Mitarbeiterhandbuch

mbi GmbH

Stand 15.12.2023

Verantwortlich: Bereich Personal

Inhaltsverzeichnis

Vorwort

Liebe Mitarbeiterin, lieber Mitarbeiter,

wir freuen uns, dass du Teil unseres Teams bist und deine Fähigkeiten und deine Zeit mbi zur Verfügung stellst.

Das Mitarbeiterhandbuch soll dir wichtige Informationen über mbi und über unsere Zusammenarbeit geben. Es ist eine Ergänzung zu deinem Arbeitsvertrag und beinhaltet Unternehmensrichtlinien, Arbeitsbedingungen und Verhaltensregeln, welche verbindlich festgelegt sind. Diese sollen dazu dienen, um dich an deinem Arbeitsplatz zurechtzufinden und dich mit den Abläufen bei mbi vertraut zu machen.

Im Mitarbeiterhandbuch findest du auch unsere Unternehmensmission und Unternehmensziele, welche die Grundlage unserer Arbeit bilden.

Falls du Anregungen oder Verbesserungsvorschläge zu dem Mitarbeiterhandbuch hast, sind wir immer offen für Feedback. Du kannst diese gerne an die Personalabteilung weitergeben.

Die aktuelle Version des Mitarbeiterhandbuches findest du im mbi Intranet. Sollten wichtige Änderungen in diesem Handbuch vorgenommen werden, informieren wir dich und alle mbi Mitarbeiter.

Wir hoffen, dass du dich wohlfühlst und wir gemeinsam im Team unsere Unternehmensziele erreichen.

Mit herzlichen Grüßen

Benjamin Löw
Personalleiter

Unternehmensmission

Die mbi GmbH unterstützt durch innovative Softwareprodukte weltweit Organisationen, ihre Geschäftsprozesse einfacher, effizienter und transparenter zu gestalten. Die Software und die begleitenden Dienstleistungen werden ständig an die neuesten Anforderungen angepasst und verbessern damit den Nutzen der Software für unsere Kunden. Dadurch können Organisationen ihre Verantwortung für die Gesellschaft immer besser wahrnehmen. Wir leisten dadurch einen Beitrag zur gesellschaftlichen Entwicklung und zur Verbesserung der Lebensqualität von Menschen weltweit.

Unternehmensziele

Unsere Mitarbeiter

Unsere Mitarbeiter sind unsere wichtigste Ressource. Wir wollen, dass unsere Mitarbeiter begeistert davon sind für mbi zu arbeiten.

Dies wollen wir erreichen, indem wir große Wertschätzung jedem einzelnen entgegenbringen und ihm ein Umfeld schaffen, indem er gerne arbeitet und gemäß seinen Begabungen und Fähigkeiten optimal eingesetzt und gefördert wird.

Unsere Kunden

Unsere Kunden sind die Grundlage unseres Unternehmenserfolgs. Ihre Zufriedenheit ist zentrales Ziel unseres Unternehmens und wir geben täglich unser Bestes, um unsere Kunden zu begeistern.

Wir sehen jeden Menschen als Person an, der Verständnis und Respekt verdient, und versuchen dies in unserem geschäftlichen Umgang zu leben. Offenheit, Ehrlichkeit und große Wertschätzung im Umgang mit unseren Kunden ist daher für uns sehr wichtig.

Produkte und Dienstleistungen

Wir bieten unsere Produkte und Dienstleistungen nur dann an, wenn wir davon überzeugt sind, dass sie unseren Kunden Vorteile bringen. Die Zahl der Unternehmen und Organisationen und auch Anwender wächst ständig und bietet uns dadurch die Möglichkeit, unsere Produkte und Dienstleistungen zum Nutzen unserer Kunden immer weiter zu optimieren.

Unsere Partner

Höchstleistung kann man nur erbringen durch Konzentration. Wir wollen uns auf unsere Kernkompetenz konzentrieren und wo es sinnvoll ist Partner zur Unterstützung heranziehen. Dabei ist uns eine langfristige, faire und ständig verbesserte Zusammenarbeit mit unseren Partnern wichtig.

Unsere Finanzen

Stetig wachsende Umsätze mit stabilem Gewinnanteil erhöhen unser Eigenkapital und sorgen für Stabilität des Unternehmens.

Dies stärkt das Vertrauen unserer Mitarbeiter, Kunden und Partner in das Unternehmen und lässt Mitarbeiter lange bei mbi arbeiten und Kunden und Partner in langfristigen und bedeutsamen Projekten zusammenarbeiten.

Soziale Verantwortung

Wir sehen unsere soziale Verantwortung für die Gesellschaft und engagieren uns im Rahmen unserer Möglichkeiten.

Von unserem erwirtschafteten Gewinn geben wir einen stetig wachsenden Anteil für Projekte zum Nutzen der Menschen ab. Den Schwerpunkt setzen wir dabei auf Projekte unserer Kunden in den Entwicklungsländern und Projekte für Menschen in unserer Region.

Nachhaltigkeit

Wir verfolgen eine konsequente Nachhaltigkeitsstrategie, die es uns ermöglicht, unseren ökologischen Fußabdruck immer weiter zu reduzieren bis hin zu dem Ziel, ein klimaneutrales Unternehmen zu werden.

Unternehmensstandorte

Wetzlar

Konrad-Adenauer-Promenade 17

35578 Wetzlar

Rechtenbach

Weidenhäuser Straße 27

35625 Hüttenberg

Arbeitszeit

Tägliche Arbeitszeit und Pausen

Die regelmäßige Arbeitszeit beträgt 35 Stunden pro Woche. Die tägliche Arbeitszeit sollte, wie im ArZG §3 beschrieben, grundsätzlich nicht mehr als 8 Stunden betragen. Sie kann auf 10 Stunden verlängert werden, wenn innerhalb von sechs Kalendermonaten oder innerhalb von 24 Wochen im Durchschnitt acht Stunden werktäglich nicht überschritten werden. Länger als 6 Stunden am Stück darf der Arbeitnehmer nicht arbeiten. Bei einer Arbeitszeit von mehr als 6 Stunden ist eine Ruhepause von 30 Minuten vorgeschrieben, bei mehr als 9 Stunden 45 Minuten. Die Verantwortung hierfür liegt beim Arbeitnehmer. Der Arbeitgeber wird ihn hierbei unterstützen.

Die Mittagspause sollte zwischen 12:00 Uhr und 14:00 Uhr genommen werden. Für die Pause können die Aufenthaltsräume genutzt werden. Am Arbeitsplatz sollte die Pause nur in Ausnahmefällen stattfinden.

Die Kernarbeitszeit liegt zwischen 9:00 Uhr und 15:30 Uhr und soll die interne und externe Erreichbarkeit durch Kollegen, Partner und Kunden erleichtern. Am Freitag endet die Kernarbeitszeitzeit um 13:00 Uhr. Sie gilt für alle Mitarbeiter mit Vollzeitstellen (d.h. mit 35 Stunden oder mehr). Aus betrieblichen Gründen kann es vorkommen, dass Termine außerhalb dieser Zeiten wahrgenommen werden müssen.

Zeiterfassung

Für die Erfassung der täglichen Arbeitszeit führt der Mitarbeiter eine Excel-Datei, in welche die Arbeits- sowie die Fehlzeiten durch Krankheit, Urlaub und Sonstiges erfasst werden. Die Vorlage dazu wird jährlich zentral vom Bereich Personal angelegt und für jeden Mitarbeiter in dessen Mitarbeiterverzeichnis bereitgestellt. Zusätzlich erfolgt eine kurze Beschreibung der einzelnen Tätigkeiten sowie die Zuordnung zu den Kostenstellen und Kostenträgern tagesaktuell in der mbi base. Die erfasste tägliche Arbeitszeit in der Excel-Datei und in der mbi base muss übereinstimmen.

Überstunden

Die Arbeitszeit der Mitarbeiter darf innerhalb von sechs Kalendermonaten im Durchschnitt acht Stunden werktäglich nicht überschreiten. In einem Zeitrahmen von sechs Monaten müssen Über- und Minusstunden ausgeglichen sein. Innerhalb dieses Rahmens gelten folgende Vereinbarungen:

Grüner Bereich

Alle Mitarbeiter verfügen über einen festgelegten zeitlichen Rahmen, den grünen Bereich, in dem sie ihre Über- oder Minusstunden aufbauen und eigenverantwortlich verwalten können. Dieser Bereich liegt zwischen 30 Minusstunden und 30 Überstunden. Solange dieses Stundenkontingent nicht überzogen wird, bewegt es sich im definierten grünen Bereich. Die Mitarbeiter können innerhalb dieses Stundenkontingentes Überstunden anhäufen oder abbauen.

Gelber Bereich

Über- oder unterschreitet die Stundenzahl auf seinem Zeitkonto den Rahmen des grünen Bereichs, muss er sich sofort mit dem Vorgesetzten in Verbindung setzen. Das Über- oder Unterschreiten des Kontingents liegt nicht mehr im alleinigen Verantwortungsbereich des Mitarbeiters, es kann nur noch in Absprache und mit Erlaubnis des Vorgesetzten gehandelt werden. Überstunden im gelben Bereich werden auf dem Arbeitszeitkonto nur berücksichtigt, wenn sie vom jeweiligen Vorgesetzten angeordnet oder genehmigt wurden.

Roter Bereich

Bei 60 Über- oder Minusstunden beginnt der rote Bereich. Die Überschreitung dieser Grenze darf nur ausnahmsweise und auf ausdrückliche Genehmigung hin stattfinden. Sie macht die Rücksprache mit der Geschäftsleitung notwendig. Gleichzeitig wird die Geschäftsleitung gemeinsam mit dem Mitarbeiter eine Strategie festlegen, wie er sein Stundenguthaben wieder ab- oder aufbauen kann.

Unberührt von den oben genannten Regelungen besteht für die Mitarbeiter die Möglichkeit, ein Langzeitkonto für Arbeitsstunden zu eröffnen. Dies kann nur in Absprache mit der Geschäftsleitung erfolgen um z. B.:

- längerfristige Auslastungsschwankungen zu bewältigen
- einen Langzeiturlaub (z. B. für Weiterbildungszwecke) anzusparen
- zeitweise auf Teilzeitarbeit bei unverändertem Entgelt übergehen zu können

Arbeit an Sonn- und Feiertagen

Der Sonntag und die gesetzlichen Feiertage sollen der Erholung der Arbeitnehmer dienen und daher grundsätzlich nicht als Arbeitstage genutzt werden.

Nur in besonders begründeten Ausnahmefällen und nach Rücksprache mit der Geschäftsführung kann von dieser Regelung abgewichen werden.

Fehlzeiten

Fehlzeiten durch Urlaub, Sonderurlaub und Krankheit werden mit der gemäß Arbeitsvertrag üblichen Arbeitszeit berechnet.

Im Krankheitsfall ist der Vorgesetzte bzw. bei Nichtanwesenheit dessen Stellvertreter umgehend persönlich zu informieren. Spätestens am dritten Tag muss die Arbeitsunfähigkeit (AU) vom Arzt bescheinigt werden.

Geht ein Mitarbeiter während des Tages auf Grund von Krankheit nach Hause, wird sein Stundenkonto auf die täglich übliche Stundenzahl aufgefüllt.

Planbare Arztbesuche sollten in Randzeiten vorgenommen werden und werden somit nicht als Arbeitszeit anerkannt; nicht planbare Arztbesuche, z. B. bei Unwohlsein, können als Arbeitszeit erfasst werden.

Dienstreisen

Fehlzeiten durch Dienstreisen werden vergütet. Während einer Dienstreise werden die reinen Fahrt- und Arbeitszeiten vergütet, maximal aber 10 Stunden je Tag. Für die Fahrtzeiten gelten folgende Regelungen:

- Für reine Reisetage wird die tatsächliche Reisezeit angesetzt, allerdings maximal 8 Stunden. Geht die An- oder Abreise über zwei Tage so können für beide Tage jeweils maximal 4 Stunden angesetzt werden.
- Reist der Arbeitnehmer auf Anweisung der Geschäftsführung im PKW kann die Reisezeit als Arbeitszeit angesetzt werden. Bei einer Reise mit dem Flugzeug oder der Bahn zählt die Zeit nur dann als Arbeitszeit, wenn sie auch zum Arbeiten genutzt wird.

Tagungen, Kongresse und Fortbildungsveranstaltungen werden mit max. 8 Stunden je Tag berechnet.

Sonn- und Feiertage werden dabei gleichermaßen, wie in Hessen berücksichtigt.

Dienstliche Fahrten zwischen Unternehmensstandorten

Dienstliche Fahrten mit einem privaten PKW zwischen unseren beiden Unternehmensstandorten werden von mbi mit 0,30 Cent pro gefahrenen Kilometer erstattet, wenn kein Firmenwagen zur Verfügung steht. Für die Abrechnung der Fahrten ist das Musterformular „Fahrtkostenabrechnung WZ-RE“ zu verwenden. Am Ende jedes Quartals wird die Fahrtkostenabrechnung von der Verwaltung geprüft und das Geld je nach Höhe des Betrags bar ausbezahlt oder überwiesen. Die ausbezahlten Fahrtkostenabrechnungen liegen im Mitarbeiterverzeichnis im Ordner „Ausbezahlt“ als PDF ab.

Urlaub

Jahresurlaub

Die Urlaubsregelung richtet sich nach § 7 BUrlG:

Der Urlaub sollte im laufenden Kalenderjahr genommen werden. Bei der Festlegung des Urlaubs sind die Wünsche des Mitarbeiters und die des Unternehmens zu berücksichtigen, die Abstimmung sollte mit dem Vorgesetzten erfolgen. Eine Übertragung des Urlaubs ist bis März des nächsten Kalenderjahres erlaubt, in Ausnahmefällen kann der Urlaub, in Absprache mit der Geschäftsführung, auch später genommen werden. Dies muss durch den Vorgesetzten per Mail bei der Geschäftsführung beantragt werden.

Während des Urlaubs darf der Arbeitnehmer keine dem Urlaubszweck widersprechende Erwerbstätigkeit leisten.

Sonderurlaub

Zu den folgenden Anlässen gewährt mbi Sonderurlaub:

Anlass	**Tage**
Hochzeit	1
Silberhochzeit	1
Geburt eines Kindes	1
Einschulung des Kindes in die Grundschule	1
Tod eines nahen Angehörigen (Verwandter ersten Grades)	1
Prüfungsvorbereitung Abschlussprüfung Auszubildende	1
25-jähriges Dienstjubiläum	1

Für die Geburt eines Kindes erhält der Mitarbeiter einen Tag Sonderurlaub, allerdings nur, wenn keine Elternzeit im ersten Lebensmonat des Kindes in Anspruch genommen wird. Der Tag der Geburt fällt dann bereits in die Elternzeit.

Sonstige Urlaubsregelungen

Fallen folgende Tage auf einen Werktag, sind diese als „halbe“ Arbeitstage anzusehen:

- Heiligabend
- Silvester

Möchte man an diesen Tagen Urlaub nehmen, ist somit nur ein „halber“ Urlaubstag einzubringen.

Sonstige Regelungen

Kleiderordnung

Jeder Mitarbeiter hat auf ein gepflegtes äußeres Erscheinungsbild zu achten. Hierbei hat er die Freiheit, seine Kleidung selbst zu wählen und muss keine Dienstkleidung tragen. Es wird Wert daraufgelegt, dass die Kleidung nicht zu lässig wirkt und der Mitarbeiter sich jederzeit zu einem eventuellen Kundenbesuch bei mbi präsentieren kann.

Für Termine mit Kunden sollte die Kleidung so gewählt werden, dass man immer „etwas besser gekleidet ist“ als der Kunde. Dem Kunden wird hiermit Wertschätzung entgegengebracht.

Mitarbeitergespräch

Einmal pro Jahr findet ein Gespräch zwischen dem Mitarbeiter und seinem Vorgesetzten statt. Hierbei soll besonders über die persönliche Arbeits- und Berufssituation, Orientierung und Engagement des Mitarbeiters bei seiner Arbeit sowie seine Identifikation mit mbi gesprochen werden. Zwei Wochen vor dem Termin versendet der Personalbereich Vorbereitungsdokumente an den Mitarbeiter.

Nähere Informationen und die notwendigen Dokumente zum Mitarbeitergespräch sind im Intranet zu finden.

mbi News

Das Intranet ist unser firmeninternes Veröffentlichungsmedium. Auf der Startseite des Intranets sollen sich alle Mitarbeiter wöchentlich über aktuelle Themen und wichtige Neuigkeiten informieren. Ältere Beiträge werden jeweils im Verzeichnis des zugehörigen Bereichs abgelegt. Im Intranet befindet sich auch die Ressourcen-Datei, sowie die Anwesenheitsliste und die aktuellen Monatskennzahlen.

Mitarbeiterbesprechung

Mindestens drei Mal im Jahr findet eine gemeinsame Mitarbeiterbesprechung für alle mbi Mitarbeiter statt. Diese dient vor allem dem Informationsaustausch. Unter anderem werden darin die Mitarbeiter über die aktuelle Situation von mbi, die einzelnen Projekte in den Bereichen, die finanzielle Situation und über weitere relevante Themen informiert.

Mitarbeiterküche

Jeder Mitarbeiter kann die Einrichtungen der Mitarbeiterküche nutzen. Getränke und frisches Obst werden den Mitarbeitern von der mbi GmbH unentgeltlich zur Verfügung gestellt. Die Küche sollte gewissenhaft genutzt und so verlassen werden, wie sie vorgefunden wurde.

Private Telefonate

Private Telefonate von Mitarbeitern sollten während der Arbeitszeit vermieden werden. Wenn wichtige Gründe für einen privaten Anruf während der Arbeitszeit vorliegen, sollten die Telefonate kurzgehalten- oder bei längeren Gesprächen die Zeit aus der Zeiterfassung herausgenommen werden.

Die Nutzung des Smartphones sollte während der Arbeitszeit vermieden werden und sich auf die Pausen beschränken.

Internetnutzung

Das Internet ist aus dem täglichen Arbeitsablauf nicht mehr wegzudenken, da es als wichtige Informationsquelle dient. Die Nutzung des Internets während der Arbeitszeit sollte sich aber auf rein berufliche Aufgaben beschränken.

Auch das Lesen und Senden von privaten E-Mails sollte deshalb auf Pausen oder die Freizeit verschoben werden. Hierfür sollten die Mitarbeiter dann einen E-Mail-Account nutzen, der über einen Web-Browser erreichbar ist (z. B. gmx oder web.de). Der mbi-E-Mail-Account darf weder innerhalb noch außerhalb der Arbeitszeit für private Zwecke genutzt werden; andere Mitarbeiter müssen – beispielsweise im Rahmen der Urlaubs- oder Krankheitsvertretung - jederzeit Zugriff auf den dienstlichen E-Mail-Account haben können, ohne dabei auf private Inhalte zu stoßen.

Umgang mit E-Mail Anhängen

Die Anhänge von E-Mails sind sehr vorsichtig zu behandeln. Es gibt immer wieder Virusübertragungen durch Dateianhänge an E-Mails. Der Schaden, den ein solcher Virus anrichten kann, ist enorm.

Es sollte die Regel beherzigt werden, Dateien nur dann zu öffnen, wenn sie für die Arbeit notwendig sind und aus einer sicheren Quelle stammen. Ist das nicht der Fall, sollte die E-Mail gelöscht werden.

Zutritt zu den Geschäftsräumen

Während der Geschäftszeiten kann die Eingangstür nur in Verbindung mit der Eingabe eines regelmäßig wechselnden Codes geöffnet werden. Dieser Türcode darf nicht an Dritte weitergegeben werden. Die Eingangstüren sind ständig geschlossen zu halten. Auch bei kurzen Pausen vor der Tür darf die Verriegelung nicht deaktiviert oder blockiert werden.

Besucher müssen klingeln und werden von Mitarbeitern im Sekretariat eingelassen. Sie dürfen sich nicht unbeaufsichtigt im Gebäude bewegen und allein in Büros zurückgelassen werden.

Alarmanlage

Wenn sich niemand im Firmengebäude befindet, muss das Gebäude alarmgeschützt sein. Der letzte Mitarbeiter, der bei Arbeitsschluss das Gebäude verlässt, muss sicherstellen, dass:

- keine anderen Mitarbeiter versehentlich eingeschlossen werden,
- alle Fenster und Außentüren geschlossen sind,
- die Rollläden heruntergelassen sind und das Licht ausgeschaltet ist,
- die Eingangstür abgeschlossen und die Alarmanlage aktiviert ist.

Um den Aufwand zu reduzieren, sollten die Mitarbeiter, die als letzte ihre Etage verlassen, dort bereits die Fenster schließen, Rollläden herunterlassen und das Licht ausschalten. Mitarbeiter, die nicht über einen Schlüssel verfügen, sollten sich abends mit Mitarbeitern abstimmen, die Schlüssel haben.

Im Protokoll des Alarmsystems ist vom IT-Administrator einsehbar, welcher Schlüssel wann genutzt wurde, um die Alarmanlage ein- oder auszuschalten.

Passwörter und Benutzerkonten

Alle Mitarbeiter haben einen persönlichen, passwortgeschützten PC-Zugang. Dieser dient beispielsweise dazu, Zugriffsrechte auf Systeme und Verzeichnisse individuell zu steuern, Mitarbeiter bei der Zusammenarbeit an Dokumenten zu identifizieren oder die Erreichbarkeit auf MS Teams zu kennzeichnen.

Niemand darf den PC-Zugang eines anderen Mitarbeiters nutzen. Passwörter jeder Art dürfen, auch im eigenen Interesse des Mitarbeiters, grundsätzlich nicht an andere weitergegeben werden. An- und Abmeldungen an den Systemen werden protokolliert und sind vom IT-Administrator einsehbar.

Die Mitarbeiter müssen bei jedem Verlassen des Arbeitsplatzes – auch für kurze Zeit – den PC sperren. Passwörter dürfen nicht für andere zugänglich am Arbeitsplatz aufbewahrt werden.

In regelmäßigen Abständen fordert das System dazu auf, das Passwort zu ändern. Dabei sind möglichst unterschiedliche Passwörter zu verwenden, die nicht von anderen erraten werden können.

Lesezugriffe auf Outlook-Kalender

Die Outlook-Kalender sind das zentrale System für die Verwaltung der Termine bei mbi. Zur Vereinfachung der Terminplanung ist es jedem Mitarbeiter möglich, mit einem Lesezugriff die Kalender und somit die internen und externen Termine der anderen Mitarbeiter einzusehen.

Datenschutz

Der rechtskonforme und nachhaltige Schutz personenbezogener Daten im Unternehmen ist in den Dokumenten „Unternehmensrichtlinie Datenschutz“ und der „Benutzerrichtlinie IT“ geregelt. Beide Dokumente befinden sich im Anhang des Mitarbeiterhandbuches und sind ebenfalls Vertragsbestandteil.

Musik

Es sollte während der Arbeitszeit keine Musik gehört werden, da dies die Konzentration beeinträchtigt und auch die anderen Mitarbeiter stören könnte.

Rauchen

Regelung nach dem §5 ArbStättV:

Das Rauchen im Firmengebäude ist nicht gestattet. Es wird darum gebeten, hierfür den Außenbereich aufzusuchen. Für Raucher steht deshalb im Eingangsbereich sowie im Garten ein Aschenbecher zur Verfügung.

Alkohol und Drogen

Alkoholische Getränke und Rauschmittel dürfen grundsätzlich nicht während der Arbeitszeit zu sich genommen werden. Auch sollen die Mitarbeiter nicht im angetrunkenen Zustand oder im Rausch zur Arbeit kommen.

Parkplätze

Vor den mbi Gebäuden stehen den Mitarbeitern Parkplätze zur Verfügung. Parkplätze mit Ladesäule sollten für E-Autos freigehalten werden.

Home-Office

Um die Unternehmensinteressen und persönliche Bedürfnisse unserer Mitarbeiter gut in Einklang zu bringen und ein flexibles Arbeiten zu ermöglichen, bietet mbi einem Großteil der Mitarbeiter die Möglichkeit zum Arbeiten im Home-Office (HO) an. Folgende Übersicht soll dabei helfen die Voraussetzungen dafür möglichst einheitlich und transparent zu regeln:

	1	2	3	4	5
Mitarbeiter-gruppe	Reinigungs-kräfte Hausmeister	Mitarbeiter in Probezeit/Einarbeitung Praktikanten Aushilfen Auszubildende	Führungskräfte Verwaltung IT-Administrator PE F&C Werkstudenten	Software-entwickler Berater Business-Analysten Marketing Softwaretester Übersetzer	Mitarbeiter, bei denen besondere Situationen Berücksichtigung finden.
Anforderung an Präsenz	Für die Aufgaben-erledigung und/oder Betreuung ist die An-wesenheit im Unternehmen zwingend erforderlich.	Für die Aufgaben-erledigung ist die An-wesenheit temporär erforderlich oder HO aufgrund der geringen Stundenzahl nicht sinnvoll.	Es müssen viele Aufgaben vor Ort erledigt werden (bspw. Sekretariats-aufgaben, Dienste, Assistenz-aufgaben, Betreuung von Mitarbeitern) oder durch die Stellenprofile ist eine Anwesenheit besonders wichtig.	Zeitweise Anwesenheit des Mitarbeiters ist erforderlich.	Individuelle Situation des Mitarbeiters wird berücksichtigt (langer Fahrtweg, besondere familiäre Situation, etc.)
Anzahl HO Tage pro Woche	0 Tage	0 Tage	Bis zu 1 Tag	Bis zu 2 Tage	Flexibel

Die Festlegung der HO Tage erfolgt in Absprache mit dem Vorgesetzten. Mitarbeiter, die aufgrund ihrer persönlichen Situation eine individuelle Regelung wünschen (Mitarbeitergruppe 5), stimmen dies über ihren Vorgesetzten mit der Geschäftsleitung ab. Sollten bestimmte Unternehmensinteressen die Anwesenheit des Mitarbeiters im Unternehmen erfordern (bspw. Präsenztermine, Krankheitsvertretung), kann an diesen Tagen kein HO in Anspruch genommen werden. Bei Mitarbeitern, die regelmäßig weniger als 5-Tage pro Woche arbeiten, werden die HO Tage anteilig im Verhältnis zu den Arbeitstagen berechnet.

Folgende Voraussetzungen müssen für die Arbeit im HO erfüllt sein:

- Unterzeichnung der Richtlinie zum Home Office/Mobile Office
- Ein geeigneter Arbeitsplatz muss vorhanden sein
- Der Mitarbeiter zeigt verantwortungsbewusstes Verhalten im Umgang mit der Arbeit von zuhause und erbringt eine vergleichbare Arbeitsleitung

Die Einräumung der Arbeit von zu Hause aus erfolgt durch die entsprechende Ausübung des Direktionsrechts durch mbi. Hierdurch wird – auch bei längerer Tätigkeit von zu Hause oder in mobiler Arbeit – kein Rechtsanspruch begründet. D.h., dass mbi unter Berücksichtigung der Grenzen des § 106 GewO, insbesondere billigen Ermessens, die Möglichkeit des „Home-Office“ oder mobiler Arbeit beenden und zukünftig wieder die Tätigkeit in den Betriebsstätten von mbi anordnen kann.

Nebenleistungen

Private Nutzung des Firmenwagens

Auch wenn dies im Arbeitsvertrag nicht näher geregelt ist, kann die Geschäftsführung einem Mitarbeiter im Einzelfall erlauben, einen Firmenwagen für private Zwecke zu nutzen. Die Fahrten müssen dann mit den gefahrenen Kilometern im Fahrzeug liegenden Fahrtenbuch als Privatfahrt gekennzeichnet werden. Sämtliche Kosten, die das Fahrzeug im Laufe des Jahres verursacht hat (Tanken, Versicherung, Steuern, Reparaturen, Abschreibung), werden am Ende des Jahres zusammengerechnet und durch die Anzahl der gefahrenen Kilometer geteilt. Die privat gefahrenen Kilometer werden dann mit der berechneten Kostenpauschale je Kilometer multipliziert und mit dem Januargehalt des nächsten Jahres verrechnet. Vor der erstmaligen privaten Nutzung ist eine entsprechende Nutzungsvereinbarung durch den Nutzer zu unterzeichnen.

Gesundheitsbudget

mbi bietet seinen Mitarbeitern mit dem Gesundheitsbudget eine besondere Form der betrieblichen Krankenversicherung in Zusammenarbeit mit der Halleschen Krankenversicherung.

Durch monatliche Beitragszahlungen von mbi wird festangestellten Mitarbeitern ohne Befristung wird nach Ende der Probezeit ein Budget von 300€ pro Jahr von der Halleschen

Krankenversicherung zur Verfügung gestellt, welches von den Mitarbeitern für verschiedene Gesundheitsleistungen genutzt werden kann.

Das Gesundheitsbudget wird über eine App der Halleschen Krankenversicherung abgewickelt, in der bspw. Rezepte und Rechnungen hochgeladen werden können, um Kosten zurückerstattet zu bekommen.

Betriebliche Altersvorsorge

Für Mitarbeiter, die nach Ablauf der Probezeit mit zehn oder mehr Wochenstunden unbefristet angestellt sind, bietet mbi den Abschluss einer Rentenversicherung im Rahmen der betrieblichen Altersvorsorge bei der Debeka oder Allianz Versicherung an. Der Mitarbeiter erhält dazu abhängig von der Anzahl der Wochenstunden einen Arbeitgeberzuschuss von 50 € (bei 10 bis 29 Wochenstunden) bzw. 100 € (bei 30 bis 40 Wochenstunden).

Vermögenswirksame Leistungen

Bei Abschluss eines VL-Sparvertrages erhalten alle festangestellten Mitarbeiter monatlich 40 € vermögenswirksame Leistungen. Dazu muss eine Kopie des Vertrages vorgelegt werden. Die vermögenswirksamen Leistungen werden dann direkt an das Unternehmen überwiesen, mit dem der Sparvertrag geschlossen wurde.

Elektroauto-Leasing

Das Unternehmen bietet Mitarbeitern die Möglichkeit, über eine Gehaltsumwandlung ein E-Auto (kein Hybrid) als Firmenwagen zu nutzen. Als Grundlage für die monatliche Gehaltsumwandlung dienen die Leasingrate, die Kosten für die Fahrzeugwartung sowie die Versicherung. Detaillierte Regelungen zur Ausgestaltung und zur Kostentragung werden in dem zu schließenden Zusatz zum Arbeitsvertrag „Nutzungsvereinbarung für einen Firmenwagen“ getroffen. Damit wollen wir als Unternehmen einen Beitrag zu den Themen Nachhaltigkeit und Umweltschutz leisten. Diese Regelung gilt für Mitarbeiter, die nach Ablauf der Probezeit mit zwanzig oder mehr Wochenstunden unbefristet angestellt sind.

Fahrrad-Leasing

mbi hat einen Rahmenvertrag für Leasingfahrräder mit dem Unternehmen BusinessBike GmbH abgeschlossen. Für Mitarbeiter, die nach Ablauf der Probezeit mit zehn oder mehr Wochenstunden unbefristet angestellt sind, bietet das Unternehmen einen Zuschuss für ein Leasingfahrrad pro Mitarbeiter bei einem Händler seiner Wahl mit dem oben genannten Anbieter an. Das Unternehmen übernimmt dabei 50% der monatlichen Leasingkosten, maximal jedoch 25€ monatlich. Zusätzlich wird die Vollkaskoversicherung für das Leasingfahrrad von mbi getragen.

Jobticket

mbi möchte im Sinne der Nachhaltigkeit den Mitarbeitern einen Anreiz schaffen, mehr öffentliche Verkehrsmittel zu nutzen. Für alle Mitarbeiter besteht die Möglichkeit, das Jobticket und somit den ÖPNV unbegrenzt zu nutzen. Mitarbeiter können das Jobticket über unseren Rahmenvertrag online bestellen und zahlen. mbi gibt den Mitarbeitern einen Zuschuss von 24,50€/Monat zum Jobticket, welche als Rückerstattung über die Gehaltsabrechnung erfolgt.

Die Anleitung für die Bestellung des Jobtickets ist im Intranet unter der Personalbetreuung zu finden.

Weiterbildungsmodelle

mbi will die Weiterbildung von Mitarbeitern im Rahmen der Personalentwicklung fördern. Hierzu gibt es verschiedene Konzepte, die in verschiedenen Situationen der Mitarbeiter gültig sind. Das Konzept soll abhängig von der jeweiligen Dringlichkeit, die das Unternehmen in diesem Bereich für diesen Mitarbeiter sieht, gemacht werden.

Pflichtfortbildungen

Zu Pflichtfortbildungen gehören diejenigen Fortbildungen, die mbi als unbedingt notwendig für den Mitarbeiter sieht. Diese „geforderten“ Fortbildungen werden in Zeit und Kosten von mbi übernommen.

Empfohlene, erwünschte Fortbildungen

Weitere Fortbildungen, die zwar keine Pflichtfortbildungen darstellen, aber von einem Mitarbeiter ausdrücklich gewünscht werden, können unter Umständen auch von mbi unterstützt werden. Die Art der Unterstützung wird vom Vorgesetzten in Abstimmung mit der Geschäftsführung entschieden.

Selbständige Fortbildungszeit

Das selbständige Lesen von Fachzeitschriften ist im Rahmen der festgelegten jährlichen Budgets während der Arbeitszeit gestattet und wird bei den Zeitaufschrieben unter der entsprechenden Aktivität vermerkt. Die Auswahl der einzelnen Fachzeitschriften soll in Abstimmung mit dem jeweiligen Vorgesetzten getroffen werden.

Betriebssport

mbi bietet allen Mitarbeitern Betriebssport an. Der Betriebssport findet einmal monatlich statt. Er wird durch den Personalbereich organisiert. Die Kosten übernimmt mbi. Während des Betriebssports einschließlich Hin- und Rückfahrt, Umkleiden, Duschen sind die Mitarbeiter über die Berufsgenossenschaft unfallversichert. Voraussetzung hierfür ist, dass nur Mitarbeiter und keine Außenstehende teilnehmen, dass der Betriebssport mindestens monatlich stattfindet und dass während dieser Zeiten keine Wettkämpfe durchgeführt werden.

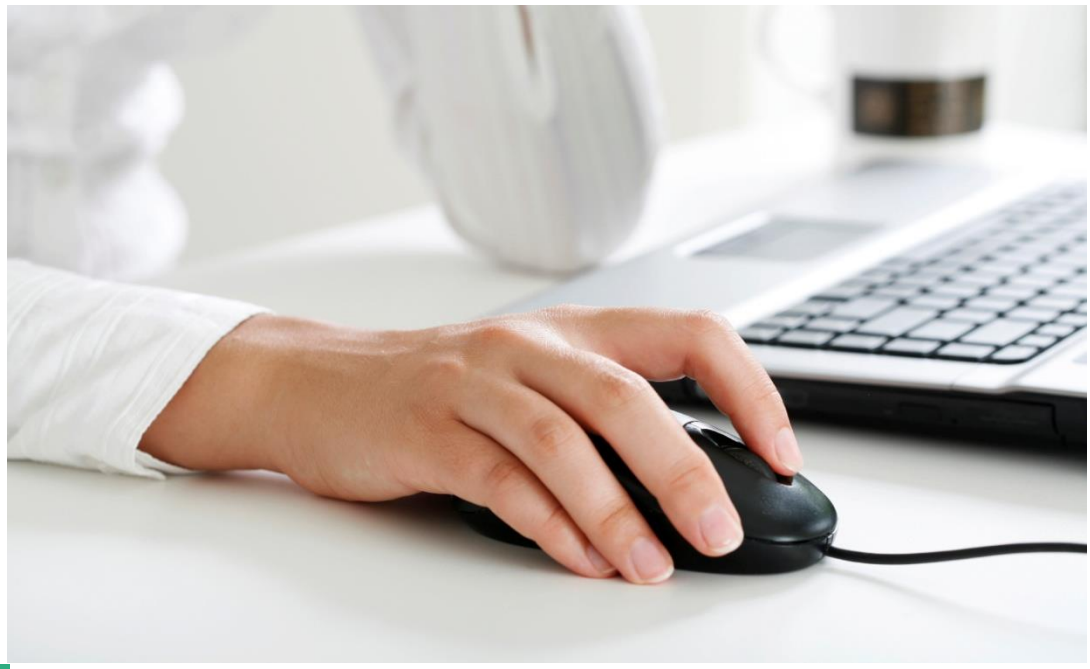
Anhang

Anlage 1: Unternehmensrichtlinie Datenschutz

Unternehmensrichtlinie

Datenschutz

Stand 28.02.2022



Bedeutung, Ziel, Zugänglichkeit

(1) Diese Unternehmensrichtlinie ist die verbindliche Basis für einen rechtskonformen und nachhaltigen Schutz personenbezogener Daten in unserem Unternehmen.

(2) Mit dieser Unternehmensrichtlinie sollen die Grundrechte und Grundfreiheiten von Betroffenen, insbesondere ihr Recht auf Schutz personenbezogener Daten gewahrt und geschützt werden.

(3) Die Unternehmensrichtlinie soll zudem den Beschäftigten ergänzend zu den regelmäßigen Datenschutzschulungen einen Überblick über die datenschutzrechtlichen Anforderungen in unserem Unternehmen geben.

(4) Die Unternehmensrichtlinie muss für alle Beschäftigten und leitenden Angestellten jederzeit leicht zugänglich sein.

Geltungsbereich

(1) Sie gilt persönlich für alle Beschäftigten sowie leitenden Angestellten unseres Unternehmens.

(2) Die Gebote und Verbote dieser Unternehmensrichtlinie gelten für jeglichen Umgang mit personenbezogenen Daten, unabhängig ob dieser elektronisch oder in Papierform vonstattengeht. Ebenso beziehen sie alle Arten von Betroffenen (Kunden, Beschäftigte, Lieferanten etc.) in ihren Geltungsbereich ein.

Begriffsbestimmungen

(1) Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Betroffener). Kundendaten gehören dabei ebenso zu den personenbezogenen Daten wie Personaldaten von Beschäftigten. Beispielsweise lässt der Name eines Ansprechpartners ebenso einen Rückschluss auf eine natürliche Person zu, wie seine E-Mail-Adresse. Es genügt, wenn die jeweilige Information mit dem Namen des Betroffenen verbunden ist oder unabhängig hiervon aus dem Zusammenhang hergestellt werden kann. Ebenso kann eine Person bestimmbar sein, wenn die Information mit einem Zusatzwissen erst verknüpft werden muss, so z. B. beim Autokennzeichen. Das Zustandekommen der Information ist für einen Personenbezug unerheblich. Auch Fotos, Video- oder Tonaufnahmen können personenbezogene Daten darstellen.

(2) Besondere Arten personenbezogener Daten sind Informationen, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen sowie eine eventuelle Gewerkschaftszugehörigkeit hervorgehen kann sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben bzw. der sexuellen Orientierung einer natürlichen Person.

(3) Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter 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, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(4) Einschränkung der Verarbeitung ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

(5) Profiling bezeichnet jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

(6) Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

(7) Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(8) Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(9) Empfänger ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

(10) Dritter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

(11) Eine Einwilligung des Betroffenen ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer

sonstigen eindeutigen bestätigenden Handlung, mit der der Betroffene zu verstehen gibt, dass er mit der Verarbeitung der ihn betreffenden personenbezogenen Daten einverstanden ist.

Datenschutzorganisation

(1) Das Unternehmen hat einen Datenschutzbeauftragten bestellt. Diesen erreichen Sie unter folgenden Kontaktdaten:

GenoRisk GmbH, Frau Heidrun Pautsch, E-Mail: datenschutz@mbi.de

(2) Der Datenschutzbeauftragte überwacht die Einhaltung der DS-GVO sowie anderer gesetzlichen Vorgaben, einschließlich der Vorgaben dieser und anderer Richtlinien des Unternehmens zum Datenschutz. Der Datenschutzbeauftragte berät und unterrichtet die Unternehmensleitung hinsichtlich bestehender Datenschutzpflichten und ist zuständig bei der Kommunikation mit Aufsichtsbehörden. Ausgewählte Prozesse werden stichprobenartig, risikoorientiert und in angemessenen Zeitabständen durch ihn auf ihre Datenschutzkonformität hin kontrolliert.

(3) Der Datenschutzbeauftragte nimmt seine Aufgaben weisungsfrei und unter Anwendung seines Fachwissens wahr. Er berichtet unmittelbar der Unternehmensleitung.

(4) Das Unternehmen bzw. seine Mitarbeiter haben den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen.

(5) Das Unternehmen stellt sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

Umgang mit personenbezogenen Daten

(1) Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten, es sei denn, eine gesetzliche Norm erlaubt explizit den Datenumgang. Personenbezogene Daten dürfen nach der DS-GVO grundsätzlich verarbeitet werden:

- Bei einem bestehenden Vertragsverhältnis mit dem Betroffenen.

  Beispiel: Die Speicherung und Verwendung erforderlicher personenbezogener Daten im Rahmen eines Nutzungsvertrages.

- Im Zuge vorvertraglicher Maßnahmen auf Anfrage des Betroffenen sowie der Vertragsabwicklung mit dem Betroffenen.

  Beispiel: Kunde K fordert Informationen zu Produkt X an und erwirbt dieses. Die erforderlichen Daten zur Zusendung des Informationsmaterials sowie zur Abwicklung des Rechtsgeschäfts (Lieferung der Ware sowie Zahlung des Kaufpreises) dürfen verarbeitet werden.

- Wenn und soweit der Betroffene eingewilligt hat.

Beispiel: Der Betroffene meldet sich zum Erhalt eines Newsletters an.

- Wenn eine rechtliche Verpflichtung besteht, der das Unternehmen unterliegt.

  Beispiel: Gesetzliche Aufbewahrungsfristen nach Handelsgesetzbuch (HGB) und Abgabenordnung (AO).

- Wenn berechtigte Interessen des Unternehmens bestehen, sofern nicht die Interessen oder Grundrechte des Betroffenen überwiegen, insbesondere wenn es sich um ein Kind handelt. Datenverarbeitungen unter Berufung auf ein berechtigtes Interesse sollten jedoch nicht ohne vorherige Beratung durch den Datenschutzbeauftragten vorgenommen werden.

  Beispiel: Die Nutzung der postalischen Anschrift zur Aussendung von Werbeschreiben.

(2) Betroffene dürfen nicht einer ausschließlich auf einer automatisierten Verarbeitung – so auch dem Profiling – beruhenden Entscheidung unterworfen werden, die ihnen gegenüber eine rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

(3) Personenbezogene Daten sind für einen zuvor festgelegten, eindeutigen und legitimen Zweck zu verarbeiten. Eine Datenhaltung ohne Zweck, so beispielsweise die Speicherung von Daten auf Vorrat, ist unzulässig.

(4) Falls möglich, sollte auf einen personenbezogenen Datenumgang verzichtet werden. Pseudonyme oder anonyme Datenverarbeitungen sind vorzuziehen.

(5) Die Änderung einer Ziel- und Zweckbestimmung, die einem Datenumgang ursprünglich zugrunde gelegt wurde, ist – neben der erklärten Einwilligung durch den Betroffenen – nur zulässig, wenn der Zweck der Weiterverarbeitung mit dem ursprünglichen Zweck vereinbar ist. Hierbei sind insbesondere die vernünftigen Erwartungen des Betroffenen hinsichtlich einer solchen Weiterverarbeitung gegenüber dem Unternehmen, die Art der verwendeten Daten, die Folgen für den Betroffenen sowie Möglichkeiten einer Verschlüsselung oder Pseudonymisierung zu berücksichtigen.

(6) Der Betroffene ist bei der Erhebung seiner personenbezogenen Daten umfassend über den Umgang mit seinen Daten zu informieren. Die Information hat die Zweckbestimmung, die Identität der verantwortlichen Stelle, die Empfänger seiner personenbezogenen Daten sowie alle sonstigen Information im Sinne des Art. 13 DS-GVO zu beinhalten, um eine faire und transparente Verarbeitung zu gewährleisten. Die Information ist in einer verständlichen und leicht zugänglichen Form sowie einer möglichst einfachen Sprache zu verfassen. Die Umsetzung in unserem Unternehmen erfolgt unter anderem durch Verlinkung der Datenschutzinformationen in jeder E-Mail-Signatur.

(7) Werden personenbezogene Daten nicht beim Betroffenen erhoben, sondern werden beispielsweise bei einem anderen Unternehmen beschafft, ist der Betroffene nachträglich und umfassend gem. Art. 14 DS-GVO über den Umgang mit seinen zu Daten informieren. Dies gilt auch für die Änderung einer Ziel- und Zweckbestimmung der Datenverarbeitung.

(8) Personenbezogene Daten müssen sachlich richtig und möglichst auf dem neusten Stand sein. Der Umfang der Datenverarbeitung sollte hinsichtlich der festgelegten Zweckbestimmung erforderlich und relevant sein. Die jeweilige Fachabteilung hat für die Umsetzung durch die Etablierung entsprechender Prozesse Sorge zu tragen. Ebenso sind Datenbestände regelmäßig auf ihre Richtigkeit, Erforderlichkeit und Aktualität hin zu überprüfen.

Besondere Kategorien personenbezogener Daten

Besondere Kategorien personenbezogener Daten dürfen grundsätzlich nur mit Einwilligung des Betroffenen oder ausnahmsweise aufgrund einer expliziten gesetzlichen Erlaubnis erhoben, verarbeitet oder genutzt werden. Ferner sind zusätzliche technische und organisatorische Maßnahmen (z. B. Verschlüsselung beim Transport, minimale Rechtevergabe) zum Schutz besonderer personenbezogener Daten zu ergreifen.

Datenübermittlung

(1) Die Übermittlung von personenbezogenen Daten an Dritte ist nur aufgrund gesetzlicher Erlaubnis oder der Einwilligung des Betroffenen zulässig.

(2) Befindet sich der Empfänger personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, bedarf es besonderer Maßnahmen zur Wahrung von Rechten und Interessen Betroffener. Eine Datenübermittlung ist zu unterlassen, wenn bei der empfangenden Stelle kein angemessenes Datenschutzniveau vorhanden ist oder beispielsweise über besondere Vertragsklauseln nicht hergestellt werden kann.

Externe Dienstleister

(1) Sofern externe Dienstleister Zugriff auf personenbezogene Daten erhalten sollen, ist der Datenschutzbeauftragte vorab zu informieren.

(2) Dienstleister mit einem möglichen Zugriff auf personenbezogene Daten sind vor der Auftragserteilung sorgfältig auszuwählen. Die Auswahl ist zu dokumentieren und sollte insbesondere die folgenden Aspekte berücksichtigen:

- Fachliche Eignung des Auftragnehmers für den konkreten Datenumgang
- Technisch-organisatorische Sicherheitsmaßnahmen
- Erfahrung des Anbieters im Markt
- Sonstige Aspekte, die auf eine Zuverlässigkeit des Anbieters schließen lassen (Datenschutz-Dokumentationen, Kooperationsbereitschaft, Reaktionszeiten etc.)

(3) Soll ein Dienstleister personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen, bedarf es des Abschlusses eines Vertrags zur Auftragsverarbeitung. Hierin sind Datenschutz- und IT-Sicherheitsaspekte zu regeln.

(4) Der Dienstleister ist im Hinblick auf die mit ihm vertraglich vereinbarten technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen. Das Ergebnis ist zu dokumentieren.

Datenminimierung, Privacy by Design/Privacy by Default

(1) Der Umgang mit personenbezogenen Daten ist an dem Ziel auszurichten, so wenige Daten wie möglich von einem Betroffenen zu erheben, zu verarbeiten oder zu nutzen („Datenminimierung“). Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist. Beispielsweise wird es im Rahmen einer statistischen Auswertung von Daten nicht notwendig sein, den vollen Namen eines Betroffenen zu kennen und zu verwenden. Vielmehr kann diese Information durch einen Zufallswert ersetzt werden, der eine Unterscheidbarkeit der zugrunde liegenden Information ebenfalls gewährleisten kann.

(2) Entsprechendes gilt für die Auswahl und Gestaltung von Datenverarbeitungssystemen. Der Datenschutz ist von Anfang an in die Spezifikationen und die Architektur von Datenverarbeitungssystemen zu integrieren, um die Einhaltung der Grundsätze des Schutzes der Privatsphäre und des Datenschutzes zu erleichtern, so insbesondere den Grundsatz der Datenminimierung.

Rechte von Betroffenen

(1) Betroffene haben das Recht auf Auskunft über die im Unternehmen über ihre Person gespeicherten personenbezogenen Daten. Hierfür ist in unserem Unternehmen ein Prozessablauf definiert.

(2) Bei der Bearbeitung von Anträgen ist die Identität des Betroffenen zweifelsfrei festzustellen. Bei begründeten Zweifeln an der Identität können zusätzliche Angaben vom Antragsteller angefordert werden.

(3) Die Auskunftserteilung erfolgt schriftlich, es sei denn der Betroffene hat den Antrag auf Auskunft elektronisch gestellt. Der Auskunft ist eine Kopie der Daten des Betroffenen beizufügen, die, neben den zur Person vorhandenen Daten, auch die Empfänger von Daten, den Zweck der Speicherung sowie alle weiteren gesetzlich geforderten Informationen nach Art. 15 DS-GVO beinhaltet, um den Betroffenen die Verarbeitung bewusst zu machen und die Rechtmäßigkeit selbst beurteilen zu lassen. Auf besonderen Wunsch des Betroffenen werden die Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt. Die zuständige IT-Abteilung legt den hierfür vorzusehenden Standard fest.

(4) Betroffene haben einen Anspruch auf Berichtigung ihrer personenbezogenen Daten, wenn sich diese als unrichtig erweisen. Ebenso können sie die Vervollständigung unvollständiger personenbezogener Daten verlangen.

(5) Der Betroffene hat das Recht auf Löschung seiner personenbezogenen Daten unter den folgenden Voraussetzungen:

- die Kenntnis der Daten ist für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich.
- der Betroffene hat eine Einwilligung widerrufen und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung
- ihre Verarbeitung ist unzulässig,
- der Betroffene legt Widerspruch gegen die Verarbeitung zu Werbezwecken ein oder beruft sich auf ein Widerspruchsrecht aufgrund einer besonderen – zu begründenden – persönlichen Situation,
- es handelt sich um besondere personenbezogene Daten, deren Richtigkeit nicht bewiesen werden kann, oder
- es besteht eine anderweitige rechtliche Verpflichtung zur Datenlöschung.

Besteht eine Verpflichtung zur Löschung und wurden die personenbezogenen Daten zuvor öffentlich gemacht, sind weitere Verantwortliche für die Datenverarbeitung über ein Löschbegehren des Betroffenen hinsichtlich aller Kopien seiner Daten sowie aller Links zu diesen Daten zu informieren.

(6) Der Betroffene kann die Einschränkung der Verarbeitung seiner Daten verlangen, wenn

- die Richtigkeit der personenbezogenen Daten strittig ist, jedoch nur so lange, wie die Richtigkeit durch die zuständige Fachabteilung überprüft wird oder
- die Verarbeitung unzulässig ist, der Betroffene die Datenlöschung aber ablehnt, oder
- das Unternehmen die personenbezogenen Daten für Zwecke der Verarbeitung nicht mehr benötigt, der Betroffene die Daten jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder
- der Betroffene Widerspruch gegen die Verarbeitung aufgrund einer besonderen Situation eingelegt hat und die zuständige Fachabteilung noch mit der Prüfung des Widerspruchs befasst ist.

(7) Der Betroffene ist spätestens innerhalb eines Monats über alle ergriffenen Maßnahmen, die auf seinen Antrag hin erfolgt sind, zu informieren.

(8) Der Datenschutzbeauftragte steht bei der Wahrung der Betroffenenrechte beratend zur Verfügung.

Auskunftsersuchen Dritter über Betroffene

Sollte eine Stelle Informationen über Betroffene fordern, so beispielsweise Kunden oder Beschäftigte dieses Unternehmens, ist eine Weitergabe von Informationen nur zulässig, wenn

- die Auskunft gebende Stelle ein berechtigtes Interesse hierfür darlegen kann, und
- eine gesetzliche Norm zur Auskunft verpflichtet, sowie

- die Identität des Anfragenden oder der anfragenden Stelle zweifelsfrei feststeht.

Verzeichnis von Verarbeitungstätigkeiten

(1) Das Unternehmen hat ein Verzeichnis über alle Datenverarbeitungen zu führen. Jede Fachabteilung hat eine verantwortliche Person zu benennen, die alle notwendigen Informationen zu den Verfahren der jeweiligen Abteilung nach den gesetzlichen Anforderungen des Art. 30 DS-GVO dokumentiert. Der Datenschutzbeauftragte kann zur Beratung hinsichtlich der gesetzlich geforderten Informationen hinzugezogen werden.

(2) Das Unternehmen stellt der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung. Zuständig hierfür ist der Datenschutzbeauftragte im Einvernehmen mit der Unternehmensleitung.

Werbung

(1) Die werbliche Ansprache von Betroffenen per Brief, Telefon, Fax, oder E-Mail ist grundsätzlich nur zulässig, wenn der Betroffene zuvor in die Verwendung seiner Daten zu Werbezwecken eingewilligt hat.

(2) Ausnahmen sind nur beim Vorliegen einer Erlaubnisnorm zulässig. Bitte konsultieren Sie diesbezüglich den Datenschutzbeauftragten.

Schulung

Beschäftigte, die ständig oder regelmäßig Zugang zu personenbezogenen Daten haben, solche Daten erheben oder Systeme zur Verarbeitung solcher Daten entwickeln, sind in geeigneter Weise über die datenschutzrechtlichen Vorgaben zu schulen. Der Datenschutzbeauftragte entscheidet über Form und Turnus der entsprechenden Schulungen.

Datengeheimnis

Beschäftigten ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Sie sind vor Aufnahme ihrer Tätigkeit auf einen vertraulichen Umgang mit personenbezogenen Daten zu verpflichten. Die Verpflichtung erfolgt durch die Geschäftsleitung unter Verwendung des hierzu vorgesehenen Formulars.

Audits

(1) Um ein hohes Datenschutzniveau zu gewährleisten, werden relevante Prozesse durch regelmäßige Audits interner Stellen oder durch externe Auditoren überprüft. Im Falle der Feststellung eines Verbesserungspotentials sind unmittelbare Abhilfemaßnahmen zu treffen.

(2) Die beim Audit gewonnenen Erkenntnisse sind zu dokumentieren. Die Dokumentation ist dem Datenschutzbeauftragten, der Unternehmensleitung sowie den Fachverantwortlichen für den jeweiligen Prozess zu übergeben.

(3) Ein Audit ist erfolgreich abgeschlossen, wenn alle im Bericht dokumentierten Maßnahmen umgesetzt sind. Bei Bedarf werden Follow-up-Audits durchgeführt, indem Empfehlungen des initialen Audits einer Überprüfung ihrer Implementierung unterzogen werden.

Interne Ermittlungen

(1) Maßnahmen zur Sachverhaltsaufklärung und zur Vermeidung oder Aufdeckung von Straftaten oder schwerwiegenden Pflichtverletzungen im Arbeitsverhältnis sind unter genauer Beachtung der einschlägigen gesetzlichen Datenschutzvorschriften durchzuführen. Insbesondere muss die damit einhergehende Datenerhebung und -verwendung zum Erreichen des Ermittlungszwecks erforderlich, angemessen und mit Blick auf die schutzwürdigen Interessen des Betroffenen verhältnismäßig sein.

(2) Der Betroffene ist so bald wie möglich über die zu seiner Person durchgeführten Maßnahmen zu informieren.

(3) Bei allen Formen der internen Ermittlungen ist der Datenschutzbeauftragte hinsichtlich der Auswahl und Ausgestaltung der Maßnahmen vorab einzubeziehen.

Verfügbarkeit, Vertraulichkeit und Integrität von Daten

(1) In Abhängigkeit der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit hat für jedes Verfahren eine dokumentierte Schutzbedarfsfeststellung und Analyse hinsichtlich der Risiken für Betroffene zu erfolgen.

(2) Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität von Daten wird ein allgemeines Sicherheitskonzept in Abhängigkeit der Schutzbedarfsfeststellung und Risikoanalyse erstellt, das für alle Verfahren verbindlich ist. Hierin ist insbesondere der Stand der Technik ebenso zu berücksichtigen, wie Mittel und Maßnahmen zur Verschlüsselung und Datensicherung. Das Sicherheitskonzept ist hinsichtlich der Wirksamkeit der dort vorgesehenen technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen, zu bewerten und zu evaluieren.

(3) Zugriffe auf personenbezogene Daten sollen nur diejenigen Personen erhalten, die im Zuge ihrer Aufgabenwahrnehmung Kenntnis von den jeweiligen Daten erhalten müssen („Need-to-know-Prinzip“). Zugriffsberechtigungen müssen genau und vollständig festgelegt und dokumentiert sein.

(4) Datenübertragungen durch öffentliche Netze sind nach Möglichkeit zu verschlüsseln. Eine Verschlüsselung hat zwingend zu erfolgen, falls der Schutzbedarf der personenbezogenen Daten dies erfordert.

(5) Zu unterschiedlichen Zwecken erhobene personenbezogene Daten sind getrennt voneinander zu verarbeiten. Die Trennung von Daten ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen.

(6) Wartungsarbeiten an Systemen oder Telekommunikationseinrichtungen durch externe Dienstleister sind zu beaufsichtigen. Ferner ist zu gewährleisten, dass Dienstleister nicht unbefugt auf personenbezogene Daten zugreifen können. Fernwartungszugänge sind nur im Einzelfall zu gewähren und müssen dem Prinzip der minimalen Rechtevergabe folgen. Fernwartungsaktivitäten sind nach Möglichkeit aufzuzeichnen oder zu protokollieren.

Verletzungen des Schutzes von Daten („Datenpanne“)

(1) Sollten Unternehmensdaten unrechtmäßig Dritten offenbart worden sein, ist darüber unverzüglich die Geschäftsleitung zu informieren. Diese informiert unverzüglich den Datenschutzbeauftragten.

(2) Die Erfüllung einer etwaigen Informationspflicht gegenüber der Aufsichtsbehörde erfolgt ausschließlich durch den Datenschutzbeauftragten. Betroffene werden durch die Geschäftsleitung informiert, wobei der Datenschutzbeauftragte beratend hinzugezogen wird.

Folgen von Verstößen

Ein fahrlässiger oder gar mutwilliger Verstoß gegen diese Richtlinie kann arbeitsrechtliche Maßnahmen nach sich ziehen, einschließlich einer fristlosen oder fristgerechten Kündigung. Ebenso kommen strafrechtliche Sanktionen und zivilrechtliche Folgen wie Schadenersatz in Betracht.

Aktualisierung der Richtlinie; Nachweisbarkeit

(1) Im Rahmen der Fortentwicklung des Datenschutzrechts sowie technologischer oder organisatorischer Veränderungen wird diese Richtlinie regelmäßig auf einen Anpassungs- oder Ergänzungsbedarf hin überprüft.

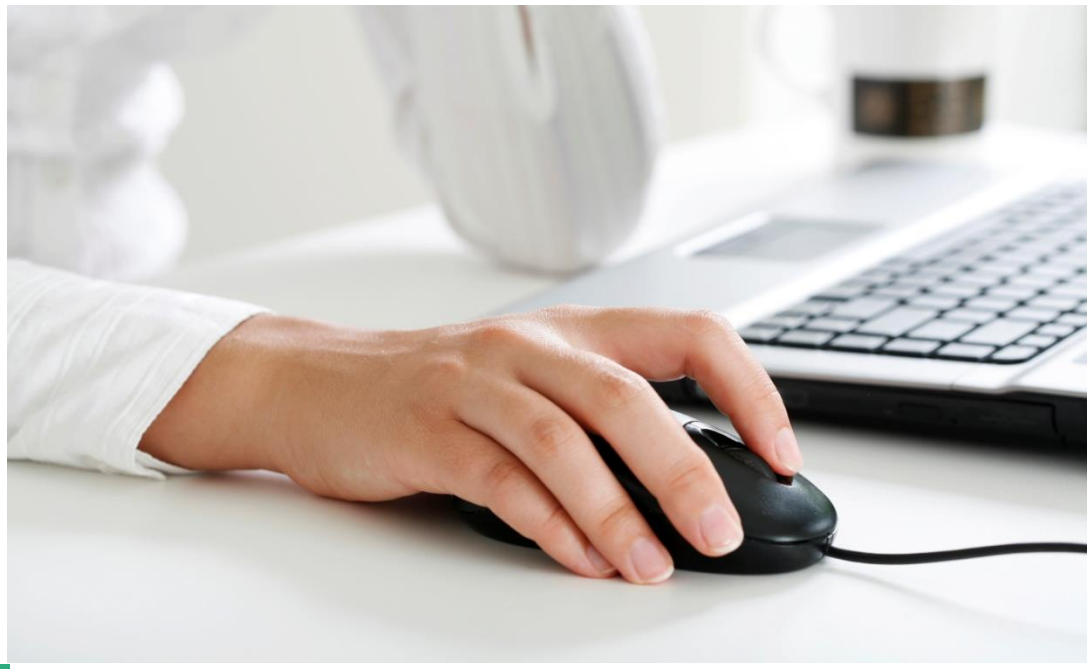
(2) Änderungen an dieser Richtlinie sind formlos wirksam. Die Beschäftigten und leitenden Angestellten sind umgehend und in geeigneter Art und Weise über die geänderten Vorgaben in Kenntnis zu setzen.

Anlage 2: Benutzerrichtlinie IT

Benutzerrichtlinie

IT

Stand 30.04.2020



Zielsetzung

Ziel dieser Richtlinie ist es, den Einsatz einer leistungsfähigen und zeitgemäßen Technik und die in absehbarer Zeit erforderlichen Neuerungen offener informations- und kommunikationstechnischer Infrastruktur mit dem Schutz der Persönlichkeitsrechte für die betroffenen Mitarbeiter/Innen und den neuen datenschutzrechtlichen Vorgaben der DS-GVO in Einklang zu bringen.

Die zur Verfügung gestellten Dienste dienen der Information und Kommunikation im Interesse des Unternehmens. Bei ihrer Nutzung muss die Sicherheit des IT-Systems bzw. Firmennetzes gewährleistet bleiben. Deshalb soll diese IT-Richtlinie auch zur Sensibilisierung des Sicherheitsbewusstseins aller Mitarbeiter/Innen dienen, da der Umgang mit den neuen Medien erhebliche Gefahren für die IT-Sicherheit und damit für die Daten der MBI GmbH, der Beschäftigten und Kunden birgt.

Allgemeine Regeln

- Der Arbeitsplatz muss technisch und organisatorisch so geschützt sein, dass keine Informationen ausgespäht, manipuliert oder gelöscht werden können. Als Arbeitsplatz wird jeder Ort bzw. jede technische Instanz bezeichnet, mit der Benutzer auf firmeninterne Informationen zugreifen können.
- Schützenswerte Informationen dürfen nicht in die Hände Unbefugter gelangen. Diese Informationen dürfen weder durch Kopieren, Ausspähen oder Mithören an Unbefugte gelangen.
- Schlüssel und andere Authentisierungsmittel (z. B. Chipkarten), die den Zutritt zu Gebäuden oder Räumen bzw. Zugang zu IT-Systemen ermöglichen, müssen jederzeit sicher aufbewahrt werden und dürfen nicht an Unbefugte weitergegeben werden.
- Zugriffsmechanismus und Passwort müssen physisch voneinander getrennt aufbewahrt werden (z. B. getrennte Verwahrung von Token oder Karte und Passwort bzw. PIN).
- Das Erzeugen und/oder Verbreiten von Schadsoftware ist strengstens verboten.
- Voreingestellte Sicherheitseinstellungen, Schutzmechanismen, Filter oder Ähnliches dürfen nicht umgangen werden.
- Untersagt ist das Anschließen privater USB-Sticks oder anderer privater Datenträger an IT-Systeme der MBI GmbH.

Allgemeine Nutzerhinweise zu Internet und E-Mail-Nutzung

Auch beim normalen Surfen im Internet lauern Gefahren, die nicht gleich als solche erkannt werden.

Bitte beachten Sie folgende Punkte:

- Gebrauchen Sie Ihren gesunden Menschenverstand! Wenn Sie z.B. keinen Handyvertrag mit O2 oder T-Mobile haben, handelt es sich bei eingegangen E-Mails von O2 oder T-Mobile meistens um betrügerische E-Mails.
- Übermitteln Sie keine persönlichen Daten, vor allem nicht, wenn die Verbindung nicht als sicher (HTTPS) markiert wird.
- Misstrauen Sie grundsätzlich Websites, die mit dem Download kostenloser Zusatzsoftware oder unseriösen Gewinnspielen locken.
- Das Herunterladen von Dateien kann – abgesehen von der Gefahr des Einschleppens von Schadsoftware – auch zu lizenz- und urheberrechtlichen Problemen führen. Das gilt auch für Software, die nicht installiert oder ausgeführt wurde und nur auf dem Bürorechner gespeichert ist.
- Meiden Sie Hackerseiten und solche, auf denen kommerzielle Software, möglicherweise in gecrackter Form, zum Download angeboten wird.
- Rufen Sie keine Websites mit pornografischen, gewaltverherrlichenden oder strafrechtlich bedenklichen Inhalten auf. Das kann gravierende rechtliche Probleme – auch für mbi – nach sich ziehen.
- Fragen Sie lieber einmal zu viel bei Ihrer IT-Abteilung nach.

E-Mail gehört zur Standardausrüstung eines Arbeitsplatzes. Dadurch lohnt es sich auch für Kriminelle diese Form der Kommunikation zu nutzen. Somit landen aber auch Spam-, Hoax- oder Phishing-Mails sowie mit Schadprogrammen verseuchte Nachrichten in Ihrem Posteingang. Solche unerwünschten Nachrichten – mit mehr oder weniger gefährlichem Inhalt – machen ca. zwei Drittel des weltweiten E-Mail-Aufkommens aus.

Bitte beachten Sie folgende Punkte:

- Öffnen Sie keine E-Mails, wenn Ihnen Absender oder Betreffzeile verdächtig erscheinen.
- Öffnen Sie niemals Dateianhänge, die Ihnen verdächtig vorkommen. Auch bei vermeintlich bekannten und vertrauenswürdigen Absendern ist zu prüfen: Passt der Text der E-Mail zum Absender (englischer Text von deutschsprachigem Absender, unsinniger Text, fehlender Bezug zu aktuellen Vorgängen etc.)? Erwarten Sie die angehängten Dateien und passen sie zum Absender, oder kommen sie völlig unerwartet?
- Öffnen Sie keine E-Mails mit Spaßprogrammen, da diese Schadsoftware enthalten können.
- Sogenannte Phishing-Mails, die zur Übermittlung von persönlichen Online-Banking-Daten oder Passwörtern (z.B. PIN oder TAN) auffordern, müssen gelöscht werden. Die angeforderten, vertraulichen Informationen dürfen Sie auf keinen Fall weitergeben.
- Oftmals kann in einer E-Mail ein Link angeklickt werden, um eine Webseite aufzurufen. Seien Sie dabei vorsichtig: In betrügerischen E-Mails wird diesen Links oft eine völlig andere Internet-Adresse hinterlegt, als in der E-Mail zu sehen ist. Beim Anklicken wird

dann eine gefälschte Phishing-Webseite aufgerufen oder sogar Schadsoftware installiert. Sicherer ist es, den Link mittels „Hyperlink kopieren“ in den Browser zu übertragen und ihn vor dem Aufrufen noch einmal zu überprüfen.

- Beantworten Sie keine Spam-Mails! Die Rückmeldung bestätigt dem Spam-Versender nur die Gültigkeit Ihrer Mail-Adresse und erhöht dadurch Ihr Risiko, weitere Zusendungen zu erhalten. Das Abbestellen von E-Mails ist nur bei seriösen Zustellern sinnvoll.
- Benachrichtigen Sie auch Ihre Kolleginnen und Kollegen über verdächtige Zusendungen, ohne diese an sie weiterzuleiten.
- Fragen Sie Ihre IT-Abteilung, falls Sie sich unsicher sind.
- Sollten Sie über Ihr dienstliches Mailkonto doch einmal eine private Mail erhalten, löschen Sie diese bitte sofort, da es sein kann, dass bei Ihrer Abwesenheit Ihr Vertreter oder Ihre Vertreterin Ihre dienstlichen Mails bearbeiten muss.

Umgang mit schützenswerten Dokumenten und Datenträgern

- Werden Dokumente oder Datenträger benutzt, die sensible personenbezogene Daten enthalten, dürfen sie nicht unbeaufsichtigt gelassen werden und sind nach Gebrauch verschlossen aufzubewahren.
- Nach Besprechungen müssen alle Unterlagen mit Inhalten aus den jeweiligen Besprechungsräumen entfernt werden.
- Dokumente und Datenträger müssen immer vor Verlust, Beschädigung, Manipulation, Zerstörung und Verwechslung sowie vor Zugriff Unbefugter geschützt werden.
- Dokumente und Datenträger müssen vor dem Versand so verpackt werden, dass sie gegen Verlust, Beschädigung, Manipulation und Zerstörung gesichert sind.
- Dokumente, die sensible personenbezogene Daten enthalten, dürfen nur dann auf frei zugänglichen Druckern ausgegeben werden, wenn der Druckvorgang persönlich überwacht werden kann.
- Datenträger oder wichtige Dokumente dürfen auf keinen Fall im Papierkorb entsorgt werden! Sofern es sich um Inhalte handelt, die Außenstehenden nicht zugänglich gemacht werden dürfen oder diese personenbezogenen Daten enthalten, müssen die Datenträger und Dokumente sicher vernichtet werden.

Informationssicherheit beim Kopieren und Drucken von schützenswerten Unterlagen

- Nach dem Kopieren von Unterlagen muss darauf geachtet werden, dass weder Kopien noch Originale im Kopierer zurückgelassen werden.
- Fehlkopien von Unterlagen müssen vernichtet und entsorgt werden.
- Vergessene Kopien oder Originale eines anderen sollen diesem zugestellt oder, falls der andere nicht ermittelt werden kann, angemessen vernichtet werden.
- Bei aufgetretenen Fehlern an Kopierern oder Druckern sind die laufenden Aufträge entweder kontrolliert abzubrechen oder nach Fehlerbehebung zu beenden.

Firmeninternes Netz und Firewall

- Zur Netzwerkadministration, zum Schutz des Netzwerkes gegen Angriffe und zur Benutzerunterstützung wird dokumentierte Software auf lokalen Servern eingesetzt. Soweit mittels Fernsteuerungs-Software ein Zugriff auf die Arbeitsplatzrechner von Mitarbeiter/Innen möglich ist, so wird diese so installiert, dass nur die berechtigten Administratoren Zugriff auf die Endgeräte haben können und jeder Endbenutzer diesen Zugriff ausdrücklich erlauben muss und seinerseits jederzeit auch wieder beenden kann.
- Der Einsatz von Softwareprodukten mit Eskalationsmanagement (automatische Erzeugung von Alarm- und Aufmerksamkeitsmeldungen) bleibt auf technische Fehlermeldungen der Server- und Systemsoftware begrenzt.

Kontrollen

Die Einhaltung dieser Richtlinien kann stichprobenartig und/oder anlassbezogen kontrolliert werden.

Sanktionen

Zuwiderhandlungen und Verstöße gegen die Richtlinie werden arbeitsvertraglich verfolgt. Verstöße können zudem ggf. strafrechtliche Folgen haben.