		Entgeltgruppe lt. AV	D.9.2.1 Informationspflicht für MA	D.9.2.2 FO Verpflichtung Vertraulichkeit für Mitarbeiter	D.9.2.4 Arbeitsanleitung z. Nutzung von IT Infrastruktur	D.9.2.5 Nutzung von Emails	D.9.2.6 Private Nutzung des betrieblichen Internetzugangs	D.9.2.7 Nutzung privater Endgeräte	D.9.2.8 FO- Mobiles Arbeiten	D.9.2.11 Nutzung von Whatsapp	D.9.5.2 Hinweisgeberschutzgesetz	B.1.4.31 Selbstauskunft PUEG
Funktion												
☐	Stationshilfe	2	x	x	x	x	x	x	-	x	x	x
☐	Pflege-Assistenz	3	x	x	x	x	x	x	-	x	x	x
☐	Alltagsbegleitung §43b	3	x	x	x	x	x	x	-	x	x	x
☐	Betreuung-Assistenz	3	x	x	x	x	x	x	-	x	x	x
☐	Pflege-Helfer, Pflege-Assistenz mit Zusatzaufgabe	4	x	x	x	x	x	x	-	x	x	x
☐	Pflege-Helfer mit Zusatzaufgabe	5	x	x	x	x	x	x	-	x	x	x
☐	Pflege-Fachkraft	7	x	x	x	x	x	x		x	x	x
☐	Ergo-Therapeut	7	x	x	x	x	x	x		x	x	x
☐	Pflege-Fachkraft mit Zusatzaufgabe	8	x	x	x	x	x	x		x	x	x
☐	Wohnbereichsleitung	8	x	x	x	x	x	x	x	x	x	x
☐	Teamleitung PsoD/ ohne Studium	8	x	x	x	x	x	x	x	x	x	x
☐	QB –Pflege	9	x	x	x	x	x	x	x	x	x	x
☐	Stellv. PDL	9	x	x	x	x	x	x	x	x	x	x
☐	Teamleitung PsoD / mit Studium	9	x	x	x	x	x	x		x	x	x
☐	PDL/ Leitung QM	10	x	x	x	x	x	x	x	x	x	x
☐	Azubi 1-jährig		x	x	x	x	x	x	-	x	x	x
☐	Azubi 3-jährig		x	x	x	x	x	x	-	x	x	x

		Entgeltgruppe lt. AV	D.9.2.1 Informationspflicht für MA	D.9.2.2 FO Verpflichtung Vertraulichkeit für Mitarbeiter	D.9.2.4 Arbeitsanleitung z. Nutzung von IT Infrastruktur	D.9.2.5 Nutzung von Emails	D.9.2.6 Private Nutzung des betrieblichen Internetzugangs	D.9.2.7 Nutzung privater Endgeräte	D.9.2.8 FO- Mobiles Arbeiten	D.9.2.11 Nutzung von Whatsapp	D.9.5.2 Hinweisgeberschutzgesetz	B.1.4.31 Selbstauskunft PUEG
Funktion												
☐	Reinigung Helfer, Hol- und Bringdienste	2	x	x	x	x	x	X	-	x	x	
☐	Reinigung Vorarbeiterin	3	x	x	x	x	x	X	-	x	x	
☐	Küche Helfer	3	x	x	x	x	x	X	-	x	x	
☐	Küche Fachkraft	4	x	x	x	x	x	X	-	x	x	
☐	Reinigung VorarbeiterIn	4	x	x	x	x	x	x	-	x	x	
☐	Sekr. / allg. Verwaltung - Mitarbeit	4	x	x	x	x	x	x	-	x	x	
☐	Küche stv. Leitung	5	x	x	x	x	x	x	-	x	x	
☐	Sekr. / allg. Verwaltung	5	x	x	x	x	x	x	x	x	x	
☐	Haustechnik	5	x	x	x	x	x	x	-	x	x	
☐	Sekr. / allg. Verwaltung - Fachkraftaufgaben	6	x	x	x	x	x	x	x	x	x	
☐	Küche FK-Ltg.	7	x	x	x	x	x	x	-	x	x	
☐	Haustechnik - Fachkraftaufgaben	7	x	x	x	x	x	x	-	x	x	
☐	QB	9	x	x	x	x	x	x	x	x	x	
☐	EL	11	x	x	x	x	x	x	x	x	x	
☐	Geringfügig Beschäftigt		x	x	x	x	x	x	-	x	x	

Unser Umgang mit Ihren Daten und Ihre Rechte
– Informationen nach Artikeln 13, 14 und 21
der Datenschutz-Grundverordnung (DSGVO) –

Sehr geehrte Mitarbeiterin, sehr geehrter Mitarbeiter,

nachfolgend informieren wir Sie über die Verarbeitung Ihrer personenbezogenen Daten durch uns und die Ihnen nach den datenschutzrechtlichen Regelungen zustehenden Ansprüche und Rechte.

1. Wer ist für die Datenverarbeitung verantwortlich und an wen kann ich mich wenden?

Verantwortliche Stelle ist:

Hsde gGmbH
Schimmelpfengstr. 4

34613 Schwalmstadt

Sie erreichen unseren Datenschutzbeauftragten unter:

Betriebsbeauftragte für Datenschutz der Hephata Diakonie
Elisabeth-Seitz-Straße 2
34613 Schwalmstadt

E-Mail: datenschutz@hephata.de

2. Welche Quellen und Daten nutzen wir?

Wir verarbeiten personenbezogene Daten, die wir von Ihnen erhalten oder bei Ihnen entweder im Rahmen der Einstellung oder während des Beschäftigungsprozesses erheben. In bestimmten Fällen erheben wir Daten auch bei anderen Stellen. Dazu zählen etwa anlassbezogene Abfragen von steuerrelevanten Informationen beim zuständigen Finanzamt oder Informationen über Arbeitsunfähigkeitszeiten bei der jeweiligen Krankenkasse.

Relevante personenbezogene Daten sind Daten aus dem Beschäftigungsverhältnis, insbesondere solche, die für die Gewährung von Vergütungs-, Renten- und sonstigen Leistungen erforderlich sind, wie z. B. Beschäftigungszeiten, Arbeitszeiten, Gehaltsparameter, Personalien (Name, Adresse und andere Kontaktdaten, Geburtstag und -ort und Staatsangehörigkeit), Informationen, die Ihren beruflichen Werdegang betreffen (z. B. Aus- und Weiterbildung, Zeugnisse), Leistungsnachweise und Beurteilungen (z. B. aus einem Assessment Center), Protokolldaten aus der Nutzung von IT-Systemen und öffentlich-rechtliche oder privatrechtliche Daten (z. B. Sozialversicherungs-, Versicherungs-, Konto und Steuernummern). Ferner können hierunter auch besondere Kategorien personenbezogener Daten wie etwa Gesundheitsdaten fallen.

3. Wofür verarbeiten wir Ihre Daten (Zweck der Verarbeitung) und auf welcher Rechtsgrundlage[1]?

Wir verarbeiten personenbezogene Daten im Einklang mit den Bestimmungen der Europäischen Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG) sowie der weiteren einschlägigen arbeitsrechtlichen Vorschriften (z. B. Betriebsverfassungsgesetz).

3.1 Zur Durchführung vertraglicher oder nachvertraglicher Maßnahmen oder zur Erfüllung von Pflichten (Artikel 6 Abs. 1b DSGVO)

Die Verarbeitung personenbezogener Daten (Artikel 4 Nr. 2 DSGVO) erfolgt zur Begründung, Durchführung, Beendigung und Abwicklung des Beschäftigungsverhältnisses. Die Rechtsgrundlage hierzu ist Art. 6 Abs. 1 lit b) DSGVO i.V.m. § 26 BDSG. Daneben können auch Kollektivvereinbarungen (insbesondere Betriebsvereinbarungen und tarifvertragliche Regelungen) gemäß Art. 6 Abs. 1 lit) b, Art. 88 Abs. 1 DSGVO i.V.m. § 26 Abs. 4 BDSG für die Verarbeitung herangezogen werden. Schließlich verarbeiten wir Ihre personenbezogenen Daten, wenn Sie uns hierzu Ihre Einwilligung erteilt haben (Art. 6 Abs. 1 lit. a), 7 DSGVO i.V.m. § 26 Abs. 2 BDSG.

3.2 Im Rahmen der Interessenabwägung (Artikel 6 Abs. 1f DSGVO)

Soweit erforderlich verarbeiten wir Ihre Daten zudem zur Wahrung unserer berechtigten Interessen. Dies gilt insbesondere zum Zwecke der internen Kommunikation sowie zu Verwaltungszwecken. Ferner verarbeiten wir Ihre Daten auch zur Wahrung der berechtigten Interessen Dritter, z. B. zur Geltendmachung oder Abwehr von Ansprüchen, zur Gewährleistung der IT-Sicherheit und des IT-Betriebs des Unternehmens, für Videoaufzeichnungen und -auswertungen, insbesondere in Bereichen mit Kundenverkehr oder für Maßnahmen der Gebäude- und Anlagensicherheit (z. B. Zutrittskontrollen).

3.3 Aufgrund Ihrer Einwilligung (Artikel 6 Abs. 1a DSGVO)

Soweit Sie uns eine Einwilligung zur Verarbeitung von personenbezogenen Daten für bestimmte Zwecken erteilt haben (z. B. Veröffentlichung von Bildmaterial für den Internetauftritt des Unternehmens), führen wir die Verarbeitung auf dieser Grundlage durch. Dies gilt grundsätzlich auch für Gesundheitsdaten (Art. 9 Abs. 2 lit. a) und lit. b) DSGVO i.V.m. § 26 Abs. 3 BDSG), sofern nicht eine Verarbeitung aufgrund gesetzlicher Vorgaben oder im öffentlichen Interesse erfolgt (siehe dazu nachfolgend 3.4). Eine einmal erteilte Einwilligung können Sie jederzeit widerrufen.

Bitte beachten Sie, dass der Widerruf erst für die Zukunft wirkt. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen.

3.4 Aufgrund gesetzlicher Vorgaben (Artikel 6 Abs. 1c DSGVO) oder im öffentlichen Interesse (Artikel 6 Abs. 1e DSGVO)

Daneben verarbeiten wir Ihre Daten auch, um unsere rechtlichen Pflichten als Arbeitgeber, insbesondere im Bereich des Steuer- und Sozialversicherungsrechts erfüllen zu können. (Art. 6 Abs. 1 lit. c) DSGVO i.V.m. § 26 BDSG). Insbesondere die Abführung von Lohnsteuer und Sozialversicherungsbeiträgen im Beschäftigungsverhältnis erfordert die Verarbeitung Ihrer Daten.

Besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO (insbesondere Gesundheitsdaten) verarbeiten wir ebenfalls nur in der Ausübung von Rechten und der Erfüllung von Pflichten aus dem Arbeitsrecht sowie dem Sozialrecht (z.B. Erfassung einer Schwerbehinderung). Rechtsgrundlage dafür ist Art. 9 Abs. 2 lit. b) DSGVO i.V.m. § 26 Abs. 3 BDSG.

[1] § 26 BDSG-neu

4. Wer bekommt meine Daten?

Innerhalb des Unternehmens erhalten diejenigen Stellen Zugriff auf Ihre Daten, die diese zur Erfüllung unserer vertraglichen und gesetzlichen Pflichten brauchen (z. B. Personalabteilung, die jeweiligen Führungskräfte). Auch von uns eingesetzte Auftragsverarbeiter (Artikel 28 DSGVO) können zu diesen genannten Zwecken Daten erhalten. Dies sind Unternehmen in den Kategorien Gehaltsabrechnungen, Personaldienstleistungen, Druckdienstleistungen, Telekommunikation (z. B. Diensthandy), IT-Dienstleistungen, Finanzdienstleistungen (z. B. vermögenswirksame Leistungen), Beratung und Consulting.

Informationen über Sie dürfen wir ferner weitergeben, sofern dies im Rahmen unserer wirtschaftlichen Tätigkeit oder zur Erfüllung unserer vertraglichen oder gesetzlichen Pflichten als Arbeitgeber erforderlich ist oder sofern Sie eingewilligt haben. Unter diesen Voraussetzungen können Empfänger personenbezogener Daten z. B. sein:

- Behörden und öffentliche Einrichtungen (z. B. Sozialversicherungsträger, Rentenversicherungsträger, Versorgungswerke, Finanzbehörden)
- Bank des Mitarbeiters
- Private Stellen (z. B. Anbieter von Produkten zur Anlage von vermögenswirksamen Leistungen oder von Produkten der betrieblichen Altersvorsorge)

5. Wie lange werden meine Daten gespeichert?

Soweit erforderlich, verarbeiten und speichern wir Ihre personenbezogenen Daten für die Dauer unserer Vertragsbeziehung. Dies umfasst auch die Abwicklung eines Vertrages.

Nach Beendigung des Vertragsverhältnisses speichern wir Ihre personenbezogenen Daten, solange wir dazu gesetzlich verpflichtet sind. Derartige Dokumentations- und Aufbewahrungspflichten ergeben sich beispielsweise aus dem Handelsgesetzbuch (HGB)[2], dem Sozialgesetzbuch (SGB)[3] und dem Einkommenssteuergesetz (EStG)[4]. Die dort vorgegebenen Fristen zur Dokumentation bzw. zur Aufbewahrung von personenbezogenen Daten betragen bis zu zehn Jahre bzw. müssen darüber hinaus bis zum Ende einer Geschäftsbeziehung mit dem Kunden erfolgen.

Schließlich beurteilt sich die Speicherdauer auch nach den gesetzlichen Verjährungsfristen, die zum Beispiel nach den §§ 195 ff. des Bürgerlichen Gesetzbuches (BGB) in der Regel drei Jahre, in gewissen Fällen aber auch bis zu dreißig Jahre betragen können.

6. Werden Daten in ein Drittland oder an eine internationale Organisation übermittelt?

Eine Datenübermittlung in Drittstaaten (Staaten außerhalb des Europäischen Wirtschaftsraums – EWR) findet nur statt, soweit dem Drittland durch die EU-Kommission ein angemessenes Datenschutzniveau bestätigt oder angemessene Datenschutzgarantien (z.B. EU-Standardvertragsklauseln) vorhanden sind. Liegen diese Voraussetzungen nicht vor, findet eine Übermittlung nur statt, sofern diese zur Erfüllung unserer arbeitsvertraglichen Pflichten erforderlich ist oder Sie uns Ihre Einwilligung nach Information über etwaige Risiken einer solchen Übermittlung erteilt haben. Detaillierte Information zu unseren Dienstleistern mit Drittstaatenbezug sowie zu dem dort bestehenden Datenschutzniveau erhalten Sie unter der oben genannten Kontaktinformation.

---

[2] §§ 238, 257 Abs. 4 HGB.

[3] § 28f Abs. 1 Satz 1 SGB IV in Verbindung mit § 8 BVV, § 165 Abs. 4 Satz 2 SGB VII, § 163 Abs. 1 SGB IX

[4] § 41 Abs. 1 Satz 9 EStG, § 39 Abs. 3 EStG, § 39e Abs. 8 EStG

7. Welche Datenschutzrechte habe ich?

Jede betroffene Person hat das Recht auf **Auskunft** nach Artikel 15 DSGVO, das Recht auf **Berichtigung** nach Artikel 16 DSGVO, das Recht auf **Löschung** nach Artikel 17 DSGVO, das Recht auf **Einschränkung der Verarbeitung** nach Artikel 18 DSGVO sowie das Recht auf **Datenübertragbarkeit** aus Artikel 20 DSGVO. Beim Auskunftsrecht und beim Löschungsrecht gelten die Einschränkungen nach §§ 34 und 35 BDSG. Darüber hinaus besteht ein Beschwerderecht bei einer Datenschutzaufsichtsbehörde (Artikel 77 DSGVO i. V. m. § 19 BDSG).

8. Besteht eine Pflicht zur Bereitstellung von Daten?

Im Rahmen des Beschäftigungsverhältnisses müssen Sie diejenigen personenbezogenen Daten bereitstellen, die uns die Erfüllung unserer arbeitsvertraglichen und gesetzlichen Pflichten ermöglicht. Davon umfasst sind auch solche personenbezogenen Daten, zu deren Erhebung wir gesetzlich verpflichtet sind.
Gegebenenfalls kann im Rahmen einer Zuverlässigkeitsprüfung auch die Vorlage eines polizeilichen Führungszeugnisses erforderlich werden.

9. Inwieweit gibt es eine automatisierte Entscheidungsfindung im Einzelfall?

Zur Durchführung des Beschäftigungsverhältnisses nutzen wir grundsätzlich keine vollautomatisierte Entscheidungsfindung gemäß Artikel 22 DSGVO. Sollten wir diese Verfahren in Einzelfällen einsetzen, werden wir Sie hierüber gesondert informieren, sofern dies gesetzlich vorgegeben ist.

Information über Ihr Widerspruchsrecht nach Artikel 21 Datenschutz-Grundverordnung (DSGVO)

Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1e DSGVO (Datenverarbeitung im öffentlichen Interesse) und Artikel 6 Absatz 1f DSGVO (Datenverarbeitung auf der Grundlage einer Interessenabwägung) erfolgt, Widerspruch einzulegen; Legen Sie Widerspruch ein, werden wir Ihre personenbezogenen Daten nicht mehr verarbeiten, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Der Widerspruch kann formfrei erfolgen und sollte möglichst gerichtet werden an:

Hsde gGmbH
Schimmelpfengstr. 4
34613 Schwalmstadt

wurde darauf verpflichtet, dass es untersagt ist, personenbezogene Daten unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlauben oder eine Verarbeitung dieser Daten vorgeschrieben ist. Die Grundsätze der DS-GVO für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten müssen

1. auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
2. für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
3. dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
4. 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;
5. 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;
6. 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“);

Verstöße gegen diese Verpflichtung können mit Geldbuße und/oder Freiheitsstrafe geahndet werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder spezieller Geheimhaltungspflichten darstellen. Auch (zivilrechtliche) Schadenersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben. Ihre sich aus dem Arbeits- bzw. Dienstvertrag oder gesonderten Vereinbarungen ergebende Vertraulichkeitsverpflichtung wird durch diese Erklärung nicht berührt.

Die Verpflichtung gilt auch nach Beendigung der Tätigkeit weiter.
Ich bestätige diese Verpflichtung. Ein Exemplar der Verpflichtung nebst Anlage habe ich erhalten.

Anlage zur Verpflichtung auf die Vertraulichkeit

Die vorliegende Auswahl gesetzlicher Vorschriften soll Ihnen einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalten Sie beim betrieblichen Datenschutzbeauftragten.

Begrifflichkeiten

Art. 4 Nr. 1 DS-GVO: „**Personenbezogene Daten**“ [sind] 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 identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Art. 4 Nr. 2 DS-GVO: „**Verarbeitung**“ [meint] jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Grundsätze der Verarbeitung

Art. 5 Abs. 1 lit. a DS-GVO: Personenbezogene Daten müssen […] auf **rechtmäßige Weise**, nach Treu und Glauben und in einer für die betroffene Person **nachvollziehbaren Weise** verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“).

Art. 5 Abs. 1 lit. f DS-GVO: Personenbezogene Daten müssen […] 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“).

Art. 29 DS-GVO: Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten **ausschließlich auf Weisung** des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Art. 32 Abs. 2 DS-GVO: Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch **Vernichtung**, **Verlust** oder **Veränderung**, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte **Offenlegung** von beziehungsweise unbefugten **Zugang** zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Art. 33 Abs. 1 Satz 1 DS-GVO: Im Falle einer **Verletzung** des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der […] zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Haftung

Art. 82 Abs. 1 DS-GVO: Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf **Schadenersatz** gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Art. 83 Abs. 1 DS-GVO: Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von **Geldbußen** gemäß diesem Artikel für Verstöße gegen diese Verordnung […] in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

§ 42 BDSG

(1) Mit **Freiheitsstrafe** bis zu drei Jahren oder mit **Geldstrafe** wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht

und hierbei gewerbsmäßig handelt.

(2) Mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

§ 202a Abs. 1 StGB: Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit **Freiheitsstrafe** bis zu drei Jahren oder mit **Geldstrafe** bestraft.

§ 303a Abs. 1 StGB: Wer rechtswidrig Daten […] löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** bestraft.

§ 88 TKG

(1) [1]Dem Fernmeldegeheimnis unterliegen der **Inhalt der Telekommunikation und ihre näheren Umstände**, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. [2]Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) [1]Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. [2]Die Pflicht zur Geheimhaltung besteht **auch nach dem Ende der Tätigkeit** fort, durch die sie begründet worden ist.

(3) [1]Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. [2]Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. [3]Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. [4]Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang. […]

Sozialgeheimnis

§ 78 Abs. 1 Satz 2 & 3 SGB X: […] [2]Eine Übermittlung von Sozialdaten an eine nichtöffentliche Stelle ist nur zulässig, wenn diese sich gegenüber der übermittelnden Stelle verpflichtet hat, die Daten nur zu dem Zweck zu verarbeiten, zu dem sie ihr übermittelt werden. [3]Die Dritten

haben die Daten **in demselben Umfang geheim zu halten** wie die in § 35 [SGB I] genannten Stellen.

D.9.2.4 Arbeitsanleitung z. Nutzung von IT Infrastruktur Arbeitsanweisung zur Nutzung der IT-Infrastruktur

- Auf der IT-Infrastruktur der hsde darf ausschließlich ausreichend lizenzierte Software verwendet werden.

- Die Beschaffung sowie die Installation der Programme erfolgt ausschließlich über die IT-Abteilung bzw. die Geschäftsführung.

- Firmeneigene Software darf nicht kopiert werden.

- Sie als Mitarbeiter bringen keine eigene Hard- oder Software und keine eigenen Datenträger in das Unternehmen ein und verbringen keine im Rahmen Ihrer Aufgabenerfüllung verarbeiteten Daten außerhalb des betrieblichen Aufgabenbereichs, sofern dies nicht ausdrücklich zugelassen wurde.

- Die IT-Systeme der hsde dürfen nur von autorisierten Personen genutzt werden, die Autorisierung zur Nutzung des Systems erfolgt durch die Übergabe einer persönlichen Benutzerkennung.

- Die Nutzung der IT-Infrastruktur beschränkt sich auf als PC-Arbeitsplätze deklarierte IT-Komponenten; weitere, unter Umständen vorhandene EDV-Systeme (z.B. Server, Laptops, Tablets usw.) dürfen nur mit ausdrücklicher Genehmigung der Geschäftsleitung und unter Einbeziehung der notwendigen Formulare (Überlassungs- und Nutzungsvereinbarungen der Hephata Diakonie e.V.) genutzt werden.

- Es ist vom Benutzer der IT-Systeme sicherzustellen, dass keine betriebsfremden Personen Zugriff auf Daten des Unternehmens erhalten, daher ist beim Verlassen des Büros immer der Bildschirm zu sperren (Tastenkombination „Windows + L“).

- Ebenso ist das IT-System auch unterwegs zu schützen (siehe entsprechende Arbeitsanweisung zu mobilen Geräten (D.9.2.8 FO- Nutzung mobiler Geräte).

D.9.2.5 Arbeitsanleitung zur Email-Nutzung

Den Mitarbeitern des Unternehmens wird aufgrund ihrer Tätigkeit von der Geschäftsleitung die Berechtigung erteilt, aus betrieblichen Gründen Mails zu versenden und Mails zu empfangen. Dies geschieht über den Mailclient Microsoft Outlook /Medifox.
Die Berechtigung ist an nachfolgende Bedingungen gebunden. Diese Bedingungen sind Bestandteil des Arbeitsvertrages und können bei Verstößen gegen die unten angeführten Regeln zu arbeitsrechtlichen Konsequenzen führen.

1. Grundsätze

Der Zugang zum Mailverkehr wird den Unternehmensmitarbeitern als Arbeitsmittel zur Verfügung gestellt. Mitarbeiter, die am Mailverkehr teilnehmen, treten als Mitarbeiter der Hephata Soziale Dienste und Einrichtungen gemeinnützige GmbH auf. Es ist deshalb alles zu unterlassen, was dem Ruf des Unternehmens schaden könnte. Nachfolgende Punkte sind hierbei grundsätzlich zu unterlassen:

- das Abrufen oder Anbieten von Texten, die gegen datenschutz-, persönlichkeits-, urheber- oder -strafrechtliche Bestimmungen verstoßen
- das Abrufen oder Anbieten von weltanschaulicher, politischer oder kommerzieller Werbung
- das Abrufen oder Anbieten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen oder pornographischen Äußerungen oder Abbildungen

2. Versand von Mails

Nicht verschlüsselte Mails können von Unbefugten abgefangen, gelesen und auch verändert werden. Eine Mail ist mit einer nicht unterschriebenen Postkarte zu vergleichen. Mails sollten keine Inhalte enthalten, die Sie nicht auch in Papierform veröffentlichen würden!
Es werden keine Mails über ungesicherte Verbindungen (z.B. Internet) versendet, die sensible Kundendaten enthalten.

3. Kundenaufträge, die uns per Mail zugehen

Aufträge, die uns per Mail zugehen, werden nur unter folgenden Gesichtspunkten ausgeführt:

- Absenderadresse ist bekannt
- Absenderadresse kann als zutreffend ermittelt werden
- Kunde hat Mail mit Auftrag angekündigt
- Kunde tätigt ähnliche Geschäfte schon länger telefonisch oder schriftlich

4. Versand und Empfang von Dateianhängen

Dateianhänge mit firmen- oder kundensensiblen Daten werden grundsätzlich verschlüsselt verschickt.
Dazu gehen Sie wie folgt vor:-> Verschlüsseln Sie die Datei mittels 7-Zip und vergeben ein sicheres Passwort (mindestens 12 Stellen, Groß- und Kleinschreibung, Sonderzeichen, kein Wörterbucheintrag). Das Passwort teilen Sie entweder auf einem anderen Kommunikationsweg (per Telefon) oder per weiterer Mail dem Kunden mit.
Wenden Sie sich an die EDV-Abteilung Hephata Diakonie e.V., wenn Sie Hilfestellung zur Datenversendung benötigen.

5. Private Email-Nutzung

Die private Email-Nutzung ist untersagt, da bei nicht ausschließlich geschäftlicher Nutzung der Mailboxen rechtliche Unsicherheiten in Bezug auf - Stellvertreterregelungen und deren Zugriffsrechten, - Archivierungen und - Sicherheitsprüfungen bestehen.

Das Unternehmen ist verpflichtet, die Einhaltung des Verbots der privaten Nutzung zu kontrollieren. Hierzu wird ein Kontrollteam gebildet, welches aus folgenden Personen/ Funktionen besteht:

- Einrichtungsleitung
- ZQM Verwaltung der hsde

Das Kontrollteam trifft sich regelmäßig einmal jährlich. Hierbei prüft das Kontrollteam Stichproben des im jeweiligen Zeitraum protokollierten Email-Verkehrs. Diese Stichproben werden elektronisch ermittelt. Bei Auffälligkeiten sind tiefergehende Prüfungen möglich, ggf. auch Sichtkontrollen an den jeweiligen Arbeitsplätzen. Sollten sich Tatsachen ergeben, die die nachhaltige Nichteinhaltung der vorliegenden Arbeitsanweisung bestätigen, kommt folgender Hinweis an den Mitarbeiter

- Ermahnung des Mitarbeiters und Hinweis an den Vorgesetzten
- Gespräch zwischen Mitarbeiter und der Geschäftsleitung
- Abmahnung des Mitarbeiters
- weitere personelle Maßnahmen

Alle Prüfungen und Handlungen sind zu dokumentieren und der Geschäftsleitung zur Kenntnis zu geben.

6. Missbrauch

Bei Verdacht auf Missbrauch der Mailfunktion besteht unter Einbeziehung der Geschäftsleitung die Möglichkeit, Rückschlüsse auf den Anwender zu ziehen, was arbeitsrechtliche Konsequenzen nach sich ziehen kann.

7. Protokollierungen und Kontrollen, Filter

Jeder durch TK-Dienste entstehender Datenverkehr wird einer automatischen, systembedingten Protokollierung unterzogen.
Die protokollierten Daten dienen der Gewährleistung der Systemsicherheit und Systemverfügbarkeit, der Systemoptimierung sowie der Analyse technischer Fehler und des Lastverhaltens des Systems. Des Weiteren können (saldierte) Daten zur Kostenanalyse verwendet werden.
Der Zugriff auf die Protokolldaten ist auf die Systemadministratoren des Hauses sowie ergänzend bei extern administrierten Diensten auf die Systembetreuer der jeweiligen Dienstanbieter beschränkt.
Zusätzlich können Programme eingesetzt werden, die den Datenverkehr analysieren und filtern (z.B. Content-, Viren- oder Spamfilter). Auch eine Datenarchivierung zur Erfüllung gesetzlicher Anforderungen ist möglich.
Da eine private E-Mail Nutzung untersagt ist, kann auf die Einwilligung zur Protokollierung verzichtet werden.

8. Vertretungsregelung

Um im Falle einer Abwesenheit des Mitarbeiters, weiterhin agieren zu können wird folgende Vereinbarung zur Vertretungsregelung getroffen:

Eine in diesem Fall durch die Geschäftsführung benannte Person darf uneingeschränkt auf das Postfach des abwesenden Mitarbeiters zugreifen.

D.9.2.6 Arbeitsanleitung zur privaten Nutzung des betrieblichen Internetzugangs

1. Ich akzeptiere die folgenden, mit der Privatnutzung des Internets verbundenen Nutzungsbedingungen:

- Die private Nutzung des betrieblichen Internetzugangs ist **nicht gestattet**.
- Zum Schutz der IT-Systeme vor Viren, Trojanern und ähnlichen Bedrohungen sind der Download von Programmen aus dem Internet, sowie entsprechende Downloads von Dateianhängen im Rahmen der privaten Nutzung nicht gestattet.

- Eine vorsätzliche Nutzung, welche geeignet ist, den Interessen der hsde oder deren Ansehen in der Öffentlichkeit zu schaden oder die gegen geltende Rechtsvorschriften verstößt, insbesondere
    - der Abruf für den Arbeitgeber kostenpflichtigen Internetseiten,
    - das Abrufen, Verbreiten oder Speichern von Inhalten, die gegen persönlichkeitsrechtliche, datenschutzrechtliche, lizenz- und urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
    - Aktivitäten, die sich gegen die Sicherheit von IT-Systemen richten (z.B. Angriffe auf externe Webserver) oder
    - Aktivitäten, die sich gegen das Unternehmen richten (z.B. Compliance-Verstöße [*konkret benennen*])

  unzulässig ist.

- Die hsde ist berechtigt, den Aufruf bestimmter Internet-Seiten durch den Einsatz geeigneter Filter-Programme zu verhindern. Es besteht kein Rechtsanspruch auf einen Zugriff auf gefilterte Internet-Inhalte.

Das Unternehmen ist verpflichtet, die Einhaltung des Verbots der privaten Nutzung zu kontrollieren. Hierzu wird ein Kontrollteam gebildet, welches aus folgenden Personen/ Funktionen besteht:

- Einrichtungsleitung
- ZQM Verwaltung der hsde

Das Kontrollteam trifft sich regelmäßig einmal jährlich. Hierbei prüft das Kontrollteam Stichproben des im jeweiligen Zeitraum protokollierten Email-Verkehrs. Diese Stichproben werden elektronisch ermittelt. Bei Auffälligkeiten sind tiefergehende Prüfungen möglich, ggf. auch Sichtkontrollen an den jeweiligen Arbeitsplätzen. Sollten sich Tatsachen ergeben, die die nachhaltige Nichteinhaltung der vorliegenden Arbeitsanweisung bestätigen, kommt folgender Hinweis an den Mitarbeiter

- Ermahnung des Mitarbeiters und Hinweis an den Vorgesetzten
- Gespräch zwischen Mitarbeiter und der Geschäftsleitung
- Abmahnung des Mitarbeiters
- weitere personelle Maßnahmen

Alle Prüfungen und Handlungen sind zu dokumentieren und der Geschäftsleitung zur Kenntnis zu geben.

6. Missbrauch

Bei Verdacht auf Missbrauch der Mailfunktion besteht unter Einbeziehung der Geschäftsleitung die Möglichkeit, Rückschlüsse auf den Anwender zu ziehen, was arbeitsrechtliche Konsequenzen nach sich ziehen kann.

D.9.2.7 Arbeitsanleitung zur Nutzung privater Endgeräte

- Die Nutzung privater Endgeräte (Smartphones, Laptops usw.) für betriebliche Zwecke ist **nicht gestattet**.
- Firmeneigene Daten können in Ausnahmefällen auch außerhalb des Betriebes verarbeitet werden. Diese Verarbeitung ist jedoch ausschließlich auf firmeneigenen Geräten, z.B. mobilen Arbeitsplätzen oder durch das Unternehmen verwaltete Smartphones und Tablets (iPhone's/iPad`s) zulässig.
- Mit der schriftlichen Anerkenntnis der „Überlassungsvereinbarung Notebook" oder der „Überlassungsvereinbarung Mobiles Endgerät" sind hierfür erforderlichen Regelungen kommuniziert und vereinbart.

B.1.4.22 Vereinbarung Mobiles Arbeiten

mit folgenden Inhalten:

1. Einleitung

Sofern Arbeitnehmern der HSDE die Heimarbeit („Mobiles Arbeiten") erlaubt wird, sind die Vorgaben aus dieser „Vereinbarung Mobiles Arbeiten" für die betreffenden Arbeitnehmer verbindlich einzuhalten.

Um eine rechtskonforme Verarbeitung von personenbezogenen Daten im „Mobilen Arbeiten" zu gewährleisten, sind neben den allgemeinen Verhaltensanweisungen dieser Richtlinie auch ergänzende Weisungen durch Vorgesetzte an die Arbeitnehmer möglich. Auch diesen ist Folge zu leisten.

2. Geltungsbereich

Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten durch Arbeitnehmer der HSDE im „Mobilen Arbeiten". Diese Richtlinie gilt für alle Standorte des Arbeitgebers.

Diese Richtlinie verpflichtet alle Arbeitnehmer der HSDE zur Einhaltung der hier festgelegten Pflichten und Vorgaben, soweit eine Verarbeitung personenbezogener Daten im „Mobilen Arbeiten" erfolgt.

3. Ziele

Diese Richtlinie soll dazu beitragen, dass die Rechtsvorschriften zur Verarbeitung personenbezogener Daten eingehalten werden und insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten gewährleistet werden kann.

4. Grundsätze für den Umgang mit personenbezogenen Daten

Die nachfolgenden Grundsätze sind von allen Arbeitnehmern der HSDE einzuhalten, die im „Mobilen Arbeiten" tätig sind:

- Es wird ausschließlich die vom Arbeitgeber bereitgestellte oder genehmigte Hard- und Software genutzt.
- Arbeitnehmer der HSDE sind verpflichtet, alle sie oder ihre Tätigkeit betreffenden Richtlinienvorgaben oder Anweisungen im Umgang mit personenbezogenen Daten auch bei der Arbeit im „Mobilen Arbeiten" einzuhalten. Dies gilt insbesondere für Vorgaben, die die Sicherheit personenbezogener Daten betreffen.
- Arbeitnehmer melden mögliche **Datenschutzvorfälle** unverzüglich an den internen Datenschutzkoordinator bzw. den externen Datenschutzbeauftragten. Ein Datenschutzvorfall liegt insbesondere vor, wenn die Annahme besteht, dass die Datensicherheit, insbesondere die Vertraulichkeit von Daten, gefährdet sein kann. Ein Datenschutzvorfall liegt auch bei jedem Sachverhalt vor, bei dem die Annahme besteht, dass Dritte unbefugt Zugriff oder Zugang zu personenbezogenen Daten haben oder hatten.

5. Grundsätze der Nutzung von IT-Systemen im „Mobilen Arbeiten“

Die Verarbeitung von personenbezogenen Daten im „Mobilen Arbeiten“ birgt Risiken für die Integrität, Vertraulichkeit und Verfügbarkeit von Daten in sich. Um diese Risiken auszuschließen oder zu minimieren, sind die nachfolgenden Grundsätze bei der Verarbeitung von personenbezogenen Daten im „Mobilen Arbeiten“ durch die Arbeitnehmer einzuhalten:

- Daten sind grundsätzlich nicht auf lokalen Festplatten oder Datenspeichern von Endgeräten zu speichern, die nicht im Eigentum oder Besitz des Arbeitgebers stehen.
- Die Speicherung von Daten hat grundsätzlich in den Verzeichnissen/Ordnern von Servern bzw. zentralen IT-Systemen des Arbeitgebers zu erfolgen, die für den Benutzer freigegeben sind. Ausnahmen hiervon dürfen nur gemacht werden, wenn eine Internet-Anbindung an die zentralen IT-Systeme und damit eine Speicherung auf den IT-Systemen nicht möglich ist. In diesen Fällen dürfen personenbezogene Daten auf den von den Arbeitnehmern im „Mobilen Arbeiten“ verwendeten Geräten gespeichert werden, wenn sichergestellt ist, dass die Daten auf den verwendeten Datenträgern verschlüsselt gespeichert werden. Arbeitnehmer, die nicht sicher sind, ob ihre verwendeten Datenträger verschlüsselt speichern, könnten dies beim IT-Support nachfragen.
- Arbeitnehmer, die im „Mobiles Arbeiten“ arbeiten, haben sicherzustellen, dass andere Personen keinen Zugang zu den im Zusammenhang mit der Beschäftigung verarbeiteten Daten erhalten. Dies gilt insbesondere für Personen, die in demselben Haushalt leben. Arbeitnehmer müssen daher beim Verlassen des „Mobilen Arbeiten“-Arbeitsplatzes unverzüglich eine Bildschirmsperre aktivieren, die nur mit einem Passwort aufgehoben werden kann, das dem Arbeitnehmer bekannt ist.
- Dokumente sollten grundsätzlich nicht im „Mobiles Arbeiten“ ausgedruckt werden. Sollte dies für die Erledigung von betriebsbedingten Aufgaben zwingend erforderlich sein, hat der Arbeitnehmer Sorge dafür zu tragen, dass die ausgedruckten Informationen auch direkt vor Ort geeignet vernichtet werden können.

- Besonders schutzbedürftige Informationen sollten nach Möglichkeit nur an Orten im „Mobilen Arbeiten“ verarbeitet werden, die von Dritten nicht einzusehen sind. Sollte dies nicht möglich sein, muss der Nutzer einen Ort bzw. Platz zur Verarbeitung von Daten wählen, der gewährleistet, dass der Bildschirm nicht von Dritten eingesehen werden kann.

6. Zugang zum Firmennetzwerk

Der Zugang zum Firmennetzwerk des Arbeitgebers darf nur mittels des eingerichteten VPN-Zugangs erfolgen. Informationen zur Nutzung des Zugangs erhalten die Arbeitnehmer in der hauseigenen IT-Abteilung bzw. beim externen IT-Dienstleister.

7. Datensicherung

Der Nutzer hat Sorge dafür zu tragen, dass Daten, die ausschließlich auf dem Gerät gespeichert werden, bei nächster Gelegenheit auf Datenspeicher übertragen werden, die der Arbeitgeber üblicherweise für die Speicherung von Unternehmensdaten verwendet.

Bei Fragen zu der Vorgehensweise der Übertragung der Daten hat sich der Nutzer an die IT-Abteilung zu wenden.

8. Ausnahmen

Der Arbeitgeber kann Ausnahmen von den vor genannten Grundsätzen in begründeten Einzelfällen erlauben. Genehmigte Ausnahmen sind inklusive einer Begründung zu dokumentieren:

☐
☐
☐

9. Sanktionen

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

10. Laufzeit dieser Vereinbarung

Diese Vereinbarung läuft unbefristet.

11. Änderung der Vereinbarung

Die Gewährung der Arbeit im „Mobilen Arbeiten“ steht im freien Ermessen des Arbeitgebers. Es entsteht kein Rechtsanspruch auf Gewährung für die Zukunft. Es können auch einzelne Bestandteile dieser Vereinbarung gekündigt werden ohne dass andere deshalb ihre Wirksamkeit verlieren.

D.9.2.11 Arbeitsanleitung zur Nutzung von Messenger-Diensten (Whattsapp)

Der Einsatz von WhatsApp und anderen Messenger-Diensten im Unternehmen ist mittels dieser Arbeitsanleitung geregelt. Eine darüber hinaus gehende Nutzung ist ausdrücklich untersagt und kann zu arbeitsrechtlichen Konsequenzen führen.

Bei der Nutzung von Whatsapp und anderen Messenger-Diensten auf den vom Unternehmen bereitgestellten Geräten gelten folgende Regeln:

1. Es ist bei der Kommunikation zwingend darauf zu achten, dass nur unkritische, personenbezogene Daten über den Messenger-Dienst verteilt werden dürfen.

2. Folgende beispielhaft aufgeführten Sachverhalte dürfen keinesfalls über den Messenger-Dienst mitgeteilt werden:
   - Krankmeldungen / Urlaubsscheine / Gesundheitsdaten.
   - Persönliche Unterlagen wie Gehaltsdaten / Mitarbeiter oder Kundendaten.
   - Weitere sensible Arten von Daten, die nicht in einen öffentlichen Raum gehören.

Zwar bieten Whatsapp und andere Messenger-Dienste eine eigene Verschlüsselung an, jedoch ist durch das Inkrafttreten der DSGVO im Mai 2018 insbesondere der Datenschutz verschärft worden. Durch die Zugehörigkeit von Whatsapp zum Facebook-Konzern ist keinesfalls sichergestellt, dass mit den Daten auf den Geräten datenschutzkonform umgegangen wird, außerdem liegt der Firmensitz datenschutzrechtlich in einem Drittland (USA).

Für die Nutzung von Whatsapp und anderen Messenger-Diensten gilt daher:
Senden Sie über diesen Dienst nur Daten, die allgemein /öffentlich auch zur Schau gestellt werden könnten (Postkartenprinzip). Wenn Sie Daten mit hoher Kritikalität von außerhalb erhalten, weisen Sie den Gesprächspartner ausdrücklich auf die Datenschutzbestimmungen hin und bieten einen anderen Kommunikationsweg (z.B. verschlüsselte E-Mail) an.

Bei Fragen zu der Arbeitsanleitung stehen Ihnen sowohl der interne Datenschutzkoordinator sowie der ext. Datenschutzbeauftragte als auch die Geschäftsleitung zur Verfügung.

D.9.5.2 Informationsschreiben zum Hinweisgeberschutzgesetz (HinSchG)

Sehr geehrte Damen und Herren,

mit diesem Schreiben möchten wir Sie über das erst kürzlich verabschiedetes Hinweisgeberschutzgesetz (HinSchG) und dessen Umsetzung innerhalb der hsde informieren.

Gesetzliche Grundlage

Das Gesetz wurde als Artikel 1 des Gesetzes v. 31.5.2023 I Nr. 140 vom Bundestag mit Zustimmung des Bundesrates beschlossen. Es tritt gem. Art. 10 Abs. 2 dieses Gesetzes am 2.7.2023 in Kraft.

Zielsetzung

Das Hinweisgeberschutzgesetz will einen umfassenden Schutz von „Whistleblowern“ sicherstellen.
„Whistleblower“, sind „HinweisgeberInnen“ - also Personen, die Hinweise auf Verstöße gegen gesetzliche Vorgaben oder Missstände in Unternehmen geben.

Dazu sieht das Gesetz folgende Maßnahmen vor:

- Unternehmen und Organisationen ab 50 Beschäftigten müssen sichere interne Hinweisgebersysteme installieren und betreiben.
- Whistleblower müssen die Möglichkeit erhalten, Hinweise mündlich, schriftlich oder auf Wunsch auch persönlich abzugeben.
- Wird ein Hinweis abgegeben, muss die interne Meldestelle dies dem Hinweisgeber innerhalb von sieben Tagen bestätigen.
- Binnen drei Monaten muss die Meldestelle den Whistleblower über die ergriffenen Maßnahmen informieren, beispielsweise über die Einleitung interner Untersuchungen oder die Weiterleitung einer Meldung an eine zuständige Behörde, etwa eine Strafverfolgungsbehörde.
- Als zweite, gleichwertige Möglichkeit zur Abgabe von Hinweisen wird beim Bundesamt für Justiz eine externe Meldestelle eingerichtet. Die Bundesländer können darüber hinaus eigene Meldestellen einrichten.
- Whistleblower können sich frei entscheiden, ob sie eine Meldung an die interne Meldestelle ihres Unternehmens abgeben oder die externe Meldestelle nutzen möchten. Misstände oder Verstöße die voraussichtlich innerhalb des Unternehmens behoben werden können sollen aber intern gemeldet werden.
- Auch anonymen Hinweisen soll nachgegangen werden.
- Zum Schutz der Whistleblower vor "Repressalien" enthält das Gesetz eine weitgehende Beweislastumkehr: Wird ein Whistleblower im Zusammenhang mit seiner beruflichen Tätigkeit "benachteiligt", wird vermutet, dass diese Benachteiligung eine Repressalie ist. Zudem kommen Schadensersatzansprüche des Whistleblowers aufgrund von Repressalien in Betracht.

Geschützter Personenkreis nach § 1 HinSchG:

- HinweisgeberInnen
  =natürliche Personen, die im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld einer beruflichen Tätigkeit Informationen über Verstöße erlangt haben und diese melden
- Personen, die Gegenstand einer Meldung oder Offenlegung sind,
- sonstige Personen, die von einer Meldung oder Offenlegung betroffen sind

ACHTUNG:
Den Schutz des HinSchG genießen nach § 33 nur Personen, die

- eine interne oder eine externe Meldung gemacht haben
  (oder im Ausnahmefall mit ihrer Meldung an die Öffentlichkeit gegangen sind, sog. Offenlegung, § 32 HinSchG) und
- bei ihrer Meldung hinreichenden Grund zu der Annahme haben, dass
  - die gemeldeten Informationen der Wahrheit entsprechen,
  - und die Informationen Verstöße betreffen, die in den Anwendungsbereich des Gesetzes fallen.

Ein Schutz für hinweisgebende Personen besteht nicht, wenn

- es sich um eine vorsätzliche oder grob fahrlässige Weitergabe unrichtiger Informationen handelt.
- In solchen Fällen ist die böswillige hinweisgebende Person sogar zum Ersatz des Schadens verpflichtet (§ 38 HinSchG).

Interne Meldestelle - an wen können HinweisgeberInnen sich wenden?

Um das Hinweisgeberschutzgesetz umzusetzen hat die hsde gGmbH zum 01.07.2023 eine interne Meldestelle eingerichtet. Wenn Sie also einen begründeten Hinweis auf Verstöße oder Missstände geben möchten können Sie diesen schriftlich, telefonisch oder auf expliziten Wunsch auch persönlich an diese richten. Die Meldung kann personalisiert oder auch anonym erfolgen.

Verantwortliche Stelle:
Hsde gGmbH
ZQM Verwaltung
Schimmelpfengstr. 4
34613 Schwalmstadt
Mail: Hinweisgeber@hsde.de

Stellv. verantwortliche Stelle:
Hsde gGmbH
ZQM Pflege
Schimmelpfengstr. 4
34613 Schwalmstadt
Mail: Hinweisgeber@hsde.de

Was passiert nach Eingang der Meldung?

Die interne Meldestelle

- bestätigt der hinweisgebenden Person den Eingang einer Meldung spätestens nach sieben Tagen,
- prüft, ob der gemeldete Verstoß in den sachlichen Anwendungsbereich nach § 2 fällt,
- hält mit der hinweisgebenden Person Kontakt,
- prüft die Stichhaltigkeit der eingegangenen Meldung,
- ersucht die hinweisgebende Person erforderlichenfalls um weitere Informationen und
- ergreift angemessene Folgemaßnahmen nach § 18.

Die interne Meldestelle gibt der hinweisgebenden Person innerhalb von drei Monaten nach der Bestätigung des Eingangs der Meldung oder, wenn der Eingang nicht bestätigt wurde, spätestens drei Monate und sieben Tage nach Eingang der Meldung eine Rückmeldung. Die Rückmeldung umfasst die Mitteilung geplanter sowie bereits ergriffener Folgemaßnahmen sowie die Gründe für diese.
Eine Rückmeldung an die hinweisgebende Person darf nur insoweit erfolgen, als dadurch interne Nachforschungen oder Ermittlungen nicht berührt und die Rechte der Personen, die Gegenstand einer Meldung sind oder die in der Meldung genannt werden, nicht beeinträchtigt werden.

Dokumentation

Jeder Hinweis zum HinSchG, auch wenn er abschließend nicht zu weiteren Maßnahmen führt, ist zwingend ausführlich zu dokumentieren. Die Dokumentation erfolgt durch die zuständige interne Meldestelle unter RS der GF und ggf. bei Bedarf des Datenschutzbeauftragten.

Sollten Sie Rückfragen haben können Sie sich gerne an unsere Einrichtungsleitungen, die Verwaltungen oder auch direkt an die interne Meldestelle wenden.