Datenschutz in der SHK-Gruppe

Selbsthilfe Körperbehinderter Main-Kinzig e.V.
SHK Service “gem.“ GmbH
SHK BeWo gUG (haftungsbeschränkt)

(2024)

Grundschulung Datenschutz

Fahrplan Datenschutzunterweisung Grundschulung - 2024

Station 1 (Grundlagen)

- 1.1 | Warum und was ist Datenschutz ? - ,,Die drei Akteure“
- 1.2 | Rechtsgrundlagen

Station 2 (Umsetzung in der SHK)

- 2.1 | Übersicht personenbezogene Daten in der SHK
- 2.2 | Tätigkeit und Funktionen des Datenschutzbeauftragten
- 2.3 | Beispiele, Verhalten und Maßnahmen bei Datenpannen
- 2.4 | Beispiele, Verhalten und Maßnahmen bei Betroffenenersuchen
- 2.5 | Verpflichtung zur Vertraulichkeit, interne Regeln zur Nutzung der IT, physischen Unterlagen und dem Umgang mit Daten
- 2.6 | Technische und organisatorische Maßnahmen ,,TOM´s“

Station 3 (Fragerunde zum Datenschutz)

Dokumentenname:	Stand:	Anzahl Seiten gesamt: 26
10.01.01 | Unterweisung Datenschutz 2024_GS	16.09.2024	
Klassifizierung: 02 - INTERN	Ver.: 01.00	

Patrick Bäcker

(Inhaber wavesun-technologies)

E-Mail: info@wavesun-technologies.de

Telefon: 06074 / 3709395

- **IT-Systemkaufmann (IHK)**
- **IT-Forensiker (DESAG geprüft & anerkannt)**
- **Datenschutzbeauftragter & Datenschutzauditor (TÜV)**
- **Sachverständiger für Datenschutz und Datensicherheit (DESAG geprüft & anerkannt)**
- **Information Security Auditor/Lead Auditor ISO/IEC 27001 (TÜV)**
- **Information Security Officer ISO/IEC 27001 (TÜV)**
- **KRITIS-Prüfer für § 8a BSIG (TÜV)**
- **Sicherheitsbeauftragter**

Meine Kerntätigkeit

Branchenübergreifende Beratung und Betreuung in den Bereichen Informationssicherheit & Datenschutz als

Externer ISMS-Berater

Externer Datenschutzbeauftragter

Mein Antrieb

Leidenschaft und Wissensdrang

Mein Ziel

Auf den Kunden zugeschnittene, praktikable und zugleich konforme Lösung planen, einführen, überprüfen & aufrechterhalten

Was dürfen Sie erwarten und was bitte nicht?

Grundsätze des Datenschutzes in der SHK zu erlernen

Interne Leitlinien und Aushänge zum Datenschutz verstehen

Praktische Tipps zur Umsetzung von technischen und organisatorischen Maßnahmen

X Alles über Datenschutz zu lernen

X Mit den Informationen immer rechtlich abgesichert zu sein

X Das alle Tipps für eine sicheren Umgang mit personenbezogenen Daten ausreichen

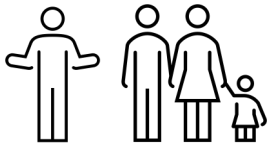
1.1 | Warum Datenschutz? - Ziele -

Diese Ziele sollen durch die DS-GVO erreicht werden

- Schutz der Grundrechte und Grundfreiheiten
  natürlicher <u>Personen</u> und deren Recht auf Schutz personenbezogener Daten

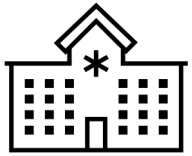
- Regelung der Pflichten der **<u>Verantwortlichen</u>** (= Organisationen)
  hinsichtlich des gesetzeskonformen Umgangs
  mit personenbezogenen Daten

1.1 | Was ist Datenschutz? - Die drei Akteure -



Verbraucher

Eine Person, die ihre personenbezogenen Daten weitergibt



Organisationen

Jede Organisation (Unternehmen / Verein), die personenbezogene Daten verarbeitet

---

Gesetzgeber

Regelt die Rechte der Verbraucher und schreibt den Organisationen (Unternehmen / Verein) Pflichten vor

1.1 | Was ist Datenschutz? - Was ist personenbezogen -

Art. 4 Abs. 1 DS-GVO: „personenbezogene Daten“ **alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen**; als identifizierbar wird eine natürliche Person angesehen, die 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 der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

Allgemeine Personendaten
(Name, Geburtsdatum, Geburtsort, Alter, E-Mail-Adresse, Telefonnummer etc.)

Kennnummern
(Sozialversicherungs-, Kunden-, Personalaus-, Steueridentifikations-, Kontonummer etc.)

Standortdaten und IP-Adressen

Besonders schützenswerte Daten
(Geschlecht, Religions-/ Gewerkschaftszugehörigkeit, Gesundheitsdaten, Sexualleben, biometrische Daten etc.)

Daten von Geschäfts-/Vertragspartnern und Kunden/Klienten
(Namen, Anschriften, E-Mail-Adressen)

Mitarbeiterdaten
(Alle Daten zur Begründung, Durchführung und Beendigung eines Beschäftigtenverhältnisses)

1.1 | Was ist Datenschutz? - Definition Verarbeitung -

- Was versteht man unter Verarbeitung?

Jede „***mit*** oder ***ohne*** Hilfe automatisierter Verfahren“ ausgeführten Vorgänge im Zusammenhang mit personenbezogenen Daten, die in einem ,,Dateisystem“ geführt werden.

- Das bedeutet: Sobald personenbezogene Daten auf **Papier oder digital** niedergeschrieben und verwendet werden, spricht man von Verarbeitung.

- ***Beispiele:*** Exceldatei, Adressbuch, Gesprächsnotizen/Protokolle, Lohnabrechnung, **Beratung und Dokumentation von Assistenzdienstleistungen**, **Dokumentation von Fahrdiensten, Wohnungsverwaltung**, Bewerberverfahren, Besucherliste, Kunden/Klienten Datenbank.

1.2 | Was ist Datenschutz? - Rechtsgrundlagen -

Personenbezogene Daten dürfen nur verarbeitet werden,
wenn

---

1) <u>Eine Rechtsgrundlage vorliegt, d.h. maßgeblich</u>

- **Vertragsgrundlage (z.B. Erstellung eines Angebots, Durchführung eines Arbeitsvertrags, Kunden / Klienten Auftrags, Rechnungsstellung)**
- **Rechtliche Verpflichtung (z.B. Aufbewahrungspflichten) oder**
- **Ein berechtigtes Interesse die Verarbeitung erlaubt.**

---

2) <u>Eine Einwilligung gegeben wird, d.h.</u>

z.B. wenn Fotos von Personen gemacht werden. Die Notwendigkeit einer Einwilligung ist i.d.R. aus den Dokumenten und internen Prozessen der SHK ersichtlich.
Bei Zweifeln den disziplinarischen Vorgesetzten oder Datenschutzbeauftragten fragen!

2.1 | Übersicht personenbezogene Daten in der SHK

Welche?

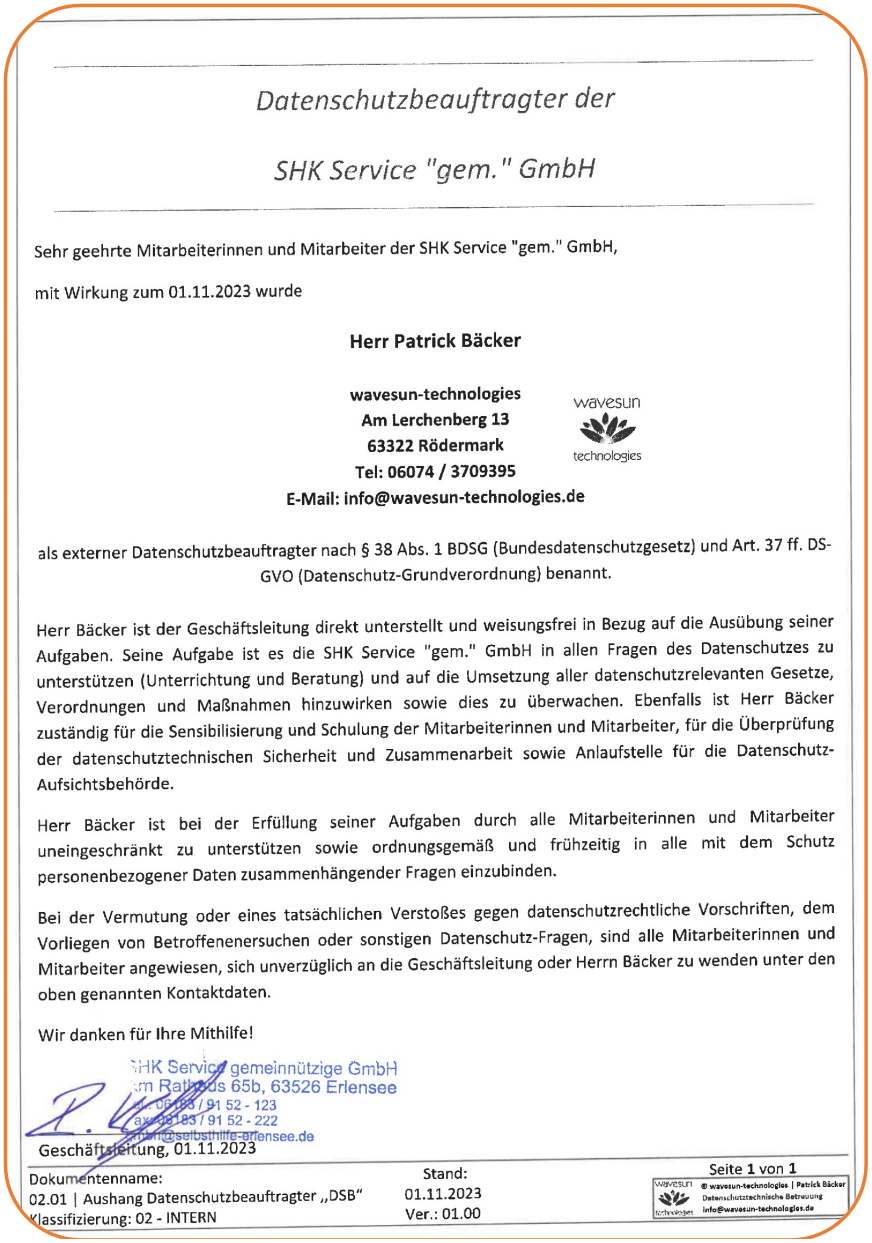
- Mitarbeiter- und Bewerberdaten (Personaldaten):
  - Name und Vorname
  - Adresse
  - Geburtsdatum
  - Lebenslauf, Zeugnisse etc.
- Kunden / Klienten / Dienstleister / Lieferanten Daten
  - Name, Vorname
  - Anschrift
  - Rechnungsdaten
  - E-Mail / Telefon
- **Behandlungsdaten**
- Systemdaten
- Kommunikationsdaten

Wo?

- Geschäftsleitung / Vorstand
- Verwaltung (Finanz- und Lohnbuchhaltung)
- EUTB
- Fahrdienst
- Schulassistenz
- Ambulanter Assistenzdienst & Ambulante Teilhabeassistenz (qualifizierte Assistenz / kompensatorische Assistenz beim Wohnen)
- IT und Telekommunikation
- Telefonzentrale Empfang
- BeWo

Wie?

- Vereinsverwaltung
- Bewerber- und Beschäftigtenverwaltung
- Wohnungsverwaltung
- Durchführung von Assistenzdiensten (Hilfen für Menschen mit Behinderungen) sowie zugehörige Dokumentation und Kommunikation mit Klienten und deren Angehörigen sowie ggf. Behörden
- Vertragsabwicklung und Rechnungsstellung



Datenschutzbeauftragter der

SHK Service "gem." GmbH

Sehr geehrte Mitarbeiterinnen und Mitarbeiter der SHK Service "gem." GmbH,

mit Wirkung zum 01.11.2023 wurde

Herr Patrick Bäcker

wavesun-technologies
Am Lerchenberg 13
63322 Rödermark
Tel: 06074 / 3709395
E-Mail: info@wavesun-technologies.de

als externer Datenschutzbeauftragter nach § 38 Abs. 1 BDSG (Bundesdatenschutzgesetz) und Art. 37 ff. DS-GVO (Datenschutz-Grundverordnung) benannt.

Herr Bäcker ist der Geschäftsleitung direkt unterstellt und weisungsfrei in Bezug auf die Ausübung seiner Aufgaben. Seine Aufgabe ist es die SHK Service "gem." GmbH in allen Fragen des Datenschutzes zu unterstützen (Unterrichtung und Beratung) und auf die Umsetzung aller datenschutzrelevanten Gesetze, Verordnungen und Maßnahmen hinzuwirken sowie dies zu überwachen. Ebenfalls ist Herr Bäcker zuständig für die Sensibilisierung und Schulung der Mitarbeiterinnen und Mitarbeiter, für die Überprüfung der datenschutztechnischen Sicherheit und Zusammenarbeit sowie Anlaufstelle für die Datenschutz-Aufsichtsbehörde.

Herr Bäcker ist bei der Erfüllung seiner Aufgaben durch alle Mitarbeiterinnen und Mitarbeiter uneingeschränkt zu unterstützen sowie ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängender Fragen einzubinden.

Bei der Vermutung oder eines tatsächlichen Verstoßes gegen datenschutzrechtliche Vorschriften, dem Vorliegen von Betroffenenersuchen oder sonstigen Datenschutz-Fragen, sind alle Mitarbeiterinnen und Mitarbeiter angewiesen, sich unverzüglich an die Geschäftsleitung oder Herrn Bäcker zu wenden unter den oben genannten Kontaktdaten.

Wir danken für Ihre Mithilfe!

SHK Service gemeinnützige GmbH
im Rathaus 65b, 63526 Erlensee
Tel.: 06183 / 91 52 - 123
Fax: 06183 / 91 52 - 222
[illegible]@selbsthilfe-erlensee.de

Geschäftsleitung, 01.11.2023

Dokumentenname: 02.01 | Aushang Datenschutzbeauftragter „DSB"
Klassifizierung: 02 - INTERN
Stand: 01.11.2023
Ver.: 01.00
Seite 1 von 1

2.2 | Einbindung des Datenschutzbeauftragten

- **Aufgaben** des Datenschutzbeauftragten („DSB") **siehe Aushang DSB (der Aushang ist für den Verein und BeWo gleich)**
- Der **DSB** ist **bei Betroffenenersuchen sowie** (möglichen) **Datenpannen unverzüglich** zu **informieren**, siehe Notfallkarten
- Bei der **Neuanschaffung von Datenverarbeitungsanlagen** (Hard- und Software sowie Systemen), **welche personenbezogene Daten verarbeiten können**, ist der **DSB vor der Einführung zu informieren**, um die datenschutzrechtliche und datenschutztechnische Vorabkontrolle durchzuführen, die neue Verarbeitungstätigkeit zu dokumentieren und ggf. ergänzende Maßnahmen auszusprechen
- Die **Prüfung und Dokumentation** („Rechenschaftspflicht" nach Art. 5 Abs. 2 DS-GVO) ist **für den Verantwortlichen** (Geschäftsleitung / Vorstand) **Pflicht**, der **DSB unterstützt** Ihn hierbei. **Bei der Nichteinhaltung** können seitens der Aufsichtsbehörde die bekannten **Bußgelder** und seitens betroffener Personen **Schadensersatzforderungen** drohen

2.3 | Datenpannen – Berichte und Maßnahmenempfehlungen

Ransomware-Angriff auf hessischen IT-Dienstleister mit weitreichenden Folgen

Eine Cyber-Attacke auf eine IT-Firma lähmt seit Tagen einige Unternehmen im Rhein-Main-Gebiet. Experten arbeiten an einer Lösung, doch das kann dauern.

Quelle: heise.de, 15.06.2022, 02:31 Uhr

Verdächtige E-Mails der IT zur Überprüfung auf Viren melden - E-Mails NICHT weiterleiten und Anhänge NICHT öffnen!

Insb. Updates von Betriebssystemen / Anwendungen / Diensten zeitnah installieren!

123456 – Deutschlands häufigste Passwörter im Jahr 2021

Die deutschen Passwort-Charts des Hasso-Plattner-Instituts für das Jahr 2021 sind erschreckend. Alte Bekannte lassen grüßen.

Quelle: heise.de, 16.12.2021, 18:12 Uhr

Passwörter nach betrieblichen Vorgaben vergeben! Sofern möglich Zwei-Faktor-Authentifizierung aktivieren.

33.000 hochsensible Mails aus dem Ausländeramt Lübeck bei eBay verkauft

eBay ist eine Fundgrube für ausgemusterte Firmen- und Behörden-PCs. Mitunter findet man aber brisante Daten, die keinesfalls an die Öffentlichkeit gehören.

Quelle: heise.de, 28.01.2022, 06:00 Uhr

Zur Vernichtung bestimmte Unterlagen schreddern / in Datencontainer werfen sowie nicht mehr benötigte Datenträger der IT übergeben!

2.3 | Datenpannen - Weitere Berichte

Fahrradhersteller: Prophete nach Cyber-Angriff in Insolvenz gerutscht

Der Insolvenzverwalter beim Fahrradhersteller Prophete hat als Ursache für die Insolvenz einen Cyber-Angriff ausgemacht, der einen Betriebsstillstand auslöste.

Quelle: heise.de, 11.01.2023, 12:54 Uhr

Nach Cyberangriff: Frankfurter Hochschule trifft Sicherheitsmaßnahmen

Die Frankfurter University of Applied Sciences ist am Samstag Opfer eines Cyberangriffs geworden. IT-Systeme wurden heruntergefahren, auch der Fahrstuhl.

Quelle: heise.de, 08.07.2024, 14:27 Uhr

Cyberangriff beim Darmstädter Energieversorger Entega

Bei Entega sind E-Mailkonten und die Webseiten einem Angriff zum Opfer gefallen. Die kritische Infrastruktur sei besonders geschützt und nicht betroffen.

Quelle: heise.de, 12.06.2022, 17:44 Uhr

Cyberangriff: IHK-Verbände weitgehend offline, auch telefonisch nicht erreichbar

Nach einem Cyberangriff auf die Industrie- und Handelskammern sind die weitgehend offline. An der Behebung werde gearbeitet, heißt es in sozialen Netzen.

Quelle: heise.de, 04.08.2022, 10:06 Uhr

Flugzeuge am Boden, Kliniken operieren nicht

Stand: 19.07.2024 15:29 Uhr

Ein fehlerhaftes Update legt weltweit Flughäfen, Krankenhäuser oder Medienunternehmen still. Experten sprechen vom größten IT-Ausfall aller Zeiten. Was darüber bekannt ist - und welche Folgen die Störung hat.

Quelle: tagesschau.de, 19.07.2024, 15:29 Uhr

Gesundheit Nord bestätigt Cyber-Angriff und Datenabfluss

Die Bremer Kliniken im "Gesundheit Nord"-Verband sind Opfer eines Cyber-Angriffs geworden, bestätigt der Verband jetzt. Es sind Daten abgeflossen.

Quelle: heise.de, 31.05.2023, 14:31 Uhr

2.3 | Erläuterung Cyber-Sicherheit & Cyber-Angriff

Cyber-Sicherheit

„**befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik.**

Das **Aktionsfeld der Informationssicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet**. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Häufig wird bei der Betrachtung von Cyber-Sicherheit auch ein spezieller Fokus auf Angriffe aus dem Cyber-Raum gelegt."

→ Ausweitung der Informations- und Datensicherheit auf IT-Systeme, welche mit dem Internet verbunden sind.

Ein Cyber-Angriff

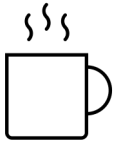
„ist eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyber-Raum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen."

→ Angriff auf IT-Systeme, welche mit dem Internet verbunden sind.

Quellen: bsi.bund.de

2.3 | Wieso Cyber-Sicherheit? Ein Beispiel

Es ist 8 Uhr morgens. Sie kommen nach einem verlängerten Wochenende ins Büro.



Sie trinken Ihren ersten Kaffee, gehen an Ihren Arbeitsplatz und schalten den PC an.

Ihr PC sagt Ihnen ,,Ihre Daten wurden verschlü$$elt. Zahlen Sie 20 Bitcoins oder ALLE Ihre Daten werden vom Computer gelöscht und ins Internetzzz gestellt!?!“

Sie überlegen – Was mache ich jetzt?
Aha, erstmal schauen, was so ein Bitcoin kostet, wird schon nicht so viel sein.
Ohhhh, Cheeeeef, wir haben ein Problemchen.

,,Rufen Sie unseren externen IT-Dienstleister an, der regelt das“

,,Die Telefonanlage funktioniert nicht, Kunden können uns nicht erreichen!“
,,Dann versuchen Sie es über´s Handy!“

,,Die XY Computerdienstleistungs GmbH kann wegen des Cyber-Angriffs leider nicht auf Ihre Systeme zugreifen und die Anfahrt zu Ihnen dauert eine Stunde, bewahren Sie Ruhe!“

Unsere IT-Systeme funktionieren nicht, Kunden können nicht bedient werden, Hilfe fehlt, Daten sind eventuell nicht mehr da, verändert oder sogar an Dritte gelangt und irgendwas war doch mit einer Meldung an die Behörden bei sowas. Hätten wir doch lieber vorgesorgt…

2.3 | Auswirkungen von Cyber-Angriffen

Cyberangriffe größte Gefahr für Firmen

Stand: 18.01.2022 08:50 Uhr

Gefährlicher als die Pandemie oder Naturkatastrophen: Fach- und Führungskräfte, die vom Versicherungskonzern Allianz befragt wurden, sehen Hackerangriffe und deren Folgen als Risiko Nummer eins für ihr Unternehmen.

Die größte Gefahr für die Unternehmen weltweit sehen Experten in der IT ihrer Firmen. Erpressung oder Schäden wie ein Produktionsstopp durch Cyberangriffe rangieren noch vor den befürchteten Schäden durch die Pandemie, Naturkatastrophen oder den Klimawandel.

Quelle: tagesschau.de

Bei Cyber-Angriffen wird meist die

- **Vertraulichkeit,**
- **Integrität,**
- **Verfügbarkeit**

von Daten verletzt.

Weitere mögliche Folgen / Schäden:

- Betriebsbeeinträchtigungs- und Unterbrechungskosten
- Kosten für Schadensermittlung und Wiederherstellung der Daten (insb. IT-Forensik)
- Verstoß gegen gesetzliche, branchenspezifische oder vertragliche Vorgaben -> Vertragsstrafen und Bußgelder
- Insb. Datenschutzverstöße können bei unzureichend getroffenen technischen und organisatorischen Maßnahmen (i.S.d. Art. 32 DS-GVO) Bußgelder (i.S.d. Art. 83 DS-GVO) und Schadensersatzforderungen (i.S.d. Art. 82 DS-GVO) mit sich ziehen
- Kosten für (Rechts-) Berater
- Imageschäden und Reputationskosten
- Zeit- und Kostenaufwände für Präventionsmaßnahmen

[DATENSCHUTZ]

Verhalten bei möglicher Datenpanne

Ruhe bewahren & Datenpanne melden

Lieber einmal mehr als einmal zu wenig anrufen!

Anzeichen für eine mögliche Datenpanne

Melden Sie eine Datenpanne, wenn Sie z.B. folgendes feststellen:

- Ihr PC, Laptop, Tablet, Smartphone etc. meldet Schadsoftware
- Sie haben auf eine im Nachhinein verdächtige E-Mail reagiert und auf einen Link geklickt, um Daten einzugeben (insb. Zugangs- und Kontodaten)
- Sie haben personenbezogene Daten ,,pbD“ an eine falsche Adresse (bspw. E-Mail-Adresse oder postalische Adresse) geschickt
- Ihnen wurde anscheinend ein Datenträger mit dem Inhalt von pbD (darunter fallen auch ,,Papier-Dokumente“) oder ein (mobiles) Endgerät gestohlen
- Sie haben einen Datenträger oder ein (mobiles) Endgerät verloren
- Ein Datenträger wurde auf dem falschen Weg entsorgt (bspw. nicht geschreddert oder nicht in den Datencontainer geworfen)
- Ungewöhnliches Systemverhalten/Systemstörung/Systemausfall
- Vertrauliche Daten der SHK-Gruppe wurden im Internet gefunden
- Veröffentlichung von gestohlenen Informationen durch Dritte
- Hinweise von Dritten auf ungeschützte Daten der SHK-Gruppe
- Offensichtlich manipulierte Daten im System
- Offensichtlich fehlende Daten im System
- Versuch einer Erpressung über E-Mail oder eine andere Nachricht

Wenden Sie sich **unverzüglich** an die Geschäftsleitung, an die IT, wenn Systeme betroffen sind sowie immer an den externen Datenschutzbeauftragten der SHK-Gruppe (Verein, Service, BeWo):

wavesun-technologies
Patrick Bäcker

Telefon: 06074 / 3709395
E-Mail-Adresse: info@wavesun-technologies.de

Weitere Verhaltensweise

- **Wenn IT-Systeme betroffen sind die Netzwerk-Verbindungen trennen und weitere Arbeit einstellen**
- **Beobachtungen zeitlich und genau dokumentieren**
- **Maßnahmen nur nach Anweisung einleiten**

2.3 | Notfallkarte Datenpanne

- **Datenpanne = Jede Verletzung des Schutzes (personenbezogener) Daten.**
- **Bei** einer **Datenpanne oder** auch nur der **Vermutung** (Beispiele siehe Aushang) ist **unverzüglich** die **Geschäftsleitung / Vorstand** und die **IT (bei betroffenen Systemen)** zu **informieren**. **,,Weitere Verhaltensweise“ auf dem Aushang beachten!**
- **Bei** der **zusätzlichen Verletzung** des **Schutzes personenbezogener Daten oder** auch nur der **Vermutung** ist zusätzlich **unverzüglich** der **externe Datenschutzbeauftragte** ,,DSB“ (**Patrick Bäcker** – Kontaktdaten siehe Aushang) zu **informieren**.
- **Alle den Vorfall betroffenen Informationen müssen dokumentiert werden** (erfolgt durch DSB und Geschäftsleitung / Vorstand) zwecks **Rechenschaftspflicht** und möglicher Meldepflichten an die Aufsichtsbehörde (HBDI) und ggf. Betroffene. Bei einer notwendigen **Datenpannen-Meldung** muss das HBDI möglichst **innerhalb 72 Stunden** informiert werden, ansonsten können allg. **Bußgelder** (**bis zu 20 Millionen oder 4 % des weltweiten Vorjahresumsatzes**) und Schadensersatzforderungen von Betroffenen drohen.

[DATENSCHUTZ]

Verhalten bei Betroffenenersuchen

Beschwerden, Forderung nach Auskunft, Berichtigung, Einschränkung der Verarbeitung, Widerspruch, Löschung und Datenübertragbarkeit von personenbezogenen Daten

Unabhängig vom Kommunikationskanal (Telefon, Fax, E-Mail, Post oder persönliches Erscheinen) und unabhängig davon, über welchen Kontaktpunkt (Büro, Außendienst, Personalabteilung etc.) ein Ersuchen eintrifft, ist bereits bei Kontaktaufnahme darauf zu achten, dass der

a) Name der betroffenen Person,

b) die Art des Ersuchens und

c) eine valide Kontaktmöglichkeit für Rückfragen (Telefonnummer und/oder E-Mail-Adresse) aufgenommen werden.

Leiten Sie das Ersuchen **unverzüglich** an die Geschäftsleitung sowie immer an den externen Datenschutzbeauftragten der SHK-Gruppe (Verein, Service, BeWo) weiter:

wavesun-technologies
Patrick Bäcker

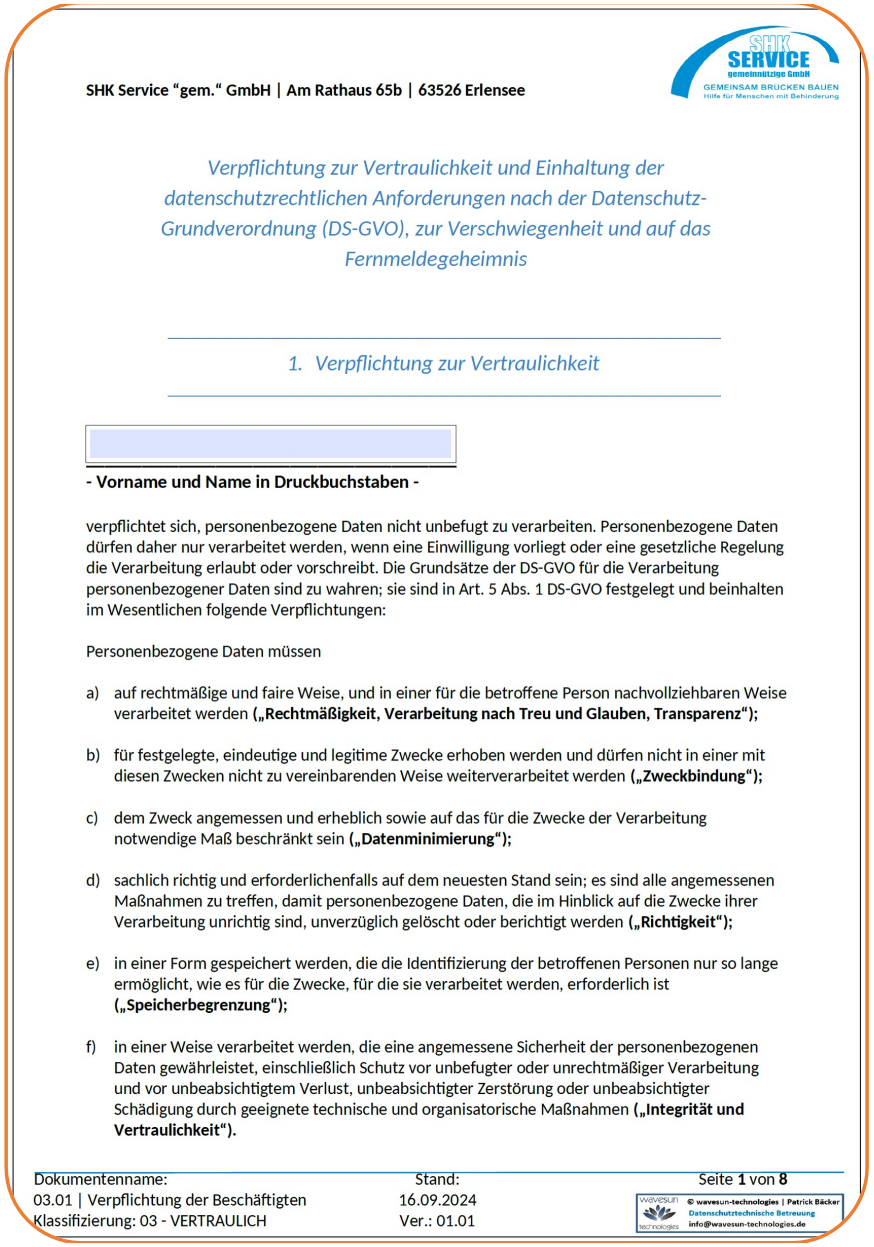
Telefon: 06074 / 3709395
E-Mail-Adresse: info@wavesun-technologies.de

2.2 | Notfallkarte Betroffenenersuchen

- **Betroffenenersuchen = Jede Anfrage eines Betroffenen** (Interessent, Kunde / Klient, Lieferant, Dienstleister, Mitarbeiter, Bewerber) **nach seinen personenbezogenen Daten, welche bei der SHK verarbeitet werden.**

- Betroffenenersuchen sind **unverzüglich** dem **externen Datenschutzbeauftragten** ,,DSB“ (**Patrick Bäcker** – Kontaktdaten siehe Aushang) **und** der **Geschäftsleitung / Vorstand** über die bekannten Kontaktwege zu **melden**, **mit** dem **im Aushang befindlichen Angaben**.

- **Alle über das Betroffenenersuchen bekannten Informationen müssen dokumentiert werden** (erfolgt durch DSB und Geschäftsleitung / Vorstand) **zwecks Rechenschaftspflicht sowie Mitteilungspflichten an die Betroffenen**. Ein Auskunftsersuchen muss bspw. spätestens innerhalb eines Monats beantwortet werden. Die Recherche nach den vorhandenen personenbezogenen Daten kann u.U. lange dauern, weshalb diese Frist praktisch gesehen sehr kurz ist und **bei** der **Nichtbearbeitung Bußgelder** und **Schadensersatzforderungen** drohen können.



SHK Service "gem." GmbH | Am Rathaus 65b | 63526 Erlensee

Verpflichtung zur Vertraulichkeit und Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO), zur Verschwiegenheit und auf das Fernmeldegeheimnis

1. Verpflichtung zur Vertraulichkeit

- Vorname und Name in Druckbuchstaben -

verpflichtet sich, personenbezogene Daten nicht unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung vorliegt oder eine gesetzliche Regelung die Verarbeitung erlaubt oder vorschreibt. Die Grundsätze der DS-GVO für die Verarbeitung personenbezogener Daten sind zu wahren; sie sind in Art. 5 Abs. 1 DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten müssen

a) auf rechtmäßige und faire Weise, und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden **(„Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz");**

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden **(„Zweckbindung");**

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein **(„Datenminimierung");**

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden **(„Richtigkeit");**

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist **(„Speicherbegrenzung");**

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen **(„Integrität und Vertraulichkeit").**

Dokumentenname: 03.01 | Verpflichtung der Beschäftigten
Klassifizierung: 03 - VERTRAULICH
Stand: 16.09.2024
Ver.: 01.01
Seite **1** von **8**
© wavesun-technologies | Patrick Bäcker Datenschutztechnische Betreuung info@wavesun-technologies.de

2.5 | Verpflichtung zur Vertraulichkeit

- Jeder SHK-Beschäftigte (Voll- und Teilzeit, Auszubildene, Praktikanten) ist vor Aufnahme der Tätigkeit bzw. vor der Einsichtnahme und Verarbeitung von personenbezogenen Daten, für welche die SHK verantwortlich ist, zur Vertraulichkeit und Einhaltung der datenschutzrechtlichen Anforderungen nach den Grundsätzen aus Art. 5 Abs. 1 i.V.m. Art. 29 DS-GVO verpflichtet worden (siehe Dokument „Verpflichtung zur Vertraulichkeit"). Zudem nach Arbeitsbereich Beachtung Verpflichtung zur Verschwiegenheit nach § 203 Abs. 4 StGB und auf das Fernmeldegeheimnis nach § 3 TDDDG.

- **Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine betriebliche Weisung vorliegt, es sei denn, eine gesetzliche Regelung schreibt eine Verarbeitung vor**. Unter Weisungen fallen u.a. Prozessbeschreibungen, Ablaufpläne, Dienstvereinbarungen, allgemeine Dienstanweisungen, Einzelweisungen von Vorgesetzen sowie betriebliche Dokumentationen und Handbücher.

- Die Verpflichtungen **gelten während und auch nach** Beendigung des Beschäftigtenverhältnisses.

2.5 | Sicherheitsmaßnahmen am Arbeitsplatz (Übersicht)

Im Büro

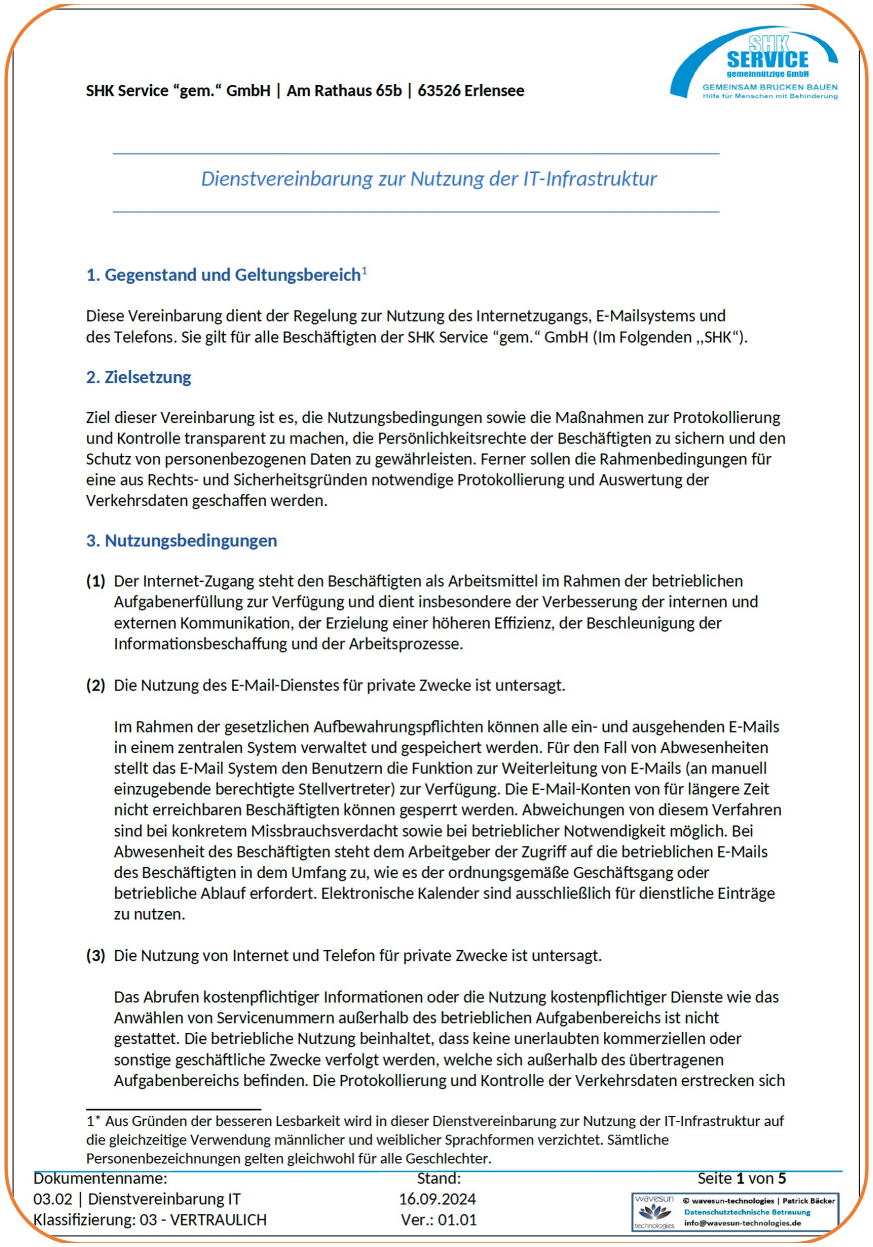
- Verarbeitung personenbezogener Daten in **fest definierten Räumlichkeiten der SHK**
- Physische Unterlagen können in abschließbaren Büros / abschließbaren Schränken sicher aufbewahrt werden
- Datenverarbeitungsanlagen und Peripheriegeräte (Desktop Rechner, Speichermedien, Drucker, etc.) sind durch die Ortsbindung physisch vor dem Zutritt Dritter geschützt (bspw. durch die Videoüberwachung, organisatorische Zutrittsregelungen, abschließbare Büros)

→ Regelungen zum Umgang mit personenbezogenen Daten siehe 03.02 „Dienstvereinbarung IT“

In der mobilen Arbeit

- Verarbeitung personenbezogener Daten **außerhalb der Räumlichkeiten der SHK**
- Physische Unterlagen werden in Aktentaschen o.ä. transportiert, welche beaufsichtigt / geschützt gelagert werden müssen
- Der Zugriff auf Datenverarbeitungsanlagen und Peripheriegeräte (Laptops, Smart-phones, etc.) ist für Dritte (bspw. bei vor Ort Kunden / Klienten Terminen oder der Arbeit in öffentlichen Räumen) vereinfacht möglich

→ Regelungen zum Umgang mit personenbezogenen Daten siehe 03.03 „Mobile- und Telearbeit-Vereinbarung IT“



SHK Service "gem." GmbH | Am Rathaus 65b | 63526 Erlensee

Dienstvereinbarung zur Nutzung der IT-Infrastruktur

1. Gegenstand und Geltungsbereich[1]

Diese Vereinbarung dient der Regelung zur Nutzung des Internetzugangs, E-Mailsystems und des Telefons. Sie gilt für alle Beschäftigten der SHK Service "gem." GmbH (Im Folgenden „SHK").

2. Zielsetzung

Ziel dieser Vereinbarung ist es, die Nutzungsbedingungen sowie die Maßnahmen zur Protokollierung und Kontrolle transparent zu machen, die Persönlichkeitsrechte der Beschäftigten zu sichern und den Schutz von personenbezogenen Daten zu gewährleisten. Ferner sollen die Rahmenbedingungen für eine aus Rechts- und Sicherheitsgründen notwendige Protokollierung und Auswertung der Verkehrsdaten geschaffen werden.

3. Nutzungsbedingungen

(1) Der Internet-Zugang steht den Beschäftigten als Arbeitsmittel im Rahmen der betrieblichen Aufgabenerfüllung zur Verfügung und dient insbesondere der Verbesserung der internen und externen Kommunikation, der Erzielung einer höheren Effizienz, der Beschleunigung der Informationsbeschaffung und der Arbeitsprozesse.

(2) Die Nutzung des E-Mail-Dienstes für private Zwecke ist untersagt.

Im Rahmen der gesetzlichen Aufbewahrungspflichten können alle ein- und ausgehenden E-Mails in einem zentralen System verwaltet und gespeichert werden. Für den Fall von Abwesenheiten stellt das E-Mail System den Benutzern die Funktion zur Weiterleitung von E-Mails (an manuell einzugebende berechtigte Stellvertreter) zur Verfügung. Die E-Mail-Konten von für längere Zeit nicht erreichbaren Beschäftigten können gesperrt werden. Abweichungen von diesem Verfahren sind bei konkretem Missbrauchsverdacht sowie bei betrieblicher Notwendigkeit möglich. Bei Abwesenheit des Beschäftigten steht dem Arbeitgeber der Zugriff auf die betrieblichen E-Mails des Beschäftigten in dem Umfang zu, wie es der ordnungsgemäße Geschäftsgang oder betriebliche Ablauf erfordert. Elektronische Kalender sind ausschließlich für dienstliche Einträge zu nutzen.

(3) Die Nutzung von Internet und Telefon für private Zwecke ist untersagt.

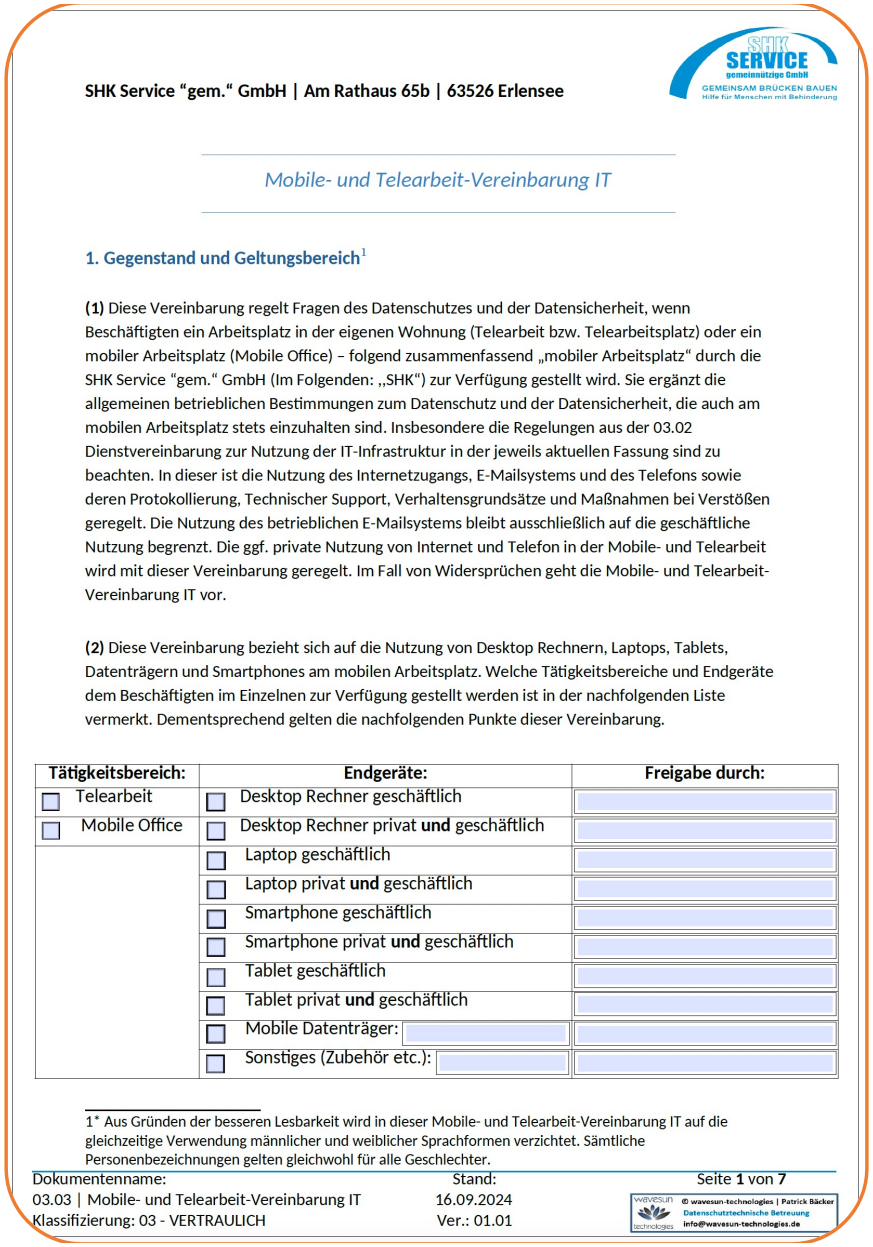
Das Abrufen kostenpflichtiger Informationen oder die Nutzung kostenpflichtiger Dienste wie das Anwählen von Servicenummern außerhalb des betrieblichen Aufgabenbereichs ist nicht gestattet. Die betriebliche Nutzung beinhaltet, dass keine unerlaubten kommerziellen oder sonstige geschäftliche Zwecke verfolgt werden, welche sich außerhalb des übertragenen Aufgabenbereichs befinden. Die Protokollierung und Kontrolle der Verkehrsdaten erstrecken sich

1* Aus Gründen der besseren Lesbarkeit wird in dieser Dienstvereinbarung zur Nutzung der IT-Infrastruktur auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für alle Geschlechter.

2.5 | Dienstvereinbarung IT

- Jeder SHK-Beschäftigte (Voll- und Teilzeit, Auszubildende, Praktikanten) ist mit den **maßgeblichen Regelungen zum Umgang mit Geräten und Unterlagen im Büro, welche personenbezogene Daten beinhalten**, unterrichtet worden (siehe Dokument „Dienstvereinbarung zur Nutzung der IT-Infrastruktur")

- Die Dienstvereinbarung IT enthält insbesondere Informationen zur **geschäftlichen Nutzung von Internet, E-Mail und Telefon**, den **Verhaltensgrundsätzen** und **Vorgaben** zu deren **Nutzung** sowie der **Protokollierung** und **Maßnahmen bei Verstößen**



SHK Service "gem." GmbH | Am Rathaus 65b | 63526 Erlensee

Mobile- und Telearbeit-Vereinbarung IT

1. Gegenstand und Geltungsbereich[1]

(1) Diese Vereinbarung regelt Fragen des Datenschutzes und der Datensicherheit, wenn Beschäftigten ein Arbeitsplatz in der eigenen Wohnung (Telearbeit bzw. Telearbeitsplatz) oder ein mobiler Arbeitsplatz (Mobile Office) – folgend zusammenfassend „mobiler Arbeitsplatz" durch die SHK Service "gem." GmbH (Im Folgenden: „SHK") zur Verfügung gestellt wird. Sie ergänzt die allgemeinen betrieblichen Bestimmungen zum Datenschutz und der Datensicherheit, die auch am mobilen Arbeitsplatz stets einzuhalten sind. Insbesondere die Regelungen aus der 03.02 Dienstvereinbarung zur Nutzung der IT-Infrastruktur in der jeweils aktuellen Fassung sind zu beachten. In dieser ist die Nutzung des Internetzugangs, E-Mailsystems und des Telefons sowie deren Protokollierung, Technischer Support, Verhaltensgrundsätze und Maßnahmen bei Verstößen geregelt. Die Nutzung des betrieblichen E-Mailsystems bleibt ausschließlich auf die geschäftliche Nutzung begrenzt. Die ggf. private Nutzung von Internet und Telefon in der Mobile- und Telearbeit wird mit dieser Vereinbarung geregelt. Im Fall von Widersprüchen geht die Mobile- und Telearbeit-Vereinbarung IT vor.

(2) Diese Vereinbarung bezieht sich auf die Nutzung von Desktop Rechnern, Laptops, Tablets, Datenträgern und Smartphones am mobilen Arbeitsplatz. Welche Tätigkeitsbereiche und Endgeräte dem Beschäftigten im Einzelnen zur Verfügung gestellt werden ist in der nachfolgenden Liste vermerkt. Dementsprechend gelten die nachfolgenden Punkte dieser Vereinbarung.

Tätigkeitsbereich:	Endgeräte:	Freigabe durch:
☐ Telearbeit	☐ Desktop Rechner geschäftlich	
☐ Mobile Office	☐ Desktop Rechner privat **und** geschäftlich	
	☐ Laptop geschäftlich	
	☐ Laptop privat **und** geschäftlich	
	☐ Smartphone geschäftlich	
	☐ Smartphone privat **und** geschäftlich	
	☐ Tablet geschäftlich	
	☐ Tablet privat **und** geschäftlich	
	☐ Mobile Datenträger:	
	☐ Sonstiges (Zubehör etc.):	

1* Aus Gründen der besseren Lesbarkeit wird in dieser Mobile- und Telearbeit-Vereinbarung IT auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für alle Geschlechter.

2.5 | Mobile- und Telearbeit Vereinbarung IT

- Jeder SHK-Beschäftigte (Voll- und Teilzeit, Auszubildende, Praktikanten) ist mit den **maßgeblichen Regelungen zum Umgang mit Geräten und Unterlagen in der Mobile- und Telearbeit, welche personenbezogene Daten beinhalten**, unterrichtet worden (siehe Dokument „Mobile- und Telearbeit-Vereinbarung IT")

- Die Mobile- und Telearbeit-Vereinbarung IT enthält insbesondere Informationen zur **geschäftlichen und privaten Nutzung von Internet, E-Mail und Telefon**, den **ausgehändigten Geräten**, den **Verhaltensgrundsätzen** und **Vorgaben** zu deren **Nutzung** sowie der **Protokollierung** und **Maßnahmen bei Verstößen**

2.5 | Auszüge Best Practices Sicherheitsmaßnahmen am Arbeitsplatz

Im Büro

Empfängeradressen (E-Mail, Post) auf Richtigkeit prüfen

Möglichst keine lokale Speicherung

Anrufer identifizieren vor der Herausgabe von Informationen

Aktenvernichter oder Datenschutzcontainer nutzen

Betroffenenersuchen und Datenpannen unverzüglich melden

In der mobilen Arbeit

Unterlagen und Geräte beaufsichtigen bei Anwesenheit Dritter

Geräte bei Nichtbenutzung sperren

Keine unbekannten Datenträger anschließen

Verlust von Unterlagen und Geräten unverzüglich melden

Nur mit sicheren Netzen verbinden

2.5 | Fazit Sicherheitsmaßnahmen am Arbeitsplatz

Büro Arbeit

≈

Besondere Beachtung bei der Herausgabe von Daten

Mobile Arbeit

≈

Besondere Beachtung, dass Dritte keine Daten einsehen können

Technische und organisatorische Maßnahmen

„TOM´s“

Beachtung der geltenden Richtlinien, Prozesse, Weisungen

(insb. „Dienstvereinbarung IT“ und „Mobile- und Telearbeit-Vereinbarung IT“)

Meldung von Betroffenenersuchen und (möglichen) Datenpannen

(siehe Aushänge Notfallkarte Datenpanne Anzeichen und Notfallkarte Betroffenenersuchen)

2.6 | Die 13 Datenschutz-Shortcuts

1) Mögliche Datenpannen und Betroffenenersuchen unverzüglich melden!

-> Siehe Aushänge Datenschutz-Notfallkarten

2) Daten nach Vertraulichkeit klassifizieren und schützen!

Keine lokale Speicherung, sofern nicht zwingend notwendig!

3) Daten nur zum vorgesehenen Zweck und innerhalb des übertragenen Aufgabenbereichs verarbeiten!

4) Auftragsdaten nur nach Weisung verarbeiten!

Fernwartungsarbeiten (sofern nicht vertraglich geregelt) nur mit Freigabe zulassen!

5) Nur berechtigten Personen Auskunft geben – Identifizierung durchführen!

E-Mail- und Postempfängeradressen auf Richtigkeit prüfen!

6) Unberechtigten Einblick in Daten verhindern -> Vertrauliche Dokumente und Datenträger verschließen!

7) Sichere Übertragungswege bei externer Kommunikation nutzen

(Gesichertes Netzwerk)!

8) Transport von Dokumenten und Datenträgern in geschlossenen ,,Behältern“!

9) Dokumente und Datenträger bei Kundenbesuchen unter ständiger Aufsicht halten!

Computer sperren oder abmelden!

10) Nur freigegebene Hard- und Software einsetzen!

11) Verdächtige E-Mails der IT zur Überprüfung auf Viren melden – E-Mails nicht weiterleiten und Anhänge nicht öffnen!

12) Nicht mehr benötigte Dokumente und Datenträger entsprechend interner Regelungen entsorgen

13) Dokumente und Datenträger nach Dienstschluss aus Firmenwagen mitnehmen und sicher verwahren!

Vielen Dank für Ihre Teilnahme und das Interesse am Datenschutz in der

SHK-Gruppe

Fragen ?

Zögern Sie bitte nicht mich zu kontaktieren

Kontaktdaten Datenschutzbeauftragter „DSB“
Herr Patrick Bäcker

Telefon: 06074 / 3709395
E-Mail: info@wavesun-technologies.de