

Technische und organisatorische Maßnahmen zur Wahrung des Datenschutzes

Zusatz 2 zur AVV vom

zwischen

und der Stiftung Kinder forschen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, welche die Stiftung „Kinder forschen“ in eigener Verantwortung sowie als Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der eigenen sowie der im Auftrag verarbeiteten Informationen.

Pseudonymisierung & Verschlüsselung

Die folgenden Maßnahmen gewährleisten, dass die Verarbeitung personenbezogener Daten in einer Weise passiert, 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 getrennten und abgesicherten Systemen (mögl. verschlüsselt)	☐ Interne Anweisung, personenbezogene; Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren
☐ Verschlüsselung alle Verbindungen zu Webanwendungen grundsätzlich nach Stand der Technik; per SSL/TLS gesichert. Die Güte der Verschlüsselung wird regelmäßig mit https://www.ssllabs.com/ssltest/ getestet.	
☐ Laptops und Computer sind grundsätzlich nach dem Stand der Technik verschlüsselt.	
☐ Backups können verschlüsselt werden, der geheime Schlüssel ist wiederum verschlüsselt in getrennten Systemen abgelegt	

Gefördert vom:

Partner:



Bundesministerium
für Bildung, Familie, Senioren,
Frauen und Jugend

Siemens Stiftung

Dietmar Hopp Stiftung

Dieter Schwarz Stiftung

Sicherstellung Vertraulichkeit

Zutrittskontrolle

Folgende Maßnahmen gewährleisten, dass Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Alarmanlage	☐ Schlüsselregelung / Liste
☐ Automatisches Zugangskontrollsystem	☐ Empfang / Rezeption / Pförtner
☐ Biometrische Zugangssperren	☐ Besucherbuch / Protokoll der Besucher
☐ Chipkarten / Transpondersysteme	☐ Mitarbeiter- /Besucherausweise
☐ Manuelles Schließsystem	☐ Besucher in Begleitung Mitarbeitender
☐ Sicherheitsschlösser	☐ Sorgfalt bei Auswahl des Wachpersonals
☐ Schließsystem mit Codesperre	☐ Sorgfalt bei Auswahl der Reinigungsdienste
☐ Absicherung der Gebäudeschächte	☐ Anweisung zur Verschließung der Diensträume
☐ Türen mit Knauf Außenseite	
☐ Klingelanlage mit Kamera	
☐ Videoüberwachung der Eingänge	
☐ Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken geschützt	

Zugangskontrolle

Folgende Maßnahmen gewährleisten, dass Unbefugten Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, nicht nutzen können.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Firewall	☐ Verwalten von Benutzerberechtigungen
☐ Login mit biometrischen Daten	☐ Erstellen von Benutzerprofilen
☐ Anti-Viren-Software Server	☐ Zentrale Passwortvergabe
☐ Anti-Virus-Software Clients	☐ Richtlinie „Löschen / Vernichten“
☐ Anti-Virus-Software mobile Geräte	☐ Richtlinie „Sicheres Passwort“
☐ Endpoint-Security-Software auf Servern und Clients	☐ Allg. Richtlinie Datenschutz und / oder Sicherheit

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Login mit Benutzername und Passwort	☐ Anleitung „Manuelle Desktopsperre“
☐ Intrusion Detection Systemen	☐ Mobile Device Policy
☐ Einsatz von VPN bei Remote-Zugriffen	
☐ Mobile Device Management	
☐ Verschlüsselung von Notebooks und Tablets	
☐ Verschlüsselung von Datenträgern	
☐ Verschlüsselung Smartphones	
☐ Gehäuseverriegelung	
☐ BIOS-Schutz	
☐ Automatische Desktopsperre	
☐ Sperre externer Schnittstellen (USB)	

Zugriffskontrolle

Folgende Maßnahmen gewährleisten, dass Unbefugten keinen Zugriff auf Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, erhalten.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Aktenschredder (mind. Stufe 3, cross cut)	☐ Berechtigungsvergabe nach dem Minimalprinzip
☐ Externer Aktenvernichter nach Stand der Technik	☐ Es existieren geregelte Ein- und Austrittsprozesse für beschäftigte Personen und eine umfassende Dokumentation der zentralen Berechtigungsvergaben
☐ Physische Löschung von Datenträgern	☐ Minimale Anzahl an Administratoren
☐ Protokollierung von Zugriffen auf Anwendungen, konkret bei Eingabe, Änderung und Löschung von Daten	☐ Verwaltung Benutzerrechte durch Administratoren und die Fachanwendungsverantwortlichen
	☐ Einsatz Berechtigungskonzepte
	☐ Datenschutztresor

Trennungsgebot

Folgende Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

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

Sicherstellung Integrität

Eingabekontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
☐ Manuelle oder automatisierte Kontrolle der Protokolle	☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
☐ Systemzugriffe werden durch Firewalls protokolliert	☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	☐ Klare Zuständigkeiten für Löschungen

Weitergabekontrolle

Folgende Maßnahmen 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:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Einsatz von VPN	☐ Weitergabe in anonymisierter oder pseudonymisierter Form
☐ E-Mail Transportverschlüsselung	☐ Persönliche Übergabe mit Protokoll
☐ Protokollierung von Zugriffen und Abrufen	☐ Übersicht regelmäßiger Abruf- und Übermittlungsvorgänge
☐ Sichere Transportbehälter	☐ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☐ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	
☐ Plattform zum verschlüsselten Austausch von Daten	
☐ Nutzung von Signaturverfahren	
☐ Mobile Datenträger sind verschlüsselt	
☐ aussortierte oder defekte Datenträger werden sicher gelöscht und in Abhängigkeit des Schutzbedarfs physisch zerstört	

Sicherstellung Verfügbarkeit

Verfügbarkeitskontrolle

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Feuerlöscher Serverräume	☐ Backup & Recovery-Konzept (ausformuliert)
☐ Temperatur- und Feuchtigkeitsüberwachung im Serverraum	☐ Kontrolle des Sicherungsvorgangs
☐ Datenschutztresor	☐ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse

Technische Maßnahmen	Organisatorische Maßnahmen
☐ fensterloser, redundant klimatisierter Serverraum	☐ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☐ USV	☐ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☐ Schutzsteckdosenleisten im Serverraum	☐ Existenz eines Notfallplans (z.B. BSI ITGrundschutz 100-4)
☐ RAID System / Festplattenspiegelung	☐ Getrennte Partitionen für Betriebssystem und Produktivdaten
☐ Virenschutz-Software auf Servern und Clients	
☐ Videoüberwachung Serverraum	
☐ Festplatten werden regelmäßig ersetzt	
Getrennte Partitionen für Betriebssystem- und Produktivdaten	
☐ Monitoring aller kritischen Systeme	
☐ redundante Auslegung kritischer Systeme	
☐ Feuer- und Rauchmeldeanlage	

Auftragskontrolle

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

Technische Maßnahmen	Organisatorische Maßnahmen
	☐ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	☐ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (u.a. Datenschutz und Datensicherheit)
	☐ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
	☐ Schriftliche Weisungen an den Auftragnehmer

Technische Maßnahmen	Organisatorische Maßnahmen
	☐ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	☐ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
	☐ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	☐ Regelung zum Einsatz weiterer Subunternehmer
	☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
	☐ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Belastbarkeit

Folgende Maßnahmen stellen die ausreichende Dimensionierung von Speicher-, Zugriffs- und Leistungskapazitäten sicher:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Einsatz von Firewalls und regelmäßige Aktualisierung dieser	☐ geregeltes Patch-Management
☐ Betrieb von Intrusion Detection Systemen (IDS)	
☐ Betrieb von Intrusion Prevention Systemen (IPS)	
☐ Die Internetanbindung ist bedarfsgerecht ausgelegt	
☐ Die Serverinfrastruktur ist redundant ausgelegt und ausreichend dimensioniert	
☐ Kritische Systeme werden, unter anderem, auf Festplatten-, Arbeitsspeicher- und CPU-Auslastung hin überwacht	
☐ Festplatten in Speichersystemen in einem Ausfallsicherheit erhöhenden RAIDVerbund	
☐ Betrieb einer ausreichend dimensionierten USV	

Rasche Wiederherstellung

Folgende Maßnahmen gewährleisten eine rasche Wiederherstellung der Systeme und Anwendungen:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Backups werden außerhalb des Serverraums und außerhalb der Geschäftsräume aufbewahrt	☐ Es existiert ein Datensicherungskonzept
☐ Datensicherungen werden stichprobenartig und auf Basis von Protokollen geprüft	☐ für alle kritischen Systeme existieren Datensicherungspläne, anhand derer die Datensicherung nachvollzogen und die Wiederherstellung durchgeführt werden kann
☐ es finden regelmäßige Wiederherstellungsübungen statt	
☐ Backups werden außerhalb des Serverraums und außerhalb der Geschäftsräumlichkeiten aufbewahrt	

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Folgende Maßnahmen stellen die laufende Funktionsfähigkeit der Datenschutz Organisation sicher:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Software-Lösungen für DatenschutzManagement im Einsatz	☐ Interner / externer Datenschutzbeauftragter
☐ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf und Berechtigung	☐ Regelmäßige, mindestens jährliche Schulung der Mitarbeiter
☐ Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	☐ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
☐ Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mindestens jährlich durchgeführt	☐ Es ist ein Datenschutzteam eingerichtet, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt
☐ Anderweitiges dokumentiertes Sicherheitskonzept	☐ Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	☐ Interner / externer Informationssicherheitsbeauftragter Name / Firma Kontakt

Technische Maßnahmen	Organisatorische Maßnahmen
	☐ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	☐ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

Datenschutzfreundliche Voreinstellungen

Die folgenden Angaben sind insbesondere dann zu treffen, wenn es um Webdesign, Softwareherstellung (oder Anpassung) oder um SaaS-Dienste handelt, bei denen die Grundeinstellungen zum Datenschutz eingestellt, oder hergestellt werden. Alternativ gilt dieser Abschnitt für Dienstleister deren Dienstleistungen/Produkte datenschutzfreundliche Grundeinstellungen, respektive datenschutzfreundliche Erstellung der Produkte/Dienstleistungen berücksichtigen.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Es sind technische Maßnahmen getroffen worden, welche die Grundsätze von Privacy by Design / Privacy by Default unterstützen. Wenn ja, welche? ☐ Privacy by Default ist standardmäßig aktiviert. ☐ Wenn ja, welche Einstellungen oder Funktionen sind standardmäßig privat? (beispielsweise Datenschutzfreundliche Voreinstellungen bei Auslieferung/nach Installation)	☐ Es sind organisatorische Maßnahmen getroffen worden, welche die Grundsätze von Privacy by Design / Privacy by Default unterstützen. Wenn ja, welche? _____ (Alternativ Anlage)
☐ Es können nur die personenbezogenen Daten eingegeben werden, die zur Zweckerreichung erforderlich sind.	☐ Es werden nur notwendige personenbezogene Daten erhoben, die zur Erreichung des Zwecks erforderlich sind.
☐ Die Ausübung der Betroffenenrechte ist mittels technischer Maßnahmen barrierearm umgesetzt. (bspw. mittels (Web-)Formular)	☐ Wurden Datenschutzprüfungen oder -bewertungen durchgeführt, um sicherzustellen, dass Privacy by Design und Privacy by Default effektiv umgesetzt wurden?

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Gibt es Funktionen oder Kontrollen, die es Benutzern ermöglichen, ihre Privatsphärepräferenzen einfach anzupassen?	
☐ Haben Sie Mechanismen implementiert, um sicherzustellen, dass Benutzeraktivitäten standardmäßig privat bleiben, es sei denn, sie ändern aktiv ihre Einstellungen?	