Datenschutz- und IT-Nutzungsrichtlinie

Verantwortliche Stelle

Schirm GmbH
Geschwister-Scholl-Straße 127
39218 Schönebeck (Elbe)
Germany

Tel.: +49-3928-456-199
Fax: +49-3928-456-300
E-Mail: schirm@schirm.com

Geschäftsführung/Management board

Thomas Schulz
Johannes Steinel

Datenschutzbeauftragter

FKC CONSULT GmbH
Eschenburgstr. 5
23568 Lübeck

Tel.: +49 451 400510
E-Mail: Datenschutz@schirm.com

IT-/Systemadministration

Frank Steuer
Schirm GmbH
Geschwister-Scholl-Straße 127
39218 Schönebeck (Elbe)
+49 3928 456325
+49 172 7088032

Vorwort

Für die Schirm GmbH (im Folgenden Unternehmen genannt), hat der sichere Umgang mit den personenbezogenen Daten seiner Kunden, Mitarbeiter Geschäftspartner und Dienstleister strategische Bedeutung. Als Mitarbeiter tragen Sie dazu wesentlich bei, dieses Ziel einzuhalten. Im Folgenden werden die internen Richtlinien zur Sicherheit in der Verarbeitung personenbezogener Daten definiert. Die Mitarbeiter verpflichten sich in einer Zusatzerklärung zum Mitarbeitervertrag auf die Einhaltung des Datenschutzes im Betrieb.

Allgemeines

Die IT-Einrichtungen des Unternehmens sind ausschließlich zur betrieblichen Nutzung für den im Mitarbeitervertrag geregelten Zweck vorgesehen. Dem Mitarbeiter werden die Arbeitsmittel vollständig vorkonfiguriert zur Erfüllung der jeweiligen Aufgaben zur Verfügung gestellt. Hierzu zählen Internetzugang, E-Mail-Zugang, Handy, Mobile Devices, Laptops, PC oder Tablets. Es ist kein weiteres eigenmächtiges Eingreifen in die Konfiguration gestattet. Die betriebliche IT-Abteilung steht in der Regel werktags von 7 bis 20 Uhr zur Verfügung. Außerhalb dieser Zeiten können jederzeit Wartungsarbeiten und Systemneustarts durchgeführt werden. Der Mitarbeiter hat pflichtbewusst, umfangreich und wahrheitsgemäß mit der IT-Abteilung zu kooperieren und zu kommunizieren. Für Vorsatz, grobe Fahrlässigkeit oder Begehen einer Straftat haftet der Mitarbeiter persönlich. Die Regelungen gelten auch für die Nutzung außerhalb der Betriebsräume.

1. IT-Nutzung

1.1 Private Nutzung betrieblicher IT

Dem Mitarbeiter ist es untersagt, die zur Verfügung gestellte betriebliche IT in jeglicher Form privat zu nutzen. Dies betrifft insbesondere

- das Laden, Speichern und Bearbeiten privater Dokumente;
- die Benutzung privater Datenträger;
- die private Benutzung von Browsern oder sonstiger Internetfähiger Software zum Abruf von Information, Daten oder Apps;
- Versand und Empfang von privaten Nachrichten, Bildern oder Videos per E-mail, Chat, Messenger oder sonstiger Kommunikationssoftware (Weitere Information unter dem Punkt „Betriebliche Kommunikation“);
- Abruf, Anbieten, Verbreiten oder Speichern von Inhalten, die gegen das Persönlichkeitsrecht, Urheberrecht, Datenschutzrecht oder Strafrecht verstoßen ist untersagt insbesondere gilt das für das unerlaubte Herunterladen oder Anbieten von Musik, Filmen, Software oder anderen urheberrechtlich geschützten Inhalten;
- Abruf, Anbieten, Verbreiten oder Speichern von rufschädigenden, beleidigenden, verleumderischen, diskriminierenden, menschenverachtenden, rassistischen, verfassungsfeindlichen, sexistischen, gewaltverherrlichenden oder pornografischen Inhalten;
- Abruf, Anbieten, Verbreiten oder Speichern von Computerviren oder anderer Schadsoftware sowie sonstige Aktivitäten, die sich gegen die Sicherheit von IT-Systemen richten (z. B. Hacking, Portscans);
- Abruf von für das Unternehmen kostenpflichtigen Inhalten, soweit dies nicht mit Zustimmung des Vorgesetzten zu betrieblichen Zwecken erfolgt;
- Anbieten oder Verbreiten religiöser, weltanschaulicher oder politischer Inhalte;
- Anbieten oder Verbreiten von Informationen, Behauptungen oder Meinungsäußerungen jeder Art (z. B. durch Einstellen in Diskussionsforen, Mitarbeit an Wikipedia-Beiträgen), wenn dabei entweder
- die Betriebszugehörigkeit erkennbar ist (z. B. die IP-Adresse gespeichert wird oder eine Angabe erfolgt) oder
- die Informationen, Behauptungen oder Meinungsäußerungen einen Bezug zur betrieblichen Tätigkeit haben, soweit dies nicht mit Zustimmung des Vorgesetzten zu betrieblichen Zwecken erfolgt;

Nicht gestattet sind:

- eigenmächtige Änderungen an Hard- oder Software oder Konfiguration;
- selbstständige Installation von Programmen, Apps oder sonstiger Software;
- die Nutzung der IT zu einem anderen als dem betrieblichen Zweck zur Erfüllung der betrieblichen Aufgabe;
- Preisgabe oder Gefährdung von Geschäfts- und Betriebsgeheimnissen, vertraulicher Daten aller Art (insbesondere von denen welche als vertraulich eingestuft werden oder bei denen, welche sich die Vertraulichkeit aus der Art der Information ergibt;
- private Lieferungen an die Geschäftsadresse zu veranlassen;
- Sicherheitseinrichtungen zu umgehen;
- Private Geräte zum Laden an die USB-Anschlüsse der betrieblichen IT anzuschließen. Dies gilt auch für alle anderen Arten von Anschlüssen;
- Nutzung privater IT im Firmennetzwerk;

Das Unternehmen behält sich stichprobenartige oder bei Verdacht auf Missbrauch weitergehende Kontrollen vor. Die Foto-Funktion von privater IT ist bei Betreten der Betriebsräume zu deaktivieren. Fotoaufnahmen in den Betriebsräumen sind grundsätzlich vom Vorgesetzten zu genehmigen.

1.2 Behandlung & Pflege

Die zur Verfügung gestellte IT ist sorgsam zu behandeln und regelmäßig mit den vorgegebenen Hilfsmitteln zu reinigen (Bildschirm, Tastatur, Maus). Eine weitergehende Wartung wird ausschließlich durch Mitarbeiter der IT-Abteilung durchgeführt. Defekte sind umgehend der IT-Abteilung zu melden. Außer Sichtprüfungen (bspw. Kabel entfernt) hat der Mitarbeiter keine eigenständigen Reparaturversuche zu unternehmen. Weitergehender Umgang mit Störungen wird gesondert in den Notfallplänen geregelt.

1.3 Betriebliche Kommunikation, E-Mail-Zugang

- Private Nutzung der betrieblichen E-Mail-Adresse und -Programme ist untersagt. Dies gilt sowohl für ausgehende Nachrichten als auch für eingehende (etwa Angabe der betrieblichen E-Mail-Adresse bei privaten Bestellungen). Zur betrieblichen Nutzung im Sinne dieses Absatzes gehören auch die sogenannte betrieblich veranlasste Privatnutzung, etwa wenn der Mitarbeiter wegen kurzfristiger Überstunden einen privaten Termin absagt und die Kommunikation mit betrieblichen Interessenvertretungen, dem Betriebsarzt, dem Datenschutzbeauftragten und der betrieblichen Beschwerdestelle. Sämtliche betriebliche Korrespondenz – einschließlich des E-Mail-Zugangs – unterliegt der ausschließlichen Verfügungsbefugnis vom Unternehmen.
- Empfänger sind vor Versand als Berechtigter zum Erhalt der enthaltenen Information zu prüfen;
- Besonders bei Auswahl-Listen von Vorschlägen (bspw. „AN:“-Feld in Outlook) ist Vorsicht walten zu lassen;
- Auf die korrekte Nutzung der Felder CC: und BCC: ist zu achten. Vor dem Versand an mehrere Empfänger ist zu prüfen, ob diese notwendigerweise die Information erhalten müssen;
- Für betriebliche Kommunikation dürfen ausschließlich die vom Unternehmen zur Verfügung gestellten technischen Einrichtungen genutzt werden, insbesondere nur der betriebliche E-Mail-Zugang und keine privaten E-Mail-Accounts und keine privaten Computer oder IT;
- Die Umleitung, Weiterleitung oder Speicherung dienstlicher Informationen, Nachrichten oder Dateien (insbesondere E-Mails) an private Accounts oder auf privaten Datenträgern oder Speicherdiensten (insbesondere Cloud-Services) ist verboten;
- Die Weitergabe personenbezogener Daten an Dritte ist nur gestattet, wenn sie datenschutzrechtlich zulässig ist;
- Bei Eingang privater Nachrichten Absender darauf hinzuweisen, dass der betriebliche E-Mail-Zugang nur für betriebliche Zwecke verwendet werden darf und daher keine weiteren privaten Nachrichten an die betriebliche Anschrift gesandt werden sollen;
- Im Rahmen der Vertretung oder sonstiger betrieblicher Aufgaben (insbesondere Systemadministration, Kontrollen, Vorlagepflichten) kann nicht ausgeschlossen werden, dass Nachrichten privaten Charakters von anderen Personen als dem jeweiligen Inhaber des E-Mail-Zugangs zur Kenntnis genommen werden. Über den Inhalt ist in diesem Fall Stillschweigen zu bewahren, soweit nicht besondere

Erlaubnistatbestände außerhalb dieser Vereinbarung (z.B. gesetzliche Erlaubnis zur Verfolgung von Straftaten) vorliegen. Im Rahmen der Systemadministration ist die Erforderlichkeit des Zugriffs auf fremde Nachrichten stets gesondert zu prüfen;

- Ein- und ausgehende elektronische Nachrichten werden vom Unternehmen automatisch für die Dauer gesetzlicher Aufbewahrungspflichten (vgl. § 147 AO, § 257 HGB) und gegebenenfalls betrieblicher Notwendigkeiten, insbesondere im Rahmen von Rechtsstreitigkeiten, archiviert. Ebenfalls werden regelmäßig Sicherungskopien des E-Mail-Zugangs angefertigt. Hierbei erfolgt aus technischen Gründen keine Unterscheidung zwischen Nachrichten betrieblichen und privaten Charakters. Eine selektive Löschung bestimmter, insbesondere privater, Nachrichten ist nicht möglich. Es liegt daher auch im Interesse des Persönlichkeitsrechts des Mitarbeiters, das Verbot der privaten Nutzung des E-Mail-Zugangs strikt einzuhalten.

1.4 Mobile Devices

Mitarbeiter, welche mobile Geräte (bspw. Notebooks, Smartphones, Tablets) zur Verfügung gestellt bekommen, beachten folgende Grundsätze:

- keine eigenmächtige Installation von Software oder Apps;
- Passwortschutz bei Nichtbenutzung;
- sichere Aufbewahrung;
- fremde Netzwerke nur mit aktivierter VPN-Verbindung nutzen;
- umgehende Meldung bei Verlust oder Beschädigung;
- keine dauerhafte lokale Speicherung betrieblicher Daten;
- die Geräte sind sorgsam zu behandeln und vor Beschädigung zu schützen;
- vor Zugriff oder Zugang für Dritte (bspw. Sicht auf Bildschirm an öfftl. Plätzen, Mithören von Telefonaten) ist das Device zu schützen;
- die Verschlüsselung der Datenträger ist, soweit technisch möglich, zu aktivieren.

1.5 Drucker

Ausdrucke sind umgehend am Drucker abzuholen. Insb. bei Druck von Personalunterlagen ist besondere Sorgfältigkeit geboten. Fehldrucke sind direkt am im Aktenvernichter/-container zu entsorgen. Bitte nutzen Sie Ausdrucke nur, wenn eine Bearbeitung am Bildschirm ausgeschlossen ist.

1.6 Dateien

Alle personenbezogenen Dateien sind in den dafür vorgesehenen Netzwerklaufwerke zu verarbeiten. Andere betriebliche Dateien sind grundsätzlich in den vorgesehenen Ordnern der Netzwerklaufwerke zu sichern. In Bearbeitung befindliche Dateien können temporär im persönlichen Ordner des Netzwerklaufwerks gesichert werden. Eine lokale Speicherung ist nur in einzelnen Ausnahmefällen (Serverausfall, nur lesender Zugriff bis zur unmittelbaren Löschung) erlaubt.

1.7 Telefon/ Telefax

Es darf keine Auskunft zu personenbezogenen Daten bei nicht authentifizierten Anrufen (Ein-/Ausgehend) gegeben werden, sondern ggf. den Verweis auf einen schriftlichen Versand der Auskunft. Die private Nutzung von Telefon und Telefax ist untersagt. Ausgenommen sind Informationen an Familienangehörige, die im direkten bzw. indirekten Zusammenhang mit der aktuellen Berufsausübung stehen.

1.8 Attachments/Anhänge

Unbekannte oder unerwünschte E-Mails mit Anhängen sind in keinem Fall zu öffnen und umgehend ungelesen zu löschen. Bei Bedarf ist die IT-Abteilung zu informieren.

1.9 Spam

Es wird ein vorgegebener SPAM-Filter zur Aussortierung betrieblich unerwünschten E-Mail-Verkehr genutzt.
Der Mitarbeiter hat keinen Anspruch auf Zustellung einer bestimmten E-Mail. Es tritt in Einzelfällen auch das Löschen erwünschter E-Mails auf. Bei Verdacht nimmt der Mitarbeiter Kontakt mit dem IT-Administrator auf.
Besondere Vorsicht ist bei unbekannten Absendern mit Links in der E-Mail zu wahren. In keinem Fall darf der Link angeklickt werden.

1.10 Passwörter

Die Vergabe von Passwörtern stellt den Zugangsschutz zu personenbezogenen Daten dar. Passwörter sind vom Mitarbeiter gegenüber allen anderen Personen (auch IT-Administration, Geschäftsleitung, Datenschutzbeauftragter) geheim zu halten und nicht schriftlich zu notieren. Für Mitarbeiter, die umfangreiche Passwörter verwalten müssen, wird ein Passwort-Safe zur Verfügung gestellt.
Folgende Passwortrichtlinien sind einzuhalten.

- Prüfen Sie welche Möglichkeiten Ihre Systeme zur Vergabe von Passwörtern besitzen
- Verwenden Sie mindestens 8 Zeichen
- Jeweils mit mindestens 1 Zeichen groß- oder kleingeschrieben, 1 Zahl und einem Sonderzeichen
- Verwenden Sie keine Post-It zum Notieren der Passwörter

Arbeiten mit Administrationsrechten werden ausschließlich von befugten Personen oder der IT-Abteilung ausgeführt.

Im Falle eines Passwort-Verlustes ist der Vorgesetzte oder Systemadministrator zu informieren zur Neuerstellung des Passwortes.

Bei Verdacht auf unbefugte Benutzung ist unmittelbar die Geschäftsleitung oder der Datenschutzbeauftragte zu informieren.

Für unterschiedliche Anwendungen sind unterschiedliche Passwörter zu verwenden. Für unterschiedliche Schutzstufen können Passwörter unterschiedlicher Komplexität verwendet werden.
Merksätze:
Um sich Passwörter merken zu können, haben sich „Merksätze“ bewährt.
„Heute werden 3 Regentropfen auf 5 Blumen fallen!“ ergibt bspw. durch Verwendung der Anfangsbuchstaben ein Passwort von „Hw3Ra5Bf!“.Je kreativer, desto leichter zu merken.

Stellvertreterregelung:
Mitarbeiter tauschen untereinander in KEINEM FALL Passwörter zur Vertretung aus. Sollte in Abwesenheit ein Zugang zum Benutzer-Account eines anderen Benutzers erfolgen, sollte dies idealerweise durch Übernahme der Rechte durch einen anderen Account erfolgen. Jeder Mitarbeiter ist dafür verantwortlich, was unter seinem Account geschieht. Vertreter dürfen nur während der Abwesenheit oder nach dem Ausscheiden des Mitarbeiters auf dessen E-Mail-Zugang zugreifen. Dies gilt auch zur nachträglichen Einstellung eines Abwesenheitsassistenten, wenn dieser nicht eingestellt wurde.

Nach dem Ausscheiden des Mitarbeiters kann der Arbeitgeber den persönlichen E-Mail-Zugang noch bis zu drei Monate aufrechterhalten und einem Vertreter Zugriff gewähren bzw. eingehende Nachrichten an diesen weiterleiten. Alle Absender sind durch den Vertreter oder automatisch darauf hinzuweisen, dass der Mitarbeiter nicht mehr unter dieser Anschrift erreichbar ist und, im Fall betrieblicher Nachrichten, wer neuer betrieblicher Kontakt ist.

2. Betriebliche Organisation und IT-Sicherheit

Der beste Schutz vor Sicherheitsverletzungen sind geschulte Mitarbeiter.
Das Unternehmen legt Wert auf umfangreiche Qualifizierung und Weiterbildung, um die Einhaltung des Sicherheitsniveaus zu gewährleisten. Zur Unterstützung der Mitarbeiter bei der Einhaltung der Sicherheitsrichtlinien stellt der Betrieb technische und organisatorische Maßnahmen zur Verfügung.

2.1 Clean-Desk-Policy

Auf dem Schreibtisch und dem virtuellen Desktop befinden sich grundsätzlich nur Akten und Dateien, die zur Bearbeitung des aktuellen Sachverhaltes dienen. Nach Abschluss werden diese wieder eingeordnet.
Bei Verlassen des Arbeitsplatzes oder Betreten des Raumes betriebsfremder Personen sind alle offenen Akten zu schließen und der Bildschirm vor Einsicht zu schützen.

2.2 Verlassen des Arbeitsplatzes

Bei Arbeitsende ist der PC herunterzufahren, Schreibtisch von offenliegenden Akten zu befreien, Fenster und Türen zu schließen. Der Arbeitsplatz muss sicher vor Einsicht oder Zugang Dritter zu personenbezogenen Daten gesichert sein.

2.3 Virenschutz

Es wird ein mehrstufiger Virenschutz zur Verfügung gestellt.
Unbekannte Dateien oder Dateien von unbekannten Empfängern sind nicht zu öffnen.
Betrieblich nicht zugelassene mobile Datenträger (CD/DVD, USB-Stick, externe Festplatten, Speicherkarten) dürfen vom Mitarbeiter nicht an die IT-Systeme angeschlossen werden. Bei Bedarf wird die IT-Abteilung informiert. Besteht der Verdacht auf Virenbefall sind umgehend alle Arbeiten einzustellen, der Netzstecker zu ziehen und die IT-Abteilung oder der Vorgesetzte zu informieren. Selbstreparaturversuche sind zu unterlassen.

2.4 Besuch

Besucher der Betriebsräume werden in die ausgewiesenen Besucherzonen geleitet. Ein Zutritt zu den Büroräumen ist nur in Begleitung eines Mitarbeiters gestattet. Telefonate und Akten sind vor Besuchern geheim zu halten. Besucher erhalten keinen Zugang zu internen IT-Systemen. Bei Bedarf steht ein Gäste-WLAN zur Verfügung. Mitarbeiter können das Gäste-WLAN zu privaten Zwecken nutzen.

2.5 Homeoffice

Mitarbeiter können bei Bedarf und in Absprache nach den Regelungen im Mitarbeitervertrag im Homeoffice arbeiten. Das Schutzniveau der betrieblichen Anforderung ist dabei in keinem Fall zu unterschreiten. Mitgenommene Akten sind vor dem Zugriff und Zugang Dritter geheim zu halten. Es erfolgt keine lokale Speicherung betrieblicher Daten auf privater IT. Der Zugang zum Firmennetzwerk erfolgt ausschließlich per VPN-Verbindung.

2.6 Sicherheitsvorkehrungen

Jegliche Umgehung betrieblicher Sicherheitsmaßnahmen ist dem Mitarbeiter untersagt.
Hierzu zählen unter anderem:

- Deaktivieren des Passwortschutzes;
- Umgehung der betrieblichen Internetverbindung,
- Deaktivieren von Virenschutz, Firewall und Sicherheitssoftware;
- Eigenmächtige Inbetriebnahme externer Datenträger;
- Ausführen nicht betrieblich genehmigter Software und Apps;
- Maßnahmen, die zur Verschlechterung des Datenschutzniveaus führen.

2.7 Fernwartung

Dem Mitarbeiter ist bewusst, dass die IT-Abteilung die Möglichkeit zur Fernwartung für Support und Administrationszwecke erhält. Der Zugriff erfolgt immer in Absprache mit dem Mitarbeiter.

2.8 Akten

Papierdokumente sind in der jeweiligen Ablage einzuordnen. Akten mit besonderem Schutzbedürfnis (Mitarbeiter-/Personalakten) sind gesondert unter Verschluss aufzubewahren. Bei Verwendung außerhalb der

Betriebsräume ist besondere Vorsicht auf Verlust und Einsichtsmöglichkeit durch Dritte zu wahren. Nicht mehr benötigte Akten sind ordnungsgemäß zu entsorgen oder einem speziellen Dienstleister zur Vernichtung zu übergeben.

2.9 Ahndung von Verstößen

Bei grober Fahrlässigkeit oder vorsätzlicher Verletzung dieser Sicherheitsrichtlinien behält sich der Arbeitgeber das Recht auf disziplinare Maßnahmen gegenüber dem Mitarbeiter vor.

2.10 Zutritt / Zugang zu Serverräumen

Zutritt zu dem Serverraum haben nur berechtigte Personen. Der Serverraum ist ausschließlich zur Verwahrung von IT-Komponenten gedacht. Der Serverraum und der Serverschrank sind verschließbar. Schlüsselausgabe erfolgt nur an berechtigte Personen.

2.11 Social Hacking

Die Kommunikation personenbezogener Daten erfolgt ausschließlich an eindeutig authentifizierte Personen.
Behörden werden in keinem Fall die mündliche Herausgabe von Daten verlangen. Bei ungewöhnlichen Anweisungen durch Vorgesetzte werden diese auf einem zweiten Kommunikationsweg um Bestätigung gefragt.
Bei nicht eindeutig identifizierten Kommunikationspartnern erfolgt nur schriftliche Auskunft an die im Verwaltungsprogramm hinterlegte Adresse. Übt die betroffene Person Druck zur Herausgabe von Daten auf den Mitarbeiter aus, ist der Vorgesetzte zu informieren. Ansonsten ist der Mitarbeiter auf Geheimhaltung betrieblicher Informationen verpflichtet.

2.12 Datenpannen

Bei Kenntnisnahme einer Datenpanne und vor weiterer Bearbeitung und Kommunikation ist der Datenschutzbeauftragte und/oder die Geschäftsleitung zu konsultieren. Es werden keinerlei Schritte außerhalb der Anweisungen eigenmächtig ausgeführt.

2.13 Betroffenenrechte

Wird während Ihrer Tätigkeit ein Betroffenenrecht Ihnen gegenüber geltend gemacht, melden Sie sich umgehend bei unserem Datenschutzbeauftragten.

Betroffenenrechte die geltend gemacht werden können sind:

- **Recht auf Auskunft** über die von uns zu der Person verarbeiteten personenbezogenen Daten. Bei einer Auskunftsanfrage, die nicht schriftlich erfolgt, bitten wir um Verständnis dafür, dass wir dann ggf. Nachweise von der Person verlangen, die belegen, dass Sie die Person ist, für die Sie sich ausgibt. Informieren Sie Ihren Vorgesetzten oder den Datenschutzbeauftragten.
- **Recht auf Berichtigung** oder **Löschung** oder auf **Einschränkung der Verarbeitung**.
- **Widerspruchsrecht** gegen die Verarbeitung.
- **Recht auf Datenübertragbarkeit**.
- **Recht auf Beschwerde bei einer zuständigen Landesbehörde**.

3. Störungen, Ausfälle und Sicherheitsvorfälle

Liegt eine der in der Überschrift vorkommenden Fälle vor ist der jeweilige Ansprechpartner unverzüglich zu informieren.

- Ein **Sicherheitsvorfall** ist ein unerwünschtes Ereignis, das Auswirkungen auf die Informationssicherheit und/oder den Schutz von personenbezogenen Daten hat und in der Folge große Schäden nach sich ziehen kann.
- Eine **Störung** ist eine Situation, in der Prozesse oder Ressourcen des Unternehmens nicht wie vorgesehen funktionieren. Die dadurch entstehenden Schäden sind als *gering* einzustufen. Die Beseitigung einer Störung kann im allgemeinen Tagesgeschäft vorgenommen werden.

- Ein **Ausfall** liegt vor, wenn ein Teil oder Teile der IT-Infrastruktur ihre Funktionsfähigkeit verloren haben.

Hier finden Sie eine Übersicht der verantwortlichen Personen für die genannten Bereiche:

Name / Rufbereitschaft	Telefon (intern)	Handy/Privat-Nr.	Funktion/Bemerkung
Schirm GmbH	03928/456-0		Notfallverantwortlicher / Hausmeister/ Gebäudetechnik
Thomas Schulz		+49-3928 456 365	IT-Leiter
FKC CONSULT GmbH	0451-400510		Datenschutzbeauftragter

4. Datenspeicherung / Backup und Recovery Konzept

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

4.1 Grundsätze der Speicherung von Daten

Grundsätzlich sind Daten nicht auf lokalen Festplatten oder Datenspeichern von Endgeräten zu speichern. Hintergrund ist neben der dann fehlenden Verfügbarkeit der Daten vor allem auch, dass dann eine Sicherung der Daten nicht in hinreichender Weise erfolgt.

Die Speicherung von Daten hat grundsätzlich in den Verzeichnissen/Ordnern von Servern bzw. IT-Systemen zu erfolgen, die für den Benutzer freigegeben sind. Die Daten sind stets in den jeweils einschlägigen Abteilungs-, Gruppen- oder Projektordnern zu speichern. Bei der Verwendung von mobilen IT-Systemen und mobilen Datenträgern sind die insoweit geltenden Richtlinien zu beachten.

4.2 Datensicherung

Das Unternehmen stimmt mit ihren Administratoren ab, welche Daten in welchem Rhythmus und auf welchen Medien bzw. an welchen Orten gesichert werden. Die Datensicherungsstrategie ist von den zuständigen Administratoren zu dokumentieren. Datensicherungen sind mindestens täglich anzufertigen.

4.3 Regelungen für Administratoren

- Die Administratoren sind verpflichtet, alle für das Unternehmen bereitgestellten Speicherorte zu dokumentieren und mit dem jeweiligen Zweck des Verzeichnisses in ein Verzeichnis aufzunehmen. In dem Verzeichnis sind ggf. auch die erforderlichen Berechtigungen (Gruppen/Rollen) zu hinterlegen.
- Wenn neue Speicherstrukturen durch Administratoren erstellt werden, ist dies mit der Unternehmensleitung abzustimmen.
- Die Administratoren erstellen ein Backup und Recovery Konzept um im Bedarfsfalle Daten wiederherstellen bzw. einsehen zu können.
- Die Wiederherstellung wird durch regelmäßige und dokumentierte Tests geprüft.

5. Löschkonzept

5.1 Allgemeines

Das Datenschutzrecht geht im Regelfall davon aus, dass personenbezogene Daten zu löschen sind, soweit nicht gesetzliche oder vertragliche Aufbewahrungsfristen oder schutzwürdige Belange der bzw. des Betroffenen dem entgegenstehen. Unter Löschen versteht man das unkenntlich machen gespeicherter personenbezogener Daten. Eine Unkenntlichmachung in diesem Sinne liegt erst vor, wenn jede Kenntnisnahme des Informationsgehalts

irreversibel unmöglich gemacht wurde, egal auf welchem Wege, sei es durch Durchstreichen, Übermalen, Zerstörung des Datenträgers o. ä. Informationen müssen sicher gelöscht werden, wenn Datenträger ausgesondert oder gesetzliche Aufbewahrungsfristen überschritten werden. Die Dauer der Speicherung personenbezogener Daten ist grundsätzlich an die Erforderlichkeit zur Aufgabenerfüllung geknüpft. Sind die für eigene Zwecke verarbeiteten personenbezogenen Daten für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich, so sind diese Daten zu löschen. Personenbezogene Daten dürfen eigentlich jederzeit gelöscht werden – es sei denn, dem stehen Aufbewahrungsfristen oder Interessen des Betroffenen entgegen.

5.2 Löschfristen

Die personenbezogenen Daten sind u.a. zu löschen, wenn:

- Die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind;
- Die betroffene Person ihre Einwilligung, auf die sich die Verarbeitung stützte, widerruft und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt;
- Die betroffene Person Widerspruch gegen die Verarbeitung einlegt und keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen;
- Die personenbezogenen Daten unrechtmäßig verarbeitet wurden;
- Die Löschung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.

Die Löschfrist ist dann erreicht, wenn der Zweck der Datenerhebung erfüllt und die Aufbewahrungsfrist abgelaufen ist. Die Löschung ist dann gemäß dieser Richtlinie durchzuführen.

Zu beachtende Aufbewahrungsfristen ergeben sich

- z.B. handels- und steuerrechtliche Aufbewahrungsfristen sowie insbesondere
- bestimmte Aufbewahrungsfristen laut Vertrag mit dem Kunden, ferner
- der Aufbewahrung aus Gründen der Gewährleistung, des Regresses u.v.m.

5.2.1 Aufbewahrungspflichten nach der Abgabenordnung

Gemäß 147 Abs. 1 Nr. 5 AO sind „Unterlagen, soweit sie für die Besteuerung von Bedeutung sind“, geordnet aufzubewahren. § 147 Abs. 1 AO führt dazu noch einzelne Unterlagen gesondert auf, die aufbewahrt werden müssen:

- Bücher, Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, Eröffnungsbilanzen, außerdem dazugehörige Arbeitsanweisungen und andere Organisationsunterlagen;
- Handelsbriefe und Geschäftsbriefe, die in Empfang genommen wurden;
- Kopien von Handelsbriefe/n und Geschäftsbriefe/n, die versendet wurden;
- Buchungsbelege.

5.2.2 Aufbewahrungspflichten nach dem Handelsgesetzbuch

Für Kaufmänner nach dem Handelsrecht gelten gemäß § 257 Abs. 1 HGB folgende Aufbewahrungspflichten:

- Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse;
- Handelsbriefe, die in Empfang genommen wurden;
- Kopien von Handelsbriefen, die versendet wurden;
- Buchungsbelege.

5.2.3 Dauer der Aufbewahrung

Zehn Jahre müssen aufbewahrt werden: Bücher, Aufzeichnungen, Jahresabschlüsse, Inventare, Lageberichte, Eröffnungsbilanzen (auch zu deren Verständnis erforderliche Organisationsunterlagen oder Arbeitsanweisungen), Buchungsbelege, Rechnungen.
Sechs Jahre müssen aufbewahrt werden: Handelsbriefe und Geschäftsbriefe (empfangene im Original, versendete in Wiedergaben). Sonstige steuerlich relevante Unterlagen.

6. Folgen von Verstößen

Im Fall eines Missbrauchs ist das Unternehmen berechtigt, sämtliche arbeitsrechtlichen Maßnahmen anzuwenden, einschließlich einer fristlosen oder fristgerechten Kündigung. Ebenfalls kommen strafrechtliche Sanktionen und zivilrechtliche Folgen wie Schadensersatz in Betracht.

7. Normenhierarchie

Soweit Regelungen dieser Vereinbarung im Widerspruch zu anderen Vereinbarungen oder Weisungen stehen, geht diese Vereinbarung vor.

8. Schlussbestimmungen

(1) Änderungen dieser Vereinbarung durch individuelle Vertragsabreden sind formlos wirksam. Im Übrigen bedürfen Vertragsänderungen der Schriftform; dies gilt auch für die Änderung dieser Schriftformabrede. Dies bedeutet, dass keine Ansprüche aus betrieblicher Übung entstehen.

(2) Sollte eine Bestimmung dieser Vereinbarung unwirksam oder undurchführbar sein oder werden, wird dadurch die Wirksamkeit des Vertrags im Übrigen nicht berührt. Die Parteien verpflichten sich, in diesem Fall über eine wirksame und durchführbare Regelung zu verhandeln, die dem von den Parteien mit der unwirksamen beziehungsweise undurchführbaren Bestimmung verfolgten Zweck möglichst nahekommt, soweit die Bestimmungen dieser Vereinbarung ohne die unwirksame beziehungsweise undurchführbare Regelung eine unzumutbare Härte für eine der Parteien darstellen würden.

Schirm GmbH