HOPE FACTORY | TU'S FÜR DICH!

DATENSCHUTZ- & SICHERHEITSHANDBUCH

[VERSION 1.0 VOM 27. FEBRUAR 2021]

Hinweis: Diese allgemeine Verfahrensanweisung soll Dienstanweisungen ergänzen, den notwendigen Umgang mit Informationstechnologie beschreiben und die Anforderungen an das interne Compliance- und Risk-Management unterstützen.

Die sich aus dieser Policy ergebenden Anforderungen basieren auf Management-Standards, unter anderem der ***ISO 2700X-Normenreihe****.*

Inhalt

Präambel

Die Sicherheit der Informationen und der informationsverarbeitenden Systeme sowie der damit verbundenen Prozesse wird stetig zu einem unabdingbaren Pfeiler der Unternehmensvorsorge. Der Erfolg, das Image und die Stabilität von Hope Factory hängen von qualifizierten Prozessen und Systemen ab.

Das hier vorliegende Handbuch soll Mitarbeiterinnen und Mitarbeiter von Hope Factory bei der täglichen Arbeit unterstützen. Der Geltungsbereich umfasst:

- Angestellte Mitarbeiterinnen und Mitarbeiter in Voll- oder auch in Teilzeit
- Mini- und Midijobber
- Praktikantinnen und Praktikanten
- Auszubildende

Darüber hinaus gelten die Verhaltensregeln unabhängig vom Einsatzort, vom Arbeitsplatz oder Tätigkeitsbereich.

Um eine möglichst praxisorientierte und verständliche Hilfe zu schaffen, wurde bewusst darauf verzichtet, einzelne Verhaltensregeln mit langen Paragraphen auszuschmücken.

Nachfolgend wird Hope Factory auch vereinfachend als Unternehmen bezeichnet.

Anmerkung zur männlichen/weiblichen Schreibweise: Um den Lesefluss nicht zu stören, wird in diesem Handbuch in der Regel auf die männliche Schreibweise zurückgegriffen, zum Beispiel „der Datenschutzbeauftragte“, „der Inhaber“ etc. Es sei an dieser Stelle ausdrücklich darauf hingewiesen, dass sich diese Darstellungen sowohl auf männliche als auch weibliche Personen beziehen.

Aufgaben des Datenschutzbeauftragten

Im Paragraph 4g des Bundesdatenschutzgesetzes (BDSG) sind die wesentlichen Aufgaben der für den Datenschutz Beauftragten geregelt:

(1) Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann sich der Beauftragte für den Datenschutz in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden. Er kann die Beratung nach § 38 Abs. 1 Satz 2 in Anspruch nehmen. Er hat insbesondere

1. *die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,*

2. *die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.*

Kontakt zum Datenschutzbeauftragten von Hope Factory

Bei allen Fragen zum Thema „Datenschutz“ steht unsere Beauftragte für den Datenschutz zur Verfügung:

Nicole Zieseniss | E-Mail: nicole.zieseniss@hopefactory.de

Schutz von Informationen & Systemen

Alle Beschäftigten von Hope Factory sind für die IT-Sicherheit sowie für das Zusammenspiel von Systemen und Menschen verantwortlich. Die Inhaber sowie leitende Angestellte üben eine absolute Vorbildfunktion aus. Die Verpflichtung zur Einhaltung dieser Policy gilt in Verbindung mit dem Hinweis auf arbeitsrechtliche und strafrechtliche Folgen bei Verstoß und/oder Missbrauch.

Alle Personen sind aufgefordert, entdeckte Sicherheitsprobleme aufzuzeigen und an den betrieblichen Datenschutzbeauftragten weiterzuleiten.

Informationen & Systeme des Unternehmens, seiner Mitglieder, Mitarbeiter und Partner sind so zu behandeln, dass …

- ✓ die Integrität der Informationen gewahrt wird: Nur autorisierte Personen dürfen Informationen ändern!
- ✓ die Vertraulichkeit gewahrt ist: Zugriff erfolgt nur durch vom Informationseigner – sprich: von dem für diese Informationen zuständigen Mitarbeiter – autorisierte Personen!
- ✓ die Verfügbarkeit gewährleistet ist.
- ✓ die gesetzlichen und vertraglichen Verpflichtungen eingehalten werden.

Die Verpflichtung auf das Datengeheimnis bildet die Basis für den Datenschutz. Aus diesem Grund muss jeder/jede Beschäftigte, der mit der Verarbeitung oder Nutzung personenbezogener Daten betraut ist, eine Datenschutzverpflichtung unterzeichnen.

Besonderer Schutz personenbezogener Daten

Personenbezogene Daten gelten generell als vertraulich *(siehe Abschnitt „Klassifizierung von Informationen“)*. Darunter fallen z. B.:

- Name
- Wohnort
- Geburtsdatum, Alter
- Telefonnummern, E-Mail-Adressen
- Beruf
- Gehalt
- Bankverbindung
- Gesundheitsbezogene Daten

Für personenbezogene Daten gelten besondere datenschutzrechtliche Anforderungen:

- ✓ Für die **Zulässigkeit** muss der Betroffene seine Einwilligung zur Erhebung und Verwendung seiner Daten erteilen – oder es müssen rechtliche Grundlagen vorliegen, z. B. Gesetze, Verträge, Vereinbarungen.
- ✓ Eine Verarbeitung ist nur im Rahmen der jeweiligen konkreten **Zweckbindung**, **Datenvermeidung** und **Datensparsamkeit** erlaubt.
- ✓ Die **Datenqualität** muss gegeben sein, d. h. die erhobenen Daten müssen sowohl sachlich als auch inhaltlich korrekt sein. Falsche Angaben sind zu korrigieren oder zu löschen.
- ✓ Nach Zweckerfüllung besteht ein **Löschungsgebot**.
- ✓ Für eine längerfristige Speicherung besteht ein **Anonymisierungsgebot**.
- ✓ Der **Verhältnismäßigkeitsgrundsatz** ist zu beachten.
- ✓ Für Betroffene besteht der **Grundsatz der Transparenz**. Sie haben ein Recht, zu erfahren, welche Daten zu welchem Zweck gespeichert werden.

Stellen außerhalb des Unternehmens erhalten keinerlei Auskünfte über personenbezogene Daten, sofern keine besonderen Anweisungen bestehen. Alle Mitarbeiterinnen und Mitarbeiter des Unternehmens, die mit personenbezogenen Daten umgehen, haben an einer Grundschutzdatenschulung teilzunehmen.

Es gilt eine Verpflichtung zur Löschung sämtlicher Unternehmensdaten vor der Entsorgung von Geräten, die personenbezogene Daten gespeichert hatten. Speichersysteme sind zu löschen, Daten unwiederbringlich zu zerstören.

Personenbezogene Daten von Beschäftigten & Bewerbern

Personenbezogene Daten von Beschäftigten und Bewerbern dürfen nur dann verarbeitet werden, wenn sie

- ✓ zur Eingehung, Durchführung, Abwicklung oder Beendigung eines Dienst- bzw. Arbeitsverhältnisses
- ✓ oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen

erforderlich sind. Darüber hinaus ist eine Verarbeitung auch gestattet, wenn sie auf

- ✓ einer Rechtsvorschrift
- ✓ einem Tarifvertrag
- ✓ oder einer Dienstvereinbarung

beruht.

Personenbezogene Daten dürfen ausschließlich dann an Personen oder Stellen des öffentlichen Bereiches weitergeleitet werden, wenn der Empfänger ein rechtliches Interesse begründet, der Dienstverkehr es erforderlich macht oder der Betroffene einwilligt. Eine Übermittlung an künftige Arbeitgeber bedarf der Zustimmung des Betroffenen.

Personenbezogene Daten, die aus ärztlichen oder psychologischen Untersuchungen sowie aus Tests im Rahmen des Bewerbungsverfahrens resultieren, dürfen nur mit schriftlicher Zustimmung der betroffenen Person verarbeitet werden. Dabei übermittelt der untersuchende Arzt bzw. Psychologe in der Regel nur das Ergebnis der Eignungsuntersuchung und hierbei festgestellte Risikofaktoren.

Nach einem Austritt aus dem Dienst- bzw. Arbeitsverhältnis werden personenbezogene Daten gelöscht, sofern diese nicht mehr benötigt werden und keine Rechtsvorschriften einer Löschung entgegenstehen.

Klassifizierung von Informationen

Klare Zuständigkeiten von Informationseigentümern und -nutzern sind zu definieren und zu dokumentieren.

Es gilt die Verpflichtung der Informationsnutzer, dass Informationen, die nicht für diese bestimmt sind, nicht einzusehen und nicht zu verwenden sind.

Zu beachten ist dabei eine sinnvolle Klassifizierung der Informationen entsprechend ihrer Anforderungen an die Vertraulichkeit. Diese Klassifizierung wird wie folgt festgelegt:

Streng vertrauliche Informationen

Eine unberechtigte Veröffentlichung oder Weitergabe solcher Informationen kann größere negative Folgen oder einschneidende Störungen von Unternehmensaktivitäten nach sich ziehen.

Der Zugriff auf streng vertrauliche Informationen ist auf eine geringe und namentlich genau festgelegte Anzahl von Personen begrenzt. Für den Informationszugang gilt das „Need-to-know"-Prinzip: Der Zugang zu streng vertraulichen Informationen darf nur in dem Maße erfolgen, wie es für die Erfüllung der Arbeit notwendig ist.

Ein sparsamer Umgang mit dieser Klassifikation ist angebracht. Die Erfordernis der Unterzeichnung einer besonderen Vertraulichkeitserklärung ist obligatorisch.

Informationen der Klassifizierung „streng vertraulich" dürfen nicht über Festnetz- oder Mobiltelefon übermittelt werden. Eine sonstige elektronische Übermittlung darf nur mit Verschlüsselung erfolgen.

Beispiele:

- Strategieunterlagen
- Passwörter

Vertrauliche Informationen

Darunter fallen Informationen, deren Veröffentlichung der zukünftigen Entwicklung des Unternehmens erheblichen Schaden zufügen könnte: Wettbewerb, Finanzen, Rechtslage. Personenbezogene Daten sind grundsätzlich als vertraulich zu klassifizieren.

Zugriff kann nur durch vom Informationseigner legitimierte Personen nach Unterzeichnung einer gesonderten Vertraulichkeitserklärung erteilt werden. Zugriff durch Externe ist nur mit Freigabe durch den Inhaber möglich. Für den Informationszugang gilt das „Need-to-know"-Prinzip: Der Zugang zu vertraulichen Informationen darf nur in dem Maße erfolgen, wie es für die Erfüllung der Arbeit notwendig ist.

Beispiele:

- Personenbezogene Daten von Mitgliedern
- Personenbezogene Daten von Bewerbern & Mitarbeitern
- Informationen, die im Rahmen von Vertraulichkeitsvereinbarungen erlangt wurden
- Arbeitsverträge
- Mitarbeiterbeurteilungen

Interne Informationen

Bei internen Informationen handelt es sich um für alle Mitarbeiterinnen und Mitarbeiter zugängliche Informationen, die jedoch nicht für die Öffentlichkeit bestimmt sind. Eine Weiterleitung darf nur an interne Mitarbeiterinnen und Mitarbeiter erfolgen. Ein Zugriff durch Externe darf nur nach Freigabe durch den Inhaber ermöglicht werden.

Beispiele:

- Präsentationen und Schulungen
- Protokolle
- Projektinformationen

Mitgliedsbezogene Informationen

Für Mitglieder – und ggf. Geschäftspartner – zugängliche Informationen, die jedoch nicht für die Öffentlichkeit bestimmt sind.

Beispiele

- Planungen & Zeichnungen
- Prozessbeschreibungen
- Verfahrensanweisungen

Öffentliche Informationen

Für alle Informationen, die für die allgemeine Öffentlichkeit zugelassen sind, sind keine weiteren Schutzmaßnahmen erforderlich. Darunter fallen zum Beispiel Informationen, die auch auf den Webseiten bzw. Social Media Seiten des Unternehmens und dessen Satelliten zu finden sind.

Nicht klassifizierte Informationen

Alle nicht klassifizierten Informationen gelten grundsätzlich als vertraulich!

Autorisierung

Das „Need-to-know"-Prinzip *(sprich: Kenntnis nur bei Bedarf)* gilt auch für die Vergabe von Berechtigungen. Es gibt erweiterte Rechte von zusätzlich zur Grundberechtigung vergebenen Privilegien, für deren Vergabe ein besonderes Verfahren existieren muss.

Rollendefinierte Berechtigungen, Verfahren bei Versetzungen, Löschen der Berechtigungen beim Verlassen des Unternehmens sind – auch im Rahmen des BDSG – in separaten Verfahrensanweisungen zu regeln.

Regelungen für Berechtigungen, die nur im Rahmen von Projekten vergeben wurden *(z. B. mit zeitlicher Befristung, Löschung nach Fristablauf etc.)* sind ebenfalls in separaten Verfahrensanweisungen zu regeln. So ist zu unterscheiden:

- ✓ Antrag „Netzwerkbenutzer wegen Neueinstellung"
- ✓ Antrag „Änderungen der Berechtigungen/Software-Nutzung wegen Versetzung"
- ✓ Antrag „Entzug des Netzwerkbenutzers wegen Austritt"

Im Antrag sind u. a. anzugeben: E-Mail Account, Hardware, Software, Antragsgrund, Laufwerks-/Ordnernutzung. Abschließend ist bei Bedarf eine kurze Begründung anzugeben. Der Antrag muss unter Angabe des Datums vom Antragsteller unterschrieben werden, der allerdings nicht zugleich betroffener Mitarbeiter sein darf. Eine Ausnahme bilden: Unternehmensinhaber und leitende Angestellte mit Handlungsvollmacht.

Es wird ausdrücklich darauf hingewiesen, dass es ein Bestandteil der Unternehmenskultur ist, dass sich Mitarbeiter auch mit Themen beschäftigen können und sollen, die außerhalb des engeren eigenen Aufgabenfeldes liegen. Deshalb besteht innerhalb des Unternehmens ein freier Zugang für Mitarbeiterinnen und Mitarbeiter zu allen Dokumenten, die als „intern" klassifiziert wurden.

Es gilt ein ausdrückliches Hacking-Verbot sowie das Verbot der Umgehung von Autorisierungsmechanismen.

Umgang mit Passwörtern

Es gilt eine sofortige Änderungspflicht bei erstmaliger Benutzung eines persönlichen Passortes, z. B. für den E-Mail-Account eines neuen Mitarbeiters. Gleiches gilt nach einer Passwort-Rücksetzung, beispielsweise aufgrund eines Passwortverlustes. Anschließend sollte es in regelmäßigen Abständen geändert werden, möglichst alle 90 Tage. Dies gilt auch für Systeme und Programme, die keine automatische Passwortänderung voraussetzen.

Bei der Auswahl eines neuen Passwortes gelten folgende Anforderungen in Bezug auf die Passwortsicherheit:

- ✓ Mindestlänge: 8 Zeichen
- ✓ Komplexität: Kombination aus Klein- und Großbuchstaben, Ziffern und Sonderzeichen
- ✓ Es darf nicht leicht zu erraten sein, sprich: kein Username, kein Name des Haustieres, kein KFZ-Kennzeichen, kein Begriff aus dem Wörterbuch, keine Geburtsdaten

Es kann hilfreich sein, ein Passwort aus einem leicht zu merkenden Satz zu generieren:

Im Sommer 18 war ich 2 Wochen in Norwegen!

IS18wi2WiN!

Passwörter dürfen nicht händisch aufgeschrieben, an Dritte weitergegeben oder elektronisch gespeichert werden – dies gilt auch für Internetzugangsdaten und Hardware. Eine Änderungspflicht für Passwörter bei erfolgten bzw. bevorstehenden Gefährdungen der Vertraulichkeit oder bei Systemmissbrauch ist obligatorisch.

Passwörter werden grundsätzlich nicht abgefragt. Elektronische Passwortnachfragen außerhalb der üblichen Zugangsfunktion für die betroffene Software dürfen nicht beantwortet werden.

Virenschutz

Bei Computerviren handelt es sich um Programmsegmente, die sich selbst in andere Programme kopieren. Die Aktivierung erfolgt, sobald ein infiziertes Programm auf dem Gerät ausgeführt wird. Der Virus kann dann zunächst unbemerkt die auf einem Computer oder Notebook gespeicherten Daten verändern oder auch löschen. Im schlimmsten Fall wird das Gerät blockiert. Besonders riskant sind Programme aus allgemein zugänglichen Quellen im Internet, unverlangt zugesandte Dateianhänge und Datenträger unbekannter Herkunft.

Maßnahmen zur Erkennung, Verhinderung und Wiederherstellung zum Schutz vor Schadsoftware sowie ein angemessenes Bewusstsein der Benutzer müssen umgesetzt werden. Es gilt eine Installierungspflicht einer aktuellen Virenschutzsoftware auf allen Rechnern des Unternehmens.

Für den Benutzer gilt:

- ✓ ein Deaktivierungs- und Änderungsverbot in Bezug auf die Virenschutzsoftware.
- ✓ ein generelles Verbot der Verwendung nicht lizenzierter Software.
- ✓ ein generelles Verbot der Nutzung externer Speichermedien.
- ✓ ein generelles Verbot der Ablage/Speicherung privater Dateien.
- ✓ ein generelles Verbot der privaten Nutzung des Internets oder E-Mail-Accounts.
- ✓ ein Verbot der Ausführung von E-Mail-Dateianhängen mit der Endung .exe oder .vbs
- ✓ das Gebot, den Rechner bei einem festgestellten Virenbefall umgehend herunterzufahren und den Unternehmensinhaber bzw. den Datenschutzbeauftragten unverzüglich zu informieren.

Datensicherung

Es sind regelmäßig BackUp-Kopien von Informationen und von Software zu erstellen und zu testen. Hierzu ist bei Bedarf von den Mitarbeiterinnen und Mitarbeitern auch eine mobile Datensicherungsmethode für Notebook-Rechner anzunehmen. Geprüft werden auch Diebstahlschutzeinrichtungen für bewegliche Rechner mit besonders schutzwürdigen Daten. Externe Festplatten und USB-Sticks dürfen nur mit integrierter Datenverschlüsselung verwendet werden.

Es gelten besondere Verschwiegenheitsverpflichtungen für die mit Aufgaben der Datensicherung beauftragten Personen, falls sie Einblick in vertrauliche, nicht für sie bestimmte Daten erhalten.

Arbeitsplatzgestaltung: Clean Desk

Es gilt das **Clean-Desk-Prinzip**, um auch dem Risiko der unerlaubten Datensammlung durch unberechtigte Dritte *(z. B. bei Diebstahl)* vorzubeugen. Dies bedeutet:

- ✓ Bildschirmschutz mit Passwortsicherung ist obligatorisch.
- ✓ Es dürfen nur die Unterlagen am Arbeitsplatz liegen, die bearbeitet werden oder einen ständigen Zugriff erfordern.
- ✓ Dokumente müssen umgedreht werden.

Am Kopiergerät sind folgende Sicherheitshinweise zu beachten:

- ✓ Gemäß der Datensparsamkeit dürfen nur Inhalte kopiert werden, die tatsächlich benötigt werden. Irrelevante Stellen sind abzudecken.
- ✓ Dies gilt auch in Bezug auf die Kopien-Anzahl: So viele wie nötig, so wenig wie möglich!
- ✓ Es ist zu prüfen, ob ein Personenbezug im Sinne der Anonymisierung zu schwärzen ist.
- ✓ Es dürfen weder Originale noch Kopien im Bereich des Kopiergerätes verbleiben.

Hinweis: Das Übersenden von Originaldokumenten ist grundsätzlich untersagt!

Beim Verlassen des Arbeitsplatzes …

- ✓ sind alle Fenster zu verschließen.
- ✓ sind Notebooks und sonstige Geräte gegen Diebstahl abzusichern.
- ✓ ist der Bildschirm zu sperren oder das Gerät herunterzufahren.
- ✓ sind alle streng vertraulichen und vertraulichen Unterlagen wegzuschließen.
- ✓ ist der Schreibtisch aufzuräumen.
- ✓ ist das Büro, wenn unbeaufsichtigt, zu verschließen.

Dieses Verfahren ist auch außerhalb des eigenen Arbeitsplatzes anzuwenden, soweit dies umsetzbar ist, z. B. auch auf Messen, in Hotels/Pensionen/Jugendherbergen, bei Seminaren etc. Jede Information kann für andere Personen interessant sein!

Internet-Zugang, Mail & Kommunikation

Die **Internetnutzung** ist ausschließlich zu Geschäftszwecken erlaubt und erwünscht. Unzulässige Nutzungen – wie jede Nutzung, die geeignet ist, den Interessen des Unternehmens oder dessen Ansehen in der Öffentlichkeit zu schaden – jedoch nicht. Auch Nutzungen, die gegen geltende Rechtsvorschriften oder gegen Richtlinien und Organisationsanweisungen des Unternehmens verstoßen, sind nicht erlaubt; dazu zählen:

- ✓ das Abrufen oder Verbreiten von Inhalten, die gegen datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen.
- ✓ das Abrufen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen oder pornografischen Äußerungen oder Abbildungen.

Es gilt das Verbot des Aufbaus von Internet- oder anderen Netzwerkverbindungen, die Externen einen Zugang zu unternehmensinternen Systemen und Daten verschaffen.

Es gilt ferner ein Vorbehalt für die eventuelle Filterung des Internet-Zugangs, wobei aber nur der Zugang zu solchen Seiten gesperrt wird, deren Nutzung gemäß den Regelungen der Unternehmensrichtlinien nicht erlaubt ist. In einem solchen Fall erfolgt eine Benachrichtigung an den Benutzer mit der Möglichkeit, auf Antrag die Freigabe der gesperrten Seiten zu erhalten.

Die Nutzung des **E-Mail-Dienstes** ist nur zu geschäftlichen Zwecken gestattet. Das E-Mail-Programm muss während der Arbeitszeit aktiviert sein. Bei längerer Abwesenheit, z. B. in Urlaubszeiten, ist der Abwesenheitsassistent mit Hinweis auf die Vertretung zu nutzen oder eine Weiterleitung einzurichten. Ausgehende E-Mails müssen mit der der Corporate Identity übereinstimmenden Signatur ausgestattet sein:

[Vorname] [Nachname]
[Funktion]
Hope Factory | Tu’s für dich!
Straße und Hausnummer
PLZ und Ort

Tel.:
info@hopefactory.de
www.hopefactory.de

Es ist zu beachten, dass Empfänger bei Kommunikationen über die Unternehmens-Mailadresse davon ausgehen, dass man als Vertreter des Unternehmens auftritt. Deshalb dürfen insbesondere keine politischen oder religiösen Meinungen über die Unternehmens-Mailadresse verbreitet werden.

Streng vertrauliche wie auch vertrauliche Dokumente dürfen nur verschlüsselt per E-Mail weitergeleitet werden.

Auf Grundlage des Handelsgesetzbuches *(HGB)* und der Abgabenordnung *(AO)* müssen E-Mails archiviert werden. Eine Unterscheidung zwischen geschäftlichen *(Handels- und Geschäftsbriefen)* und privaten E-Mails ist technisch nicht möglich. Auch aus diesem Grunde sind private E-Mails nicht erlaubt. Dem Mitarbeiter ist damit bewusst, dass etwaige private E-Mails somit auch archiviert und an weiterer Stelle abgespeichert werden.

Auch am **Telefon** ist das Risiko einer unerlaubten Datensammlung durch unberechtigte Dritte unbedingt zu minimieren. Auskünfte zur Erfüllung des Geschäftszweckes sind grundsätzlich zulässig – doch es ist sicherzustellen, dass der Gesprächspartner auch ein Recht auf die gewünschten Informationen hat. Behörden, z. B. Staatsanwaltschaft oder Kriminalpolizei, richten ihre Anfragen in der Regel auf schriftlichem Wege an das Unternehmen. Am Telefon kann die Identität einer Person nicht geprüft werden, damit sind Verletzungen des Datenschutzes leicht möglich. Um dies zu vermeiden, gelten folgende Vorsichtsmaßnahmen:

- ✓ Kontrollfragen zur Identität, die nur durch die betroffene Person beantwortet werden können, z. B. nach der Mitgliedsnummer, nach der Adresse, nach dem Geburtsdatum etc.
- ✓ Rückrufe bei nachprüfbaren Identitäten, z. B. Ehepartnern, Behörden, Versicherungen, Polizei, etc.: „Ich muss das prüfen, kann ich Sie bitte zurückrufen?“
- ✓ Schriftliche Anfragen, wenn noch immer Zweifel an der Identität des Anrufers bestehen und keine Eile geboten ist.

Bei Unsicherheiten sind Interessenten an den Inhaber oder an den Datenschutzbeauftragten zu verweisen. Bei allen Anfragen müssen Name des Interessenten, Datum und Uhrzeit der Kontaktaufnahme sowie die gewünschten Auskünfte dokumentiert werden.

Das gesprochene Wort unterliegt dem Persönlichkeitsrecht. Ohne das ausdrückliche Einverständnis des Gesprächspartners dürfen Telefonate weder mitgeschnitten noch von Dritten über Lautsprecher mitgehört werden.

Entsorgung (streng) vertraulicher Daten

Unterlagen, die personenbezogene Daten enthalten, sind durch das Datenschutzgesetz geschützt – dies gilt auch für nicht mehr benötigte Dokumente wie überzählige Kopien, Formulare, Briefe, fehlerhafte Unterlagen, Notizen und sonstige nicht aufbewahrungspflichtige Vorgänge.

Zu unterscheiden ist also, ob Unterlagen vernichtet oder im Rahmen rechtlicher Aufbewahrungsfristen archiviert werden müssen:

VERNICHTET WERDEN DÜRFEN	ZU ARCHIVIEREN SIND
Überzählige oder fehlerhafte Etiketten, Geschäftsbriefe	Personalakten
Nicht mehr benötigte Urlaubspläne, Dienstpläne	Alle Arten von Bild- und Tonträgern
Unbedeutendes Schriftgut	Geschäftsbücher
etc.	etc.

Bei einer Entsorgung ist sicherzustellen, dass die Schweigepflicht gewahrt bleibt. Eine Offenbarung gegenüber Unbefugten kann einen Straftatbestand begründen und eine Geld- oder Freiheitsstrafe nach sich ziehen. Das bedeutet:

- ✓ Kontrollierte Zutrittsregelungen zu Räumen, in denen derartige Dokumente verwahrt werden
- ✓ Ggf. Aufbewahrung in geschlossenen Behältnissen bis zur endgültigen Vernichtung
- ✓ Keine Entsorgung im normalen Müll oder Altpapier, auch nicht in zerrissener Form

Publikation dieser Policy

Für unterschiedliche Adressaten wird dieses Datenschutz-Handbuch mit einer allgemeinverständlichen Darstellung der sie betreffenden Inhalte veröffentlicht. Aus diesem Grund ist das hiermit vorliegende Dokument mit Beispielen ergänzt.

Dieses Handbuch wird laufend überarbeitet und erhebt noch keinen Anspruch auf Vollständigkeit. Es sollte jedoch bei internen Verfahrensanweisungen hinterlegt sein.

Firmeninformationen

Hope Factory | Tu's für dich!
Straße und Hausnummer
PLZ und Ort

Tel.:
E-Mail: info@hopefactory.de
Web: www.hopefactory.de

Bestätigung der Kenntnisnahme

Dieses Handbuch wurde zur Kenntnis genommen, gelesen und verstanden.

Ort & Datum: _____

Name in Druckbuchstaben: _____

Funktion im Unternehmen: _____

_____
Unterschrift