[Name]
[Adresse]
[PLZ, Ort]
[Datum der letzten Änderung]

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

Verantwortlicher gemäß Art 30 Abs 1 DSGVO

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Gemäß Art 32 DSGVO hat der Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitungen sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen geeignete technische und organisatorische Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dazu zählen insbesondere folgende allgemeinen technischen und organisatorischen Maßnahmen, wobei insbesondere die mit der Datenverarbeitung zusammenhängenden Risiken (etwa unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugte Offenlegung oder unbefugter Zugang) zu berücksichtigen sind. Die Überschriften in der Beschreibung unten dienen lediglich der besserein Einordnung und haben keinen Einfluss auf das Ausmaß der jeweiligen Maßnahme:

Anmerkung WKO Gesundheitsberufe: beispielhaft ausgefüllt, bitte korrigieren und gegebenenfalls auch ergänzen

1. ALLGEMEINES

Gemäß Art 32 DSGVO können insbesondere folgende allgemeinen Sicherheitsmaßnahmen getroffen werden:

	Pseudonymisierung personenbezogener Daten
	Verschlüsselung personenbezogener Daten
X	Dauerhafte Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Datenverarbeitung
X	Verfügbarkeit der personenbezogenen Daten und Zugang zu ihnen bei einem phsyischen oder technischen Zwischenfall rasch wiederherstellbar
X	Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung
	Einhaltung genehmigter Verhaltensregeln gemäß Art 40 DSGVO
	Einhaltung eines genehmigten Zertifizierungsverfahrens gemäß Art 42 DSGVO
X	Sicherstellung, dass die dem Verantwortlichen unterstellen natürlichen Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten

2. ZUTRITTSKONTROLLE/-BESCHRÄNKUNG

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu den Verarbeitungstätigkeiten und den personenbezogenen Daten zu verwehren.

X	Alarmanlage
	Zugangskontrollsystem
	Schließsystem mit Codesperre
	Biometrische Zugangssperren
	Lichtschranken / Bewegungsmelder

X	Absicherung von Gebäudeschächten
	Chipkarten-/Transponder-Schließsystem
	Manuelles Schließsystem
	Videoüberwachung der Zugänge
X	Sicherheitsschlösser

[Name]
[Adresse]
[PLZ, Ort]
[Datum der letzten Änderung]

X	Schlüsselregelung (Schlüsselausgabe etc)		Personenkontrolle beim Pförtner/Empfang
	Protokollierung der Besucher		Tragepflicht von Berechtigungsausweisen
	Festlegung von Sicherheitszonen		Absicherung der Sicherheitszonen durch ein Ausweislesesystem
	closed-shop-/closed-user-Betrieb für das Rechenzentrum		Zutrittsregelung und Protokollierung für das Datenträgerarchiv
	Sorgfältige Auswahl von Wachpersonal		Sorgfältige Auswahl von Reinigungspersonal
x	versperrbarer Aktenschrank		sonstige:

3. ZUGANGSKONTROLLE/-BESCHRÄNKUNG

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

	Zuordnung von individuellen Benutzerrechten		Erstellen von individuellen Benutzerprofilen mit jeweiligen Zugriffsberechtigungen
	Pseudonymisierung der Daten		Verschlüsselung der Daten
	Authentifikation mit individuellem Benutzernamen / Passwort		Authentifikation mit biometrischen Verfahren
	Personenkontrolle beim Pförtner/Empfang	**X**	Zuordnung von Benutzerprofilen zu IT-Systemen
	Gehäuseverriegelungen der IT Devices		Einsatz von VPN-Technologie
X	Sperrung von externen Schnittstellen (zB USB) - Data Leak Prevention		Sorgfältige Auswahl von Reinigungspersonal
	Schlüsselregelung (Schlüsselausgabe etc)		Sicherheitsschlösser
	Protokollierung der Besucher		Tragepflicht von Berechtigungsausweisen
	Sorgfältige Auswahl von Wachpersonal		Verschlüsselung von mobilen Datenträgern
	Einsatz von Intrustion-Detection-Systemen	**X**	Verschlüsselung von Datenträgern in Laptops / Notebooks
	Verschlüsselung von Smartphone-Inhalten		Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
	Einsatz von Anti-Viren-Software		Einsatz einer Software-Firewall
	Einsatz einer Hardware-Firewall		Nachverfolgung (Tracking) des Nutzerverhaltens
	Sonstige:		

4. ZUGRIFFSKONTROLLE/-BESCHRÄNKUNG

Maßnahmen, die gewährleisten, dass die zur Benutzung der Verarbeitungstätigkeiten Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

[Name]
[Adresse]
[PLZ, Ort]
[Datum der letzten Änderung]

X	Berechtigungskonzept mit individuellem Zugriffsberechtigungssystem und Passwortschutz		Protokollierung von Zugriffen auf Anwendungen und Daten, insb bei Eingabe, Änderung und Löschung von Daten
	Anzahl der Administratoren auf das Notwendigste reduziert	X	Passwortrichtlinie inkl Passwortlänge, regelmäßiger Passwortwechsel
	Protokollierung der Vernichtung		Sichere Aufbewahrung von Datenträgern
	physische Löschung von Datenträgern vor Wiederverwendung		ordnungsgemäße Vernichtung von nicht mehr benötigten Datenträgern
	Automatische Protokollierung insb unberechtigter Zugriffe		Aktuelle Verschlüsselungssoftware
	Einsatz von Aktenvernichtern bzw geeigneten Dienstleistern		Analyse der Protokolle über unbefugte Zugriffe durch die Revision
X	Verschlüsselung von Daten und Datenträgern (client- und serverseitig)		Protokollierung der Vernichtung
	Regelmäßige Auswertung sämtlicher Logfiles auf Angriffe und Datenlecks		Aktuellste Firewal, Viren- und Trojanerschutz
	Monitoring der Server und sonstiger IT-Systeme in Echtzeit		Bewertung der IT von Geschäftspartnern
	Datenspeicherung in zertifizierten Rechenzentren		Sensibilisierung und Schulung der Mitarbeiter
	Verwaltung der Zugriffsrechte durch den Systemadministrator	X	Möglichkeit für IT Nutzer, Zugriffe durch andere einzuschränken
	Sonstige:		

5. WEITERGABEKONTROLLE/-BESCHRÄNKUNG

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der Übermittlung oder Speicherung auf einem Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung welcher personenbezogener Daten vorgesehen ist oder stattgefunden hat.

	Einrichtung von Standleitungen bzw VPN-Tunneln		Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
X	Keine Datenweitergabe außerhalb des Europäischen Wirtschaftsraumes	X	Übersicht aller tatsächlichen Abruf- und Übermittlungsvorgänge
X	Verschlüsselungssoftware		E-Mail-Verschlüsselung
	Sonstige:		

6. EINGABEKONTROLLE

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

[Name]
[Adresse]
[PLZ, Ort]
[Datum der letzten Änderung]

	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)	**X**	Übersicht, aus der sich ergibt, mit welchen Applikationen welche Nutzer welche Daten eingeben, ändern und löschen können
X	Protokollierung/Dokumentation der Eingabe, Änderung, Entfernung und Löschung von Daten		Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts		
	Sonstige:		

7. VERFÜGBARKEITSKONTROLLE

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei Zwischenfällen rasch wiederhergestellt werden können.

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

8. 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 Berechtigungs-/Zugriffskonzepts		Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
	Versehen der Datensätze mit individualisierten Zweckattributen	**X**	Pseudonymisierung (insb Trennung der Zuordnungsdaten und der Aufbewahrung auf einem getrennten, abgesicherten System)
	Festlegung von Datenbankrechten		Trennung von Produktiv- und Testsystem

[Name]
[Adresse]
[PLZ, Ort]
[Datum der letzten Änderung]

	Sonstige:

9. WEITERE DATENSICHERHEITSMAßNAHMEN
