer“);

Bei Fragen zur Anwendung und Auslegung dieser Grundsätze kann sich jede*r Beschäftige an die Geschäftsführerin wenden.

Ausnahmen

BeWo Durchblick kann Ausnahmen von den unter Ziff. 4 genannten Grundsätzen in begründeten Fällen erlauben. Ausnahmen sind mit der Geschäftsführung abzustimmen und von ihr zu prüfen. Genehmigte Ausnahmen sind inklusive einer Begründung zu dokumentieren.

Schulungsmaßnahmen

Alle Beschäftigten von BeWo Durchblick sind zeitnah nach Beginn der Aufnahme ihrer Tätigkeit für BeWo Durchblick und sodann regelmäßig (mindestens jährlich) in Datenschutzschulungen mit den Rechtsvorschriften zur Verarbeitung personenbezogener Daten vertraut zu machen.
Alle Beschäftigten, die für die Einrichtung oder Durchführung von Verarbeitungen personenbezogener Daten bei BeWo Durchblick verantwortlich sind, tragen Sorge dafür, dass alle Beschäftigten, die über diese Verarbeitungen Zugang zu personenbezogenen Daten haben, zuvor zum Datenschutz geschult wurden.

Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

14. Richtlinie „Meldung von Verstößen gegen Datenschutz und Datensicherheit gemäß Art. 33 und Art. 34 DSGVO“

Einleitung

BeWo Durchblick beachtet die gesetzlichen Vorschriften zur Sicherheit der Verarbeitung von personenbezogenen Daten. Das schließt alle Formen der bei BeWo Durchblick praktizierten oder durch Auslagerung bei Dienstleistern durchgeführten Datenverarbeitungen ein. Datenpannen werden ausnahmslos bewertet und – falls ein meldepflichtiger Sachverhalt festgestellt wird – der zuständigen Datenschutzaufsichtsbehörde sowie dem Betroffenen – insoweit diese Datenpanne ein hohes Risiko für dessen persönliche Rechte und Freiheiten zur Folge hat – gemäß Art. 33 und Art. 34 DSGVO gemeldet.

Geltungsbereich

Diese Richtlinie gilt für alle Standorte von BeWo Durchblick.
Diese Richtlinie verpflichtet alle Beschäftigten von BeWo Durchblick zur Einhaltung der hier festgelegten Pflichten und Vorgaben.

Ziele

Diese Richtlinie soll dazu beitragen, dass die Rechtsvorschriften für die Meldung von Datenpannen sowie die Wahrung der Rechte der betroffenen Personen eingehalten werden.

Bestimmungen zur Meldepflicht

Vermutete oder erwiesene Verstöße gegen Datensicherheit und Datenschutz („Datenpannen“) bei BeWo Durchblick sind meldepflichtig gemäß den nachfolgenden Bestimmungen:

1 Die interne Meldepflicht wird für diejenigen Mitarbeitenden ausgelöst, die in ihrem Arbeitsbereich auf eine vermutete oder erwiesene „Datenpanne“ stoßen oder hingewiesen werden. Mitarbeitende melden derartige Beobachtungen sofort ohne zeitliche Verzögerung der Geschäftsführung, die nach den nachfolgenden Bestimmungen verfährt.
2 Die hier festgelegte Meldepflicht bezieht sich auf interne Informationspflichten und deren Wege; die Entscheidung, inwieweit dann eine Offenlegung nach außen geboten beziehungsweise rechtlich vorgeschrieben ist, obliegt gemäß Ziffer 8 der Geschäftsführung. Sofern eine Datenpanne an die zuständige Aufsichtsbehörde (https://www.ldi.nrw.de/) gemeldet werden muss, ist diese Meldung unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, zu machen. Erfolgt die Meldung an die Aufsichtsbehörde später als nach 72 Stunden, so ist eine Begründung für die Verzögerung beizufügen. Vor Abgabe einer Meldung ist zu prüfen, ob die zuständige Aufsichtsbehörde Vorgaben zum Meldeweg (Onlineformular, Briefpost, Telefax, Email) macht.

Datenpannen

Als „Datenpannen“ werden alle schädlichen Ereignisse bei der Datenverarbeitung angesehen, die vom Datenschutzrecht geschützte personenbezogene Daten, innerhalb von BeWo Durchblick insbesondere Leistungsberechtigten- und Mitarbeiterdaten, sowie solche personenbezogene Daten betreffen, die im Auftrag verarbeitet werden. Namentlich sind als „Datenpannen“ definiert:

1 Formen bewusster oder unbewusster, unbefugter oder rechtswidriger Verarbeitung personenbezogener Daten.
2 Unbefugte Aktivitäten zur Umgehung von Sicherheitsvorkehrungen, die dem Schutz personenbezogener Daten dienen.
3 Angriffe auf die IT-Infrastruktur von BeWo Durchblick, die vermutlich oder offensichtlich erfolgreich waren.

Unter „Verarbeitung von Daten“ ist hier zu verstehen: 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.

Wahrnehmung von Datenpannen

Datenpannen können unterschiedlich wahrgenommen werden. Zu unterscheiden ist zwischen:

Internen Datenpannen:

1 Alarme aufgrund von Warnmechanismen
2 Anomalien in der Erhebung, Verarbeitung und Nutzung personenbezogener Daten
3 Erkenntnisse aus dem Feedbackmanagement
4 Erkenntnisse aus Prüfungen
5 Erkenntnisse aus Mitarbeitendengesprächen

1 Externen Datenpannen:

1.1 Hinweise Dritter (zum Beispiel LB, Dienstleistende und Behörden)
1.2 Medienberichte
1.3 Polizeiliche Anzeigen

Berichtswege und interne Abstimmung

Mitarbeitende, die eine tatsächliche oder vermutete Datenpanne wahrnehmen, informieren sofort ohne zeitliche Verzögerung die Geschäftsführerin.

Weiteres Vorgehen

Über das weitere Vorgehen entscheidet die Geschäftsführung.

Mögliche Handlungen können sein:

1. Benachrichtigung der Aufsichtsbehörde für den Datenschutz,
2. Personelle Maßnahmen,
3. Beendigung der Zusammenarbeit mit einem betroffenen Unternehmen,
4. Geltendmachung von Haftungsansprüchen,
5. Strafanzeige,
6. Einzelbenachrichtigung der von der Datenpanne betroffenen Personen oder
7. Alternativ durch öffentliche Bekanntmachung nach Art. 34 Abs. 3 lit. c
8. Änderungen in bestehenden Verfahren, um Wiederholungen zu verhindern.
9. Sonstige:

Hinweise

Alle Vorkommnisse werden intern und vertraulich behandelt.

Mitarbeitende, die vermutete oder tatsächliche Datenpannen wahrgenommen und gemeldet haben, haben analog zu einem Hinweisgebersystem keine nachteiligen Auswirkungen auf ihr Arbeitsverhältnis zu befürchten.

Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

Protokoll zur internen Bewertung und Dokumentation
Meldung von Verstößen gegen Datenschutz und Datensicherheit gemäß Art. 33, 34 DSGVO

Datum:

Gemeldet von:

Mitarbeiter*in:

Protokoll erstellt von:

 Führungskraft:
 Mitarbeiter*in:

Empfänger:

 Geschäftsführung

1. Name der meldepflichtigen bzw. verantwortlichen Stelle
(Vollständige Bezeichnung inklusive Adresse)

2. Name und Kontaktdaten der Geschäftsführerin oder eines sonstigen Ansprechpartners für weitere Informationen
(Name und Position des Ansprechpartners)

3. Zeitraum oder Zeitpunkt des Vorfalls
(Möglichst „exakte“ Zeitangabe)

4. Zeitpunkt der Feststellung des Vorfalls
(Möglichst „exakte“ Angabe, wann und wie vom Vorfall Kenntnis erlangt wurde)

5. Ursache bzw. Ort der Datenpanne
(Möglichst „exakte“ Sachverhaltsbeschreibung)

6. Welche Dritten haben Kenntnis erlangt bzw. hatten Möglichkeit zur Kenntnisnahme?
(Möglichst „exakte“ Benennung des relevanten Personenkreises)
7. Art und Inhalt der betroffenen personenbezogenen Daten
(Zutreffende ankreuzen)

- □ Besondere Arten von Daten im Sinne von Art. 9 DSGVO
- □ Einem Berufsgeheimnis unterliegende Daten (siehe § 203 Abs. 1 StGB)
- □ Daten zu Straftaten oder Ordnungswidrigkeiten, einschließlich Verdacht darauf
- □ Daten zu BeWo Durchblick- oder Kreditkartenkonten
- □ Angabe (soweit möglich) der Kategorien der betroffenen Daten, der ungefähren Anzahl der betroffenen Personen sowie Erläuterungen:

8. Anzahl der ungefähren betroffenen personenbezogenen Datensätze *(ggf. Schätzung)*

9. Beschreibung der ergriffenen oder vorgeschlagenen (technischen und organisatorischen) Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Folgen, die die meldepflichtige Stelle wegen der Datenpanne in Bezug auf die betroffenen personenbezogenen Daten ergriffen hat (oder ergreifen wird).
(Möglichst „exakte" Beschreibung, was bereits veranlasst wurde und was zu einem späteren Zeitpunkt -wann- noch veranlasst werden soll)
(Zutreffende ankreuzen)

□ Strafanzeige
□ Personelle Maßnahmen
□ Beendigung der Zusammenarbeit mit betroffenem Unternehmen
□ Geltendmachung von Haftungsansprüchen
□ Prüfung / Änderung von bestehenden Verfahren, um Wiederholungen zu vermeiden

Ggf. nähere Erläuterungen hierzu:

10. Mögliche Folgen bzw. nachteilige Auswirkungen für Betroffene (z. B. finanzieller Schaden, Ruf-/Imageschädigung, Bloßstellung)
(Möglichst „exakte" Einschätzung der Folgen bzw. Auswirkungen, die für die Betroffenen durch die Datenpanne drohen können)

11. Benachrichtigung der Betroffenen

□ Benachrichtigung ist bereits erfolgt am _____ (Datum)
per _____ (Kommunikationsmittel)
□ Benachrichtigung ist geplant für _____ (Datum)
per _____ (Kommunikationsmittel)
□ Benachrichtigung ist nicht geplant, da kein hohes Risiko für die Betroffenen besteht

Als Anhang zu diesem Protokoll ist die Benachrichtigung der Aufsichtsbehörde sowie die Benachrichtigung der Betroffenen über die Datenpanne im Originaltext beizulegen beziehungsweise die Begründung(en), warum auf Meldung(en) verzichtet werden konnte.

_____ _____

Datum Unterschrift

15. Richtlinie Berechtigungsmanagement

Einleitung

Bei BeWo Durchblick kommen diverse Anwendungen auf verschiedenen IT-Systemen zum Einsatz. Bei der Einrichtung und Änderung von IT-Systemen und Anwendungen („IT-Ressourcen“) ist zu gewährleisten, dass Anforderungen an die Informationssicherheit und datenschutzrechtliche Vorgaben eingehalten werden. Dies soll auch durch die verbindlichen Vorgaben in dieser Richtlinie zum Berechtigungsmanagement umgesetzt werden. Die Vorgaben dieser Richtlinie sind an das IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI) – insbesondere den Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* – angelehnt.

Geltungsbereich

Diese Richtlinie gilt für alle Standorte von BeWo Durchblick. Sie verpflichtet alle Beschäftigten von BeWo Durchblick zur Einhaltung der hier festgelegten Vorgaben.

Vorgaben für das Berechtigungsmanagement

Grundsätzliche Vorgaben zum Management von Berechtigungen

Die Geschäftsführerin ist verantwortlich, Mitarbeiter*innen bei BeWo Durchblick je nach Tätigkeitsprofil, Rollen in der Software https://app.bewo-durchblick.de/ zuzuweisen, die den Zugriff und die Bearbeitung von Daten regeln. Dies erfolgt im Rahmen des “Least Privilege“-Prinzip. Danach sind dem*der Nutzer*in nur die Rechte zuzuweisen, der für die ihm*ihr zugewiesenen Aufgaben im Unternehmen tatsächlich erforderlich sind.

Regelung für die Änderung und Entzug von Berechtigungen

Bei personellen Veränderungen von Benutzern sind die Berechtigungen von der Geschäftsführerin bzw. dem*der Administrator*in anzupassen. Die Geschäftsführung informiert den*die Administrator*in über personelle Veränderungen, wenn diese Auswirkung auf den tatsächlichen Bedarf von Berechtigungen für Nutzer*innen haben können. Eine Information muss insbesondere erfolgen, wenn ein Benutzer das Unternehmen verlässt.

Regelung des Passwortgebrauchs

Soweit technisch möglich, ist sicherzustellen, dass alle IT-Ressourcen erst nach hinreichender Authentifizierung des Nutzers nutzbar sind. Die Authentifizierung erfolgt in der Regel durch die Verwendung der Kombination Benutzername/Passwort. Soweit möglich oder angeordnet, werden Zwei-Faktor-Authentifizierungs-Systeme verwendet.
Der*die Administrator*in einer IT-Ressource sind verpflichtet, beim Zurücksetzen von Passwörtern sichere Verfahren zur Vergabe von neuen Passwörtern für Benutzer*innen einzusetzen. Ziel ist es, sicherzustellen, dass ein Unbefugter durch eine Passwortzurücksetzung keinen Zugriff auf IT-Ressourcen erhält.
Die Ausgestaltung der konkreten Passwortregelungen finden sich in der „IT-Richtlinie für Nutzer“.

Regelmäßige Aktualisierung („Monitoring“)

Jede*r Verantwortliche ist verpflichtet, in regelmäßigen Abständen – mindestens jedoch einmal jährlich – zu überprüfen, ob die Berechtigungen der Benutzer*innen aktuell noch dem „Least Privilege“-Prinzip entsprechen (danach sind dem*r Nutzer*in nur die Rechte zuzuweisen, die für die ihm*ihr zugewiesenen Aufgaben im Unternehmen tatsächlich erforderlich sind).

Sanktionen

Ein Verstoß gegen diese Richtlinie kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

16. Richtlinie zum Mobilen Arbeiten

1 Einleitung

Sofern Beschäftigten von BeWo Durchblick Mobiles Arbeiten erlaubt wird, sind die Vorgaben aus dieser „Richtlinie zum Mobilen Arbeiten“ für die betreffenden Beschäftigten verbindlich einzuhalten. Verpflichtend ist in jedem Fall zusätzlich die zu unterzeichnende “Vereinbarung für Mitarbeiter*innen zum Mobilen Arbeiten“.
Um eine rechtskonforme Verarbeitung von personenbezogenen Daten beim Mobilen Arbeiten zu gewährleisten, sind neben den allgemeinen Verhaltensanweisungen dieser Richtlinie, der Vereinbarung für Mitarbeiter*innen zum Mobilen Arbeiten auch ergänzende Weisungen durch Vorgesetzte an die Beschäftigten möglich. Auch diesen ist Folge zu leisten.

2 Geltungsbereich

Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten durch Beschäftigte von BeWo Durchblick beim „Mobilen Arbeiten“.
Diese Richtlinie gilt für alle Standorte von BeWo Durchblick.
Diese Richtlinie verpflichtet alle Beschäftigten von BeWo Durchblick zur Einhaltung der hier festgelegten Pflichten und Vorgaben, soweit Verarbeitung personenbezogener Daten beim Mobilen Arbeiten erfolgt.

3 Ziele

Diese Richtlinie soll dazu beitragen, dass die Rechtsvorschriften zur Verarbeitung personenbezogener Daten eingehalten werden und insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten gewährleistet werden kann.

4 Grundsätze für den Umgang mit personenbezogenen Daten

Die nachfolgenden Grundsätze sind von allen Beschäftigten von BeWo Durchblick einzuhalten, die beim Mobilen Arbeiten tätig sind:
Es gelten die Regelungen der Richtlinie “IT-Richtlinie für Nutzer*innen” bezüglich der Nutzung privater Hardware.
Beschäftigte von BeWo Durchblick sind verpflichtet, alle sie oder ihre Tätigkeit betreffenden Richtlinienvorgaben oder Anweisungen im Umgang mit personenbezogenen Daten auch bei der Arbeit beim Mobilen Arbeiten einzuhalten. Dies gilt insbesondere für Vorgaben, die die Sicherheit personenbezogener Daten betreffen.
Beschäftigte melden mögliche Datenschutzvorfälle unverzüglich an die Geschäftsführerin. Ein Datenschutzvorfall liegt insbesondere vor, wenn die Annahme besteht, dass die Datensicherheit,

insbesondere die Vertraulichkeit von Daten, gefährdet sein kann. Ein Datenschutzvorfall liegt auch bei jedem Sachverhalt vor, bei dem die Annahme besteht, dass Dritte unbefugt Zugriff oder Zugang zu personenbezogenen Daten haben oder hatten.

5 Grundsätze der Nutzung von IT-Systemen im „Home-Office“ und beim Mobilen Arbeiten

Die Verarbeitung von personenbezogenen Daten beim Mobilen Arbeiten birgt Risiken für die Integrität, Vertraulichkeit und Verfügbarkeit von Daten in sich. Um diese Risiken auszuschließen oder zu minimieren, sind die nachfolgenden Grundsätze bei der Verarbeitung von personenbezogenen Daten beim Mobilen Arbeiten durch die Beschäftigten einzuhalten.
Vertrauliche Informationen, Zugangskennungen sowie Passwörter, mit denen auf die dienstlichen Datenbestände zugegriffen werden kann, sind so zu schützen, dass Dritte – als Dritte zählen auch Angehörige aus dem persönlichen und familiären Personenkreis – davon keine Kenntnis erlangen können.
Sicherheitsmaßnahmen, -verfahren und Vorrichtungen wie beispielsweise Virenscanner, Firewalls, Anti-Spamfilter und Verschlüsselungsmechanismen sind zu beachten und dürfen nicht abgeschaltet, verändert oder umgangen werden.

Im Hinblick auf die Installation von Software auf den mobilen IT-Systemen gilt die „IT-Richtlinie für Nutzer*innen“.
Die elektronischen Geräte, mit denen ein Zugriff auf das Netzwerk des Unternehmens möglich ist, dürfen keinem Dritten zur Nutzung überlassen werden.

Berufliche E-Mails und Telefonate dürfen nicht auf private Postfächer oder private Telefonanschlüsse / Handys / Smartphones oder ähnliche Geräte um- oder weitergeleitet werden. Sollten vertragliche Vereinbarungen hinsichtlich der Nutzung privater Telefone / Handys / Smartphones mit der Geschäftsführerin getroffen worden sein, muss der*die Mitarbeiter*in dafür Sorge tragen, dass alle in diesem Konzept genannten Sicherheitsvorkehrungen zum Schutz personenbezogener Daten getroffen werden.

Telefonate, in deren Rahmen betriebliche Informationen ausgetauscht werden, sind außerhalb der Hörweite unbefugter Personen zu führen.
Der*Die Mitarbeitende hat sicherzustellen, dass Gespräche oder Telefonate, bei denen betriebliche Informationen ausgetauscht werden, nicht von digitalen Sprachassistenten mitgehört oder beobachtet werden können. Dies auch gilt für Geräte mit Aktivierungswörtern wie beispielsweise Siri (Apple), Google oder Echo (amazon).

Bei mobilen Endgeräten sind nicht benötigte Verbindungen wie WLAN, Bluetooth, RFID und ähnliche grundsätzlich – insbesondere während des Transportes – zu deaktivieren.

Daten sind grundsätzlich nicht auf lokalen Festplatten oder Datenspeichern von Endgeräten zu speichern, die nicht im Eigentum oder Besitz von BeWo Durchblick stehen.

Die Speicherung von Daten hat grundsätzlich gemäß der Richtlinie „Speicherorte“ in den Verzeichnissen/Ordnern von Servern bzw. zentralen IT-Systemen von BeWo Durchblick zu erfolgen, die für den*die Benutzer*in freigegeben sind. Ausnahmen dürfen nur gemacht werden, wenn eine Internet-Anbindung an die zentralen IT-Systeme und damit eine Speicherung auf den IT-Systemen nicht möglich ist. In diesen Fällen dürfen personenbezogene Daten auf den von den Beschäftigten beim Mobilen Arbeiten verwendeten Geräten gespeichert werden, wenn sichergestellt ist, dass die Daten auf den verwendeten Datenträgern sicher gespeichert werden.

Beschäftigte müssen beim Verlassen des Mobilen Arbeitsplatzes unverzüglich eine Bildschirmsperre aktivieren, die nur mit einem Passwort aufgehoben werden kann, das dem Beschäftigten bekannt ist. Unterlagen sind ebenfalls vor unbefugtem Zugriff zu schützen.

Dokumente sollten grundsätzlich nicht beim Mobilen Arbeiten ausgedruckt werden. Sollte dies für die Erledigung von betriebsbedingten Aufgaben zwingend erforderlich sein, hat der Beschäftigte Sorge dafür zu tragen, dass die ausgedruckten Informationen auch direkt vor Ort geeignet vernichtet werden können.
Besonders schutzbedürftige Informationen sollten nach Möglichkeit nur beim Mobilen Arbeiten verarbeitet werden, die von Dritten nicht einzusehen sind.
Sollte dies nicht möglich sein, muss der*die Nutzer*in einen Ort bzw. Platz zur Verarbeitung von Daten wählen, der gewährleistet, dass der Bildschirm nicht von Dritten eingesehen werden kann.
Bei der elektronischen Datenübertragung sind die vom Unternehmen vorgegebenen Sicherheitsmaßnahmen zu beachten. Beim herkömmlichen Transport der Informationen ist auf die Benutzung verschließbarer Behältnisse zu achten.

6 Datensicherung

Der*die Nutzer*in hat Sorge dafür zu tragen, dass Daten, die ausschließlich auf dem Gerät gespeichert werden, bei nächster Gelegenheit auf Datenspeicher übertragen werden, die von BeWo Durchblick üblicherweise für die Speicherung von Unternehmensdaten verwendet werden.
Bei Fragen zur Vorgehensweise der Übertragung der Daten hat sich der Nutzer an die IT-Abteilung/Geschäftsführung zu wenden.

7 Ausnahmen

BeWo Durchblick kann Ausnahmen von den vorher genannten Grundsätzen in begründeten Einzelfällen erlauben. Genehmigte Ausnahmen sind inklusive einer Begründung zu dokumentieren.

8 Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

Datenschutzhinweise für Leistungsberechtigte und andere Betroffene

Mit den folgenden Informationen möchten wir Ihnen einen Überblick über die Verarbeitung Ihrer personenbezogenen Daten durch uns und Ihre Rechte aus dem Datenschutzrecht geben. Welche Daten im Einzelnen verarbeitet und in welcher Weise genutzt werden, richtet sich maßgeblich nach den beantragten bzw. vereinbarten Dienstleistungen. Daher werden nicht alle Teile dieser Informationen auf Sie zutreffen.

1 Wer ist für die Datenverarbeitung verantwortlich und an wen kann ich mich wenden?

Die Verantwortliche für die Datenverarbeitung ist:

BeWo Durchblick, Tiara Schmitz
Feldgärtenstr. 99
50735 Köln

2 Welche Quellen und Daten nutzen wir?

Wir verarbeiten personenbezogene Daten, die wir im Rahmen unserer Geschäftsbeziehung von Leistungsberechtigten oder anderen Betroffenen erhalten.
Relevante personenbezogene Daten sind (z.B. Personalien, Name, Adresse, Telefonnummer, E-Mail-Adresse, Geburtstag und -ort, Staatsangehörigkeit, Legitimationsdaten (z.B. Ausweisdaten).
Darüber hinaus können dies auch Informationen über Ihre finanzielle Situation, Gesundheitsdaten, Dokumentationsdaten sowie andere mit den genannten Kategorien vergleichbare Daten sein.

3 Wofür verarbeiten wir Ihre Daten (Zweck der Verarbeitung) und auf welcher Rechtsgrundlage?

Wir verarbeiten personenbezogene Daten im Einklang mit den Bestimmungen der EU-Datenschutz-Grundverordnung (DS-GVO) und dem Bundesdatenschutzgesetz (BDSG).

3.1 Aufgrund Ihrer Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO)

Soweit Sie uns eine Einwilligung zur Verarbeitung von personenbezogenen Daten für bestimmte Zwecke (z. B. Lichtbilder im Rahmen von Veranstaltungen) erteilt haben, ist die Rechtmäßigkeit dieser Verarbeitung auf Basis Ihrer Einwilligung gegeben. Eine erteilte Einwilligung kann jederzeit widerrufen werden. Dies gilt auch für den Widerruf von Einwilligungserklärungen, die vor der Geltung der DS-GVO, also vor dem 25. Mai 2018, uns gegenüber erteilt worden sind.
Bitte beachten Sie, dass der Widerruf erst für die Zukunft wirkt. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen.

3.2 Zur Erfüllung von vertraglichen Pflichten (Art. 6 Abs. 1 lit. b DS-GVO)

Die Verarbeitung von Daten erfolgt zur Erbringung unserer Leistungen im Rahmen der Durchführung unserer Verträge mit den Leistungsberechtigten und den Kostenträgern. Die Zwecke der Datenverarbeitung richten sich in erster Linie nach der konkreten Dienstleistung (z.B. Qualifizierte Assistenz).

Aufgrund gesetzlicher Vorgaben (Art. 6 Abs. 1 lit. c DS-GVO)
Darüber hinaus verarbeiten wir Ihre Daten zur Erfüllung gesetzlicher Verpflichtungen (z.B. aufsichtsrechtlicher Vorgaben, handels- und steuerrechtlicher Aufbewahrungs- und Nachweispflichten).

3.3 Im Rahmen der Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO)

Soweit erforderlich verarbeiten wir Ihre Daten über die eigentliche Erfüllung des Vertrages hinaus zur Wahrung berechtigter Interessen von uns oder Dritten.

Beispiele:
- für die Durchführung und Dokumentation rechtlich oder betrieblich notwendiger rechtlicher, technischer oder wirtschaftlicher Prüfungen (z.B. internes Kontrollsystem, Prüfung des Kostenträgers)
- Geltendmachung rechtlicher Ansprüche und Verteidigung bei rechtlichen Streitigkeiten
- zur Sicherstellung ordnungsgemäßer Datenverarbeitung gemäß IT-sicherheitstechnischer und datenschutzrechtlicher Anforderungen (z.B. Protokolldateien)
- zur Analyse und Korrektur technischer Fehler
- Verhinderung und Aufklärung von Straftaten
- Maßnahmen zur Sicherstellung des Hausrechts
- zum Zwecke der Identifikation von Ansprechpartnern (z.B. Name, Telefonnummern, E-Mail-Adressen, Funktion, Abteilungs-/Teamzugehörigkeit) und Durchführung inner- und außerbetrieblicher Kommunikation

4 Wer bekommt meine Daten?

Innerhalb von BeWo Durchblick erhalten diejenigen Stellen Zugriff auf Ihre Daten, die diese zur Erfüllung unserer vertraglichen und gesetzlichen Pflichten brauchen. Daneben bedienen wir uns zur Erfüllung unserer vertraglichen und gesetzlichen Pflichten zum Teil unterschiedlicher Dienstleister. Im Hinblick auf die Datenweitergabe an Empfänger außerhalb von BeWo Durchblick ist zunächst zu beachten, dass wir Informationen über unsere Leistungsberechtigten grundsätzlich nur weitergeben dürfen, wenn gesetzliche Bestimmungen dies gebieten oder der*die Leistungsberechtigte eingewilligt hat. Unter diesen Voraussetzungen können Empfänger personenbezogener Daten sein:
- Strafverfolgungsbehörden bei Vorliegen einer gesetzlichen oder behördlichen Verpflichtung
- Dienstleister, die wir im Rahmen von Auftragsverarbeitungsverhältnissen heranziehen

5 Werden Daten in ein Drittland oder an eine internationale Organisation übermittelt?

Eine Datenübermittlung in Drittstaaten (Staaten außerhalb des Europäischen Wirtschaftsraums – EWR) findet nicht statt.

6 Wie lange werden meine Daten gespeichert?

Wir verarbeiten und speichern Ihre personenbezogenen Daten, solange dies für die Erfüllung unserer vertraglichen und gesetzlichen Pflichten erforderlich ist. Sind die Daten für die Erfüllung vertraglicher oder gesetzlicher Pflichten nicht mehr erforderlich, werden diese regelmäßig gelöscht, es sei denn, deren - befristete - Weiterverarbeitung ist erforderlich zu folgenden Zwecken:

- Erfüllung handels- und steuerrechtlicher Aufbewahrungspflichten, die sich beispielsweise ergeben können aus Handelsgesetzbuch (HGB) und Abgabenordnung (AO). Die dort vorgegebenen Fristen zur Aufbewahrung bzw. Dokumentation betragen in der Regel zwei bis zehn Jahre.
- Erhaltung von Beweismitteln im Rahmen der gesetzlichen Verjährungsvorschriften. Nach den §§ 195 ff des Bürgerlichen Gesetzbuches (BGB) können diese Verjährungsfristen bis zu 30 Jahre betragen, wobei die regelmäßige Verjährungsfrist 3 Jahre beträgt.

7 Welche Datenschutzrechte habe ich?

Jede betroffene Person hat das Recht auf Auskunft nach Art. 15 DS-GVO, das Recht auf Berichtigung nach Art. 16 DS-GVO, das Recht auf Löschung nach Art. 17 DS-GVO, das Recht auf Einschränkung der Verarbeitung nach Art. 18 DS-GVO sowie das Recht auf Datenübertragbarkeit aus Art. 20 DS-GVO. Beim Auskunftsrecht und beim Löschungsrecht gelten die Einschränkungen nach §§ 34 und 35 BDSG. Darüber hinaus besteht ein Beschwerderecht bei einer Datenschutzaufsichtsbehörde (Art. 77 DS-GVO in Verbindung mit § 19 BDSG).
Eine erteilte Einwilligung in die Verarbeitung personenbezogener Daten können Sie jederzeit uns gegenüber widerrufen. Dies gilt auch für den Widerruf von Einwilligungserklärungen, die vor der Geltung

der DS-GVO, also vor dem 25. Mai 2018, uns gegenüber erteilt worden sind. Bitte beachten Sie, dass der Widerruf erst für die Zukunft wirkt. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen.

8 Besteht für mich eine Pflicht zur Bereitstellung von Daten?

Im Rahmen unserer Geschäftsbeziehung müssen Sie diejenigen personenbezogenen Daten bereitstellen, die für die Aufnahme, Durchführung und Beendigung einer Geschäftsbeziehung und zur Erfüllung der damit verbundenen vertraglichen Pflichten erforderlich sind oder zu deren Erhebung wir gesetzlich verpflichtet sind. Ohne diese Daten werden wir in der Regel nicht in der Lage sein, einen Vertrag mit Ihnen zu schließen, diesen auszuführen und zu beenden.

9 Inwieweit gibt es eine automatisierte Entscheidungsfindung (einschließlich Profiling) im Einzelfall?

Zur Begründung und Durchführung der Geschäftsbeziehung nutzen wir grundsätzlich keine vollautomatisierte Entscheidungsfindung gemäß Artikel 22 DS-GVO. Sollten wir diese Verfahren in Einzelfällen einsetzen, werden wir Sie hierüber und über Ihre diesbezüglichen Rechte gesondert informieren, sofern dies gesetzlich vorgegeben ist.

Informationen über Ihr Widerspruchsrecht nach Artikel 21 DS-GVO

Einzelfallbezogenes Widerspruchsrecht
Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 lit. e DS-GVO (Datenverarbeitung im öffentlichen Interesse) und Artikel 6 Absatz 1 lit. f DS-GVO (Datenverarbeitung auf der Grundlage einer Interessenabwägung) erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmung gestütztes Profiling im Sinne von Artikel 4 Nr. 4 DS-GVO.
Legen Sie Widerspruch ein, werden wir Ihre personenbezogenen Daten nicht mehr verarbeiten, es sei denn, wir können zwingende berechtigte Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Datenschutzhinweise für Online-Meetings, Telefonkonferenzen und Webinare

Mit den folgenden Informationen möchten wir Ihnen einen Überblick über die Verarbeitung Ihrer personenbezogenen Daten im Zusammenhang mit der Nutzung von Viedokonferenzsoftware (z.B. Google Meet, Microsoft Teams, Whatsapp-Videoanruf) durch uns und Ihre Rechte aus dem Datenschutzrecht geben. Wir nutzen verschiedene Tools,, um Telefonkonferenzen, Online-Meetings, Videokonferenzen und/oder Webinare durchzuführen (nachfolgend: „Online-Meetings“).

Wer ist für die Datenverarbeitung verantwortlich und an wen kann ich mich wenden?
Der Verantwortliche für die Datenverarbeitung, die im unmittelbaren Zusammenhang mit der Durchführung von Online-Meetings steht, ist:

BeWo Durchblick (Inh. Tiara Schmitz)
Feldgärtenstr. 99
50735 Köln

Hinweis: Soweit Sie die Internetseite von einer Videokonferenzsoftware aufrufen, ist der entsprechende Anbieter für die Datenverarbeitung verantwortlich.

Welche Daten nutzen wir?

Bei der Nutzung von Videokonferenzsoftware werden verschiedene Datenarten verarbeitet. Der Umfang der Daten hängt dabei auch davon, ab welche Daten Sie vor bzw. bei der Teilnahme an einem „Online-Meeting“ machen. Personenbezogene Daten, die Gegenstand der Verarbeitung sind, sind (z.B. Angaben zum Benutzer (z.B. Vorname, Nachname, Telefon (optional), E-Mail-Adresse, Passwort (wenn „Single-Sign-On“ nicht verwendet wird), Profilbild (optional)), z.B. Meeting-Metadaten (z.B. Thema, Beschreibung (optional), Teilnehmer-IP-Adressen, Geräte-/Hardware-Informationen), z.B. Aufzeichnungsdaten (z.B. MP4-Datei aller Video-, Audio- und Präsentationsaufnahmen, M4A-Datei aller Audioaufnahmen, Textdatei des Online-Meeting-Chats), z.B. Telekommunikationsdaten (z.B. Angabe zur eingehenden und ausgehenden Rufnummer, Ländername, Start- und Endzeit) sowie z.B. weitere Verbindungsdaten (z.B. die IP-Adresse des Geräts)).
Text-, Audio- und Videodaten: Sie haben ggf. die Möglichkeit, in einem „Online-Meeting“ die
Chat-, Fragen- oder Umfragefunktionen zu nutzen. Insoweit werden die von Ihnen gemachten Texteingaben verarbeitet, um diese im „Online-Meeting“ anzuzeigen und ggf. zu protokollieren. Um die Anzeige von Video und die Wiedergabe von Audio zu ermöglichen, werden entsprechend während der Dauer des Meetings die Daten vom Mikrofon Ihres Endgeräts sowie von einer etwaigen Videokamera des Endgeräts verarbeitet. Sie können die Kamera oder das Mikrofon jederzeit selbst über die Videokonferenzsoftware abschalten bzw. stummstellen.
Um an einem „Online-Meeting“ teilzunehmen bzw. um den „Meeting-Raum“ zu betreten, müssen Sie ggf. Angaben zu Ihrem Namen machen.
Bei Einrichtung eines Online-Meetings wird ein Name für das Online-Meeting vom Veranstalter gewählt. Zusätzlich kann ein Passwort für die Teilnahme am Online-Meeting vorgesehen werden. Diese Daten werden nur bis zur Beendigung des jeweiligen Online-Meetings verarbeitet und anschließend gelöscht. Beachten Sie bitte, dass aber der Name von „Online-Meetings“ sowie Datum, Uhrzeit und Dauer des „Online-Meeting“ in Ihrem Browser lokal gespeichert werden können. Wenn Sie die Daten nicht weiter sehen wollen, sollten Sie Ihren Browser-Cache löschen.

Wofür verarbeiten wir Ihre Daten (Zweck der Verarbeitung) und auf welcher Rechtsgrundlage?

Wir verwenden Videokonferenzsoftware, um Online-Meetings, Videokonferenzen und/oder Webinare durchzuführen (nachfolgend: „Online-Meetings“). Wenn wir Online-Meetings aufzeichnen wollen, werden wir Ihnen das im Vorwege transparent mitteilen und – soweit erforderlich – um eine Zustimmung bitten. Wenn es

für die Zwecke der Protokollierung von Ergebnissen eines Online-Meetings erforderlich ist, werden wir die Chatinhalte protokollieren. Das wird jedoch in der Regel nicht der Fall sein.
Im Falle von Webinaren können wir für Zwecke der Aufzeichnung und Nachbereitung von Webinaren auch die gestellten Fragen von Webinar-Teilnehmenden verarbeiten.
Die in „Online-Meeting"-Tools, z.B. in "MS TEAMS" bestehende Möglichkeit einer softwareseitigen „Aufmerksamkeitsüberwachung" („Aufmerksamkeitstracking") ist deaktiviert.

Im Rahmen der Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO)

Sofern keine vertragliche Beziehung zu Leistungsberechtigten oder anderen Teilnehmern besteht, welche die „Online-Meetings" im Rahmen von Vertragsbeziehungen regelt, so verarbeiten wir die Daten im Rahmen unseres berechtigten Interesses. Unser Interesse besteht in diesen Fällen an der effektiven Durchführung von „Online-Meetings".

Wer bekommt meine Daten?

Personenbezogene Daten, die im Zusammenhang mit der Teilnahme an „Online-Meetings" verarbeitet werden, werden grundsätzlich nicht an Dritte weitergegeben, sofern sie nicht gerade zur Weitergabe bestimmt sind. Beachten Sie bitte, dass Inhalte aus „Online-Meetings" wie auch bei persönlichen Besprechungstreffen häufig gerade dazu dienen, um Informationen mit Leistungsberechtigten, Interessenten oder Dritten zu kommunizieren und damit zur Weitergabe bestimmt sind.

Werden Daten in ein Drittland oder an eine internationale Organisation übermittelt?

Die meisten Videokonferenzsoftwares, wie z.B. MS TEAMS, Google Meet, WhatsApp sind Dienste, die von Anbietern aus den USA erbracht werden. Eine Verarbeitung der personenbezogenen Daten findet damit auch in einem Drittland statt.

Wir können außerdem nicht ausschließen, dass das Routing von Daten über Internetserver erfolgt, die sich außerhalb der EU befinden. Dies kann insbesondere dann der Fall sein, wenn sich Teilnehmende an einem „Online-Meeting" in einem Drittland aufhalten.
Die Daten sind während des Transports über das Internet jedoch verschlüsselt und somit vor einem unbefugten Zugriff durch Dritte gesichert.

Wie lange werden meine Daten gespeichert?

Wir löschen personenbezogene Daten grundsätzlich dann, wenn kein Erfordernis für eine weitere Speicherung besteht. Ein Erfordernis kann insbesondere dann bestehen, wenn die Daten noch benötigt werden, um vertragliche Leistungen zu erfüllen, Gewährleistungs- und ggf. Garantieansprüche prüfen und gewähren oder abwehren zu können. Im Falle von gesetzlichen Aufbewahrungspflichten kommt eine Löschung erst nach Ablauf der jeweiligen Aufbewahrungspflicht in Betracht.

Welche Datenschutzrechte habe ich?

Jede betroffene Person hat das Recht auf Auskunft nach Art. 15 DS-GVO, das Recht auf Berichtigung nach Art. 16 DS-GVO, das Recht auf Löschung nach Art. 17 DS-GVO, das Recht auf Einschränkung der Verarbeitung nach Art. 18 DS-GVO sowie das Recht auf Datenübertragbarkeit aus Art. 20 DS-GVO. Beim Auskunftsrecht und beim Löschungsrecht gelten die Einschränkungen nach §§ 34 und 35 BDSG. Darüber hinaus besteht ein Beschwerderecht bei einer Datenschutzaufsichtsbehörde (Art. 77 DS-GVO in Verbindung mit § 19 BDSG).
Eine erteilte Einwilligung in die Verarbeitung personenbezogener Daten können Sie jederzeit uns gegenüber widerrufen. Dies gilt auch für den Widerruf von Einwilligungserklärungen, die vor der Geltung der DS-GVO,

also vor dem 25. Mai 2018, uns gegenüber erteilt worden sind. Bitte beachten Sie, dass der Widerruf erst für die Zukunft wirkt. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen.

Besteht für mich eine Pflicht zur Bereitstellung von Daten?

Grundsätzlich nein. Ohne diese Daten werden wir allerdings in der Regel nicht in der Lage sein, mittels Online-Meeting mit Ihnen zu kommunizieren.

Inwieweit gibt es eine automatisierte Entscheidungsfindung (einschließlich Profiling) im Einzelfall?

Wir nutzen grundsätzlich keine vollautomatisierte Entscheidungsfindung gemäß Artikel 22 DS-GVO zur Durchführung von Online-Meetings. Sollten wir diese Verfahren in Einzelfällen künftig einsetzen, werden wir Sie hierüber und über Ihre diesbezüglichen Rechte gesondert informieren, sofern dies gesetzlich vorgegeben ist.

Datenschutzinformation für Mitarbeiter*innen der BeWo Durchblick (Inh. Tiara Schmitz)

Unser Umgang mit Ihren Daten und Ihre Rechte. Informationen nach Artikeln 13, 14 und 21 Datenschutz-Grundverordnung – DS-GVO.

Datenschutzinformationen für Mitarbeiter*innen der BeWo Durchblick

Als Mitarbeiter*in in unseren Unternehmen möchten wir Ihnen gerne Informationen zur Verarbeitung Ihrer personenbezogenen Daten im Zusammenhang mit Ihrer Tätigkeit als Arbeitnehmer*in bei uns geben.

Wer ist für die Datenverarbeitung verantwortlich und an wen kann ich mich wenden?

Der Verantwortliche für die Datenverarbeitung ist:

BeWo Durchblick, Tiara Schmitz
Feldgärtenstr. 99
50735 Köln

Welche Quellen und Daten nutzen wir?

Wir verarbeiten **personenbezogene Daten** (Art. 4 Nr. 2 DS-GVO), die wir von Ihnen **im Rahmen des Auswahl- und Einstellungsverfahrens oder während des Beschäftigungsverhältnisses** erhalten. Wir verarbeiten die personenbezogenen Daten, die **für die Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses** erforderlich sind. Zudem verarbeiten wir – soweit für das Beschäftigungsverhältnis erforderlich – personenbezogene Daten, die wir **auf gesetzlicher Grundlage bei anderen Stellen erheben (z.B. anlassbezogene Abfragen von steuerrelevanten Daten beim zuständigen Finanzamt, Informationen über Arbeitsunfähigkeitszeiten bei der Krankenkasse)**. Zum anderen verarbeiten wir personenbezogene Daten, die wir zulässigerweise von Dritten (z.B. Personalvermittlern) erhalten und aus öffentlich zugänglichen Quellen (z.B. beruflichen sozialen Netzwerken) gewonnen haben.
Relevante personenbezogene Daten sind vor allem Ihre **Stammdaten (z.B. Name, Namenszusätze, Geschlecht, Geburtsdatum, Geburtsort, Staatsangehörigkeit, Familienstand, Lichtbild, Adresse, Personalnummer und andere Kontaktdaten)**, Daten zu Ihren **Qualifikationen (z.B. Schulbildung, Schulabschlüsse, Studienabschlüsse)** die bei der **Nutzung der IT-Systeme anfallenden Protokolldaten, weitere Daten aus dem Beschäftigungsverhältnis (z. B. Zeiterfassungsdaten, Urlaubszeiten, Arbeitsunfähigkeitszeiten, Beurteilungen, Ausbildungen, Weiter- und Fortbildungen, Sozialdaten, Bankverbindung, Sozialversicherungsnummer, Rentenversicherungsnummer, Gehaltsdaten sowie die Steueridentifikationsnummer)**, Daten die für die **Ermittlung und Abrechnung Ihres Gehalts und im Zusammenhang mit gesetzlichen Abgaben und Steuern (z.B. Sozialversicherungsbeiträge)** erforderlich sind sowie andere mit den genannten Kategorien vergleichbare Daten. Hierunter können auch besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DS-GVO (z.B. Gesundheitsdaten) fallen.
Hinzu kommen ggf. auch Daten aus dem **Bereich der Arbeitssicherheit**, dem betrieblichen Eingliederungsmanagement und **Daten über arbeitsvertragliche Pflichtverletzungen, die geahndet wurden („Abmahnungen“)**.
Sollten Sie eine von uns angebotene **betriebliche Altersversorgung nutzen, werden auch in diesem Bereich Daten verarbeitet und im Rahmen der Erforderlichkeit an die Versicherer** weitergegeben.
Die Daten werden grundsätzlich auf speziell dafür vorgesehenen IT-Systemen in unseren Räumlichkeiten verarbeitet. Auf diese IT-Systeme haben neben Administrator*innen nur Mitarbeitende der Verwaltung und der Unternehmensleitung Zugriff.
Sollten Beschäftigtendaten bei Dienstleistern verarbeitet werden, stellen wir sicher, dass dies unter Einhaltung der datenschutzrechtlichen Vorgaben erfolgt.

Unabhängig davon kann es immer Konstellationen geben, in denen wir die personenbezogenen Daten von Ihnen verarbeiten, die hier nicht beziehungsweise deren Zwecke hier nicht genannt sind. Wir werden in diesen Fällen dann – bezogen auf den jeweiligen Anlass – gesonderte Informationen zum Datenschutz für Sie bereithalten, soweit dies gesetzlich erforderlich ist.
Ihre personenbezogenen Daten werden regelmäßig direkt von Ihnen im Rahmen des Bewerbungs- und Einstellungsprozesses und/oder während der Durchführung des Arbeitsverhältnisses bei BeWo Durchblick erhoben. Werden in bestimmten Konstellationen aufgrund gesetzlicher Vorschriften oder aufgrund einer datenschutzrechtlichen Erlaubnisnorm personenbezogene Daten über Sie bei einer anderen Stelle erhoben, werden wir Sie hierüber gesondert nach den Vorgaben des Art. 14 DSGVO in Verbindung mit § 33 BDSG informieren.

Wofür verarbeiten wir Ihre Daten (Zweck der Verarbeitung) und auf welcher Rechtsgrundlage?

Wir verarbeiten personenbezogene Daten im Einklang mit den Bestimmungen der Europäischen Datenschutz-Grundverordnung (DS-GVO), dem Bundesdatenschutzgesetz (BDSG) sowie weiteren einschlägigen Gesetzen wie beispielsweise Arbeitszeitgesetz - ArbZG, Mutterschutzgesetz - MuSchG oder Abgabenordnung (AO).

Aufgrund Ihrer Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO)

Soweit Sie uns eine Einwilligung zur Verarbeitung von personenbezogenen Daten für bestimmte Zwecke (z. B. zur Durchführung eines betrieblichen Eingliederungsmanagements; Durchführung von Mitarbeiterbefragungen auf freiwilliger Basis) erteilt haben, ist die Rechtmäßigkeit dieser Verarbeitung auf Basis Ihrer Einwilligung gegeben. Eine erteilte Einwilligung kann jederzeit widerrufen werden. Dies gilt auch für den Widerruf von Einwilligungserklärungen, die vor der Geltung der DS-GVO, also vor dem 25. Mai 2018, uns gegenüber erteilt worden sind.
Bitte beachten Sie, dass der Widerruf erst für die Zukunft wirkt. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen.

Zur Erfüllung von vertraglichen Pflichten (Art. 6 Abs. 1 lit. b DS-GVO i.V.m. § 26 Abs. 1 BDSG; Art. 88 Abs. 1 DS-GVO i.V.m. § 26 Abs. 4 BDSG)

Die Verarbeitung personenbezogener Daten erfolgt in erster Linie im Beschäftigungskontext, das heißt insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen (Betriebsvereinbarungen und tarifvertragliche Regelungen) festgelegten Pflichten sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses.

Beispiele:

- zur Entscheidung über die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses
- zur Erfassung und Pflege von An- und Abwesenheitszeiten (z.B. Arbeitszeit, Fortbildungen)
- zur Gewährleistung von Gesundheit und Sicherheit am Arbeitsplatz
- zur betrieblichen Integration schwerbehinderter Menschen
- für Maßnahmen der Mitarbeiterförderung (z.B. Fortbildungen, Weiterbildungen, berufsbegleitende Studiengänge)
- zur Entgeltabrechnung sowie zur Reisekostenerstattung
- zur Personalverwaltung (z. B. Dienstwagenabwicklung, Versicherungen, betriebliche Altersversorgung)
- zur Personalaktenführung
- zum Betrieb der betrieblichen Kommunikationsmittel insbesondere des IT-Systems, der Internet- und E-Mail-Zugänge sowie der Telekommunikationsanlage

- zum Schutz des Eigentums von BeWo Durchblick, der Mitarbeiter und der Kunden
- zum Austrittsmanagement (z.B. Zeugniserstellung)

Aufgrund gesetzlicher Vorgaben (Art. 6 Abs. 1 lit. c DS-GVO i.V.m. § 26 BDSG)

Zudem unterliegen wir als Arbeitgeber diversen rechtlichen Verpflichtungen, das heißt gesetzlichen Anforderungen. Verarbeitungen erfolgen dabei z.B.

- zur Erfüllung gesetzlicher Vorschriften (z. B. steuerliche Belange, amtliche Statistiken, Sozialversicherung)
- zur Erfüllung gesetzlicher Auskunftspflichten.

Im Rahmen der Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO)

Soweit erforderlich verarbeiten wir Ihre Daten über die eigentliche Erfüllung des Vertrages hinaus zur Wahrung berechtigter Interessen von uns oder Dritten.

Beispiele:

- für die Durchführung und Dokumentation rechtlich oder betrieblich notwendiger rechtlicher, technischer oder wirtschaftlicher Prüfungen (z. B. Wirtschaftsprüfer, Innenrevision, internes Kontrollsystem)
- zur Sicherstellung ordnungsgemäßer Datenverarbeitung gemäß IT-sicherheitstechnischer und -datenschutzrechtlicher Anforderungen (z. B. Protokolldateien)
- zur Analyse und Korrektur technischer Fehler
- zur Gewährleistung der Systemsicherheit und –verfügbarkeit
- zur Optimierung und Steuerung der Systeme (z.B. Aktualisierung der Liste gesperrter Internetseiten, „Black List“; Optimierung der Netzdienste)
- zur Datenschutzkontrolle/ für Datenschutz- und Datensicherheitszwecke
- zum Zwecke der Identifikation von Ansprechpartnern (z.B. Name, Telefonnummern, E-Mail-Adressen, Funktion, Abteilungs-/Teamzugehörigkeit) und Durchführung inner- und außerbetrieblicher Kommunikation
- zur Personalplanung und Personalcontrolling
- zur Personaleinsatzplanung und -Disposition
- zur Personalführung
- zur (insbesondere personalvertretungsrechtlich) zulässigen Verhaltens- und/oder Leistungskontrolle
- zur Zugangs-/Zutrittskontrolle
- zum Personalberichtswesen
- zur Personalentwicklung (insbesondere Nachwuchssicherung, Personalaustausch, Aus- und Fortbildung, gezielte Stellenbesetzung, Zielsetzung und Zielerreichung)
- zur Speicherung von Wiedervorlagedaten (z. B. Ablauf der Probezeit, Befristung, Dauer des Mutterschutzes usw.)
- zur Durchführung der Führerscheinkontrolle im Rahmen der Halterhaftung
- zur Aufklärung von Straftaten, sofern zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betreffende Person eine Straftat begangen hat, die Verarbeitung zur Aufklärung erforderlich ist und das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. In diesem Fall erfolgt die Datenverarbeitung auf Grundlage von Art. 88 Abs. 1 DS-GVO in Verbindung mit § 26 Absatz 1 Satz 2 BDSG

Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 1 DS-GVO)

Besondere Kategorien personenbezogener Daten gem. Art. 9 Absatz 1 DS-GVO sind Angaben, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur

eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zur sexuellen Orientierung einer natürlichen Person.
Soweit wir besondere Kategorien personenbezogener Daten verarbeiten, 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. Insbesondere kann die Verarbeitung besonderer Kategorien personenbezogener Daten dabei zu folgenden Zwecken erfolgen:

Beispiele:

- Entscheidung über die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses (z.B. Beteiligung des Integrationsamts bei Kündigung schwerbehinderter Mitarbeiter, Durchführung einer Kündigung aus krankheitsbedingten Gründen)
- Angabe von Gesundheitsdaten gegenüber der Krankenkasse
- Unfallanzeigen gegenüber Unfallkassen/Berufsgenossenschaften
- Gesundheit und Sicherheit am Arbeitsplatz (z.B. insbesondere die betriebliche Suchtprävention und arbeitsmedizinischen Untersuchungen)
- Betriebliche Integration schwerbehinderter Menschen
- Erfassung der Schwerbehinderung wegen Zusatzurlaub und Ermittlung der Schwerbehindertenabgabe
- Erfüllung gesetzlich/kollektiv-vertraglich vorgesehener Rechte / Pflichten im Bereich des Arbeitsrechts, des Rechts der sozialen Sicherheit oder des Sozialschutzes gemäß Art. 9 Abs. 2 lit. b DS-GVO i.V.m. § 26 Abs. 3 BDSG (z.B. Durchführung der Wahl einer Schwerbehindertenvertretung).

Zudem kann zur Beurteilung Ihrer Arbeitsfähigkeit auch die Verarbeitung von Gesundheitsdaten gemäß Art. 9 Abs. 2 lit. h DS-GVO i.V.m. § 22 Abs. 1 Buchstabe b) BDSG erforderlich sein.
Gegebenenfalls kann die Verarbeitung besonderer Kategorien personenbezogener Daten auf einer Einwilligung nach Artikel 9 Absatz 2 Buchstabe a) DSGVO in Verbindung mit § 26 Absatz 3 und 2 BDSG oder vergleichbarer nationaler Vorschriften beruhen (z.B. Durchführung des Verfahrens zum betrieblichen Eingliederungsmanagement nach dem IX. Sozialgesetzbuch). Die Einwilligung muss sich dabei ausdrücklich auf die Verarbeitung besonderer Kategorien personenbezogener Daten beziehen.

Wer bekommt meine Daten?

Innerhalb von BeWo Durchblick erhalten diejenigen Stellen (z.B. Verwaltung, jeweilige Führungskräfte) Ihre Daten, die diese zur Erfüllung unserer vertraglichen und gesetzlichen Pflichten brauchen. Innerhalb des Unternehmens kommt eine Weitergabe Ihrer personenbezogenen Daten auch dann in Betracht, wenn beispielsweise im Zusammenhang mit einem Stellenwechsel eine Prüfung der Eignung und Qualifikation erforderlich wird. Oder falls Ihnen im Unternehmen eine andere oder zusätzlich Aufgabe übertragen wird oder werden soll.
Daneben bedienen wir uns zur Erfüllung unserer vertraglichen und gesetzlichen Pflichten zum Teil unterschiedlicher Dienstleister. Darüber hinaus können wir Ihre personenbezogenen Daten an weitere Empfänger außerhalb von BeWo Durchblick übermitteln, soweit dies zur Erfüllung der vertraglichen und gesetzlichen Pflichten als Arbeitgeber erforderlich ist.

Dies sind z.B.:

- Behörden (z. B. Rentenversicherungsträger, berufsständische Versorgungseinrichtungen Sozialversicherungsträger, Unfallkassen, Arbeitsagenturen, Finanzbehörden, Gerichte)
- sonstige Stellen, Behörden und Gerichte, die Aufgaben im Zusammenhang mit dem Beschäftigungsverhältnis wahrnehmen (z.B. Elterngeldstellen, Integrationsämter, Arbeitsschutzbehörden, Datenschutzbehörden, Arbeitsgerichte)
- Bank des Mitarbeiters (SEPA-Zahlungsträger)
- Krankenkassen
- Stellen, um Ansprüche aus der betrieblichen Altersversorgung gewährleisten zu können

- Drittschuldner im Falle von Lohn- und Gehaltspfändungen
- Insolvenzverwalter im Falle einer Privatinsolvenz

Auch von uns eingesetzte Auftragsverarbeiter (Art. 28 DS-GVO) können zu diesen genannten Zwecken Daten erhalten. Dies sind Unternehmen in den Kategorien:

- Kreditwirtschaftliche Leistungen
- Lohn- und Finanzbuchhaltung
- IT-Dienstleistungen
- Logistik
- Druckdienstleistungen
- Telekommunikation
- Beratung und Consulting
- Vertrieb und Marketing

Weitere Datenempfänger können diejenigen Stellen sein, für die Sie uns Ihre Einwilligung zur Datenübermittlung erteilt haben.

Wie lange werden meine Daten gespeichert?

Soweit für die oben (Nr. 3) genannten Zwecke erforderlich, verarbeiten und speichern wir Ihre personenbezogenen Daten für die Dauer Ihres Arbeitsverhältnisses, was beispielsweise auch die Anbahnung und Abwicklung des Arbeitsvertrages umfasst. Dabei ist zu beachten, dass das Arbeitsverhältnis ein Dauerschuldverhältnis ist, welches auf Jahre angelegt ist. Sonderregelungen kann es in einzelnen Bereichen geben. So werden beispielsweise Abmahnungen in Personalakten kürzer gespeichert.
Darüber hinaus unterliegen wir verschiedenen Aufbewahrungs- und Nachweispflichten, die sich unter anderem aus dem Handelsgesetzbuch (HGB) und der Abgabenordnung (AO) ergeben. Die Speicherfristen betragen danach bis zu zehn Jahre.
Schließlich beurteilt sich die Speicherdauer auch nach den gesetzlichen Verjährungsfristen, die zum Beispiel nach den §§ 195 ff. des Bürgerlichen Gesetzbuches (BGB) in der Regel drei Jahre, in gewissen Fällen aber auch bis zu dreißig Jahre betragen können.
Soweit keine gesetzlichen Aufbewahrungspflichten bestehen, können personenbezogene Daten gelöscht werden, wenn deren weitere Verarbeitung für die Durchführung oder Beendigung des Beschäftigungsverhältnisses nicht mehr erforderlich sind.
Nach Beendigung des Beschäftigungsverhältnisses werden Daten bis zur Verjährung etwaiger Schadensersatzansprüche jeder Partei gespeichert. Eine längere Speicherung kommt zudem in Betracht, wenn dies auch im Interesse von Ihnen ist oder Sie eine Einwilligung erteilt haben.
Sollten Sie z.B. nicht wollen, dass wir personenbezogene Daten von Ihnen nach dem Ablauf gesetzlicher Aufbewahrungspflichten weiter speichern, dann teilen Sie uns das gerne beim Ausscheiden aus unserem Unternehmen mit. Bitte beachten Sie, dass wir in dem Fall später nicht behilflich sein können, wenn Sie gegenüber der Rentenversicherung Sozialversicherungszeiträume nachweisen wollen.
Wir werden generell zum Ende eines Jahres prüfen, ob und in welchem Umfang Daten von Beschäftigten wegen eines Wegfalls der Erforderlichkeit gelöscht werden können.

Werden Daten in ein Drittland oder an eine internationale Organisation übermittelt?

Eine Datenübermittlung in Drittstaaten (Staaten außerhalb des Europäischen Wirtschaftsraums – EWR) findet nicht statt.

Welche Datenschutzrechte habe ich?

Jede betroffene Person hat das Recht auf Auskunft nach Art. 15 DS-GVO, das Recht auf Berichtigung nach Art. 16 DS-GVO, das Recht auf Löschung nach Art. 17 DS-GVO, das Recht auf Einschränkung der Verarbeitung nach Art. 18 DS-GVO sowie das Recht auf Datenübertragbarkeit aus Art. 20 DS-GVO. Beim

Auskunftsrecht und beim Löschungsrecht gelten die Einschränkungen nach §§ 34 und 35 BDSG. Darüber hinaus besteht ein Beschwerderecht bei einer Datenschutzaufsichtsbehörde (Art. 77 DS-GVO i.V.m. § 19 BDSG).

Besteht für mich eine Pflicht zur Bereitstellung von Daten?

Im Rahmen Ihrer Beschäftigung müssen Sie nur diejenigen personenbezogenen Daten bereitstellen, 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 in der Regel nicht in der Lage sein, den Arbeitsvertrag mit Ihnen durchzuführen.

Inwieweit gibt es eine automatisierte Entscheidungsfindung (einschließlich Profiling) im Einzelfall?

Zur Begründung, Durchführung und Abwicklung des Beschäftigungsverhältnisses nutzen wir grundsätzlich keine automatisierte Entscheidungsfindung – einschließlich Profiling - gemäß Art. 22 DS-GVO. Sollten wir diese Verfahren in Einzelfällen einsetzen, werden wir Sie hierüber gesondert informieren, sofern dies gesetzlich vorgegeben ist.

Änderungen an diesen Informationen

Wir können diese Datenschutzinformationen von Zeit zu Zeit aktualisieren. Wir empfehlen deshalb, diese Datenschutzinformationen regelmäßig durchzulesen, damit Sie unsere Datenschutzpraktiken kennen.

Information über Ihr Widerspruchsrecht nach Art. 21 Datenschutz-Grundverordnung (DS-GVO) für Mitarbeiter*innen

1 **Einzelfallbezogenes Widerspruchsrecht**

Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 lit. f der DS-GVO (Datenverarbeitung auf der Grundlage einer Interessenabwägung) erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmung gestütztes Profiling im Sinne von Art. 4 Nr. 4 DS-GVO.

Legen Sie Widerspruch ein, werden wir Ihre personenbezogenen Daten nicht mehr verarbeiten, 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.

Erklärung über Kenntnisnahme und Einhaltung

Ich habe das Datenschutzkonzept erhalten, gelesen und verstanden. Ich verpflichte mich zur Einhaltung der Regelungen zum Schutz personenbezogener Daten und werde alle erforderlichen Maßnahmen ergreifen, um den unbefugten Zugriff, die unbefugte Verarbeitung, Weitergabe, Veränderung oder Löschung personenbezogener Daten zu verhindern.

Köln, den _____(Unterschrift Mitarbeiter*in)

Vereinbarung für Mitarbeiter*innen zum Mobilen Arbeiten

zwischen

BeWo Durchblick (Inh. Tiara Schmitz) (im Folgenden Unternehmen)

und

_____(im Folgenden Mitarbeiter*in oder Mitarbeitende)

1. Regelungsgegenstand

(1) Gegenstand dieser Vereinbarung sind die Rahmen- und Vertragsbedingungen für die mobile Nutzung der Arbeitsmittel und die Nutzung von Co-Working-Räumlichkeiten.
(2) Mobiles Arbeiten umfasst die Erbringung der teilweisen individuellen Arbeitsleistung von unterwegs sowie die teilweise Ableistung der individuellen regelmäßigen Arbeitszeit durch die Nutzung von Co-Working-Räumlichkeiten. Mobiles Arbeiten bedarf der Zustimmung der Geschäftsführung, die hiermit erteilt wird.

2. Teilnahmebedingungen

(1) Mitarbeitende, deren Arbeitsaufgaben ohne Beeinträchtigung des Betriebsablaufs und des Kontakts zum Unternehmen eine Tätigkeit im Mobilen Arbeiten zulassen oder bei denen Mobiles Arbeiten wünschenswert sind, können sich zur Teilnahme bereit erklären. Das Unternehmen kann sowohl zur Teilnahme anregen als auch aus begründeten betrieblichen oder wirtschaftlichen Gründen vom Mobilen Arbeiten absehen.

3. Arbeitsort und -zeit

(1) Der*die Mitarbeiter*in wird seine*ihre Arbeitsleistung auch an Orten außerhalb der betrieblichen Arbeitsstätte (Mobiles Arbeiten), also auch in der eigenen Wohnung, verbringen.
(2) Regelungen zur Arbeitszeit gelten für die Arbeit von zu Hause, von unterwegs oder von Co-Working-Räumlichkeiten aus in gleicher Weise wie für die Arbeit vor Ort im Unternehmen.

4. Arbeitsmittel

(1) Die vom Unternehmen zur Verfügung gestellten Arbeitsmittel dürfen nur dann für private Zwecke benutzt werden, wenn die in diesem Konzept festgelegten Regelungen in der IT-Richtlinie für Nutzer*innen eingehalten werden. Dies beinhaltet auch, dass keine Software aufgespielt werden darf und keine Hardware ausgetauscht oder angeschlossen wird, ohne dass das Unternehmen dies schriftlich erlaubt hat.
Der*die Mitarbeiter*in sichert zu, dass er gemäß den Definitionen der Datenschutzgrundverordnung keine personenbezogenen Daten des Unternehmens auf privaten Arbeitsmitteln erheben oder verarbeiten wird. Dies beinhaltet auch das Kopieren von personenbezogenen Daten des Unternehmens auf private Arbeitsmittel des Mitarbeiters oder Dritter, wozu auch das Ausdrucken von Daten zählt. Hierzu zählen auch (mobile) Datenträger wie beispielsweise Notebooks, Smartphones, portable Festplatten, USB-Sticks oder CD´s/DVD´s.
(2) Sicherheitsmaßnahmen, -verfahren und Vorrichtungen wie beispielsweise Virenscanner, Firewalls, Anti-Spamfilter und Verschlüsselungsmechanismen sind zu beachten und dürfen nicht abgeschaltet, verändert oder umgangen werden.
(3) Bei Aufstellung und Betrieb der eingesetzten Arbeitsmittel ist auf die einschlägigen Rechtsvorschriften, betrieblichen Regelungen sowie auf die Regelungen zur technischen Sicherheit und Ergonomie zu achten. Der*die Mitarbeiter*in sichert zu, dass ihm*ihr diese bekannt sind. Defekte Geräte sind bei der Geschäftsführung im Unternehmen zu melden und abzugeben. Sollten Geräte verloren gehen oder gestohlen werden, wird der Verlust unverzüglich der Geschäftsführung im Unternehmen gemeldet.

(4) Notwendige Arbeitsunterlagen können im Einvernehmen mit der Geschäftsführung ins Mobile Arbeiten und/oder in Co-Working-Räumlichkeiten mitgenommen werden. Ziffer 5 dieser Vereinbarung ist hierbei jedoch zu beachten.
(5) Die Mitnahme von Arbeitsmitteln ins Ausland bedarf einer allgemeinen Erlaubnis seitens der Geschäftsführung.

5. Daten- und Informationsschutz

(1) Im Mobilen Arbeiten ist auf den Schutz von Daten und Informationen besonders zu achten. Alle zwischen dem Unternehmen und dem*der Mitarbeiter*in getroffenen Vereinbarungen, Verpflichtungen sowie erteilte Weisungen, insbesondere im Hinblick auf Vertraulichkeit, Verschwiegenheit und den Schutz von betrieblichen Informationen, müssen die notwendige Beachtung finden. Vertrauliche Informationen, Zugangskennungen sowie Passwörter, mit denen auf die dienstlichen Datenbestände zugegriffen werden kann, sind so zu schützen, dass Dritte davon keine Kenntnis erlangen können. Als Dritte zählen auch Angehörige aus dem persönlichen und familiären Personenkreis. Datenträger sind stets verschlüsselt aufzubewahren. Die Aufbewahrung der Unterlagen hat in verschlossenen Behältnissen zu erfolgen. Bei der elektronischen Datenübertragung sind die vom Unternehmen vorgegebenen Sicherheitsmaßnahmen zu benutzen. Beim herkömmlichen Transport der Informationen ist auf die Benutzung verschließbarer Behältnisse zu achten. Daneben dürfen die verschlüsselten Datenträger und Unterlagen während des Transports nie unbeaufsichtigt gelassen werden.

Es gelten insbesondere folgende Anforderungen für den Daten- und Informationsschutz:

- Neben den gesetzlichen Datenschutzbestimmungen gelten die innerbetrieblichen Regelungen zur Umsetzung des Datenschutzes und der Datensicherheit auch im häuslichen Umfeld des*der Mitarbeiters*in und im Mobilen Arbeiten, dem die Erledigung der dienstlichen Obliegenheiten auch zu Hause und mobil gestattet ist. Ausnahmen ergeben sich nur dann, wenn die betriebliche Regelung offensichtlich nicht den mobilen Arbeitsplatz übertragbar ist. Diese Ausnahmen sind mit dem Unternehmen abzustimmen und genehmigungspflichtig.

- Auf den Schutz von Daten und Informationen gegenüber Dritten ist im Mobilen Arbeiten besonders zu achten. Vertrauliche Daten und Informationen sind von Mitarbeitenden so zu schützen, dass unbefugte Dritte nicht Einsicht und/oder Zugriff nehmen können.

- Der*die Mitarbeiter*in stellt sicher, dass insbesondere Unterlagen, Datenträger und Altgeräte, sicher vernichtet werden. Grundsätzlich dürfen diese Arbeitsmittel nicht als regulärer Abfall behandelt werden. Vielmehr sind sie entsprechend den Vorgaben des Gesetzes und des Arbeitgebers zu vernichten, indem ein hinreichend sicherer Shredder eingesetzt wird oder die Arbeitsmittel zur Vernichtung an den Arbeitgeber zurückgegeben werden.

- Bei auch nur kurzfristigem Verlassen des häuslichen und des mobilen Arbeitsplatzes sind der PC bzw. das dienstlich genutzte Arbeitsmittel sowie Unterlagen vor unbefugtem Zugriff zu schützen. Bei längerer Abwesenheit hat sich der*die Mitarbeiter*in als Benutzer vom System abzumelden. Personenbezogene oder vertrauliche Geschäftsunterlagen sind bei Abwesenheit unter Verschluss zu halten. Der*Die Mitarbeiter*in darf die Geräte, Datenträger und Unterlagen außerhalb eines verschlossenen Raums nicht – auch nicht kurzzeitig – unbeaufsichtigt lassen.

- Verbindungen zum Unternehmensnetzwerk erfolgen ausschließlich über https://app.bewo-durchblick.de/.

- Elektronische Zugangskennungen sowie zugehörige Passwörter sind vor dem Zugriff Unbefugter in besonderem Maße zu schützen. Passwörter müssen einem sicheren Standard entsprechen. “Grundsätzlich gilt: **Je länger, desto besser**. Für ein gutes Passwort sind Länge und Komplexität entscheidend. Ein kurzes und komplexes Passwort sollte **mindestens acht Zeichen** lang sein und

aus **vier verschiedenen Zeichenarten** (Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen) bestehen. Ein langes und weniger komplexes Passwort sollte mindestens 25 Zeichen lang sein." (BSI - Sichere Passwörter erstellen)

- Die elektronischen Geräte, mit denen ein Zugriff auf das Netzwerk des Unternehmens möglich ist, dürfen keinem Dritten zur Nutzung überlassen werden.

- Berufliche E-Mails und Telefonate dürfen nicht auf private Postfächer oder private Telefonanschlüsse / Handys / Smartphones oder ähnliche Geräte um- oder weitergeleitet werden. Ausnahmen müssen mit der Geschäftsführung vereinbart und vertraglich festgehalten werden.

- Telefonate, in deren Rahmen betriebliche Informationen ausgetauscht werden, sind außerhalb der Hörweite unbefugter Personen zu führen.

- Der Mitarbeiter hat sicherzustellen, dass Gespräche oder Telefonate bei denen betriebliche Informationen ausgetauscht werden, nicht von digitalen Sprachassistenten mitgehört oder beobachtet werden können. Dies gilt auch für Geräte mit Aktivierungswörtern wie beispielsweise Siri (Apple), Google oder Echo (amazon).

- Bei mobilen Endgeräten sind nicht benötigte Verbindungen wie WLAN, Bluetooth, RFID und ähnliche grundsätzlich – insbesondere während des Transportes – zu deaktivieren.

6. Datenschutzvorfälle

(1) Mitarbeiter melden mögliche Datenschutzvorfälle unverzüglich an die Geschäftsführung von BeWo Durchblick. Ein Datenschutzvorfall liegt insbesondere vor, wenn die Annahme besteht, dass die Datensicherheit, insbesondere die Vertraulichkeit von Daten, gefährdet sein kann. Ein Datenschutzvorfall liegt auch bei jedem Sachverhalt vor, bei dem die Annahme besteht, dass Dritte unbefugt Zugriff oder Zugang zu personenbezogenen Daten haben oder hatten.

7. Versicherungsschutz und Haftung

(1) Arbeitsunfälle im Rahmen des Mobilen Arbeiten sind durch den Arbeitgeber zu versichern. Diese müssen allerdings in unmittelbarem Zusammenhang mit der Verrichtung der dienstbezogenen Tätigkeit bestehen.
(2) Die Haftung des Mitarbeiters sowie der in seinem Haushalt lebenden Familienangehörigen und berechtigter Besucher gegenüber dem Unternehmen ist auf Vorsatz und grobe Fahrlässigkeit beschränkt. Bei leichter Fahrlässigkeit haftet der Mitarbeiter anteilig, sofern der entstandene Schaden mit der beruflichen Tätigkeit in Zusammenhang steht. Verursachen berechtigte Besucher, die keine Haftpflichtversicherung besitzen, einen Schaden, haftet der Mitarbeiter im Rahmen seiner Sorgfaltspflicht, es sei denn, der Besucher handelte eigenverantwortlich. Im Schadensfall obliegt dem Mitarbeiter die Mitwirkungspflicht, den Schadenhergang nachvollziehbar darzulegen. Das Unternehmen übernimmt Schadenersatzansprüche von Dritten nur, wenn ein direkter Zusammenhang mit der außerbetrieblichen Arbeitsstätte besteht und der Mitarbeiter seiner Sorgfaltspflicht nachgekommen ist.

8. Verstöße

(1) Die Verletzung der Pflichten aus dieser Mitarbeitervereinbarung kann zu Datenschutzverstößen oder zur Beeinträchtigung des Schutzes von Geschäftsgeheimnissen führen und Ansprüche auf Unterlassung, Beseitigung, Schadenersatz oder Auskunft nach sich ziehen.
(2) Der Mitarbeiter wird ausdrücklich darauf hingewiesen, dass eine Verletzung der Pflichten aus dieser Mitarbeitervereinbarung zugleich eine Verletzung arbeitsvertraglicher Pflichten darstellt und zu arbeitsrechtlichen Maßnahmen wie Abmahnung oder fristloser Kündigung führen kann.

9. Beendigungsbedingungen

(1) Die Vereinbarung zum Mobilen Arbeiten und/oder zur Nutzung von Co-Working-Räumlichkeiten kann von beiden Seiten mit einer Ankündigungsfrist von zwei Wochen aufgegeben werden. Im Übrigen kann die Berechtigung zum Mobilen Arbeiten jederzeit aus wichtigem Grund widerrufen werden. Ein wichtiger Grund ist insbesondere dann gegeben, wenn dringende betriebliche Erfordernisse vorliegen, wenn der Mitarbeiter das der Arbeit im Mobilen Arbeiten zugrunde liegende besondere Vertrauensverhältnis missbraucht oder die gesetzlichen Anforderungen zum Schutz der betrieblichen Informationen, Weisungen des Arbeitgebers oder Vorgaben dieser Vereinbarung nicht eingehalten werden.
(2) Einen Wohnungswechsel muss der Mitarbeiter dem Arbeitgeber unverzüglich anzeigen.
(3) Die Arbeit im Mobilen Arbeiten endet spätestens mit dem Zeitpunkt des rechtlichen Endes des Arbeitsverhältnisses.
(4) Die vom Arbeitgeber überlassenen Arbeitsmittel sowie die Arbeitsunterlagen und Zugangsdaten sowie etwaige Kopien sind nach Aufgabe des Mobilen Arbeiten und/oder der Nutzung von Co-Working-Räumlichkeiten unverzüglich dem Arbeitgeber zur Verfügung zu stellen. Der Arbeitgeber kann alternativ die Vernichtung der Arbeitsmittel oder die Löschung von betrieblichen Informationen verlangen, sofern dies dem Mitarbeiter zumutbar ist und entsprechend dem Stand der Technik durchgeführt werden kann.

10. Schlussbestimmungen

(1) Ist oder wird eine Bestimmung dieser Vereinbarung unwirksam, bleibt die Wirksamkeit der übrigen Bestimmungen dieser Ergänzungsvereinbarung davon unberührt. In diesem Fall soll die unwirksame Bestimmung durch die Beteiligten durch eine wirksame Bestimmung ersetzt werden, die dem von den Beteiligten verfolgten Zweck im Rahmen des rechtlich Zulässigen so nahe wie möglich kommt.
(2) Änderungen, Ergänzungen und die Aufhebung dieser Vereinbarung haben nur Gültigkeit, wenn sie schriftlich erfolgen und von beiden Beteiligten rechtsverbindlich unterzeichnet sind. Ausgeschlossen sind damit insbesondere Vertragsänderungen durch betriebliche Übung. Individualabreden sind hiervon ausdrücklich ausgenommen.

_____	_____
Ort, Datum	Mitarbeiter*in

Verschwiegenheitserklärung für Mitarbeiter*innen

Der*die Mitarbeiter*in _____

– nachstehend einheitlich bezeichnet als **Mitarbeiter*in** –

verpflichtet sich, gegenüber **BeWo Durchblick (Inh. Tiara Schmitz)**

– nachstehend bezeichnet als **Arbeitgeber** –

die nachstehenden Bestimmungen einzuhalten:

1 Ich werde personenbezogene Daten, die mir im Rahmen meiner Tätigkeit für den Arbeitgeber bekannt werden, nur im Rahmen der mir erteilten Aufgaben und Weisungen sorgfältig verarbeiten. Ich werde jegliche Verarbeitung, die zu diesen Zwecken nicht erforderlich ist, unterlassen.
2 Mir ist bekannt, dass sich personenbezogene Daten dabei besonders auch auf Gesundheitsdaten von Leistungsberechtigten beziehen können.
3 Ich bestätige, dass ich die im Zusammenhang mit meiner Tätigkeit erlangten Unterlagen oder sonstige nicht allgemein zugängliche Informationen Dritten gegenüber vertraulich behandeln werde. Ich werde diese Unterlagen und Informationen ohne vorherige schriftliche Vereinbarung der verpflichtenden Stelle auch nicht für eigene Zwecke oder andere Arbeitgeber, Auftraggeber o.ä. benutzen.
4 Bestehende Vorschriften über den Umgang bzw. die Sicherung personenbezogener Daten sind zu beachten. Die Bestimmungen der Datenschutzgesetze sowie die einschlägigen Straf- und Bußgeldvorschriften sind mir bekannt.
5 Mir ist bewusst, dass Verstöße gegen das Datengeheimnis insbesondere nach Art. 83 DSGVO mit Bußgeldern belegt sowie nach 84 DSGVO in Verbindung mit § 42 BDSG-neu zur Strafbarkeit führen und mit Geld- oder Freiheitsstrafe geahndet werden können. Eine Verletzung des Datengeheimnisses kann zugleich eine Verletzung arbeitsvertraglicher Pflichten oder spezieller Geheimhaltungspflichten darstellen und beispielsweise zu Abmahnung, fristloser oder fristgerechter Kündigung und/oder Schadensersatzpflichten führen.
6 Ich werde den Arbeitgeber bei Verdacht auf mögliche Unregelmäßigkeiten bei der Datenverarbeitung informieren.
7 Die Pflichten zum Schutz der personenbezogenen Daten, von denen der*die Mitarbeiter*in Kenntnis oder die Verfügungsgewalt erlangte, gelten auch nach Beendigung des vertraglichen Verhältnisses zwischen dem Arbeitgeber und dem*der Mitarbeiter*in weiter.
8 Sonstige Geheimhaltungs- und Schweigepflichten arbeitsrechtlicher oder dienstrechtlicher Natur sind durch diese Verpflichtung nicht betroffen/berührt.

Eine Abschrift der Verschwiegenheitserklärung habe ich erhalten.

Ort, Datum _____,

_____ _____

Unterschrift Arbeitgeber Unterschrift Mitarbeiter*in