Bitte füllen Sie das folgende Dokument an den gelb markierten Stellen aus

und schicken Sie es mit der Unterschrift, der an Ihrer Schule für den Datenschutz zuständigen Person ausschließlich per .pdf an info@klett.support

mit dem **Betreff** „**Auftragsverarbeitungsvertrag**“ zurück.

Das Vertragsverhältnis kommt zustande durch Eingang (Eingangsbestätigung per E-Mail) des ausgefüllten und unterschriebenen Dokumentes bei uns und gilt solange keine Änderungen am Vertrag vorgenommen werden.

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO

zwischen

Auftraggeber Bezeichnung
Straße, PLZ Ort

– Verantwortlicher (Art. 4 Nr. 7 DSGVO), im Folgenden: „Auftraggeber“ –

und

Ernst Klett Verlag GmbH
Rotebühlstr. 77, 70178 Stuttgart

– Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO), im Folgenden: „Auftragnehmer“ –

1. Vertragsgegenstand

Gegenstand des Vertrages ist die Verarbeitung personenbezogener Daten im Auftrag (im Folgenden: „Auftragsverarbeitung“) gemäß Art. 28 DSGVO) zur Nutzung der vom Auftraggeber erworbenen Lizenzen für digitale Bildungsmedien des Auftragnehmers. Dieser Vertrag ergänzt den/die darüber abgeschlossenen Lizenzverträge zwischen den Parteien, im Folgenden: „Hauptvertrag“.

2. Laufzeit

Die Laufzeit der Auftragsverarbeitung entspricht der Laufzeit des Hauptvertrages und endet gleichzeitig mit dieser, ohne dass eine gesonderte Kündigung erforderlich ist.

Der Vertrag über die Auftragsverarbeitung kann jederzeit gekündigt werden. Die Kündigung bedarf zu ihrer Wirksamkeit der Textform. Die Kündigung der Auftragsverarbeitung wirkt zugleich als Kündigung der bestehenden Lizenzen für digitale Bildungsmedien des Auftragnehmers.

3. Art und Zweck der Verarbeitung

Erbringung von Leistungen gemäß den Nutzungsbedingungen der vom Auftraggeber lizenzierten Produkte des Auftragnehmers und die dafür erforderlichen Verarbeitungsvorgänge bei:

- Verwaltung von personenbezogenen Daten zur Registrierung und zum Login
- Aufruf von Online-Lehr- und Lernmedien in beliebigen Browserumgebungen
- Zugriff und Nutzung von Online-Lehr- und Lernmedien mit individualisierbaren Einstellungsmöglichkeiten, Annotationsfunktionen, Funktionen zum Teilen mit anderen Nutzern
- Verarbeitung von Testergebnissen der Schüler:innen bei der Nutzung von Online-Diensten zur Auswertung von Tests durch Lehrkräfte
- Verwaltung von Lerngruppen

4. Art der personenbezogenen Daten und betroffene Personen

4.1 Gegenstand der Auftragsverarbeitung sind folgende Arten personenbezogener Daten:

- Mailadresse und Passwort des Nutzers
- Frei eingegebene Texte des Nutzers in Online-Lehr- und Lernmedien (Annotationen)
- Passwort

4.2 Die Kategorien betroffener Personen im Rahmen der Auftragsverarbeitung:

- Schüler:innen an allgemeinbildenden und berufsbildenden Schulen
- Lehrkräfte an allgemeinbildenden und berufsbildenden Schulen
- Lernmittel- / Lernmedien-Verwalter:innen sowie Administratoren an allgemeinbildenden und berufsbildenden Schulen

5. Technische und organisatorische Maßnahmen

5.1 Der Auftragnehmer dokumentiert vor Abschluss des Vertrages die technischen und organisatorischen Maßnahmen und legt sie dem Auftraggeber zur Prüfung vor. Die dokumentierten Maßnahmen gemäß der **Anlage 1** werden Grundlage des Vertrages. Soweit die Prüfung des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

5.2 Der Auftragnehmer ergreift die erforderlichen Maßnahmen zur Gewährleistung der Datensicherheit und eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sowie der raschen Wiederherstellbarkeit der Verfügbarkeit und des Zugangs zu personenbezogenen Daten. Er berücksichtigt dabei den Stand der Technik und die Implementierungskosten sowie Art, Umfang und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen gemäß Art. 32 DSGVO.

5.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Daher ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

6. Pflichten des Auftragnehmers

6.1 **Ansprechpartner**:

– Kontaktdaten des Auftragnehmers: Ernst Klett Verlag GmbH, Rotebühlstraße 77, 70178 Stuttgart, datenschutz@klett.de

– Kontaktdaten des Datenschutzbeauftragter des Auftragnehmers Edmund Hilt dsb@klett.de. Für vertrauliche Anfragen haben Sie die Möglichkeit, sich direkt an unseren Datenschutzbeauftragten zu wenden: datenschutz@hilt-evolution.com

Zur Erteilung von Weisungen im Namen des Auftraggebers befugt:

[Name, Kontaktdaten] oder eine später vom Auftraggeber in Textform als Ansprechpartner genannte Person

Der Auftraggeber hat Weisungen im Sinne von Art. 28 Abs. 1 Satz 2 Buchst. a DSGVO an den Ansprechpartner beim Auftragnehmer zu richten.

6.2 **Verpflichtung auf die Vertraulichkeit**: Alle Mitarbeiter:innen, die im Rahmen der Auftragsverarbeitung auf personenbezogene Daten des Auftraggebers zugreifen können, müssen zuvor auf die Vertraulichkeit verpflichtet worden sein. Der Auftragnehmer und seine Beschäftigten sowie sonstige dem Auftragnehmer unterstellte Personen (Organe, freie Mitarbeiter:innen), die im Rahmen der Auftragsverarbeitung Zugang zu personenbezogenen Daten haben, dürfen diese Daten gemäß Art. 29 DSGVO ausschließlich auf Weisung des Auftraggebers verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

6.3 **Zusammenarbeit mit Aufsichtsbehörden**: Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

6.4 **Unverzügliche Information des Auftraggebers über Kontrollen und Maßnahmen der Aufsichtsbehörde**. Der Auftragnehmer informiert den Auftraggeber unverzüglich über alle Kontrollen und sonstigen Maßnahmen einer Aufsichtsbehörde, die die Auftragsverarbeitung betreffen.

6.5 **Unterstützung des Auftraggebers**: Ist der Auftraggeber einer Kontrolle einer Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt, unterstützt

ihn der Auftragnehmer angemessen. Der Auftragnehmer unterstützt den Auftraggeber ferner im Rahmen seiner Informationspflicht gegenüber der betroffenen Person zu und stellt alle relevanten Informationen unverzüglich zur Verfügung; er unterstützt den Auftraggeber bei einer Datenschutz-Folgenabschätzung des Auftraggebers und im Rahmen einer Konsultation mit der Aufsichtsbehörde.

6.6 **Dokumentation der technischen und organisatorischen Maßnahmen**: Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle erforderlichen Informationen zum Nachweis der Einhaltung seiner Pflichten zur Verfügung. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch ein IT-Sicherheits- oder Datenschutzaudit vorlegen.

6.7 **Datenschutzverletzungen**: Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn durch ihn oder eine ihm unterstellte Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder Verpflichtungen aus dem vorliegenden Vertrag verstoßen wurde.

7. Verarbeitung personenbezogener Daten außerhalb von EU/EWR

Die Datenverarbeitung findet ausschließlich in der Europäischen Union (EU) oder dem Europäischen Wirtschaftsraum (EWR) statt. Die Verlagerung in ein Drittland, einschließlich der Einschaltung eines Unterauftragnehmers (Ziffer 8.) in einem Drittland darf nur nach schriftlicher Zustimmung des Auftraggebers und unter den Voraussetzungen der Art. 44 ff. DSGVO erfolgen.

8. Unterauftragsverhältnisse

8.1 Sollen Unterauftragnehmer (weitere Auftragsverarbeiter gemäß Art. 28 DSGVO) einbezogen werden sollen, gilt:

- Die Einschaltung von Unterauftragnehmern ist nur mit schriftlicher Zustimmung des Auftraggebers gestattet. Ohne eine solche Zustimmung kann der Auftragnehmer zur Vertragsdurchführung einen Unterauftragnehmer mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies dem Auftraggeber vor Beginn der Verarbeitung schriftlich mitgeteilt hat und der Auftraggeber der Unterbeauftragung nicht innerhalb eines Monats nach Zugang der Mitteilung schriftlich widersprochen hat.

- Der Auftragnehmer gestaltet die vertraglichen Vereinbarungen mit dem Unterauftragnehmer so, dass sie Art. 28 DSGVO entsprechen.

- Die Einschaltung des Unterauftragnehmers ist unzulässig, solange nicht alle Voraussetzungen erfüllt sind.

8.2 Die vorstehenden Regelungen gelten entsprechend, wenn der Unterauftragnehmer seinerseits ein Unterauftragsverhältnis begründen will.

8.3 Erbringt der Unterauftragnehmer seine Leistungen nicht in der EU oder dem EWR stellt der Auftragnehmer sicher, dass die Verarbeitung personenbezogener Daten gemäß Art. 44 ff. DSGVO zulässig ist.

8.4 Abweichend von Ziffer 8.1, erster Spiegelstrich, gestattet der Auftraggeber bereits jetzt die Einschaltung der folgenden Unterauftragnehmer vorbehaltlich der Einhaltung der sonstigen Voraussetzungen gemäß Ziffern 8.1 bis 8.3:

- Technik / Network Operation Center, Adacor Hosting GmbH, Kaiserleistraße 8a, 63067 Offenbach am Main
- Atos Information Technology GmbH, Otto-Hahn-Ring 6, 81739 München
- develop4edu GmbH, Rotebühlstraße 77, 70178 Stuttgart

9. Weisungsbefugnis des Auftraggebers

9.1 Der Auftraggeber hat ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich schriftlich.

9.2 Der Auftragnehmer darf nur nach dokumentierter Weisung des Auftraggebers Daten berichtigen, löschen oder ihre Verarbeitung einschränken. Wendet sich eine betroffene Person an den Auftragnehmer, leitet dieser das Ersuchen an den Auftraggeber weiter. Auskünfte darf der Auftragnehmer nur nach vorheriger Zustimmung in Textform durch den Auftraggeber erteilen.

9.3 Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

9.4 Der Auftragnehmer verarbeitet gemäß Ziffer 9.1 bis 9.3 die Daten nur auf dokumentierte Weisung des Auftraggebers, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

10. Kontrollrechte des Auftraggebers

10.1 Der Auftraggeber hat das Recht, Kontrollen im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung der vertraglichen Pflichten durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

10.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO und der **Anlage** nach.

11. Löschung von Daten

11.1 Nach Aufforderung durch den Auftraggeber sowie unaufgefordert bei Beendigung der Auftragsverarbeitung wird der Auftragnehmer sämtliche in seinen Besitz gelangte Datenbestände, die im Zusammenhang mit der Auftragsverarbeitung stehen, dem Auftraggeber übermitteln oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Der Auftragnehmer kann dem Auftraggeber schriftlich eine Frist von 14 Tagen setzen, schriftlich die Übermittlung der Daten zu verlangen; äußert sich der Auftraggeber innerhalb der Frist nicht, gilt dies als Zustimmung.

11.2 Der Auftragnehmer hat an den Daten kein Zurückbehaltungsrecht.

12. Schlussbestimmungen

12.1 Dieser Vertrag ersetzt etwaige frühere Abreden der Parteien über den Vertragsgegenstand.

12.2 Wenn in diesem Vertrag Schriftform verlangt wird, genügt E-Mail oder Fax.

12.3 Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist der Sitz des Auftraggebers.

Für den Auftraggeber

_____

(Ort, Datum, Unterschrift)

Für den Auftragnehmer

Ernst Klett Verlag GmbH

Stuttgart, März 2022

Dr. Sibylle Tochtermann

Geschäftsführerin

ppa. Dr. Ilas Körner-Wellershaus

Verlagsleiter

Anlage: Technische und organisatorische Maßnahmen des Auftragnehmers

1. Vertraulichkeit (Art. 32 Abs. 1 Buchst. b DSGVO)

1.1. Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist. Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

- Sicherheitsschlösser mit Schlüsselregelung
- verschlossene Türen bei Abwesenheit
- Zutrittskontrollsystem (z.B. Ausweisleser, Magnetkarte, Chipkarte, Transponder unter Beachtung von kontrollierter Schlüsselvergabe)
- Zutrittsregelungen für betriebsfremde Personen
- Empfang, Werkschutz, Pförtner

1.2. Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern. Technische und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- Erstellen von Benutzerprofilen
- Einsatz von VPN-Technologie (auch bei Remote – Zugriffen)
- Mobile Device Management
- Identifizierung und Authentifizierung einschließlich Verfahrensregelungen zur Kennwortvergabe (Buchstaben, Groß.- Kleinschreibung, Mindestlänge, Zahlen, Sonderzeichen, regelmäßige systemseitige Aufforderung zum Wechsel des Kennworts)
- Begrenzung der Fehlversuche
- Protokollierung
- Systemverwalterbefugnisse /-protokollierung
- Dunkelschaltung des Bildschirms mit Passwortschutz bei Inaktivität
- Firewall (Hardware-Firewall, Software-Firewall)
- Virenschutz nach dem Stand der Technik
- Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)

1.3. Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern:

- Berechtigungskonzept mit differenzierten Berechtigungen
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Zugriffsprotokolle
- Identifizierung und Authentifizierung
- Aufbewahrung von Datenträgern in verschließbaren Schränken
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)

- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Protokollierung der Vernichtung

1.4. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten. Maßnahmen zur getrennten Verarbeitung von Daten mit unterschiedlichen Zwecken:

- Physikalische oder logische Trennung

1.5. Pseudonymisierung (Art. 32 Abs. 1 Buchst. a; Art. 25 Abs. 1 DSGVO)

Daten werden so verarbeitet, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer identifizierbaren betroffenen Person zugeordnet werden können; diese zusätzlichen Informationen werden gesondert aufbewahrt und sind durch technischen und organisatorischen Maßnahmen gesichert:

- aktuell keine (es werden Stammdaten verarbeitet)

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

2.1 Weitergabekontrolle

Es ist zu 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:

- E-Mail-Verschlüsselung
- Bereitstellung über verschlüsselte Verbindungen wie https, sftp
- Kennzeichnung der Datenträger
- Bestandsverzeichnis und Bestandskontrolle der Datenträger
- Festlegung der zur Abgabe von Datenträgern bzw. zur elektronischen Übertragung berechtigten Personen
- Einrichtung eines VPN (Virtual Private Network)
- Fernwartungskonzept

2.2 Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten. Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

- Manuelle oder automatische 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
- Klare Zuständigkeiten für Löschungen

3. Verfügbarkeit, Belastbarkeit und rasche Wiederherstellbarkeit (Art. 32 Abs. 1 Buchst. b und c DSGVO)

3.1 Verfügbarkeit

Die Daten sind gegen zufällige und absichtliche Zerstörung oder Verlust zu schützen. Maßnahmen zur Datensicherung (physikalisch / logisch):

- Backup-Verfahren (Festlegen von Rhythmus, Medium, Aufbewahrungszeit und -ort)
- Spiegelung von Festplatten
- Unterbrechungsfreie Stromversorgung (USV)
- Betriebsbereitschaft
- Notfallkonzept
- Brandmelder
- Feuersichere Türen
- Virenschutz nach dem Stand der Technik
- Firewall
- Zusätzliche Sicherheitskopien mit Lagerung an besonders geschützten Orten
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

3.2 Belastbarkeit

Maßnahmen zur Sicherstellung der Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung:

- Trennung zwischen Produktivsystem und Webserver/Mailserver
- Intrusion Detection Systeme
- Firewall (Hardware-Firewall, Software-Firewall)
- Virenschutz nach dem Stand der Technik

3.3 Rasche Wiederherstellbarkeit

Maßnahmen zur Sicherstellung der raschen Wiederherstellbarkeit der Verfügbarkeit der personenbezogenen Daten und des Zugang zu ihnen bei einem physischen oder technischen Zwischenfall:

- Backup-Verfahren (Festlegen von Rhythmus, Medium, Aufbewahrungszeit und -ort)
- Spiegelung von Festplatten
- Unterbrechungsfreie Stromversorgung (USV)
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenschutzverletzungen (auch im Hinblick auf die Meldepflicht gegenüber der Aufsichtsbehörde)
- Einbindung bei Sicherheitsvorfällen und Datenpannen:
    - Datenschutzbeauftragte
    - Interne Sicherheitsbeauftragte

4. Datenschutzmanagement, Auftragskontrolle, regelmäßige Überprüfung (Art. 32 Abs. 1 Buchst. d DSGVO)

4.1 Datenschutzmanagement

- Datenschutzverantwortliche intern
- Regelprozesse mit kurzfristiger Reaktionszeit auch außerhalb der Regelarbeitszeiten (nachts, Wochenende, Feiertage)
- Externer Datenschutzbeauftragter

4.2 Auftragskontrolle

Die weisungsgemäße Auftragsverarbeitung ist zu gewährleisten. Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung
- Schriftliche Festlegung der Weisungen
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- Festlegung von turnusgemäßen Kontrollen des Auftragnehmers durch den Auftraggeber
- Regelmäßige interne Kontrolle und Dokumentation des Auftragnehmers, dass Weisungen und Regelungen zur Auftragsdurchführung beachtet werden

4.3 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)
- Regelmäßige Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen
- Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
- Bedarfsgerechte Sensibilisierung der Mitarbeiter
- Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
- Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
- Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden