DSB-5seenland

Technische und organisatorische Maßnahmen (TOM)

i.S.d. Art. 32 DSGVO

Der Organisation

XXXXXXX

Stand XXX

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die o.g. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Alarmanlage		Schlüsselregelung / Liste
	Automatisches Zugangskontrollsystem		Empfang / Rezeption / Pförtner
	Biometrische Zugangssperren		Besucherbuch / Protokoll der Besucher
	Chipkarten / Transpondersysteme		Mitarbeiter- / Besucherausweise
X	Manuelles Schließsystem		Besucher in Begleitung durch Mitarbeiter
X	Sicherheitsschlösser		Sorgfalt bei Auswahl des Wachpersonals
	Schließsystem mit Codesperre	X	Sorgfalt bei Auswahl Reinigungsdienste
	Absicherung der Gebäudeschächte		
X	Türen mit Knauf Außenseite		
	Klingelanlage mit Kamera		
	Videoüberwachung der Eingänge		

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten" Passworts).

	Technische Maßnahmen		**Organisatorische Maßnahmen**
X	Login mit Benutzername + Passwort		Verwalten von Benutzerberechtigungen
	Login mit biometrischen Daten		Erstellen von Benutzerprofilen
X	Anti-Viren-Software Server		Zentrale Passwortvergabe
X	Anti-Virus-Software Clients		Richtlinie „Sicheres Passwort"
	Anti-Virus-Software mobile Geräte		Richtlinie „Löschen / Vernichten"
X	Firewall		Richtlinie „Clean desk"
	Intrusion Detection Systeme		Richtlinie Datenschutz
	Mobile Device Management		Mobile Device Policy
	Einsatz VPN bei Remote-Zugriffen		Anleitung „Manuelle Desktopsperre"
	Verschlüsselung von Datenträgern		
	Verschlüsselung Smartphones		
	Gehäuseverriegelung		
	BIOS Schutz (separates Passwort)		
	Sperre externer Schnittstellen (USB)		
X	Automatische Desktopsperre		
	Verschlüsselung von Notebooks / Tablet		

1.3. 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. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

	Technische Maßnahmen		Organisatorische Maßnahmen
X	Aktenshredder (mind. Stufe 3, cross cut)		Einsatz Berechtigungskonzepte
	Externer Aktenvernichter (DIN 32757)		Minimale Anzahl an Administratoren
X	Physische Löschung von Datenträgern		Datenschutztresor
	Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe Änderung und Löschung von Daten		Verwaltung Benutzerrechte durch Administratoren

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Trennung von Produktiv- und Test-umgebung		Steuerung über Berechtigungskonzept
	Physikalische Trennung (Systeme / Datenbanken / Datenträger)		Festlegung von Datenbankrechten
	Datensätze sind mit Zweckattributen versehen		Mandantenfähigkeit relevanter Anwendungen

1.5. Pseudonymisierung

(Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)		Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/ pseudonymisieren

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1. 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. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Email-Verschlüsselung		Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
	Einsatz von VPN		Übersicht regelmäßiger Abruf- und Protokollierung der Zugriffe und Abrufe
	Sichere Transportbehälter		Weitergabe in anonymisierter oder pseudonymisierter Form
	Bereitstellung über verschlüsselte Verbindungen wie sftp, https		Sorgfalt bei Auswahl von Transport- Personal und Fahrzeugen
	Nutzung von Signaturverfahren		Persönliche Übergabe mit Protokoll

2.2. 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. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

	Technische Maßnahmen		Organisatorische Maßnahmen
	Technische Protokollierung der Eingabe, Änderung und Löschung von Daten		Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
	Manuelle oder automatisierte Kontrolle der Protokolle		Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
			Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
			Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
			Klare Zuständigkeiten für Löschungen

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

	Technische Maßnahmen		Organisatorische Maßnahmen
	Feuer- und Rauchmeldeanlagen	X	Backup & Recovery-Konzept (ausformuliert)
	Feuerlöscher Serverraum		Kontrolle des Sicherungsvorgangs
	Serverraumüberwachung Temperatur und Feuchtigkeit		Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
	Serverraum klimatisiert	X	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Arbeitsraumes
	USV		Notfallplan (z.B. BSI Grundschutz 1004)
	Keine sanitären Anschlüsse im oder oberhalb des Serverraums	X	Getrennte Partitionen für Programme und Daten
	Schutzsteckdosenleisten Serverraum		
	Datenschutztresor		
	RAID System / Festplattenspiegelung		

	Videoüberwachung Serverraum		
	Alarmmeldung bei unberechtigtem Zutritt zum Serverraum		

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1. Datenschutz-Management

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Softwarelösungen für Datenschutz-management (Name/Firma/Kontaktdaten)		Interner/externer Datenschutzbeauftragter
	Zentrale Dokumentation aller Verfahrens-weisen mit Zugriffsmöglichkeit für Mitar-beiter nach Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	X	Mitarbeiter geschult und auf Vertraulich-keit/Datengeheimnis verpflichtet
	Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	X	Regelmäßige Sensibilisierung der Mitar-beiter mit Bedarf/Berechtigung
			Anderweitiges dokumentiertes Sicherheits-konzept
			Interner / externer Informationssicher-heitsbeauftragter Name / Firma Kontakt
			Eine Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
		X	Die Organisation kommt den Informations-pflichten nach Art. 13 und 14 DSGVO nach
		X	Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

5. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

	Technische Maßnahmen		**Organisatorische Maßnahmen**
X	Einsatz von Firewall und regelmäßige		Dokumentierter Prozess zur Erkennung

	Aktualisierung		und Meldung von Sicherheitsvorfällen / Datenpannen (Meldepflicht gegenüber Aufsichtsbehörde)
X	Einsatz von Spamfilter und regelmäßige Aktualisierung	X	Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
	Einsatz von Virenscanner und regelmäßige Aktualisierung		Einbindung von DSB und ISB in Sicherheits-vorfälle und Datenpannen
	Intrusion Detection System (IDS)		Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
	Intrusion Prevention System (IPS)		

6. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Privacy by design / Privacy by default

	Technische Maßnahmen		**Organisatorische Maßnahmen**
X	Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	X	Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

7. Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln

	Technische Maßnahmen		**Organisatorische Maßnahmen**
		X	Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
		X	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
		X	Abschluss des notwendigen AV-Vertrages
		X	Schriftliche Weisungen an den Auftragnehmer
		X	Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
			Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
		X	Sicherstellung der Übergabe/Vernichtung der Daten nach Auftragsabwicklung
			Bei längerer Zusammenarbeit: laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Ausgefüllt für die Organisation durch

Name :

Funktion:

Rufnummer:

Email: Ort, Datum