Datenschutzkonzept

1. Einleitung

Dieses Datenschutzkonzept beruht auf den in Art 5 Z 1 DSGVO formulierten Grundsätzen wie Zweckbindung, Datenminimierung, Speicherbegrenzung sowie Integrität, Recht auf Vergessenwerden und Vertraulichkeit und ist rechtmäßig (Art 6 DSGVO). Die von der DSGVO geforderte Einhaltung der Verordnungskonformität (Art. 5 Z 2; Art 24 Z 1), der Einhaltung der Betroffenenrechte (Art 13-20), der Meldepflicht bei Datenschutzverletzung (Art 33-34), der Nachweis- und Rechenschaftspflicht (Art 5 Z 2, Art 24 Z 1) ist gewährleistet. Ein Kontroll- und Verbesserungsprozess wird mindestens 1x jährlich durchgeführt (Art 32 Z 1), u.a. basierend auf der Checkliste, enthalten im letzten Kapitel dieses Datenschutzkonzeptes.

2. Sachliche und räumliche Tätigkeit

Wir verarbeiten als Kleinunternehmen (KU) personenbezogene Daten von natürlichen Personen ab dem 16. Lebensjahr (Art 8 DSGVO) ganz oder teilweise automatisiert und haben unsere Niederlassung in der EU: Stefan Rippler, Leharstraße 13, 81243 München.

3. Datenschutzbeauftragter (DSB) und Verantwortlicher für den Datenschutz

Trifft einer der nachfolgenden Kriterien zu, ist ein externer oder interner DSB notwendig und zu bestellen:

Kriterium	Ja	Nein
Verarbeitung der Daten durch eine Behörde oder eine öffentliche Stelle, mit Ausnahme der Gerichte		X
Verarbeitung der personenbezogenen Daten stellt eine Kerntätigkeit der Organisation dar und/oder erfordert eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Person		X
Verarbeitung besonders schutzwürdige Kategorien personenbezogenen Daten (Art 9 Z 1 DSGVO wie z. B. Gesundheitsdaten, ethische Herkunft, genetische bzw. biometrische Daten, Gewerkschaftszugehörigkeit, usw.) stellt eine Kerntätigkeit der Organisation dar		X

Referenzen: Art 37 DSGVO, Erwägungsgründe 97

Da für unser Kleinunternehmen keiner der obigen Kriterien zutrifft, wird kein DSB bestellt.
Der Verantwortliche und für den Datenschutz Zuständige ist:

Stefan Rippler
Leharstraße 13
81243 München

Referenzen: Art 4 Z 7 DSGVO

4. Weiterbildung und Stand der Technik

Aktivitäten	Veranstalter	sonstiges
Info- u. Weiterbildungsveranstaltungen	Webinare, etwa bei datenschutz-guru.de oder gruenderszene.de	regelmäßig
Homepages bzw. Newsletterfac	https://www.datenschutz.der	Homepage
	https://www.datenschutz-guru.de	Newsletter
	https://www.datenschutz-praxis.de/newsletter-widget/	Newsletter
	https://www.drschwenke.de	Homepage

Referenzen: Art 4, 5-11 DSGVO

5. Sensibilisierung der Mitarbeitenden / Dienstleister

Besonders wichtig ist die Sensibilisierung aller relevanten Mitarbeitenden, der wir natürlich nachkommen. Nur mit informierten und acht-samen Mitarbeitenden können Sicherheitsmaßnahmen wirksam umgesetzt und eventuelle Sicherheitsvor-fälle rechtzeitig erkannt werden.
Sobald die Ursache eines Sicherheitsvorfalls identifiziert wurde, müssen Maßnahmen zu dessen Behebung ergriffen werden. Häufig ist es notwendig, die betroffenen IT-Systeme oder Standorte zu isolieren, um die Auswirkung des Sicherheitsvorfalls einzudämmen. Die Behebung von Sicherheitsvorfällen muss ausführlich dokumentiert werden.
Ein Beispiel für eine Sensibilisierung / Verpflichtung auf Einhaltung der DSGVO der Mitarbeitenden befindet sich im Anhang. Ebenfalls im Anhang: Ein Mustervertrag zur Auftragsdatenverarbeitung.

6. Datenverarbeitungen/Datenverarbeitungszwecke

Zwecke und Beschreibung der Datenverarbeitungen:

1. **Rechnungswesen und Geschäftsabwicklung**: Verarbeitung und Übermittlung von Daten im Rahmen von Geschäftsbeziehungen mit Kunden und Lieferanten, sowie an der Geschäftsabwicklung mitwirkende Dritte und Geschäftspartner inkl. deren jeweiligen Kontaktpersonen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z. B. Rechnungen, Korrespondenzen oder Verträge) in diesen Angelegenheiten
2. **Kundenbetreuung und Marketing**: Serviceorientierte Information und Betreuung von kategorisierten Kunden, Lieferanten und an der Geschäftsabwicklung mitwirkende Dritte bzw. Geschäftspartner inkl. deren jeweiligen Kontaktpersonen und Interessenten einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) sowie Übermittlung von Newsletter, Serienbriefe und Infomaterial.
3. **Betrieb von Internetseiten**:
    a. Übermittlung von Daten im Rahmen des Stellenmarktes (Firmenname, Ansprechpartner, Telefonnummer, Webseitenadresse, Stellenbeschreibung, Lebenslauf, Adresse, Benutzername, Passwort) – gilt nur für berufsziel-socialmedia.de
    b. Newsletter-Versand: Information an Interessenten und Kunden zum Thema Social Media. Regelmäßig neue Info über Blogartikel, neue Stellenangebote – gilt nur für berufsziel-socialmedia.de
    c. Webseitenanalyse: Analyse des anonymisierten Besucherverhaltens auf der Webseite zur Optimierung und Nachvollziehbarkeit der Seitenbesuche (z.B. Einstiegs- und Ausstiegsseiten, Verweildauer…)
    d. Kommentarfunktion: Webseitenbesucher können Kommentare zu einem Blogartikel hinterlassen und dadurch eine Diskussion anstoßen oder sich daran beteiligen. Speicherung der IP-Adresse, E-Mail Adresse und des Kommentars. Adressen auf Blacklisten können dadurch als Spam identifiziert werden – gilt nur für berufsziel-socialmedia.de
    e. Gravatar: Einbindung von eigenen Profilbildern des Kommentierenden bei Webseiten Kommentaren. Der Betroffene registriert sich freiwillig bei Gravatar und hinterlegt dort sein Profilbild. Die Profilbilder werden aktuell beim Aufruf geladen und nicht auf der Webseite des Betreibers gespeichert – gilt nur für berufsziel-socialmedia.de
    f. Kontaktformular: Kontaktanfrage über die Webseite für Interessenten und Kunden zur Beantwortung einer spezifischen Anfrage / Frage – gilt für rippler-verlag.de, berufsziel-socialmedia.de, stiftung-dia.de, fasel.de, corneliasachs.com, eutonie.de
    g. Affiliate-Programme: Durch individualisierte Links der Affiliate Partner werden durch Werbekosteneinnahmen beim Kauf des Kunden Einnahmen generiert. Die Daten des Betroffenen werden durch den Affiliate Partneran den Verkäufer zur Abwicklung des Kaufs weiter gegeben. Als Affiliate Partner haben wir keinen Zugriff auf die personenbezogenen Daten des Käufers – gilt nur für berufsziel-socialmedia.de, berufsziel-pr.de, tool.porn, rippler-verlag.de, fasel.de
    h. Mitgliederbereich: User können sich auf der Webseite einloggen, um einen Mitgliederbereich zu besuchen (Blog, Fotos, Dokumente) sowie ihr Profil und ihre Kurse zu editieren – gilt nur für eutonie.de

7. Datenschutz-Folgenabschätzung durchgeführt?

Eine Datenschutz-Folgenabschätzung ist nicht durchzuführen, da sowohl aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung voraussichtlich kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht, da keine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen erfolgt und da keine umfangreichen Verarbeitung sensibler Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen oder Straftaten erfolgt. Es gibt auch keine Überwachung öffentlich zugänglicher Bereiche durch Video.

Referenzen: Art 35 Z1-3 DSGVO

8. Beschreibung der technisch-organisatorischen Maßnahmen (TOMs)

Smartphone

Maßnahmen, die geeignet sind, Unbefugten den Zugang zu personenbezogenen Daten zu verwehren.

X	Verlorene Geräte werden über den Mobilfunkanbieter umgehend gesperrt	X	Vertrauliche Daten, wie personenbezogene Daten oder Zugangsdaten werden prinzipiell nicht auf den Geräten gespeichert
X	Sicherheitsmechanismen (z. B. Eingabe einer PIN oder eines Passworts, Fingerabdruck, etc.) werden genutzt	X	Eine unumgängliche Speicherung personenbezogener Daten auf dem Gerät (inklusive Speicherkarte) erfolgt ausschließlich in verschlüsselter Form
X	Es werden nur WPA2-verschlüsselte WLAN-Netzwerke verwendet	X	Das Versenden von vertraulichen Daten darf nur über verschlüsselte Systeme erfolgen. Nicht dazu gehören Whatsapp, Facebook und Skype
X	Bluetooth ist standardmäßig deaktiviert und darf nur zur Verbindung mit firmeneigenen Geräten aktiviert werden		

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

	Alarmanlage	X	Absicherung von Gebäudeschächten
	Automatisches Zugangskontrollsystem		Chipkarten-/Transponder-Schließsystem
	Schließsystem mit Codesperre	X	Manuelles Schließsystem
	Biometrische Zugangssperren		Videoüberwachung der Zugänge (eigenes Verfahrensverzeichnis notwendig!)
	Lichtschranken / Bewegungsmelder	X	Sicherheitsschlösser
X	Schlüsselregelung (Schlüsselausgabe etc.)		Personenkontrolle beim Pförtner / Empfang
	Protokollierung der Besucher		Sorgfältige Auswahl von Reinigungspersonal
	Sorgfältige Auswahl von Wachpersonal		Tragepflicht von Berechtigungsausweisen
X	Verschlossene Türen bei Abwesenheit		Fenstersicherung (Erdgeschoss)
X	Automatische Bildschirm-Sperre nach 10 Minuten		

Zugangskontrolle
Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

X	Zuordnung von Benutzerrechten	X	Erstellen von Benutzerprofilen
X	Passwortvergabe		Authentifikation mit biometrischen Verfahren
X	Authentifikation mit Benutzername / Passwort	X	Zuordnung von Benutzerprofilen zu IT-Systemen
	Gehäuseverriegelungen		Richtlinien für Passwörter/Löschen/Clean-desk
	Sperren von externen Schnittstellen (USB etc.)	X	Sicherheitsschlösser
X	Schlüsselregelung (Schlüsselausgabe etc.)		Personenkontrolle beim Pförtner / Empfang
	Protokollierung der Besucher		Sorgfältige Auswahl von Reinigungspersonal
	Sorgfältige Auswahl von Wachpersonal		Tragepflicht von Berechtigungsausweisen
X	Einsatz von Intrusion-Detection-Systemen	X	Verschlüsselung von mobilen Datenträgern
X	Verschlüsselung von Smartphone-Inhalten		Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
X	Einsatz von Anti-Viren-Software	X	Verschlüsselung von Datenträgern in Laptops / Notebooks/USB
	Einsatz einer Hardware-Firewall	X	Einsatz einer Software-Firewall

Zugriffskontrolle
Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

X	Erstellen eines Berechtigungskonzepts	X	Verwaltung der Rechte durch Systemadministrator
X	Anzahl der Administratoren auf das „Notwendigste“ reduziert	X	Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel (Das Passwort muss mindestens 15 Zeichen lang sein, Großbuchstaben, Kleinbuchstaben und Sonderzeichen enthalten und alle zwei Monate geändert werden)
X	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	X	Sichere Aufbewahrung von Datenträgern (Data-Safe)
X	physische Löschung von Datenträgern vor Wiederverwendung	X	ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
	Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)		Protokollierung der Vernichtung
X	Verschlüsselung von Datenträgern		

Weitergabekontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

X	Einrichtungen von Standleitungen bzw. VPN-Tunneln	X	Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
X	E-Mail-Verschlüsselung bzw. www.signal.org Nutzung von Signaturverfahren		Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen (siehe Verarbeitungsverzeichnis)
X	Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen (siehe Verarbeitungsverzeichnis)		Beim physischen Transport: sichere Transportbehälter/-verpackungen
	Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen	X	Verschlüsselung der übertragenen Daten

Eingabekontrolle
Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

X	Protokollierung der Eingabe, Änderung und Löschung von Daten	X	Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. (siehe Verarbeitungsverzeichnis)
X	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen	X	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
X	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	X	Klare Zuständigkeiten für Löschungen (siehe Verfahrensverzeichnis)

Auftragskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

X	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten	X	vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen (Sollte ein Datenschutzkonzept haben!)
X	schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) siehe Anhang	X	Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (im Anhang)
X	Ob Auftragnehmer hat Datenschutzbeauftragten bestellt hat	X	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
X	Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart	X	laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
X	Vertragsstrafen bei Verstößen		

Verfügbarkeitskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

	Unterbrechungsfreie Stromversorgung (USV)		Klimaanlage in Serverräumen
	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen	X	Schutzsteckdosenleisten
	Feuer- und Rauchmeldeanlagen		Feuerlöschgeräte in Serverräumen
	Alarmmeldung bei unberechtigten Zutritten zu Serverräumen	X	Erstellen eines Backup- & Recoverykonzepts
X	Testen von Datenwiederherstellung		Erstellen eines Notfallplans
X	Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort		Serverräume nicht unter sanitären Anlagen
	In Hochwassergebieten: Serverräume über der Wassergrenze		

Trennungsgebot
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

X	physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern		Logische Mandantentrennung (softwareseitig)
X	Erstellung eines Berechtigungskonzepts		Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
	Versehen der Datensätze mit Zweckattributen/Datenfeldern	X	Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
	Festlegung von Datenbankrechten		Trennung von Produktiv- und Testsystem

Quelle: https://www.datenschutz-guru.de/files/**Ausfuellhilfe_TOM_9_BDSG_V2**.docx

9. Impressum und Datenschutzerklärungen

DSGVO-konform auf allen betriebenen (Kunden-)Webseiten, erreichbar unter den folgenden Links:

- https://rippler-verlag.de/2/datenschutzerklaerung/
- https://berufsziel-socialmedia.de/blog/impressum/
- http://berufsziel-pr.de/impressum/
- http://stiftung-dia.de/cms/impressum/
- http://erloeserkirche-marquartstein.de/cms/kontakt/impressum/
- http://oztralien.de/impressum/
- https://www.eutonie.de/impressum/
- http://fasel.de/kontakt/leitung/impressum/
- http://corneliasachs.com/impressum-und-datenschutz/

10. Betroffenenrechte wahren

Grundsätzlich stellen wir jedem Nutzer bzw. Betroffenen die jeweils aktuelle Version unseres Datenschutzkonzeptes auf unserer Homepage im Sinne von Transparenz und Vertrauen zum Download bereit (https://rippler-verlag.de/2/datenschutzerklaerung/).

Gemäß der DSGVO hat jeder Betroffene folgende Rechte:

- Recht auf Auskunft (Art 15 DSGVO)
- Recht auf Berichtigung (Art 16 DSGVO)
- Recht auf Löschung (Art 17 DSGVO)
- Recht auf Einschränkung (Art 18 DSGVO)
- Recht auf Übertragbarkeit (Art 20 DSGVO)
- Recht auf Widerspruch (Art 21 DSGVO)
- Recht auf Beschwerde bei der Datenschutzbehörde

10.1. Betroffenenrechte: Prozessketten

Wir erhalten Kenntnis, dass ein Betroffener seine Rechte geltend machen will, sei es z. B. mündlich, schriftlich, oder per E-Mail (insbesondere datenschutz@.....),

- Sollte der Betroffene mir nicht persönlich bekannt sein, so muss ich zwecks Vermeidung einer Datenschutzverletzung die Identität des Antragsstellers (Betroffenen) feststellen:
  „Sehr geehrte Frau/Herr ...,
  Da wir Sie leider noch nicht persönlich kennen lernen durften, bitten wir Sie, um keine Datenschutzverletzung zu begehen – wie z. B. personenbezogene Daten an eine falsche Person weiterzuleiten – uns eine Kopie/Scan Ihres Personalausweises/Reisepasses zukommen zu lassen.
  Ihrer Bitte in Sachen Datenschutz werden wir dann umgehend nachkommen.
  Wir danken Ihnen für Ihr Verständnis.
  Mit freundlichen Grüßen,
  P.S.: Unser aktuelles Datenschutzkonzept finden Sie hier: https://rippler-verlag.de/2/datenschutzerklaerung/
- Identität kann nicht zweifelsfrei festgestellt werden und der Betroffene meldet sich trotz Information darüber nicht mehr: => Keine Aktivitäten notwendig.
- Identität zweifelsfrei festgestellt und Anfrage ist rechtens:
  - ⇨ Der Betroffene bekommt gemäß Art 19 DSGVO innerhalb von maximal 14 Tagen abhängig von seiner Anfrage in klarer und verständlicher Sprache folgende Antworten:
    - Recht auf Auskunft (Art 15 DSGVO)
      - Der Betroffene bekommt als PDF sein Stammdatenblatt mit allen personenbezogenen Daten (Screenshot)
    - Recht auf Berichtigung (Art 16 DSGVO)
      - Der Betroffene bekommt als PDF sein Stammdatenblatt mit den berichtigten personenbezogenen Daten (Screenshot)
    - Recht auf Löschung (Art 17 DSGVO)

- Der Betroffene bekommt als PDF sein Stammdatenblatt ohne personenbezogene Daten (ausgenommen Name) als Nachweis, dass die Löschung erfolgt ist mit dem Hinweis, dass
    - die Daten anonymisiert für die interne Statistik verwendet werden
    - nach Kopie des Stammdatenblattes auch das ganze Stammdatenblatt inklusive Namen unwiderruflich gelöscht wurde (Screenshot)
    - oder bei einem bestehenden oder abgeschlossenem Vertrag mit dem Betroffenen werde ich alle Daten löschen (~ Marketingdaten) bis auf jene, wo wir nach Art 6 Z 1 lit f ein berechtigtes Interessen des Verantwortlichen bzw. lit c (gesetzliche Verpflichtungen z. B. nach der BAO und dem UGB; vor allem Buchhaltungsunterlagen) DSGVO geltend machen können und wir werden daher aufgrund der gesetzlichen Aufbewahrungsfristen diese Daten auf jeden Fall erst nach 7 Jahren löschen; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen die personenbezogen Daten löschen.
    - In diesen Fällen tritt an Stelle einer Löschung der Buchhaltungsdaten eine Sperrung (Einschränkung).

- Recht auf Einschränkung (Art 18 DSGVO)
    - Der Betroffene bekommt als PDF sein Stammdatenblatt, dem er entnehmen kann, dass bei „Recht auf Einschränkung geltend gemacht“ ein Haken gesetzt ist und somit keine Verarbeitung seiner personenbezogenen Daten erfolgt. (Screenshot)
- Recht auf Übertragbarkeit (Art 20 DSGVO)
    - Der Betroffene bekommt als PDF sein Stammdatenblatt mit allen personenbezogenen Daten (als PDF, da es maschinell lesbar sein sollte)
    - gemäß Art 20 Z2 DSGVO übermittle ich sein Stammdatenblatt mit allen personenbezogenen Daten per CC an einen anderen Verantwortlichen, den der Betroffene mir genannt hat per E-Mail, aber nur über eine sichere und verschlüsselte Übertragung. Ansonsten ausgedruckt per eingeschriebenen Brief auf Kosten des Betroffenen.
- Recht auf Beschwerde bei der Datenschutzbehörde

10.2. Meldung von Datenschutzverletzungen: Prozesskette

Die DSGVO definiert in Art. 33 eine „Verletzung des Schutzes personenbezogener Daten“ (Data-Breach) als eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

- Wir erlangen Kenntnis von einer Datenschutzverletzung.
- Innerhalb von 72 Stunden melden wir mit Hilfe des „Muster-Datenschutzverletzungsmitteilung“ (siehe Anhang) an die gemäß Art 55 DSGVO zuständige Aufsichtsbehörde, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
- Wir informieren Betroffene umgehend mit einem Anschreiben und einer Kopie der Meldemitteilung an die Datenschutzaufsichtsbehörde.
- Wir werden alle Verletzungen des Schutzes personenbezogener Daten einschließlich aller damit im Zusammenhang stehenden Fakten (Auswirkungen, ergriffene Abhilfemaßnahmen) dokumentieren. Diese Dokumentation dient der Aufsichtsbehörde zur Überprüfung der korrekten Einhaltung der Meldepflicht, siehe Art 33 Z5 DSGVO.

11. Checkliste für den jährlichen Kontroll- und Verbesserungsprozess

Die folgende Checkliste dient als Umsetzungshilfe für die Prüfung und Dokumentation des Umsetzungszustandes der Sicherheitsmaßnahmen für kleine Einrichtungen. Die Checkliste kann ebenso als Nachweis der Bemühungen zur Umsetzung der IT-Sicherheit verwendet werden.

Nr.	Frage	Verbesserungsbedarf	OK
1.	Werden neue Mitarbeitende bei der Einstellung auf bestehende Rege-lungen und Handlungsanweisungen zur Informationssicherheit hinge-wiesen?		□
2.	Sind die wichtigen Schlüsselpositionen durch einen Vertreter besetzt?		□
3.	Haben alle Mitarbeitenden eine Verpflichtung zur Wahrung des Daten-geheimnisses unterschrieben?		□
4.	Werden Backup-Datenträger in einem gesonderten Raum aufbewahrt?		□
5.	Sind auf allen Clients Virenschutzprogramme installiert?		□
6.	Werden Betriebssysteme und Anwendungen regelmäßig aktualisiert?		□
7.	Gibt es eine Checkliste für Mitarbeitende zur Beendigung des Arbeits-verhältnisses?		□
8.	Gibt es eine Benutzer- und Rechteverwaltung für IT-Systeme und An-wendungen?		□
9.	Gibt es Passwortregelungen für IT-Systeme und Anwendungen und werden diese umgesetzt?		□
10.	Werden alle Mitarbeitenden über die Regelungen zur Nutzung von Standardsoftware informiert?		□
11.	Wird ausschließlich Software aus vertrauenswürdigen Quellen instal-liert?		□
12.	Gibt es regelmäßige Kontrollen bezüglich der installierten Software?		□
13.	Sind auf Clients und Servern automatische Updates aktiviert?		□
14.	Gibt es spezielle Handlungsanweisungen und Tools zum Löschen und Vernichten von Daten?		□
15.	Sind Türen und Fenster in der Regel verschlossen, wenn die Mitarbei-tenden nicht am Platz sind?		□
16.	Sind in den Büros verschließbare Schreibtische oder Schränke vorhan-den?		□
17.	Gibt es in Büros mit Publikumsverkehr Diebstahlsicherungen für IT-Systeme?		□
18.	Sind am mobilen Arbeitsplatz verschließbare Schreibtische oder Schränke vorhanden?		□
19.	Gibt es Regelungen welche dienstlichen Unterlagen am häuslichen Arbeitsplatz bearbeitet und zwischen der Institution und dem häuslichen Arbeitsplatz hin und her transportiert werden dürfen?		□
20.	Ist auf allen Clients die Bildschirmsperre aktiviert?		□
21.	Ist der Zugriff von mobilen Laptops auf das LAN per VPN abgesichert?		□
22.	Ist die Verschlüsselung von E-Mail-Kommunikation zwischen Client und Server aktiviert?		□
23.	Ist bei allen Mobiltelefonen/Smartphones die Eingabe der Geräte-PIN aktiviert?		□
24.	Werden alle vertraulichen Daten nur verschlüsselt auf Mobiltelefonen/Smartphones oder Speicherkarten gespeichert?		□
25.	Wird bei WLAN das Verschlüsselungsverfahren WPA2 eingesetzt?		□
26.	Werden die Schlüssel für den WLAN-Zugriff regelmäßig gewechselt?		□

Zusammenfassung

Wir sehen das hier dokumentierte Datenschutzniveau mit den gesetzten TOMs für uns als Kleinunternehmen auch aufgrund unserer finanziellen, technischen und organisatorischen Beschränkungen als angemessen und ausreichend an.
Wir können also meinen Kunden mit gutem Gewissen sagen:

Liebe Kundin, lieber Kunde, liebe Interessentin, lieber Interessent!
Vertrauen ist die Grundlage und Voraussetzung für unsere Beratungs- und Produktionsleistungen. Daher sind auch alle Ihre persönlichen und beruflichen Daten bei uns in guten Händen.

Wir sichern Ihnen zu, dass wir sorgsam und streng vertraulich damit umgehen und unsere Datenschutzmaßnahmen immer dem aktuellen Gesetzesstand entsprechen und unsere Soft- und Hardware stets auf dem aktuellsten Stand sind.

Darauf können Sie vertrauen.

13.05.18, München	Die digitale Version des Datensicherheitskonzepts ist ohne Unterschrift gültig
Datum, Ort	Unterschrift

Hinweis: Ein Original dieses Datensicherheitskonzepts mit Unterschrift ist in unserem Archiv abgelegt.

Anhang

Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutzgrundverordnung (DSGVO)

Frau/Herr _____

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

a) auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
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;
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;
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“);

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 habe ich erhalten.

_____ _____

Ort, Datum Unterschrift des Verpflichteten Unterschrift des Verantwortlichen

Merkblatt zum Datengeheimnis
Art. 4 DSGVO Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. „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 identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;
2. „Verarbeitung“ 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;

Strafvorschriften des § 42 DSAnpUG-EU (BDSG-neu)

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,
    a) einem Dritten übermittelt oder
    b) 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,
    c) ohne hierzu berechtigt zu sein, verarbeitet oder
    d) durch unrichtige Angaben erschleicht

    und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.
3. Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.

Vereinbarung Auftragsverarbeitung nach Art 28 DSGVO

zwischen xxx

– Auftraggeber –

und xxx

– Auftragnehmer –

über Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO).

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Vertrag vom xxx in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung (Anmerkung: Bitte ausfüllen , sofern noch nicht im Vertrag geregelt, andernfalls streichen):

Art der Daten	Art und Zweck der Datenverarbeitung	Kategorien der betroffenen Personen
...	...	...

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).
Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

1. Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz- Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese

technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfter Wirksamkeit wird auf die vorliegende Zertifizierung nach Art. 42 DS-GVO verwiesen, deren Einhaltung durch den Auftragnehmer am tt.mm.jjjj geprüft und bestätigt wurde.
Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3. Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Artt. 33 bis 36 DS-GVO genannten Pflichten. (Anmerkung: Im Vertrag können die Parteien hierzu eine Vergütungsregelung treffen).
4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
5. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
6. Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.
7. Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
8. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.
9. Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.
10. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

§ 4 Pflichten des Auftraggebers

1. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
2. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend.
3. Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

1. Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.
2. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Der Auftraggeber stimmt der Benennung eines unabhängigen externen Prüfers durch den Auftragnehmer zu, sofern der Auftragnehmer eine Kopie des Auditberichts zur Verfügung stellt.
3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

1. Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.
2. Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten. Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt:

Name und Anschrift des Subunternehmers	Beschreibung der Teilleistungen
...	...

   Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer holt der Auftragnehmer die Zustimmung des Auftraggebers ein, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf. Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund – gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

3. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.
2. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

3. Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.
4. Es gilt deutsches Recht.

§9 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

[Ort], am [Datum]		[Ort], am [Datum]
Für den Auftraggeber:		Für den Auftragnehmer:
..... [Name samt Funktion]		..... [Name samt Funktion]

Muster-Datenschutzverletzungsmitteilung: Mitteilung einer unrechtmäßigen Datenübermittlung bzw. unrechtmäßigen Kenntniserlangung von Daten durch Dritte gemäß Art. 33 Abs. 3 DSGVO an die Datenschutzaufsichtsbehörde

Sehr geehrte Damen und Herren,

mit nachfolgenden Angaben informieren wir Sie gemäß § 42a BDSG bzw. § 15a TMG über die unrechtmäßige Datenübermittlung bzw. unrechtmäßige Kenntniserlangung von Daten durch Dritte:

1. Name der meldepflichtigen bzw. verantwortlichen Stelle

_____

(Vollständige Bezeichnung inklusive Adresse)

2. Name und Kontaktdaten des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners für weitere Informationen

_____

(Name und Position des Ansprechpartners)

3. Zeitraum oder Zeitpunkt des Vorfalls

_____

(Möglichst „exakte“ Zeitangabe)

4. Zeitpunkt der Feststellung des Vorfalls

_____

(Möglichst „exakte“ Angabe, wann und wie vom Vorfall Kenntnis erlangt wurde)

5. Ursache bzw. Ort der Datenpanne

_____

(Möglichst „exakte“ Sachverhaltsbeschreibung)

6. Welche Dritten haben Kenntnis erlangt bzw. hatten Möglichkeit zur Kenntnisnahme?

_____

(Möglichst „exakte“ Benennung des relevanten Personenkreises)

7. Art und Inhalt der betroffenen personenbezogenen Daten

(Zutreffende ankreuzen)

- ☐ Besondere Arten von Daten im Sinne von Art. 9 DSGVO
- ☐ Einem Berufsgeheimnis unterliegende Daten (siehe § 203 Abs. 1 StGB)
- ☐ Daten zu Straftaten oder Ordnungswidrigkeiten, einschließlich Verdacht darauf
- ☐ Daten zu Bank- oder Kreditkartenkonten
- ☐ Telemedien-Bestands- oder -Nutzungsdaten (einschließlich Zugangsdaten, Passworte), § 15a TMG

Ggf. nähere Erläuterungen hierzu:

_____

8. Technische und organisatorische Maßnahmen, die die meldepflichtige Stelle wegen der Datenpanne in Bezug auf die betroffenen personenbezogenen Daten ergriffen hat (oder ergreifen wird)

_____

(Möglichst „exakte“ Beschreibung, was bereits veranlasst wurde und was zu einem späteren Zeitpunkt -wann- noch veranlasst werden soll)

9. Anzahl der Betroffenen (ggf. Schätzung)

_____

10. Mögliche Folgen bzw. nachteilige Auswirkungen für Betroffene (z. B. finanzieller Schaden, Ruf- /Imageschädigung, Bloßstellung)

_____

(Möglichst „exakte“ Einschätzung der Folgen bzw. Auswirkungen, die für die Betroffenen durch die Datenpanne drohen können)

11. Benachrichtigung der Betroffenen

- ☐ Benachrichtigung ist bereits erfolgt am _____ (Datum) per _____ (Kommunikationsmittel)
- ☐ Benachrichtigung ist geplant für _____ (Datum)

Als Anhang zu dieser Meldung ist die Benachrichtigung der Betroffenen über die Datenpanne im Originaltext beizulegen.

_____ _____

Datum Unterschrift