Unternehmensrichtlinie

für RAI-BAU Baugesellschaftm.b.H

organisatorische Maßnahmen zur Datensicherheit

INHALTSVERZEICHNIS

1. Einleitung und Grundsätze

Die Einführung der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) hat für Unternehmen grundlegende Änderungen bei der Verarbeitung personenbezogener Daten zur Folge. Sie erweitert den Schutz personenbezogener Daten und legt Unternehmen zu diesem Zweck besondere Pflichten auf. Zu den personenbezogenen Daten gehören alle Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, unabhängig davon ob es sich um elektronisch oder in Papierform systematisch verarbeitete Daten handelt. Hierunter fallen Informationen wie etwa Name, Adresse, aber auch eine Personalnummer, IP-Adresse oder GPS-Daten eines Fahrers. Identifizierbar ist eine Person, wenn sie 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 seiner Identität sind, von dem Verantwortlichen oder einer anderen Person ermittelbar ist.
Obwohl es sich bei Kunden, Zulieferern und Dienstleistern häufig um juristische Personen handelt und diese nicht dem Schutz der EU-DSGVO unterliegen, werden beim Kontakt mit diesen Unternehmen personenbezogene Daten über deren Eigentümer, Geschäftsführer oder Mitarbeiter verarbeitet, weshalb sie unter den Schutz der EU-DSGVO fallen.

In der EU-DSGVO sind folgende Grundsätze definiert, die bei der Verarbeitung von personenbezogenen Daten beachtet werden müssen:

Rechtmäßigkeit
Für die Verarbeitung personenbezogener Daten muss eine rechtliche Grundlage vorliegen.
Die Voraussetzung für die Verarbeitung ist insbesondere gegeben, (a) wenn die betroffene Person ihre Einwilligung zur Verarbeitung der bestimmten Zwecke gegeben hat; (b) die Verarbeitung zur Erfüllung eines Vertrags, oder Durchführung von vorvertraglichen Maßnahmen erforderlich ist und auf Anfrage der betroffenen Person erfolgen; oder (c) die Verarbeitung zur Erfüllung rechtlicher Verpflichtungen notwendig ist (z.B. rechtliche Aufbewahrungspflichten gemäß Bundesabgabenordnung).

Transparenz und Zweckbindung
Im Rahmen der Verarbeitung müssen betroffene Personen insbesondere darüber informiert werden, wie, von wem und für welchen Zweck ihre personenbezogenen Daten verarbeitet werden. Für sie muss erkennbar sein, dass die betreffenden personenbezogenen Daten verarbeitet werden bzw. werden sollen.
Die Verarbeitung personenbezogener Daten darf nur für festgelegte, eindeutige und rechtmäßige Zwecke erfolgen. Zweckänderungen sind in der Regel nur mit Einwilligung der betroffenen Person zulässig oder wenn nationales Recht dies zulässt.

Richtigkeit und Datenminimierung
Personenbezogene Daten müssen sachlich richtig und auf dem neuesten Stand sein. Die Verarbeitung muss für ihre Zwecke "erforderlich" sein. Dies gilt für den Umfang der erhobenen Daten, für die Art ihrer Verarbeitung und die Dauer der Speicherung. Es greift der Grundsatz der Datenminimierung, d.h. die Verarbeitung muss auf das erforderliche Maß beschränkt sein. Deshalb ist stets zur überlegen, welche Daten für die Geschäftszwecke tatsächlich erforderlich sind. Personenbezogene Daten sind zu löschen, sobald die Rechtsgrundlage oder der Zweck für die Verarbeitung der Daten entfallen.

Integrität und Vertraulichkeit
Der Schutz personenbezogener Daten vor Verlust, Diebstahl sowie unbefugter oder unrechtmäßiger Verarbeitung muss insbesondere durch geeignete technische und organisatorische Maßnahmen gewährleistet werden. Bei jeder Verarbeitung müssen die Grundsätze der Vertraulichkeit und Integrität beachtet werden.

Besondere Kategorien von personenbezogenen Daten
Vorsicht ist bei der Verarbeitung von besonderen Kategorien personenbezogener Daten angebracht. Hierzu gehören die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder Gewerkschaftszugehörigkeit, die Verarbeitung von genetischen oder biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten sowie Daten zum Sexualleben oder der sexuellen Orientierung einer Person. Die Verarbeitung von strafrechtlichen Verurteilungen und Straftaten ist zudem gesondert geregelt. Daten dieser Art werden von uns nur in besonderen Ausnahmefällen verarbeitet und dürfen nicht per unverschlüsselter E-Mail oder unzureichend gesichertem Anhang kommuniziert werden. Rückfragen hierzu sind an den in Ihrem Unternehmen für Datenschutz zuständigen Ansprechpartner oder Ihren Vorgesetzten zu richten.

Diese Richtlinie dient dazu, die Einhaltung dieser Grundsätze durch Festlegung organisatorischer Maßnahmen sicherzustellen.

2. Geltungsbereich und Gegenstand

Die Unternehmensrichtlinie ist von allen Mitarbeitern, überlassenen Arbeitskräften sowie freien Dienstnehmern (gemeinsam kurz „Mitarbeiter“) [1] einzuhalten.
Um die Sicherheit und den Schutz der informationstechnischen Einrichtungen und der verarbeiteten Daten, insbesondere der personenbezogenen zu gewährleisten, haben alle Mitarbeiter unseres Unternehmens mit den informationstechnischen Einrichtungen verantwortungsbewusst und sorgfältig umzugehen.

Aufgrund gesetzlicher und vertraglicher Verpflichtung sind Daten, die Ihnen im Rahmen Ihrer beruflichen Tätigkeit anvertraut oder bekannt geworden sind, geheim zu halten.

Bei Zweifel oder Unklarheiten zum Thema Datenschutz kontaktieren Sie Ihren Vorgesetzten, den in Ihrem Unternehmen für Datenschutz zuständigen Ansprechpartner sowie den Betriebsrat.

3. Sicherer Umgang mit Computern und Daten

3.1. „Clear Desk Policy“

Clear Desk Policy bedeutet, dass alle vertraulichen Daten vor unbefugtem Zugang geschützt sein müssen, insbesondere wenn der Arbeitsplatz verlassen wird.

[1] Bei allen personenbezogenen Bezeichnungen gilt die gewählte Form für beide Geschlechter.

- Achten Sie darauf, dass Computerausdrucke oder Unterlagen mit vertraulichen Informationen nicht für Unbefugte frei zugänglich herumliegen, z.B. neben dem Drucker oder im Kopierer.
- Bewahren Sie unter keinen Umständen Passwortnotizen an Ihrem Arbeitsplatz auf (z.B. unter der Schreibtischunterlage, als Post-it am Bildschirm).
- Beim Verlassen des Arbeitsplatzes ist Ihr Computer zu sperren. Wenn Sie Ihren Arbeitsplatz für längere Zeit verlassen bzw. bei Beendigung der Arbeit, ist der Computer im Regelfall ordnungsgemäß auszuschalten. Zusätzlich wird empfohlen beim Verlassen des Arbeitsplatzes alle offenen Dokumente zu speichern, um einen eventuellen Datenverlust (z.B. Systemabsturz, Stromausfall etc.) zu vermeiden.

Betriebsdaten wie z.B. Word- oder Exceldateien sind grundsätzlich strukturiert im jeweils vorgesehenen Ordner am Netzlaufwerk nachvollziehbar zu speichern.
Betriebsdaten müssen darüber hinaus so gespeichert werden, dass bei Ausfall/Abwesenheit eines Mitarbeiters dessen Vertretung oder der Vorgesetzte auf diese Daten zugreifen kann (z. B auf ein zugängliches Abteilungslaufwerk).
Im Zweifel kontaktieren Sie Ihren Vorgesetzten oder IT-Verantwortlichen.

Jeder Mitarbeiter ist angehalten, nicht mehr benötigte Dateien und E-Mails regelmäßig zu löschen und damit beizutragen, dass die Datenbestände überschaubar bleiben. Nähere Informationen zu den einzuhaltenden Löschfristen sind dem Anhang zu entnehmen.

Verlässt ein Mitarbeiter befristet (z.B. Karenz) oder dauerhaft das Unternehmen, so hat er nicht mehr benötigte Datenbestände und E-Mails zu löschen und die verbleibenden Datenbestände an einen Kollegen zu übergeben.

Vorgesetzte sind angehalten, die ordnungsgemäße Übergabe von Datenbeständen sicherzustellen.

3.2. Entsorgung von Papierdokumenten oder digitalen Datenträgern wie z.B. USB-Sticks, Festplatten, Speicherkarten, CDs/DVDs (auch bei Archivmaterial)

Computer und digitale Datenträger, die defekt geworden sind oder nicht mehr benötigt werden, sind an die IT-Abteilung zu übergeben. Papierdokumente mit vertraulichen oder personenbezogenen Inhalten, müssen auf sichere Art entsorgt werden, z.B. durch entsprechendes Zerkleinern.

Beim Verlassen von Besprechungsräumen sind sämtliche sensiblen Informationen (z.B. auf Flipcharts) zu entfernen oder mitzunehmen.

3.3. Digitale Kommunikation

Um den Schutz personenbezogener oder sonst vertraulicher Daten, die im Rahmen Ihrer beruflichen Tätigkeit anvertraut oder bekannt geworden sind, nicht zu gefährden, ist bei der digitalen Kommunikation erhöhte Sorgfalt geboten.

Die Versendung beruflicher personenbezogener Daten von einer privaten E-Mailadresse ist nicht gestattet.

Messengerservices (WhatsApp, Viber, Hangouts, etc.) dürfen aufgrund von datenschutzrechtlichen und sicherheitsrelevanten Aspekten nur unter Anwendung besonderer Sorgfalt verwendet werden. Vertrauliche betriebliche Informationen dürfen auf keinen Fall über ein solches Service kommuniziert werden. Des Weiteren ist es untersagt, Vereinbarungen mit Kunden über ein solches Service zu betreiben und/oder Gruppen/Foren im betrieblichen Kontext zu bilden. Dies gilt unabhängig davon, ob Sie vom Dienstgeber zur Verfügung gestellte Betriebsmittel oder Privatgeräte nutzen.

Das Netz vergisst nie! Denken Sie immer daran, dass Informationen, die Sie im Netz preisgeben, öffentlich sind und oft nur schwer wieder gelöscht werden können.

3.4. Bring Your Own Device (BYOD)

Die Verwendung privater IT-Ausstattung zu betrieblichen Zwecken ist untersagt.

4. Betroffenenrechte

Verlangt ein Betroffener Auskunft, Löschung seiner personenbezogenen Daten, leiten Sie die Anfrage unverzüglich Ihren Vorgesetzten oder den in Ihrem Unternehmen für Datenschutz zuständigen Ansprechpartner weiter.

Bei Anfragen zur Berichtigung von Daten vergewissern Sie sich über die Identität des Anfragenden. Jede Änderung ist protokolliert vorzunehmen.

5. Nutzung der betrieblichen IT-Ausstattung

5.1. Allgemeine Handhabung

Die Handhabung der zur Verfügung gestellten IT-Ausstattung hat mit der entsprechenden Sorgfalt zu erfolgen. Damit sollen Beschädigungen sowie Datenmissbrauch verhindert werden. Das zur Verfügung gestellte Equipment ist ausschließlich für dienstliche Zwecke zu verwenden (ausgenommen gelegentliche Nutzung laut Punkt 5.4.).
Die unzulässige Verwendung des Equipments durch dritte Personen ist auf geeignete Art und Weise zu verhindern.

5.2. Datensicherung und –ablage

Bei der Datenablage ist zwischen zentralen Netzlaufwerken und einer lokalen Datenablage auf dem Ihnen zur Verfügung gestellten IT-Gerät zu unterscheiden.
Grundsätzlich sind Daten immer auf einem zentralen Netzlaufwerk abzulegen, da diesfalls die Daten automatisch gesichert werden.
Müssen Daten lokal abgelegt werden (etwa im Außendienst auf mobilen Geräten), sind diese in regelmäßigen Abständen auf das zentrale Netzwerk des Unternehmens zu übertragen.

5.2.1. Ablage privater Daten auf IT-Einrichtungen des Unternehmens

Die Ablage privater Daten im geringen Umfang im Zuge der gelegentlichen privaten Nutzung von E-Mail und Internet (gemäß Punkt 5.4.) auf IT-Einrichtungen des Unternehmens ist gestattet, sofern die Ablage auf einem gesondert dafür angelegten Ordner mit der Bezeichnung „**PRIVAT**“ erfolgt. Das Unternehmen haftet nicht für einen allfälligen

Verlust der abgelegten privaten Daten. Bei behördlichen Überprüfungen kann nicht ausgeschlossen werden, dass auch diese Daten von der Behörde eingesehen werden.

5.3. Zugriffsschutz

Die vom Rechenzentrum oder der IT-Abteilung servicierte IT-Ausstattung ist mit einem Zugriffsschutz (Username + Passwort) ausgestattet. Richten Sie Ihr IT-Gerät nicht so ein, dass es ohne Eingabe einer PIN oder eines Passworts verwendet werden kann. Lassen Sie die Geräte nicht entsperrt liegen und geben Sie diese nicht unbeaufsichtigt an Andere weiter.

5.3.1. Zugriffsberechtigungen

Jeder Mitarbeiter erhält für seinen Tätigkeitsbereich die notwendigen Berechtigungen. Werden zusätzliche Berechtigungen benötigt, müssen diese schriftlich mit Begründung beim zuständigen Vorgesetzten angefordert werden.

5.4. Gelegentliche private Nutzung

5.4.1. E-Mail und Internet

Soweit keine wichtigen Belange des Unternehmens dagegensprechen, ist eine private Nutzung gelegentlich erlaubt.
Die Mitarbeiter haben von dieser Möglichkeit verantwortungsbewusst unter Wahrung der Interessen des Unternehmens und ohne Störung des Dienstbetriebes Gebrauch zu machen.
Verboten sind rechtlich zweifelhafte, gewaltorientierte, oder pornografische Inhalte, Urheberrechtsverletzungen sowie Kettenbriefe oder Kettenbrief ähnlich Aktionen bzw. Massensendungen (z.B. Vereinsmitteilungen, parteipolitische Aussendungen oder nicht firmenbezogene Aussendungen an Mitarbeitergruppen.)

5.4.2. Telefonie

Die Telefonnutzung (mobil und Festnetz) zu privaten Zwecken ist in geringem Umfang im Rahmen der bestehenden Flatrate bis auf Widerruf gestattet.

5.4.3. Social Media

Grundsätzlich gilt, dass die private Nutzung – also das Auftreten als Privatperson in sozialen Netzwerken – strikt von der beruflichen Nutzung zu trennen ist. Insbesondere ist es daher untersagt, bei sozialen Netzwerken einen Account für private Zwecke unter Angabe von Firmendaten einzurichten. Davon nicht erfasst ist die Angabe des Unternehmens als Arbeitgeber.

Der Umfang einer beruflichen Nutzung richtet sich nach dem konkreten Auftrag der vorgesetzten Führungskraft. Bei Veröffentlichungen sind in jedem Fall die einschlägigen gesetzlichen Bestimmungen wie insbesondere jene des Urheberrechts einzuhalten. Ebenso sind die Persönlichkeitsrechte genannter/abgebildeter Personen zu wahren. Holen Sie deshalb stets die Zustimmung der betroffenen Personen (z.B. Kollegen, Vorgesetzte) ein, bevor Sie Inhalte wie Fotos, Videos oder Texte von diesen veröffentlichen. Zitieren Sie andere, ist immer eine Quelle anzugeben oder zu dieser zu verlinken.

5.5. Nutzung von Netzwerkverbindungen

Bei VPN-Verbindungen über betriebsfremde Netzwerke (z.B. öffentliches WLAN) ist erhöhte Vorsicht in sicherheitstechnischer Sicht walten zu lassen und die VPN-Verbindung unmittelbar zu aktivieren.
Dem Benutzer ist es untersagt, Sicherheitsmaßnahmen auf Computern oder Netzen des Unternehmens oder Dritter zu verändern bzw. sicherheitsrelevante Daten aufzuzeichnen und weiterzugeben.

5.6. Nutzung von Wechseldatenträger

Wechseldatenträger stellen ein besonderes Sicherheitsrisiko dar und sind daher mit höchster Sorgfalt und Aufmerksamkeit anzuwenden. Es dürfen nur Wechseldatenträger verwendet werden, die vom Unternehmen für die berufliche Verwendung ausgegeben oder für berufliche Zwecke vom Mitarbeiter in Abstimmung mit der IT-Abteilung neu angeschafft wurden. Keinesfalls dürfen private Wechseldatenträger verwendet werden.

Im Fall der Verwendung von Wechseldatenträgern sind folgende Hinweise zu beachten:

- Kein Upload privater Daten oder betriebsfremder Programme über Wechseldatenträger auf IT-Einrichtungen des Unternehmens; auch nicht über betriebseigene Wechseldatenträger!
- Lassen Sie Wechseldatenträger wie z.B. USB-Sticks nie unbeaufsichtigt liegen!
-
- Auch für Wechseldatenträger gilt: Jeder Verlust muss entsprechend Punkt 7. sofort gemeldet werden!

5.7. Sicherer Umgang mit mobilen IT Geräten

Der Transport mobiler IT-Geräte ist ein grundsätzliches Sicherheitsrisiko. Diese dürfen daher während des Transportes nicht unbeaufsichtigt bleiben.
Es ist unzulässig, das mobile IT-Gerät unbeaufsichtigt im PKW bzw. in öffentlichen Verkehrsmitteln zu belassen. Entsprechende Sorgfalt ist insbesondere auch in betriebsfremden Räumlichkeiten (Tagungsräume, Hotels u. dgl.) anzuwenden.

- Verwenden Sie Ihren privaten Cloud-Speicherdienst (z.B. Dropbox, i-Cloud, Google Drive) nicht für Unternehmensdaten! Fragen Sie bei Ihrem IT-Zuständigen nach, welche Möglichkeiten bestehen, um Firmendokumente über das Internet sicher abzuspeichern.
- Achten Sie darauf, dass gerade nicht benötigte Verbindungen wie z. B. WLAN deaktiviert sind. Davon ausgenommen ist Bluetooth.
- Verwenden Sie überwiegend nur Apps, die für berufliche Zwecke nützlich, in jedem Fall aber als vertrauenswürdig und sicher bekannt sind! Räumen Sie nur für den Gebrauch notwendige Zugriffberechtigungen ein. Fragen Sie im Zweifelsfall Ihren IT-Zuständigen.

Vom Unternehmen ausgegebene Geräte dürfen ausschließlich über den IT-Zuständigen außer Dienst gestellt werden.

Auch für mobile IT-Geräte gilt: Jeder Verlust muss entsprechend Punkt 7. sofort gemeldet werden!

5.8. Software

Es dürfen nur Softwareprodukte installiert und genützt werden, die rechtmäßig lizenziert sind und vom IT-Zuständigen genehmigt wurden. Dazu gehören auch Bildschirmschoner, Demoprogramme und Computerspiele.

5.9. Umgang mit E-Mails

E-Mails und deren Anhänge können Skripte mit Schadensfunktion enthalten und sind daher mit der nötigen Sorgfalt zu prüfen. Achten Sie auf die Vertrauenswürdigkeit des Absenders und öffnen Sie keine E-Mails oder Anhänge, wenn Ihnen Absender oder Betreffzeile verdächtig erscheinen. In Zweifelsfällen kontaktieren Sie Ihren Vorgesetzten oder den IT-Zuständigen ohne das E-Mail selbst weiterzuleiten.
Achten Sie bei vertraulichen/sensiblen Inhalten darauf, diese niemals an generische E-Mailadressen (nicht auf den Namen einer konkreten Person lautend – z.B. office@...at) zu übermitteln. Für Ausnahmefälle kontaktieren Sie Ihren Vorgesetzten.

6. Zentrale CRM-Datenbank

Personenbezogene Daten von Kunden bzw. Interessenten für Marketingzwecke sind nur strukturiert in der zentralen CRM Datenbank des Unternehmens zu speichern und bei jeder Marketingaktion (z.B. Mailing, SMS, Serienmail) ausschließlich von dort aktuell abzurufen.

7. Verhalten bei Störungen der IT/Verlust von IT-Geräten

Bei Verdacht auf Virengefahr, Datenspionage, Verlust von Daten bzw. IT-Geräten oder anderen Umständen, die die Sicherheit der Informationstechnologie des Unternehmens betreffen, ist unverzüglich der Vorgesetzte oder der IT-Zuständige des Unternehmens zu informieren.

8. Schlussbestimmungen

Da die Existenz des Unternehmens in hohem Maße von der Funktionsfähigkeit der informationstechnischen Einrichtungen abhängig ist, kann ein fahrlässiger Verstoß gegen eine oder mehrere vorgenannten Regel(n) große Schäden anrichten und zu einer Beendigung des Beschäftigungsverhältnisses führen.

Diese Richtlinie tritt am 25.Mai 2018 in Kraft.