Bitte füllen Sie das folgende Dokument an den gelb markierten Stellen aus und schicken Sie es mit der Unterschrift, der an Ihrer Schule, Erziehungs- oder Bildungseinrichtung oder Institution für den Datenschutz zuständigen Person ausschließlich als PDF-Datei 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 so lange 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 sowie digitale Lehr- und Lernmittel aus dem Online-Angebot des Auftragnehmers (im Folgenden zusammenfassend: „digitale Bildungsmedien“). Dieser Vertrag ergänzt den/die darüber abgeschlossenen Lizenzverträge zwischen den Parteien, im Folgenden: „Hauptvertrag“ sowie die für die Nutzung der digitalen Bildungsmedien jeweils gültigen Nutzungsbedingungen, denen der Auftraggeber vor deren Nutzung zustimmen muss.

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 Schriftform. 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 jeweiligen 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 digitalen Bildungsmedien 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

- Im Bereich „**Klett Diagnostik**“:

    - Aufruf und Nutzung von digitalen Bildungsmedien in beliebigen Browserumgebungen

    - Anlage und Verwaltung von Schüler:innen und Schulklassen oder Lerngruppen an allgemeinbildenden und berufsbildenden Schulen und sonstigen Erziehungs- oder Bildungseinrichtungen oder -Institutionen in Bezug auf die nachfolgenden Zwecke und Funktionen

    - Zugriff und Nutzung von Online-Lehr- und Lernmedien mit individualisierbaren Einstellungsmöglichkeiten, Annotationsfunktionen, Erstellung und Editierung eigener Inhalte anhand von Mustern und Vorlagen (insbesondere Lern- /Leistungs-/Sonderförderungs-Dokumentationen) sowie Funktionen zum Teilen von eigenen oder vorhandenen Inhalten mit anderen Nutzern oder Empfängern

    - Online-Bereitstellung und -Durchführung von Tests durch Schüler:innen und in Schulklassen und Lerngruppen sowie Verarbeitung, Dokumentation und Auswertung von Testergebnissen der Schüler:innen bei der Nutzung von Online-Diensten zur Bereitstellung und -Durchführung oder Dokumentation und Auswertung von Tests durch Lehrkräfte

4. Von der Verarbeitung betroffene Personengruppen und Arten der personenbezogenen Daten

4.1 Die Kategorien betroffener Personen im Rahmen der Auftragsverarbeitung:

- Lehrkräfte sowie Therapeut:innen (im Folgenden zusammenfassend „Lehrkräfte“) an allgemeinbildenden und berufsbildenden Schulen und sonstigen Erziehungs- oder Bildungseinrichtungen oder -Institutionen

- Lehr – und Lernmittel- / Lehr- und Lernmedien-Verwalter:innen sowie Administratoren an allgemeinbildenden und berufsbildenden Schulen und sonstigen Erziehungs- oder Bildungseinrichtungen oder -Institutionen

- Schüler:innen an allgemeinbildenden und berufsbildenden Schulen und sonstigen Erziehungs- oder Bildungseinrichtungen oder -Institutionen und andere, im jeweiligen Schulumfeld von Lehrkräften unterrichtete oder therapierte Personen(-gruppen) (im Folgenden zusammenfassend „Schüler:innen“)

- Eltern und andere Erziehungsberechtigte von Schüler:innen

4.2 Gegenstand der Auftragsverarbeitung sind folgende Arten personenbezogener Daten:

4.2.1 Allgemein:

- Benutzername und Passwort des Nutzers eines vom Auftraggeber lizenzierten Produkts des Auftragnehmers (im Folgenden: „Nutzer“)

- E-Mail-Adresse des Nutzers (bei Anlegen eines Nutzerkontos durch den Nutzer selbst)

- Im Benutzerkonto frei eingegebene Texte des Nutzers in Online-Lehr- und Lernmedien (Annotationen)

4.2.2 Im Bereich „**Klett Diagnostik**“:

- Im Benutzerkonto des Nutzers eingegebene und gespeicherte Daten:

  - Stammdaten von Schulklassen und Lerngruppen (Klassenstufe, Klassenzug, Schuljahr)

  - Pseudonymisierte Stammdaten von Schüler:innen (Schüler:innen-Pseudonyme, Geschlecht, Geburtsmonat und -jahr, Zuwanderungshintergrund, Familiensprache, Schulform)

  - Eigene anhand von Mustern und Vorlagen erstellte pseudonymisierte Inhalte (Lern-/Leistungs- /Sonderförderungs-Dokumentationen) entsprechend dem derzeitigen Angebot - wie insbesondere, aber nicht abschließend:

    - Schule
    - Klassenstufe
    - Lehrkraft
    - Sonderpädagogische Hilfskraft
    - Erziehungsberechtigte
    - Förderplanname, Allgemeine Informationen
    - Förderhintergrund
    - Förderbereiche, Förderschwerpunkte, Maßnahmen, Ziele und Förderbedarfe, Kompetenzfelder
    - „Ist-Stand
    - Lerndokumentationen

  - Bei der Nutzung von Online-Diensten zur Bereitstellung und -Durchführung oder Dokumentation und Auswertung von Tests durch Lehrkräfte

    - Online-Testzugangsdaten und Kennungen (Pseudonyme) von Schüler:innen
    - Pseudonymisierte Dokumentationen, Ergebnisse und Auswertungen von Tests durch Schüler:innen (entsprechend dem derzeitigen Angebot - wie insbesondere, aber nicht abschließend: Länderkennung und PLZ, Testart-/Testversion, Testeingaben, Vergleichswerte zur Testauswertung/Bezugsnormvergleich, Klassenstufe, Testdatum)
    - Pseudonymisierte Dokumentationen, Ergebnisse und Auswertungen von Tests in Schulklassen und Lerngruppen (entsprechend dem derzeitigen Angebot - wie insbesondere, aber nicht abschließend: Länderkennung und PLZ, Klasse, Testversion, Vergleichswert, Klassenstufe, Testdatum)

  - Texte des Nutzers in digitalen Bildungsmedien (Annotationen)

5. Technische und organisatorische Maßnahmen

5.1 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.

5.2 Die technischen und organisatorischen Maßnahmen des Auftragnehmers sind konkret beschrieben in den folgenden **Anlagen** zu diesem Vertrag:

5.2.1 **Anlage 1**: Allgemeine technische und organisatorische Maßnahmen der Ernst Klett Verlag GmbH für die Nutzung digitaler Bildungsmedien

5.2.2 **Anlage 2**: Technische und organisatorische Maßnahmen der Ernst Klett Verlag GmbH für die Nutzung der Klett Online Diagnostik Plattform

Die technischen und organisatorischen Maßnahmen gemäß der **Anlagen 1 und 2** werden in ihrer jeweils gültigen und unter den oben genannten Verweisen (Links) abrufbaren Fassung Bestandteil dieses Vertrages.

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 in den Anlagen 1 und 2 zu dokumentieren und zu aktualisieren. Soweit eine Prüfung des Auftraggebers nach Ziffer 10.2 einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

6. Pflichten des Auftragnehmers

6.1 Ansprechpartner:

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

Kontaktdaten des Datenschutzbeauftragten 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 schriftlich als Ansprechpartner genannte Person.

Der Auftraggeber hat Weisungen im Sinne von Art. 28 Abs. 3 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 Wahrung der Vertraulichkeit bei der Verarbeitung von personenbezogenen Daten 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 oder einen Unterauftragnehmer 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 Abs. 4 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
- VBM Service GmbH, Kurfürstenstraße 49, 60486 Frankfurt am Main

- iteratec GmbH, St.-Martin-Straße 114 81669 München

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 schriftlicher Zustimmung 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 **Anlagen 1 und 2** 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 Auftragnehmers (Stuttgart, Deutschland).

Für den Auftraggeber:

Ort, Datum, Unterschrift

Für den Auftragnehmer
Stuttgart, 11.12.2023

Tilo Knoche
Geschäftsführer
Vorsitz

Ernst Klett Verlag GmbH

Dr. Sibylle Tochtermann
Geschäftsführerin

Anlage 1 zum Vertrag über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO:

Allgemeine technische und organisatorische Maßnahmen der Ernst Klett Verlag GmbH für die Nutzung digitaler Bildungsmedien

Stand: 29.11.2023

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 66399)
- 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 technische und organisatorische Maßnahmen gesichert:

- grundsätzlich keine (es werden Stammdaten verarbeitet)
- im Rahmen der Gruppenverwaltung neu erzeugte Benutzernamen sind pseudonym (zufällig erzeugter Benutzername)

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:

- Verschlüsselte Speicherung von Passwörtern
- E-Mail-Verschlüsselung
- Bereitstellung über verschlüsselte Verbindungen wie https, sftp
- Sichere Verwahrung der zur Verschlüsselung verwendeten Schlüssel
- 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 Zugangs 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

Anlage 2 zum Vertrag über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO:

Technische und organisatorische Maßnahmen
der Ernst Klett Verlag GmbH für die Nutzung der Klett Online Diagnostik Plattform

Stand: 11.12.2023

1. Zutrittskontrolle zu den Arbeitsbereichen

Um unautorisierte Personen daran zu hindern, Zugang zu den Arbeitsbereichen zu erhalten, in denen sich Datenträger oder Datenverarbeitungsanlagen befinden, und die Datenverarbeitung zu stören, zu unterbrechen, zu manipulieren oder zu beeinträchtigen – per Zufall oder mit Absicht – müssen ausreichende Maßnahmen der Zutrittskontrolle zum Schutz der Arbeitsbereiche getroffen werden.

1.1. Organisation der Zutrittskontrolle

- Schlüssel-Regelungen
- Zugangsregelungen für betriebsfremde Personen
- Empfang
- Rollenabhängige Zutrittsregelungen für die Mitarbeiter (Administratoren, Hilfskräfte, Reinigungspersonal, etc.)

Entwicklungsdienstleister:

- Festgelegte Sicherheitsbereiche
- Zutrittsberechtigungskonzept
- Individuelle Zutrittsberechtigungsvergabe
- Dokumentation von Zutrittsberechtigungen
- Zutrittsdokumentation
- Besucherregelungen

Rechenzentren:

- Festgelegte Sicherheitsbereiche
- Alarmmeldesystem mit Aufschaltung eines Sicherheitsdienstes
- Definierter Prozess zu Zutrittsberechtigungsvergabe und -entzug
- Individuelle Zutrittsberechtigungsvergabe
- Dokumentation von Zutrittsberechtigungen
- Zutrittsdokumentation
- Rollenabhängige Zutrittsregelungen für die Mitarbeiter (Administratoren, Hilfskräfte, Reinigungspersonal, etc.)
- Autorisiertes Wachpersonal (RZ1, FFM)

- Ständig besetzte Notrufzentrale (RZ1, FFM)
- Protokollierung der Besucher

1.2. Allgemeine Gebäudesicherheit

- Sicherheitsschlösser
- Büroräume sind außerhalb der Arbeitszeit verschlossen
- Separate Brandabschnitte

Entwicklungsdienstleister:

- Manuelles Schließsystem
- Sicherheitsschlösser mit Schlüsselregelung
- Büroräume sind außerhalb der Arbeitszeit verschlossen
- Separate Brandabschnitte

Rechenzentren:

- Elektronische Schließsystem (NOC, Offenbach)
- Sicherheitstüren (RZ1, FFM und RZ2, FFM)
- Serverraum ist fensterlos, abgeschlossen und alarmgesichert (RZ1, FFM und RZ2, FFM)

1.3. Technische Sicherheitsmaßnahmen

- Schutz und Beschränkung der Zutrittswege
- Zutrittskontrollsystem mit Transponder-, Code- oder schlüsselkartenbasierter Schließanlage

Entwicklungsdienstleister:

- Zutrittskontrollsystem
- Transponder-, Code- oder schlüsselkartenbasierte Schließanlage

Rechenzentren:

- Transponder-, Code- oder schlüsselkartenbasierte Schließanlage (NOC, Offenbach)
- Perimeter-System (RZ1, FFM)
- Schutz und Beschränkung der Zutrittswege (RZ1, FFM)
- Bewegungsmelder (RZ1, FFM)
- Video-Überwachung (RZ1, FFM)
- Betreten und Verlassen des Serverraums wird elektronisch protokolliert und mittels Videoaufzeichnung aufgezeichnet (RZ1, FFM)
- Zutrittskontrollsystem
- Zusätzliche Zugangsbeschränkung der Serverräume
- Vereinzelungsanlage mit Fingerabdrucksensor (RZ2, FFM)
- Verschlossene Serverracks
- Separat gesicherter Serverraum im RZ

– Gehäuseschlösser

2. Zugangskontrolle zu Datenverarbeitungssystemen

Um unautorisierte Personen daran zu hindern, logischen Zugang zu Datenverarbeitungsanlagen zu erhalten, müssen ausreichende Maßnahmen der Zugangskontrolle getroffen werden, damit der Zugang zu personenbezogenen Daten sowie die Datenverarbeitung selbst geschützt werden können. Dazu müssen ordnungsgemäße Verfahren des Berechtigungsmanagements vorhanden sein, speziell hinsichtlich der Anwendungen und Systeme, in denen personenbezogene Daten verarbeitet werden. Diese Maßnahmen müssen dazu geeignet sein zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können oder diese Datenzugriff erhalten. Die Prinzipien der Datenminimierung und der Vergabe minimaler Zugangsrechte sollten dabei beachtet werden, um Missbrauch – zufällig oder absichtlich – zu verhindern.

2.1 Hardware- und Netzwerk-Sicherheitsmaßnahmen

– Schutz der Infrastruktur durch Hardware-Firewalls
– VPN-Beschränkungen
– Externer Zugang nur über sichere Verbindungen (VPN, RDP oder vergleichbar)
– Schutz der Infrastruktur durch Intrusion Detection-Systeme
– Protokollierung von benutzerrelevanten Aktivitäten (Anmeldung, Abmeldung, Zugangsverweigerungen, etc.)

Entwicklungsdienstleister:

– VPN-Beschränkungen
– Schutz der Infrastruktur durch Intrusion Response-Systeme
– Segmentierung des Netzwerkes
– Festplattenverschlüsselung

Rechenzentren:

– Segmentierung des Netzwerkes durch VLANs
– Demilitarisierte Zonen
– VPN-Beschränkungen
– Externer Zugang nur über sichere Verbindungen und über passwortgeschützte, verschlüsselte authentifizierte Verbindungen (VPN, RDP oder vergleichbar)
– Schutz der Infrastruktur durch Hardware-Firewalls
– Client-Zertifikate für Schutz vor unberechtigtem Zugang
– Festplattenverschlüsselung
– Nicht benötigte physikalische Schnittstellen sind deaktiviert
– Nicht benötigte Dienste sind gesperrt
– Portregeln/Sperrung von nicht erforderlichen Ports
– Verschlüsselung von Systemen oder virtualisierten Instanzen

– Systemhärtungsvorgaben, wie etwa Deaktivierung nicht erforderlicher Komponenten bzw. Funktionen

2.2 Hardware- und Netzwerk-Sicherheitsmaßnahmen

– Software-Firewall
– Antivirus-Software auf allen Systemen
– Automatische Bildschirm- und Computer-Sperre bei Inaktivität
– Verschlüsselte Speicherung von Passwörtern
– Regelmäßige Software-Updates

Rechenzentren:

– Verschlüsselte Speicherung von Passwörtern
– Software-Firewall
– Antivirus-Software auf allen Systemen
– Verschlüsselungsmechanismen
– Automatische Sitzungsbeendigung bei Inaktivität
– Automatische Bildschirm- und Computer-Sperre bei Inaktivität

2.3 Benutzerzugangsbeschränkungen

– Rollenbasierte Benutzerprofile
– Benutzerauthentifizierung für Systemzugang- und/oder Anwendungszugriff erforderlich
– Erforderliche Mindestkomplexität für Kennwörter
– Zwangs- oder Pflicht-Änderung der Benutzerkennwörter nach der erstmaligen Systemanmeldung
– Ablauf von Benutzerpasswörtern
– Automatische Deaktivierung von Benutzern nach mehreren fehlgeschlagenen Logins
– User-Login-Verlauf
– Überwachung und Protokollierung von administrativem Systemzugang und von Konfigurationsänderungen

Rechenzentren:

– Temporäre Benutzerauthentifizierung für Systemzugang- und/oder Anwendungszugriff erforderlich
– Verschlüsselte Speicherung von Passwörtern in zentralem Passwortsafe
    - Zugriff wird protokolliert und überwacht
    - Passwörter können mit Siegel und Siegelbruchkontrolle versehen werden
– Einschränkung der zeitlichen Gültigkeit der Benutzerkonten
– Zwangs- oder Pflicht-Änderung der Benutzerkennwörter
– Erforderliche Mindestkomplexität für Kennwörter

- Passwort-Historie zur Verhinderung der Mehrfachnutzung desselben Passwortes
- Angemessene Gestaltung der Benutzeraccount-Wiederherstellung im Falle eines verlorenen oder vergessenen Authentifizierungsdatensatzes
- Berechtigungen bzw. -änderungen werden protokolliert und regelmäßig überprüft

2.4 Organisatorische Sicherheitsmaßnahmen

- Geregelte Vergabeverfahren für Systemzugriffsberechtigungen
- Regelmäßige Überprüfung der Systemzugangsberechtigungen
- Deaktivierung von nicht benötigten Accounts
- Anzahl der Administratoren auf das Notwendigste beschränkt

Rechenzentren:

- Vertraulichkeitserinnerungen
- Wartung und Aktualisierung der Sicherheitssysteme nach aktuellem Stand der Technik und der Kenntnis über (neue) Schadsoftware

3. Zugriffskontrolle auf bestimmte Bereiche der Datenverarbeitungssysteme

Die Maßnahmen der Zugriffskontrolle sollen gewährleisten, dass die zur Nutzung von Datenverarbeitungssystemen oder Datenbeständen berechtigten Personen ausschließlich auf Daten zugreifen können, auf die sie zur Erfüllung ihrer Aufgaben Zugriff benötigen. Dazu müssen ordnungsgemäße Verfahren des Berechtigungsmanagements vorhanden sein, insbesondere für Anwendungen, in denen personenbezogene Daten verarbeitet werden. Um die Revisionssicherheit von Geschäftsdaten ausreichend zu gewährleisten, muss der Vergabeprozess für Zugangsberechtigungen ebenso die Anforderungen an die Revisionssicherheit erfüllen. Das Prinzip der Datenminimierung findet bei der Vergabe von Zugriffsberechtigungen durch die Vergabe minimaler Zugriffsrechte seine Entsprechung, um Datenmissbrauch – zufällig oder absichtlich – zu verhindern.

3.1 Organisatorische Sicherheitsmaßnahmen

- Rollenbasiertes Berechtigungskonzept mit minimal notwendigen Zugriffsrechten
- Zentrale Verwaltung der Benutzerrechte durch Systemadministratoren
- Beschränkung der Administrationsrechte auf das erforderliche Maß
- Minimierung der Personen mit Administrationsberechtigung
- Authentifizierung für den Daten- oder Anwendungszugriff erforderlich
- Regeln für die sichere Lagerung von physikalischen Datenträgern
- Geregeltes Löschen bzw. Vernichten und Entsorgen von Datenträgern wie Festplatten, CDs, DVDs, USB-Sticks
- Vernichtung von physikalischen Medien nach DIN 66399 oder vergleichbaren Standards
- Dokumentation der Datenträgervernichtung bzw. -löschung

Entwicklungsdienstleister:

- Minimierung der Personen mit Administrationsberechtigung

– Clean Desk Policy

Rechenzentren:

– Rollenbasiertes Berechtigungskonzept mit minimal notwendigen Zugriffsrechten (Lesen / Schreiben / Ändern / Kopieren / Löschen)
– Zugang zu IT-Systemen erhalten nur Mitarbeiter, die ausreichend geschult wurden und über fachliche Qualifikation verfügen (wird durch Ausbildungen, Weiterbildungen, Berufserfahrung und Bewertungen durch Fachabteilungen sichergestellt)
– Geregeltes Löschen bzw. Vernichten und Entsorgen von Datenträgern wie Festplatten, USB-Sticks
– Vernichtung von physikalischen Medien durch zertifiziertes Unternehmen unter Aufsicht von Mitarbeitern sowie Protokollierung
– Dokumentation der Vergabe von Zugriffsrechten
– Standardisiertes Verfahren für Erteilung und Entzug von Zugriffsrechten
– Regeln für die sichere Lagerung von physikalischen Datenträgern
– Regelmäßige Überprüfung der Datenzugriffsberechtigungen

3.2 Technische Sicherheitsmaßnahmen

– Netzwerkzugangskontrolle
– Trennung von Anwendungs- und Administrationszugängen
– Überwachung und Protokollierung allgemeiner Benutzeraktivität (Datenzugriff, Datenexport, Datenlöschung)
– Zugriffsprotokollierung
– Nutzung eines Aktenvernichters mit ausreichender Sicherheitsstufe (vgl. DIN 66399)
– Verbot/Unterbindung von nicht autorisierten Software-Installationen

Rechenzentren:

– Personalisierte Zugänge für autorisierte Mitarbeiter in Kundenprojekte zur Erfüllung der SLAs
– Zugriffe auf die IT-Systeme werden im Access-Log protokolliert und je nach Projektanforderung aufbewahrt
– Relevante Dienste auf IT-Systemen (Konsole, Datenbanken, Webserver) werden in Form von Log-Files protokolliert (Nutzer, die personenbezogene Daten verarbeiten, erhalten keinen Zugriff auf die Logfiles)
– Schnittstellen und Übertragungswege von einem IT-System zu anderen IT-Systemen definiert
– Verschlüsselung von Datenübertragungsvorgängen
– Regelmäßige Sicherheits-Updates

4. Weitergabe von personenbezogenen Daten (Weitergabekontrolle)

Durch geeignete Maßnahmen der Weitergabekontrolle, die personenbezogene Daten bei der Übermittlung oder beim Transport schützen, werden unberechtigte Zugriffe, insbesondere das Lesen, Kopieren, Verändern oder Entfernen dieser Daten durch technische Mittel verhindert. Dazu

gehören auch vertragliche Regelungen über Umfang und Zwecke der Datennutzung sowie Pflichten der Empfänger.

4.1 Technische Sicherheitsmaßnahmen

- Verschlüsselung von Daten während der Übertragung (end-to-end-Verschlüsselung)
- E-Mail-Verschlüsselung

Entwicklungsdienstleister:

- Sichere Transportbehältnisse für Datenträger

Rechenzentren:

- Personenbezogene Daten werden ausschließlich signiert, verschlüsselt und passwortgeschützt per Gnu/PGP versendet (Verschlüsselung und Signierung ebenfalls bei physischem Versand)
- Verschlüsselung von Daten während der Übertragung (SSL, TLS, IPSec und VPN)
- Verwendung von Einmalpasswörtern zur Entschlüsselung von übertragenen Daten; Schlüssel wird auf separaten Übertragungsweg übergeben
- Dokumentation bzw. Protokollierung von externen Support-Prozessen

4.2 Organisatorische Maßnahmen

- Verwaltung und Dokumentation von physischen Speichermedien
- Weitergabe von pseudonymisierten Daten
- Verbindliche Regeln für die Offenlegung von sensiblen Daten
- Regelungen für die Weitergabe von Datenträgern

Entwicklungsdienstleister:

- Dokumentation der Weitergabe von physischen Speichermedien
- Regelungen für die Aufbewahrung von Datenträgern

Rechenzentren:

- Datentransfer und -weitergabe in Übereinstimmung mit den Anweisungen des Auftraggebers
- Vollständige Löschung aller Datenkopien und Datensicherungen nach Abschluss des Auftrags
- Datentransfer und -weitergabe in Übereinstimmung mit den Anweisungen des Auftraggebers
- Verbot der Nutzung von privaten Datenträgern
- Keine Speicherung von personenbezogenen Daten dauerhaft auf mobilen Datenträgern
- Regelungen für die Verschlüsselung von Daten
- Schriftliche Richtlinien für die Datenübertragung und -weitergabe
- Dokumentation der Weitergabe von physischen Speichermedien
- Festplatten, die nicht mehr im vorgesehenen Kundenprojekt verwendet werden (RMA, Austausch, Projektende) werden in einer eigenen Shredderstation durch 7-maliges Überschreiben dauerhaft gelöscht

– Ausdrucke und CDs, die Kunden-, System- oder personenbezogene Daten enthalten, werden in einer Dokumentenvernichtungstonne gesammelt und durch ein zertifiziertes Fachunternehmen nach Sicherheitsstufe P-4 / DIN 663399-1 vernichtet

5. Überprüfbarkeit der Datenverarbeitung (Eingabekontrolle)

Maßnahmen der Eingabekontrolle dienen dazu, die Integrität der Datenverarbeitung und damit auch die Revisionssicherheit der Datenbestände zu gewährleisten. Die Maßnahmen müssen dazu geeignet sein, jederzeit mit verhältnismäßigem Aufwand überprüfen zu können, wer personenbezogene Daten in Systeme eingegeben, geändert oder aus diesen entfernt hat.

5.1 Technische Maßnahmen

– Applikationsbasierte Überprüfung der Eingabeberechtigung
– Rollenabhängige Eingabebeschränkungen und Schutz gegen nicht autorisierte Veränderungen
– Protokollierung von administrativen Änderungen
– Änderungsprotokollierung auf Datensatz- und Nutzerebene
– Protokollierung der relevanten Prozesse (Speicherung, Verarbeitung, Modifizierung, Abrufen, Übertragung, Löschung, etc.)

5.2 Organisatorische Maßnahmen

– Definition von Rollen für unterschiedliche Aufgaben
– Aufteilung der Zuständigkeiten
– Regelmäßige Analyse der Protokolldateien

Entwicklungsdienstleister, Rechenzentren:

– Vertragliche Beschränkungen der Zahl der Beschäftigten mit Zugriff auf personenbezogene Daten
– Aufteilung der Zuständigkeiten

6. Sicherstellung der weisungskonformen Datenverarbeitung (Auftragskontrolle)

Die Auftragskontrolle soll die weisungsgemäße Durchführung der Auftragsverarbeitung sicherstellen. Adressaten der Maßnahmen der Auftragskontrolle sind daher zunächst Auftragnehmer. Diese müssen ihre interne Organisation so gestalten, dass Weisungen des Auftraggebers berücksichtigt werden und sich die Datenverarbeitung innerhalb der Grenzen der vertraglich vereinbarten Tätigkeit bewegt. Die Maßnahmen der Auftragskontrolle müssen gewährleisten, dass personenbezogene Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Darüber hinaus richtet sich die Vorschrift über die Auftragskontrolle aber auch an den Auftraggeber. Dieser ist verpflichtet, seinem Auftragnehmer klare und eindeutige Weisungen zu erteilen und die Befolgung der erteilten Weisungen zu kontrollieren.

6.1 Organisatorische Maßnahmen

– Verarbeitung personenbezogener Daten erfolgt ausschließlich entsprechend den Weisungen des Auftraggebers

- Sorgfältige Auswahl von Auftragnehmern
- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- Auftragsverarbeitungsverträge mit Auftragnehmern
- Auftragsverarbeitungsverträge der Auftragnehmer mit Unterauftragnehmern
- Verpflichtung der Auftragnehmer und Unterauftragnehmer auf das Datengeheimnis
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- Regelungen zum Einsatz weiterer Subunternehmer
- Überprüfung/Auditierung von Auftragnehmern
- Regelmäßige Kontrolle externer Dienstleister
- Datenvernichtung nach Vertragsende
- Dokumentierte interne Kontrollen des Auftragnehmers zur Sicherstellung der weisungskonformen Verarbeitung personenbezogener Daten

6.2 Technische Maßnahmen

- Fern-Zugriff erfolgt nur mit starker Verschlüsselung, erfordert eine Benutzerauthentifizierung und unterliegt strikten Regeln zur Zugriffsbeschränkung
- Mechanismen zur Prävention von nicht autorisiertem Datenzugriff durch Mitarbeiter des Auftragnehmers

7. Gewährleistung der Verfügbarkeit von Datenbeständen und Datenverarbeitungsanlagen (Verfügbarkeitskontrolle)

Die Maßnahmen der Verfügbarkeitskontrolle schützen die verarbeiteten Daten einerseits vor unbeabsichtigter Zerstörung und Verlust und sollen andererseits gewährleisten, dass Daten verfügbar sind und genutzt werden können, sobald sie benötigt werden. Der Schutz von Daten vor Zerstörung und Verlust hängt unmittelbar mit dem Schutz der Verarbeitungsinfrastruktur zusammen. Neben dem schlichten physikalischen Schutz gehören hierzu die Sicherung der Strom- und Netzwerkversorgung sowie der Schutz vor Umweltgefahren wie Feuer oder Wasser, und ebenso ein angemessenes Patchmanagement von Hard- und Software, sowie ein ausreichender Schutz vor Schadsoftware. Für den Fall, dass Daten dennoch beeinträchtigt werden, sollte ein geeigneter Datensicherungsprozess vorhanden sein, um den Originalzustand von beeinträchtigten Daten wiederherstellen zu können.

7.1 Technische Maßnahmen

- Unterbrechungsfreie Stromversorgung
- Redundante Datenspeicherung
- RAID-System/Festplattenspiegelung
- Desaster-Recovery-Mechanismen für die Datenwiederherstellung, Schutz gegen versehentliche Zerstörung und Verlust
- Backups auf separat gespeicherten physischen Medien oder auf physikalisch getrennten Systemen

– Physikalisch getrennte Systeme für unterschiedliche Zwecke

Rechenzentren:

– Schutz gegen DDoS und weitere bekannte Cyberangriffe (Vergleich OWASP)
– Dedizierte Firewalls sowie Firewall-Cluster
– Unterbrechungsfreie Stromversorgung
– F90 Brandschutzabschnitte, -wände und -türen
– Brand- und Rauchmeldeanlagen
– Gaslöschanlagen
– Notstromaggregate
– Redundante Versorgungsdienste
– Überspannungsschutz
– Kühlsystem im Rechenzentren/Serverraum
– Load Balancing durch mehrere parallel arbeitende Systeme
– Tägliche inkrementelle Datensicherung

7.2 Organisatorische Maßnahmen

– Backup- und Wiederherstellungskonzept
– Notfall- und Wiederherstellungspläne sind vorhanden
– Business Recovery Plan (BRP) vorhanden, um Ausfall der IT-Infrastruktur vorzubeugen
– Brandmelder (mit Feuerwehraufschaltung)
– Räumlich getrennte Archivierung
– Regelmäßige Funktionstests
– Test der Datenwiederherstellung
– Physikalisch getrennte Systeme für unterschiedliche Zwecke

Rechenzentren:

– Notfallpläne sind vorhanden
– Regelmäßige Funktions- und Notfalltests werden durchgeführt
– Schwachstellen-Scans
– Regelmäßige Web-Application- und Server-Vulnerability-Scans
– Zeitnahes Einspielen von Patches
– Auftraggeber wird über Störungen des Betriebes schnellstmöglich in Kenntnis gesetzt oder kann direkt an das Monitoring angebunden werden
– CMDB zum Überblick und Identifikation aller eingesetzten Systeme, inklusive der Bestimmung ihrer Hardware-, Software- und Firmware-Versionen
– Regeln für die Aufbewahrung von Schlüsseln zur Entschlüsselung von Daten oder zur Verifizierung digitaler Signaturen
– Brandmelder

- Zentrale Datenhaltung
- Automatische Systemüberwachung und Benachrichtigung der Administratoren bei Irregularitäten

8. Trennung von unterschiedlichen Datenbeständen (Trennungskontrolle)

Durch Maßnahmen der Trennungskontrolle wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können und dass diese Daten derart von anderen Datenbeständen und Systemen getrennt sind, sodass eine ungeplante oder unrechtmäßige Verwendung dieser Daten zu anderen Zwecken unterbunden wird.

8.1 Technische Maßnahmen

- Mandantenfähigkeit von Anwendungen
- Physikalische Datentrennung: Getrennte Computersysteme oder Medien

Rechenzentren:

- Physikalische Datentrennung: Getrennte Computersysteme oder Medien
- Separate Instanzen für Entwicklungs- und Produktivsystemen (Sandboxes)

8.2 Organisatorische Maßnahmen

- Logische Datentrennung
- Keine Nutzung von Produktivdaten zu Testzwecken
- Datenfelder in Anwendungen sind mit zweckbestimmenden Attributen versehen worden

Rechenzentren:

- Strukturierte Dateiablage
- Spezifische Genehmigungsregelung für die Datenbank und den Anwendungszugriff
- Abschottung der unterschiedlichen Projekte durch unterschiedliche Zugriffsrechte

9. Verschleierung von Daten und Entfernung von Bezügen

Durch die Verschleierung von Daten sowie die Entfernung von Bezügen wird gewährleistet, dass eine Zuordnung der Daten zu einer spezifischen betroffenen Person ohne Kenntnis oder Hinzuziehung zusätzlicher Informationen nicht mehr möglich ist, sodass die Daten in ihrer gespeicherten Form keinen Personenbezug aufweisen oder dieser nur mit unverhältnismäßig hohem Aufwand hergestellt werden könnte.

- Pseudonymisierung der Daten auf Datenbankebene
- Getrennte Aufbewahrung des Pseudonyms und der zur Identifizierung notwendigen Daten
- Maskierung von Daten auf Anwendungsebene
- Aufhebung von Personenbezügen auf Anwendungsebene

10. Datenschutz-Management

Verantwortliche unterliegen gem. Art. 5 Abs. 2 DSGVO einer Rechenschaftspflicht und müssen nachweisen, dass sie geeignete Datenschutzmaßnahmen umsetzen. Die Maßnahmen des Datenschutz-Managements gewährleisten, dass die Einhaltung der datenschutzrechtlichen Anforderungen und die Wirksamkeit der technischen und organisatorischen Maßnahmen regelmäßig überprüft, bewertet und evaluiert werden.

10.1 Regulatorische Anforderungen

- Benennung eines Datenschutzbeauftragten
- Benennung von internen Datenschutzkoordinatoren
- Schriftliche Verpflichtung aller Mitarbeiter auf das Datengeheimnis
- Regelmäßige Schulungen der Mitarbeiter zu Datenschutz und Datensicherheit
- Verzeichnis für Verarbeitungstätigkeiten wird fortlaufend aktualisiert
- Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung
- Konzept zur Datenlöschung
- Dokumentierter Prozess zur Erkennung und Meldung von Datenschutzverstößen und Datensicherheitsvorfällen
- Prozess zur Wahrnehmung von Betroffenenrechten (insbesondere Informations- und Auskunftspflichten)
- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- Nachweise über Datenschutz-Folgenabschätzungen

10.2 Organisatorische Maßnahmen

- Regelmäßige Abstimmung mit dem Datenschutzbeauftragten
- Mobile Device Management
- Verwaltungsverfahren für kryptographische Schlüssel
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf/Berechtigung (Wiki, Intranet, etc.)
- Anlassbezogene Schulungen oder Informationen der Mitarbeiter
- Datenschutz- oder sonstige Compliance-Audits
- Datenschutz und Datensicherheitsrichtlinien
- Disziplinarmaßnahmen im Falle einer Datenschutzverletzung
- Zumindest dreistufige Klassifizierung von Daten (öffentlich, intern, vertraulich)
- Verbindliche Vorgaben für Administratoren
- Dokumentation und Prüfung über Hard- und Softwareänderungen (Evaluation vor und nach der Änderung)

- Unterschiedliche Zuständigkeiten für Anfrage, Genehmigung und Implementierung von Hard- und Softwareänderungen
- Software-Lebenszyklus-Management (SDLC)
- Schriftliche Richtlinien und zusätzliche Maßnahmen für mobiles Arbeiten und Home Office
- Schriftliche Dokumentation der Endgeräteverwaltung

Entwicklungsdienstleister:

- Geeignetes Informationssicherheitssystem (ISMS) gemäß anerkannten Standard wie etwa ISO/IEC 27001 vorhanden
- Betrieb der Infrastruktur in ISO/IEC 27001-zertifiziertem Rechenzentrum erstreckt
- BYOD-Vereinbarung

Rechenzentren:

- Benennung von IT-Compliance-Beauftragten
- Benennung von Informationssicherheitsbeauftragten
- Geeignetes Informationssicherheitssystem (ISMS) auf Basis der DIN ISO 27001 sowie dem VDA ISA-Standard
- Analyse von potentiellen Risiken und Bestimmung von Sicherheitsmaßnahmen zur Minderung der Risiken
- Regelmäßige Abstimmung mit dem Datenschutzbeauftragten
- Datenschutz und/oder Datensicherheitsrichtlinien
- Datensicherheitsaudits (intern/extern)
- Internes Kontrollsystem nach IDW PS 951 (Tyb B) und ISAE 3402 (Typ II) für Risikomanagement und Datensicherheit
- Mitarbeiter in relevanten Schlüsselpositionen erhalten entsprechende externe Schulungen und Personenzertifizierungen
- Verbindliche Vorgaben für Administratoren
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz für jeden Business Services
- Regelmäßige Schulungen oder Informationen bei Verwendung neuer Software bzw. Information über geänderte Richtlinien
- IT-Systeme werden ausschließlich in Deutschland betrieben
- Kommunikationskanäle zu Herstellern eingekaufter Hardware, um zeitnah über neue Patches und Updates informiert zu werden
- Updates und Patches werden rechtzeitig und unter Einbeziehung relevanter Stakeholder eingespielt
- Schriftlich festgelegter Prozess für Datenlöschung auf Systemkomponenten, die zum Hersteller zurückgesendet werden (Defekt, Leasing-Rückgabe, etc.)