Datenschutzanweisungen

1. Allgemeine Beschreibung

Diese Richtlinien gelten als Arbeits- und Handlungsanweisung für alle Mitarbeiter und beschreiben den Umgang mit personenbezogenen Daten und dem betrieblichen Datenschutz gem. Datenschutzgrundverordnung (DSGVO). Zusätzlich wird mit diesen Richtlinien die nach Art. 29 und 32 Abs. 4 DSGVO geforderte Organisationskontrolle umgesetzt.

2. Datenschutzgrundsatz

Unter Datenschutz versteht jeder etwas Anderes. Oft wird der Begriff mit dem Schutz von Betriebs- und Geschäftsgeheimnissen verwechselt. Oder aber mit Fragen der Datensicherheit bzw. IT-Sicherheit gleichgesetzt. Beides betrifft auch den Datenschutz, dessen eigentlicher Zweck (im rechtlichen Sinn) sich aus Art. 1 Absatz 1-3 des Datenschutzgrundverordnung (DSGVO) ergibt:

> „Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.
>
> Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.
>
> Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden."

Datenschutz ist ein Grundrecht, das sogenannte Recht auf informationelle Selbstbestimmung. Dies wird abgeleitet aus Artikel 2 Abs. 1 des Grundgesetzes. Das Recht auf Schutz der eigenen personenbezogenen Daten ist auch in Artikel 8 der EU-Grundrechtscharta konkret aufgenommen. Personenbezogene Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke verarbeitet werden. Basis muss eine Einwilligung oder eine gesetzliche Grundlage sein.

Datenschutz liegt also einerseits in den Händen jedes Einzelnen, anderseits stellt er an Firmen den Anspruch, nur gesetzlich legitime Datenverarbeitungen angemessen sicher vorzunehmen.

3. Schulung und Verpflichtung auf das Datengeheimnis

Alle Mitarbeiter werden bei Einstellung auf das Datengeheimnis verpflichtet.

Sie werden auf jährlicher Basis unterwiesen. Die Mitarbeitenden können die Schulung sowie das Schulungsportal www.datenschutzschulung.info auch als Datenschutzhandbuch nutzen. Aktuelle Informationen werden regelmäßig eingespielt.

4. Auswertung von Verkehrsdaten

Verkehrsdaten von Mitarbeitern werden grundsätzlich nicht ausgewertet, insbesondere findet keine systematische Auswertung des Telefon- oder Internetnutzungsverhaltens statt. Nur wenn besonderer Umstände eintreten, werden diese Daten ausgewertet. Das kann zum Beispiel sein, wenn Ermittlungen wegen Urheberrechtsverletzungen oder Internetkriminalität aufgenommen werden.

5. Sicherheitsgrundsätze

Folgende Grundsätze sind von jedem Mitarbeiter umzusetzen:

5.1. Nutzung Schlüssel und Schließregelung

Die Räumlichkeiten der Gesellschaften sind Teil einer Schließanlage und Alarmanlage. Mitarbeiter erhalten einen Schlüssel sowie einen Datenchip, mit welchem sie Zutritt zu den entsprechenden Bereichen erhalten. Die Ausgabe dieser Medien wird schriftlich dokumentiert. Deren Weitergabe an Dritte ist verboten. Bei Verlust ist sofort die ausgebende Stelle zu informieren, Schließ- und Alarmanlage müssen dann umgehend gesperrt werden, bzw. die Schließzylinder ausgetauscht und die Alarmanlage neu programmiert werden. Nur Sie dürfen den Ihnen übergebenen Medien persönlich nutzen.

5.2. Zugangs- und Besucherkontrolle

Besucher melden sich am Empfang und werden vom besuchten Mitarbeiter abholt. Der Besuch ist anschließend wieder zum öffentlich zugänglichen Bereich zu begleiten.

5.3. Reaktion bei telefonischen Anfragen

Anfragen zu Daten von Mitarbeitern und Kunden dürfen ohne Prüfung der Identität nicht beantwortet werden. Stellen Sie hierzu Fragen aus dem Kundenprofil, z.B. Kundennummer, Verbrauchsstellennummer. Wenden Sie sich in Zweifelsfällen an einen Kollegen, Ihren Datenschutzkoordinator oder Ihren Datenschutzbeauftragten.

Erst, wenn die Identität des Anrufers klar erwiesen ist und eine Rückrufnummer von dritter Seite vorliegt, kann der Mitarbeiter bei der Person zurückrufen. Das gilt in dringenden Fällen ganz besonders, da Betrüger gerne besonderen Druck aufbauen, um Menschen zu Handlungen zu zwingen.

Der grundsätzliche Weg für Auskünfte zu personenbezogenen Daten ist die schriftlich zu stellende Anfrage.

5.4. Bildschirmsperre

Der Bildschirm ist bei Verlassen des Arbeitsplatzes zu sperren (Windows-Taste und „L" oder STRG-ALT-ENTF), sobald Sie den Zugang zu Ihrem Bildschirm nicht mehr kontrollieren können. Die automatische Bildschirmsperre stellt lediglich eine Sicherheitsfunktion dar.

5.5. Nutzung von IT und Telefon zu privaten Zwecken

Die Nutzung von IT und Telefon zu privaten Zwecken ist nicht oder nur unter Einschränkungen (siehe evtl. Nutzungsvereinbarungen) gestattet.

Das Aufrufen oder Verbreiten pornografischer oder volksverhetzender Inhalte oder die Durchführung sonstiger strafrechtlich bedeutsamen Aktivitäten im Internet sind strengstens verboten.

Das Spielen von Onlinespielen ist verboten; über diese Spiele lässt sich sehr einfach Schadcode (Viren, Trojaner) einbringen.

5.6. Nutzung von beweglicher IT

Bewegliche IT (Laptop, Notebook, Smartphones) ist nach Nutzung möglichst verschlossen zu lagern. Bei Mitnahme zum Kunden darf sie nicht unbeaufsichtigt, bspw. im Auto, liegen gelassen werden.

5.7. Nutzung von privater IT und Software

Die Nutzung von privater IT ist verboten, diese öffnet große Sicherheitslücken im Firmennetz. Bei der Nutzung von privater Software gibt es Lizenzprobleme. Wenn die Gesellschaften Software nutzen, zu welcher die Nutzungsrechte fehlen, setzen sich diese hohen Schadenersatzforderungen aus. Daher ist auch die Nutzung von privater Software verboten.

5.8. Passwortrichtlinie

Passwörter sind nur Ihnen bekannt. Die Weitergabe von Passwörtern ist verboten. Es sind möglichst sichere Passwörter zu wählen. Solche bestehen aus mindestens acht Zeichen und enthalten Sonderzeichen, Zahlen und Buchstaben. Für Administrationskonten sollten mindestens vierzehn Zeichen vorgesehen werden. So wird bei einer „Brute-Force" Attacke auf das Passwort die Rechenzeit mehrere Jahre betragen. Ein einfaches Passwort ist innerhalb von Minuten zu errechnen.

5.8.1. Möglichkeit 1: Ein Merksatz

Eine einfache Möglichkeit, komplexe Passwörter zu generieren, ist die Zusammenstellung von Merksätzen. Ein Beispiel: Sie suchen ein Passwort für Ihr Benutzerkonto an der Arbeit. Ein Merksatz könnte lauten:

„Merk ich mir gern: Ein verlorenes Passwort kann schnell sehr teuer werden!"

Das Passwort wäre dann: Mimg:1vPkssw!

Diese Möglichkeit ist aber nur sinnvoll, wenn Sie wenige Konten nutzen.

5.8.2. Möglichkeit 2: Eine Regel

Im Kontext der Vorgabe „ein Passwort pro Anwendung" ist die Nutzung einer Regel, aus welcher sich das Passwort ableiten lässt, vorzuziehen. Hierzu wird das „Lieblingspasswort" links und rechts durch Sonderzeichen und ggf. das Geburtsdatum verstärkt und Buchstaben des genutzten Dienstes fließen mit ein.

Ihr Lieblingspasswort:	Hase123	
Verstärkung:	[$Hase123$]	
Weitere Verstärkung:	19[$Hase123$]78	
Individualisierung mit Dienst:	19w[$Hase123w$]78s	windows
Individualisierung mit Dienst:	19E[$Hase123i$]78l	E-Mail

5.8.3. Möglichkeit 3: ganze Sätze

Weiterhin ist die Eingabe eines Merksatzes als Passwort möglich, z.B.:

„MarkusundMariahabenam8.Augustgeheiratet."

Auch hierbei sollte darauf geachtet werden, Sonderzeichen mit einzusetzen.

5.8.4. Wechseln des Passwortes

Das Passwort ist nach einem Jahr zu wechseln. Nutzen Sie für verschiedene Accounts verschiedene Passwörter!

5.8.5. 2-Faktor Authentifizierung

Wenn möglich sind 2-Faktor Authentifizierungen vorzuziehen. Hierbei ist sicherzustellen, dass ein Notfallzugang eingerichtet und dokumentiert wurde.

5.9. Nutzung von sozialen Netzwerken und Apps

Viele Mitarbeiter nutzen soziale Netzwerke und Apps wie WhatsApp, XING, LinkedIn, Twitter oder Facebook. Ihnen muss klar sein, dass die von Ihnen eingestellten Informationen nicht nur von Freunden zu lesen sind, sondern auch durch Dritte, die Sie nicht kennen.

Ein Einstellen von Informationen über Firmeninterna ins Internet, auch in sozialen Netzwerken, stellt eine Verletzung der im Arbeitsvertrag geregelten Verschwiegenheitsverpflichtung dar. Darunter fällt auch der Abgleich von Kontaktdaten mit den Netzwerken.

Das Hinterlegen bzw. die Nutzung der dienstlichen E-Mailadresse, bspw. als Benutzername, in/für private Netzwerkdienste ist grundsätzlich nicht erlaubt.

5.10. Nutzung von externen Datenträgern

Die Nutzung von externen Datenträgern wie USB-Sticks, CDs, DVDs ist aufgrund der guten Vernetzung des Hauses grundsätzlich nicht notwendig, für die Weitergabe von Daten aber in Ausnahmefällen erforderlich. Verlassen Datenträger mit personenbezogenen Daten das Haus, sind diese grundsätzlich zu verschlüsseln.

Verschlüsselte Datenträger sind über die IT zu beziehen. Eigene Datenträger sind nicht erlaubt.

5.11. Nutzung von Cloud- oder Webbasierten Diensten

Die Nutzung Cloud- oder Webbasierten Diensten ist grundsätzlich nur nach schriftlicher Freigabe durch die IT/Geschäftsführung gestattet.

5.12. Vernichtung von Papier

Papiermüll mit enthaltenen personenbezogenen Daten ist in die vorgesehene Datentonne zu geben. Eine Firma ist mit der Vernichtung beauftragt, welche mindestens die Stufe P-3 gem. DIN 66399 erfüllt. Alternativ sind die Papiere zeitnah selbst zu schreddern. Hierzu muss ein Shredder genutzt werden welcher mindestens der Sicherheitsstufe P-3 der DIN 66399 entspricht.

5.13. Clean Desk Policy

Es gilt die Clean Desk Policy. Sobald Sie Ihren Arbeitsplatz für längere Zeit verlassen, befinden sich keine Dokumente mit personenbezogenen Daten mehr auf Ihrem Schreibtisch, die durch Dritte einsehbar wären. Die Unterlagen sind in geschlossenen Aktenschränken zu lagern. Sensible Unterlagen sind stets verschlossen zu lagern.

5.14. Anfragen zu Auskünften gem. Art. 15 EU-DSGVO

Anfragen auf Auskünfte zu gespeicherten Daten sind über den Datenschutzbeauftragten zu leiten. Dies bezieht sich auf Anträge, welche sich auf das Recht nach Art. 15 EU-DSGVO (Auskunftsrecht des Betroffenen) beziehen. Die Beantwortung erfolgt durch den Datenschutzbeauftragten in Verbindung mit dem Datenschutzkoordinator.

5.15. Reparatur oder Verkauf von Computern, Druckern und Kopiergeräten

Vor Reparatur oder Verkauf sind die Daten von den Geräten zu entfernen. Als datensicher gilt 5-maliges Überschreiben bei magnetischen Datenträgern. Die Reparatur oder die Absteuerung von Geräten darf nur durch die jeweiligen IT-Dienstleister erfolgen. Die Löschung der Datenträger ist zu dokumentieren. Dies gilt insbesondere auch bei Austausch in Garantiefällen.

5.16. Umgang mit E-Mails

5.16.1. Zugriff auf andere E-Mailkonten

Das Lesen von E-Mails von Kollegen ist grundsätzlich verboten. Da die private Nutzung des dienstlichen E-Mailkontos untersagt bzw. gesondert geregelt wurde, ist die Einsichtnahme in E-Mailkonten von Mitarbeitern nur im Rahmen einer schriftlichen Vertretungsregelung, z.B. Leserechte für die Dauer der Abwesenheit in besonderen Einzelfällen, zulässig. Eine Weitergabe von Passwörtern ist nicht gestattet.

5.16.2. Automatische Weiterleitung von E-Mails / Autoresponder bei Abwesenheit

Eine automatische E-Mailweiterleitung an Kollegen bei Abwesenheit ist nicht erlaubt. Wichtig ist, dass der Sender entscheiden kann, ob er diesem Kollegen die Nachricht auch zukommen lassen will. Richten Sie bei Abwesenheit eine automatische Antwort ein, die dem Sender mitteilt, dass Sie bis zu dem entsprechenden Datum nicht am Platz sind und die E-Mail nach Ihrer Rückkehr beantwortet wird. Für dringende Fälle geben Sie die Erreichbarkeit eines Kollegen an.

5.16.3. Klick auf Links, unbekannte Absender, gefälschte Absender

Ein Absender ist leicht fälschbar. Bleiben Sie wachsam, wenn Sie E-Mails öffnen, die von einem unbekannten Absender stammen oder Ihnen der Absender bekannt ist und die E-Mail ähnlich, aber nicht gleich aussieht wie sonst. Schalten Sie die automatische Vorschau von Bildern aus. Öffnen Sie Anhänge nur, wenn Sie sich absolut sicher sind, dass der Anhang von der richtigen Person stammt und Sie diesen auch angefordert haben. Bei kleinsten Zweifeln löschen Sie die E-Mail. Gerne werden Mahnungen, Rechtsanwaltsschreiben, Anhänge von bekannten Internet-Plattformen wie PayPal, Amazon, Facebook oder Ihrer Bank als Aufhänger genutzt, um Ihr Interesse zu wecken.

Klicken Sie niemals auf Links in E-Mails, die Sie nicht unmittelbar angefordert haben. Ist der Nachvollzug eines Vorgangs nötig, geben Sie die Adresse selbst im Browser ein.

5.16.4. Versand an mehrere Adressen/ Serien-E-Mails

Senden Sie niemals E-Mails an große Verteiler im AN- oder CC-Feld, nutzen Sie ausschließlich das BCC-Feld. Wichtig ist, dass sich die Adressaten nicht gegenseitig sehen können. Da E-Mailadressen personenbezogene Daten sind, würde die Übermittlung an einen großen Empfängerkreis einen Datenschutzverstoß darstellen. Newsletter und Werbemails unterliegen weiteren Regelungen die in den Prozessbeschreibungen ausgeführt sind.

5.16.5. Weiterleitung von E-Mails

Häufig entsteht ein längerer Dialog, der sich über mehrere Seiten hinzieht. Leitet man diesen weiter, kann es leicht passieren, dass sich Zulieferer und Kunde unfreiwillig kennenlernen. Denken Sie bei E-Mails an Empfänger außerhalb des Unternehmens daran eine neue E-Mail zu verfassen und nicht den alten Dialog ungefiltert weiterzuleiten.

5.16.6. Verschlüsselung

Sobald personenbezogene Daten (z.B. eine Mitarbeiterliste) übermittelt werden soll, ist diese Datei zu verschlüsseln. Sofern der Empfänger ein digitales Zertifikat besitzt, können Sie die E-Mail mit dem öffentlichen Schlüssel des Empfängers verschlüsseln. Alternativ fügen Sie die Datei einem neuen ZIP-Archiv hinzu und lassen das Passwort zur Entschlüsselung dem Empfänger auf einem zweiten Weg (Telefon, SMS) zukommen.

5.16.7. Bewerbungen

Bewerbungen dürfen nicht archiviert werden. Leiten Sie etwaige Bewerbungen an die Personalabteilung in ein gesondertes Mailpostfach/Mailadresse ohne Archivierung weiter und löschen Sie die Mail aus dem eigenen E-Mailordner (Posteingang und Postausgang). Öffnen und Speichern Sie keine Anhänge von Bewerbungsmails. Viren werden häufig über Bewerbungen verschickt indem Anhänge oder Links zu Dateien enthalten sind.

5.17. Verpackung und Versand von personenbezogenen Daten per Post / Paket

Verpackung:

Für den sporadischen Versand von personenbezogenen Daten in Kartons ist der Karton so zu versiegeln, dass ein Siegelbruch unmittelbar auffallen würde (Z.B. Aufkleber / Etikett mit Stempel). Der Karton ist so zu wählen und zu füllen, dass während des Transportes keine Schäden an den Unterlagen entstehen können:

- Stabilen Karton nutzen,
- Hohlräume ausfüllen, so dass Unterlagen nicht verrutschen können,
- ausreichende interne und äußere Umverpackung wählen, so dass bei einem Herunterfallen die Unterlagen keinen Schaden nehmen können.

Nutzen Sie besonders reißfeste und gepolsterte Umschläge, wenn Sie Datenträger versenden. Achten Sie auf die Verschlüsselung der Daten auf dem Stick und versenden Sie nicht das Kennwort im gleichen Brief. Teilen Sie dem Empfänger das Kennwort auf möglichst zweitem Weg (Telefon, E-Mail, SMS, Fax) mit.

Versand:

Bei der Wahl des Kuriers / Transportdienstes ist darauf zu achten, dass das Paket abhängig vom versendeten Inhalt ausreichend versichert ist und eine Rückverfolgung möglich ist.

5.18. Arbeiten unterwegs und zu Hause

Im Gegensatz zum Arbeitsplatz in einer Büroumgebung nutzt bei einem häuslichen Arbeitsplatz ein Mitarbeiter einen Arbeitsplatz im eigenen Wohnumfeld (sog. Telearbeit). Dabei muss eine hinreichende Trennung von beruflicher und privater Sphäre ermöglicht werden können. Die folgenden Regelungen gelten zusätzlich zu den o. g. Inhalten insbesondere für Telearbeit (und grundsätzlich für Laptop-Nutzung außerhalb der Geschäftsräume).

5.18.1. Schutz am Arbeitsplatz

- Schützen Sie den Laptop vor Unbefugten, wenn möglich in einem abschließbaren Raum. Sie dürfen keinem Unbefugten (einschließlich Familienangehörige) den Zugriff zu dem Gerät ermöglichen.

- Verschließen Sie bei Verlassen des Raumes Türen und Fenster sicher.
- Bewahren Sie Akten, Unterlagen und Datenträger in verschließbaren Behältern, um die Einsichtnahme durch Unbefugte zu verhindern, aber auch um Diebstahl oder Beschädigung von Akten und/ oder Datenträgern vorzubeugen.
- Beim Verlassen des Arbeitsplatzes ist der Rechner zu sperren (Windows-Taste + [L]). Eine automatische Bildschirmsperre sollte zusätzlich Sicherheit nach spätestens 15 Minuten in Kraft treten.
- Führen Sie eine Datensicherung durch, sobald Sie sich mit dem Firmennetzwerk verbinden.
- Vernichten Sie nicht mehr benötigte Unterlagen (keine unnötige Lagerung).
- Gerade am häuslichen Arbeitsplatz ist es wichtig, Datenträger und Ausdrucke datenschutzkonform zu entsorgen und nicht einfach in den Hausmüll zu werfen. Vernichten Sie Unterlagen mit personenbezogenen Daten daher stets mit dem zur Verfügung gestellten Aktenvernichter des Unternehmens oder halten Sie diese unter Verschluss und vernichten Sie die Unterlagen im Unternehmen.
- Geben Sie defekte oder nicht mehr benötigte digitale Datenträger zur Entsorgung ab. Achten Sie dabei auf den sicheren Transport.
- Sorgen Sie unterwegs stets für den sicheren Transport von Akten und Unterlagen (nicht unbeaufsichtigt lassen).
- Trennen Sie bei Gewitter, Stromausfall oder längerer Abwesenheit (Urlaub usw.) Netz- und Datenleitungen von den Anschlussdosen.

Informieren Sie bei technischen Störungen (Hard- oder Software) den Administrator des IT-Dienstleisters.

5.18.2. Schutz bei der Übertragung von Daten

Das Unternehmen hat technische Schutzmaßnahmen ergriffen, um die Daten bei der Übermittlung von Ihrem Laptop zum Unternehmens-Netzwerk abzusichern – dabei kommt ein VPN („Virtual Private Network") zum Einsatz und die Daten sind bei der Übertragung verschlüsselt. Wichtig ist dabei, dass Sie die festgelegten Datenübertragungswege einhalten.

5.19. Beauftragung von Fremdfirmen

Vor der Beauftragung von Fremdfirmen ist eine Vereinbarung zur Auftragsdatenverarbeitung zu schließen, wenn personenbezogene Daten (bspw. Mitarbeiter-, Kundendaten etc.) durch diese Fremdfirma verarbeitet werden. Hierzu ist vorab der Datenschutzkoordinator und die Datenschutzbeauftragte einzuschalten.

5.20. Meldung von möglichen Datenschutzvorfällen

Wenn die Möglichkeit nicht auszuschließen ist, dass Daten abhandengekommen oder Dritten unzulässig zur Kenntnis gebracht worden sind, ist sofort der IT-Administrator, der Datenschutzbeauftragte und die Geschäftsführung zu informieren.