

Datenschutz- und IT-Nutzungsrichtlinie

Verantwortliche Stelle

Schirm GmbH
Geschwister-Scholl-Straße 127
39218 Schönebeck (Elbe)
Germany
Phone: +49-3928-456-199
Fax: +49-3928-456-300
E-mail: schirm@schirm.com

Geschäftsführung

Thomas Schulz

Datenschutzbeauftragter

FKC CONSULT GmbH
Eschenburgstr. 5
23568 Lübeck
Phone: +49 451 400510
E-mail: Datenschutz@schirm.com

IT / System Administration

Sascha Kirchhoff
Schirm GmbH
Geschwister-Scholl-Straße 127
39218 Schönebeck (Elbe)
Phone: +49 3928 456325
Mobile: +49 172 7088032

Präambel

Für die Schirm GmbH hat der sichere und verantwortungsvolle Umgang mit personenbezogenen Daten sowie betrieblichen Informationen höchste Priorität. Der Schutz von Kunden-, Mitarbeiter-, Geschäfts- und Unternehmensdaten ist ein wesentlicher Bestandteil unserer Unternehmensverantwortung.

Alle Mitarbeitenden leisten durch ihr tägliches Handeln einen wichtigen Beitrag zur Informationssicherheit und zum Datenschutz. Diese Richtlinie definiert verbindliche Vorgaben für die Nutzung der betrieblichen IT-Systeme sowie für den sicheren Umgang mit personenbezogenen und vertraulichen Daten.

Die Einhaltung dieser Regelungen ist Bestandteil der arbeitsvertraglichen Pflichten aller Mitarbeitenden.

1. Allgemeine Grundsätze

Die von der Schirm GmbH bereitgestellten IT-Systeme und Kommunikationsmittel dienen ausschließlich betrieblichen Zwecken.

Hierzu zählen insbesondere:

- PCs und Laptops
- Mobiltelefone und Smartphones
- Tablets und mobile Endgeräte
- Netzwerke und Server
- Internetzugänge
- E-Mail-Systeme
- Software und Cloud-Dienste
- Druck- und Kommunikationssysteme

Alle Geräte und Systeme werden durch die IT-Abteilung vorkonfiguriert bereitgestellt. Eigenmächtige Änderungen an Hard- oder Software, Systemeinstellungen oder Sicherheitskonfigurationen sind nicht zulässig.

Die IT-Abteilung ist grundsätzlich werktags erreichbar. Außerhalb der regulären Servicezeiten können Wartungsarbeiten, Sicherheitsupdates oder Systemneustarts durchgeführt werden.

Mitarbeitende sind verpflichtet, mit der IT-Abteilung sowie mit dem Datenschutzbeauftragten vollständig, wahrheitsgemäß und kooperativ zusammenzuarbeiten.

Diese Richtlinie gilt sowohl innerhalb der Betriebsräume als auch bei mobiler Arbeit oder Homeoffice-Tätigkeiten.

2. Nutzung der betrieblichen IT

2.1 Private Nutzung

Die private Nutzung der betrieblichen IT-Infrastruktur ist grundsätzlich untersagt.

Dies betrifft insbesondere:

- das Speichern oder Bearbeiten privater Dateien
- die Nutzung privater Datenträger
- private Internetnutzung
- die Nutzung privater E-Mail-Accounts
- private Messenger- oder Chatdienste
- die Installation privater Programme oder Apps
- die Nutzung privater Cloud-Dienste
- private Downloads oder Streaming-Dienste

Untersagt ist ebenfalls:

- das Herunterladen oder Verbreiten urheberrechtlich geschützter Inhalte
- der Abruf oder die Verbreitung diskriminierender, extremistischer, rassistischer, pornografischer oder gewaltverherrlichender Inhalte
- jegliche Form von Hacking, Portscans oder sicherheitsgefährdenden Aktivitäten
- die Umgehung von Sicherheitsmaßnahmen
- die Nutzung privater Geräte innerhalb des Firmennetzwerks
- das Laden privater Geräte an betrieblichen IT-Systemen

Die Schirm GmbH behält sich stichprobenartige Kontrollen sowie weitergehende Prüfungen bei Verdacht auf missbräuchliche Nutzung vor.

Foto- und Videoaufnahmen innerhalb der Betriebsräume bedürfen grundsätzlich der vorherigen Genehmigung.

2.2 Umgang mit IT-Systemen

Die bereitgestellten Arbeitsmittel sind pfleglich und verantwortungsvoll zu behandeln.

Mitarbeitende sind verpflichtet:

- Geräte vor Beschädigungen zu schützen
- Arbeitsmittel sauber zu halten
- Störungen oder Defekte unverzüglich der IT-Abteilung zu melden
- keine eigenständigen Reparaturversuche vorzunehmen

Wartungs- und Reparaturarbeiten dürfen ausschließlich durch autorisierte Personen durchgeführt werden.

2.3 Betriebliche Kommunikation und E-Mail

Die betriebliche E-Mail-Adresse darf ausschließlich für dienstliche Zwecke genutzt werden.

Vor dem Versand von Informationen ist sicherzustellen, dass:

- Empfänger zur Kenntnisnahme berechtigt sind
- personenbezogene Daten datenschutzkonform verarbeitet werden
- Verteilerlisten korrekt verwendet werden
- die Felder „CC“ und „BCC“ sachgerecht eingesetzt werden

Die Weiterleitung oder Speicherung betrieblicher Daten auf privaten Geräten, privaten E-Mail-Postfächern oder privaten Cloud-Diensten ist untersagt.

Alle geschäftlichen E-Mails können entsprechend gesetzlicher Aufbewahrungsfristen archiviert und gesichert werden.

Private Nachrichten über betriebliche Kommunikationssysteme sollen vermieden werden.

2.4 Mobile Geräte

Für mobile Endgeräte gelten besondere Sicherheitsanforderungen.

Mitarbeitende haben insbesondere darauf zu achten, dass:

- Geräte durch sichere Passwörter geschützt sind
- mobile Geräte niemals unbeaufsichtigt zurückgelassen werden
- öffentliche Netzwerke ausschließlich mit aktiver VPN-Verbindung genutzt werden
- Datenträger verschlüsselt werden
- Verlust oder Beschädigung unverzüglich gemeldet werden

Eine dauerhafte lokale Speicherung betrieblicher Daten auf mobilen Geräten ist zu vermeiden.

2.5 Drucker und Ausdrücke

Vertrauliche Ausdrücke sind unmittelbar nach dem Druck abzuholen.

Fehldrucke oder nicht mehr benötigte Unterlagen sind datenschutzgerecht zu vernichten.

Papierausdrücke sollen auf das notwendige Maß beschränkt werden.

2.6 Speicherung von Dateien

Personenbezogene oder betriebliche Daten sind ausschließlich auf den dafür vorgesehenen Netzwerklaufwerken oder freigegebenen Speichersystemen abzulegen.

Lokale Datenspeicherung ist nur in begründeten Ausnahmefällen zulässig.

2.7 Telefon und Fax

Personenbezogene Daten dürfen telefonisch nur an eindeutig identifizierte Personen weitergegeben werden.

Bei Zweifeln an der Identität ist auf eine schriftliche Anfrage zu verweisen.

Die private Nutzung von Telefon und Telefax ist grundsätzlich untersagt.

2.8 E-Mail-Anhänge und Links

Anhänge oder Links aus unbekanntem oder verdächtigen E-Mails dürfen nicht geöffnet werden.

Verdächtige Nachrichten sind unverzüglich der IT-Abteilung zu melden.

2.9 Spam und Phishing

Zum Schutz vor Schadsoftware und unerwünschten Nachrichten werden Spam- und Sicherheitsfilter eingesetzt.

Besondere Vorsicht ist bei:

- unbekanntem Absendern
- ungewöhnlichen Zahlungsaufforderungen
- verdächtigen Links
- Dateianhängen
- unerwarteten Anfragen

geboten.

2.10 Passwörter und Zugriffsschutz

Passwörter dienen dem Schutz personenbezogener und vertraulicher Daten.

Folgende Mindestanforderungen gelten:

- mindestens 8 Zeichen
- Kombination aus Groß- und Kleinbuchstaben
- mindestens eine Zahl
- mindestens ein Sonderzeichen

Passwörter dürfen:

- nicht weitergegeben
- nicht notiert
- nicht mehrfach verwendet

werden.

Für unterschiedliche Systeme sind unterschiedliche Passwörter zu verwenden.

Die Nutzung von Passwort-Managern kann durch die IT-Abteilung bereitgestellt werden.

Administrationsrechte dürfen ausschließlich von autorisierten Personen genutzt werden.

3. Organisation und Informationssicherheit

3.1 Clean-Desk-Policy

Arbeitsplätze sind so zu organisieren, dass keine vertraulichen Unterlagen offen zugänglich sind.

Beim Verlassen des Arbeitsplatzes sind:

- Bildschirme zu sperren
 - Unterlagen wegzuräumen
 - sensible Informationen vor Einsicht Dritter zu schützen
-

3.2 Verlassen des Arbeitsplatzes

Nach Arbeitsende sind:

- Computer herunterzufahren
 - Fenster und Türen zu schließen
 - Unterlagen sicher zu verwahren
-

3.3 Virenschutz und Datenträger

Die Schirm GmbH stellt mehrstufige Sicherheits- und Virenschutzsysteme bereit.

Nicht freigegebene externe Datenträger dürfen nicht angeschlossen werden.

Bei Verdacht auf Schadsoftware sind:

- Arbeiten sofort einzustellen,
 - Netzwerkverbindungen zu trennen,
 - die IT-Abteilung oder Vorgesetzte unverzüglich zu informieren.
-

3.4 Besucherregelung

Besucher dürfen sich ausschließlich in freigegebenen Bereichen aufhalten

Der Zutritt zu Büroräumen erfolgt nur in Begleitung eines Mitarbeitenden

Ein Zugriff auf interne IT-Systeme ist Besuchern nicht gestattet

3.5 Homeoffice und mobiles Arbeiten

Auch im Homeoffice gelten sämtliche Datenschutz- und Sicherheitsanforderungen.

Insbesondere ist sicherzustellen, dass:

- Dritte keinen Zugriff auf betriebliche Daten erhalten
 - betriebliche Unterlagen sicher aufbewahrt werden
 - ausschließlich freigegebene Systeme genutzt werden
 - Verbindungen zum Firmennetzwerk ausschließlich per VPN erfolgen
-

3.6 Sicherheitsmaßnahmen

Das Umgehen oder Deaktivieren von Sicherheitsmaßnahmen ist untersagt.

Dies umfasst insbesondere:

- das Deaktivieren von Virenschutzprogrammen
 - das Umgehen von Firewalls
 - die Nutzung nicht freigegebener Software
 - das Einbringen privater Speichermedien
-

3.7 Fernwartung

Die IT-Abteilung kann im Rahmen von Support- oder Wartungsarbeiten auf Systeme zugreifen.

Ein Zugriff erfolgt grundsätzlich in Abstimmung mit den betroffenen Mitarbeitenden.

3.8 Umgang mit Papierakten

Papierdokumente sind ordnungsgemäß aufzubewahren.

Besonders schutzbedürftige Unterlagen, insbesondere Personalakten, sind verschlossen zu lagern.

Nicht mehr benötigte Unterlagen sind datenschutzgerecht zu vernichten.

3.9 Verstöße gegen Sicherheitsvorgaben

Verstöße gegen diese Richtlinie können arbeitsrechtliche Konsequenzen nach sich ziehen.

Bei vorsätzlichen oder grob fahrlässigen Verstößen behält sich die Schirm GmbH disziplinarische Maßnahmen vor.

3.10 Zutritt zu Serverräumen

Serverräume dürfen ausschließlich von autorisierten Personen betreten werden.

Serverräume und Serverschränke sind verschlossen zu halten.

3.11 Schutz vor Social Engineering

Personenbezogene Daten dürfen ausschließlich an eindeutig identifizierte Personen weitergegeben werden.

Bei ungewöhnlichen Anweisungen oder Verdachtsfällen ist stets eine zusätzliche Verifizierung vorzunehmen.

Mitarbeitende sind verpflichtet, sensible Informationen vertraulich zu behandeln.

3.12 Datenpannen

Jede vermutete oder tatsächliche Datenschutzverletzung ist unverzüglich der Geschäftsleitung oder dem Datenschutzbeauftragten zu melden.

Eigenmächtige Maßnahmen dürfen nicht vorgenommen werden.

3.13 Betroffenenrechte

Werden Betroffenenrechte geltend gemacht, ist unverzüglich der Datenschutzbeauftragte zu informieren.

Hierzu zählen insbesondere:

- Auskunftsrechte
 - Berichtigungsrechte
 - Lösungsansprüche
 - Einschränkungen der Verarbeitung
 - Widersprüche gegen Verarbeitungen
 - Datenübertragbarkeit
 - Beschwerden bei Aufsichtsbehörden
-

4. Störungen, Ausfälle und Sicherheitsvorfälle

Sicherheitsvorfälle, IT-Störungen oder Systemausfälle sind unverzüglich den zuständigen Ansprechpartnern zu melden.

Ein Sicherheitsvorfall liegt insbesondere vor, wenn:

- personenbezogene Daten gefährdet sind
 - unbefugte Zugriffe festgestellt werden
 - Systeme manipuliert oder kompromittiert wurden
-

5. Datenspeicherung, Backup und Wiederherstellung

5.1 Grundsätze der Datenspeicherung

Betriebliche Daten sind grundsätzlich auf zentralen Servern oder freigegebenen Speichersystemen abzulegen.

Die Speicherung auf lokalen Endgeräten soll vermieden werden.

5.2 Datensicherung

Die Schirm GmbH führt regelmäßige Datensicherungen durch.

Backup-Strategien und Wiederherstellungsverfahren werden dokumentiert und regelmäßig geprüft.

5.3 Regelungen für Administratoren

Administratoren sind verpflichtet:

- Speicherorte zu dokumentieren
 - Berechtigungskonzepte zu pflegen
 - Backup- und Recovery-Konzepte zu erstellen
 - regelmäßige Wiederherstellungstests durchzuführen
-

6. Löschkonzept

6.1 Allgemeine Grundsätze

Personenbezogene Daten sind zu löschen, sobald:

- der Zweck der Verarbeitung entfällt
- gesetzliche Aufbewahrungsfristen ablaufen
- keine rechtliche Grundlage mehr besteht

Die Löschung muss so erfolgen, dass eine Wiederherstellung ausgeschlossen ist.

6.2 Aufbewahrungs- und Löschfristen

Gesetzliche Aufbewahrungsfristen bleiben unberührt.

Insbesondere gelten:

- 10 Jahre Aufbewahrung für Buchungs- und Rechnungsunterlagen
 - 6 Jahre Aufbewahrung für Handels- und Geschäftsbriefe
-

7. Folgen von Verstößen

Verstöße gegen diese Richtlinie können arbeitsrechtliche, zivilrechtliche sowie strafrechtliche Konsequenzen nach sich ziehen.

Mögliche Maßnahmen umfassen insbesondere:

- Abmahnungen
- Schadensersatzforderungen
- ordentliche Kündigungen
- fristlose Kündigungen
- strafrechtliche Anzeigen

8. Rangfolge und Schlussbestimmungen

Diese Richtlinie hat Vorrang vor entgegenstehenden internen Regelungen, soweit keine zwingenden gesetzlichen Vorschriften entgegenstehen.

Änderungen oder Ergänzungen bedürfen grundsätzlich der Schriftform.

Sollten einzelne Bestimmungen dieser Richtlinie unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Regelungen unberührt.

Schirm GmbH