Vertrag
über eine Auftragsdatenverarbeitung
gemäß Art. 28 DSGVO

zwischen dem

Landkreis Börde
Bornsche Str. 2
39340 Haldensleben

vertreten durch den Landrat
Herrn Martin Stichnoth

- Verantwortlicher - nachstehend Auftraggeber genannt –

und dem Unternehmen

vertreten durch den Geschäftsführer

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

wird folgender Vertrag geschlossen:

1. Gegenstand und Laufzeit des Vertrages, Kündigung

1.1 Gegenstand

Der Auftrag umfasst Folgendes:

Übergabe von personenbezogenen Daten zur Durchführung des freigestellten Schülerverkehrs im Landkreis Börde.

Der Auftragnehmer verarbeitet dabei für den Auftraggeber personenbezogene Daten im Sinne von Art. 4 Nr. 1, 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

1.2 Dauer

Der Vertrag beginnt am 11.08.2025 und wird für die Dauer von 5 Schuljahren geschlossen.

Die Laufzeit des Vertrages kann maximal um 1 Schuljahr verlängert werden.
(Verlängerungsoption)

1.3 Kündigung

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Konkretisierung des Vertragsinhalts

Art und Zweck der vorgesehenen Verarbeitung von Daten.

Die Art und der Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret im Vertrag zur Beförderung im Freigestellten Schülerverkehr für die Schuljahre 2025/2026 bis 2029/2030 im Landkreis Börde beschrieben.

2.1 Art der Daten

Die Art der verwendeten personenbezogenen Daten sind im Vertrag zur Beförderung im freigestellten Schülerverkehr unter Punkt 16.1 beschrieben.

2.2 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☒ Schulkinder
- ☒ Personensorgeberechtigte
- ☒ besuchte Schule

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte Personen des Auftraggebers, Weisungsempfänger beim Auftragnehmer

Weisungsberechtigte Personen des Auftraggebers sind:

Amt für Bildung
Amtsleiter
Herr Daniel Günther
Tel. Nr. 03904/7240-1412 bzw. eine oder mehrere von ihm beauftragte Mitarbeiter

Weisungsempfänger beim Auftragnehmer sind:

Für Weisung zu nutzende Kommunikationskanäle:

Postalisch	Landkreis Börde Amt für Bildung Bornsche Str. 2 39340 Haldensleben
E-Mail:	schulen-kultur@landkreis-boerde.de oder Schuelerbefoerderung@landkreis-boerde.de – jeweils verschlüsselt -
Telefon:	03904/7240-1411
Fax:	03904/7240-51420

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragnehmer dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Der Auftragnehmer hat die bestehenden (IST-Zustand) Sicherheitsvorkehrungen in Anlage 1 zu dokumentieren und über die gesamte Abwicklung der Dienstleistung für den Auftraggeber Überprüfungen in seinem Bereich durchzuführen:

- insbesondere:
    - Verschlusssicherheit von Papierunterlagen
    - Passwortschutz
    - Firewall.

Das Ergebnis der Kontrollen ist zu dokumentieren.

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO).

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DSGVO sind auch in diesem Fall sicherzustellen.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen (Fernmeldegeheimnis, Sozialgeheimnis).

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 Buchstabe b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Unternehmen**.**

Beim Auftragnehmer ist als Beauftragter für den Datenschutz

Name vom Auftragnehmer

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet.

8. Löschung und Rückgabe von personenbezogenen Daten

Kopien oder Duplikate der Daten 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.

Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsbeschreibung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Vertragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Dokumentationen, die dem Nachweis der vertrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

9. Haftung/Schadensersatz

Auf Art. 82 DSGVO wird verwiesen.
Im Übrigen gelten die gesetzlichen Regelungen.

10. Vertragsstrafe

Bei einem Verstoß des Auftragnehmers gegen die ihm von Gesetzes wegen oder aufgrund dieses Vertrages obliegenden Pflichten, insbesondere zur Einhaltung des Datenschutzes, wird eine Vertragsstrafe in Höhe von 1.000,00 Euro je Verstoß vereinbart.

Die Geltendmachung von Schadensersatzansprüchen bleibt hiervon unberührt.

Datum:

Unterschriften

……	……
Auftraggeber	Auftragnehmer

Anlage 1 – Technisch-organisatorische Maßnahmen
(vom Auftragnehmer anzukreuzen)

1. Allgemeine Maßnahmen

- ☐ interne Datenschutzvorschriften und Verhaltensregeln
- ☐ Internet- und E-Mail-Nutzungsrichtlinien
- ☐
- ☐ Mitarbeiter- / Sensibilisierungs-schulungen
- ☐ Datensicherheitskonzept
- ☐

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

- Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen

- ☐ Alarmanlage
- ☐ Sicherheitsschlösser
- ☐ Schlüsselregelungen (Ausgabe, etc)
- ☐ Absicherung von Gebäudeschächten
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☐ Sorgfältige Auswahl von Reinigungspersonal
- ☐
- ☐ Zutrittskontrolle (Transponder-System, Magnetkarte, etc.)
- ☐ Türsicherung
- ☐ Personenkontrolle beim Empfang
- ☐ Protokollierung der Besucher
- ☐ Tragepflicht von Berechtigungsausweisen
- ☐ Festlegung zutrittsberechtigte Personen
- ☐

- Zugangskontrolle: Keine unbefugte Systembenutzung

- ☐ Einrichtung eines Accounts pro User (Benutzerprofil)
- ☐ Zuordnung von Benutzerrechten
- ☐ Einsatz Hard- / Software-Firewall
- ☐ Einsatz von Anti-Viren-Software
- ☐ Protokollierung der Zugänge (z.B. durch Event-Logs)
- ☐ Verschlüsselung von mobilen Datenträgern (inkl. Backup-Systemen)
- ☐ Einsatz VPN-Technologie
- ☐
- ☐ Authentifikation mit Benutzername/ Passwort
- ☐ Kennwortverfahren / Passwortvergabe (mindestens 8 Zeichen, periodische Änderung)
- ☐ Regelmäßige Kontrolle der Gültigkeit der Zugangsberechtigungen
- ☐ Automatische Bildschirm-Sperrung
- ☐ Sicherung der Arbeitsplätze bei Abwesenheit
- ☐ Sperrung von externen Schnittstellen (z.B. USB)
- ☐

- Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen

- ☐ Berechtigungskonzepte (z.B. Profile, Rollen, Transaktionen, Trennung von User- und Admin-Accounts)
- ☐ Regelmäßige Kontrolle der Gültigkeit der zugewiesenen Berechtigungen
- ☐ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ☐ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Gütesiegel)
- ☐ Protokollierung der Vernichtung
- ☐ Festlegung der Zugriffsrechte (z.B. Lesen, Ändern, Löschen, Auswerten, Administrieren)
- ☐ Festlegung der personellen Zuständigkeiten
- ☐ physische Löschung von Datenträgern vor Wiederverwendung
- ☐ Verschlüsselung von Datenträgern
- ☐ sichere Aufbewahrung von Datenträgern

- Trennungskontrolle: Getrennte Verarbeitung von Daten, die unterschiedlichen Zwecken dienen

  ☐ Funktionstrennung Produktion / Test
  ☐ Festlegung von Datenbankrechten
  ☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
  ☐ Versehen der Datensätze mit Zweck-attributen/Datenfeldern
  ☐ Aufteilung in Mandanten oder logische Trennung von Datenbeständen
  ☐ physikalische getrennte Speicherung auf gesonderten Systemen oder Datenträgern
  ☐ Erstellung Berechtigungskonzept (Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten)
  ☐

- Pseudonymisierung

  ☐ Die Verarbeitung personenbezogener Daten erfolgt 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.
  ☐ Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

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

- Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

  ☐ Verschlüsselung in Teilen
  ☐ Elektronische Signatur
  ☐ Einrichtung von Virtual Private Network (VPN), Tunnelverbindung
  ☐ Weitergabe der Daten in anonymisierter oder pseudonymisierter Form
  ☐ Erstellung einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
  ☐ Festlegung der Übermittlungswege und Datenempfänger
  ☐ Transportsicherung (z.B. verschlossener Versand, sichere Transportbehälter/ - verpackungen; Kennwortschutz bei Dateiübertragung)
  ☐ beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen
  ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarten Löschfristen
  ☐

- Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Systeme eingegeben, verändert oder entfernt worden sind

  ☐ Festlegung der Zuständigkeiten für Eingaben
  ☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
  ☐ Vergabe der Rechte nach Berechtigungskonzept
  ☐
  ☐ Protokollierung von Eingaben, Änderungen, Löschungen
  ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
  ☐ Übersicht, aus der sich ergibt, mit welcher Applikation welche Daten eingegeben, geändert und gelöscht werden können
  ☐

- Auftragskontrolle: Maßnahmen, dass personenbezogene Daten, die im Auftrag verarbei-tet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

☐ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
☐ schriftliche Weisungen an den Auftragnehmer (z.B. Auftragsdatenverarbeitungsvertrag)
☐ Auftragnehmer hat Datenschutzbeauftragten bestellt
☐ Wirksame Kontrollrechte gegenüber dem Auftragsnehmer vereinbaren
☐ Verpflichtung der Mitarbeiter des Auftragnehmers zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes nach DSGVO
☐ Vertragsstrafen bei Verstößen
☐ vorherige Prüfung und Dokumentation getroffener Sicherheitsmaßnahmen beim Auftragnehmer
☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☐ laufende Überprüfung des Auftragnehmers und seiner Tätigkeit
☐

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

- Verfügbarkeitskontrolle, rasche Wiederherstellbarkeit: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust
-

☐ Virenschutz
☐ Regelmäßige Software-Updates
☐ Regelmäßige Durchführung einer Schwachstellenanalyse zu Hard- und Software
☐ Feuer- und Rauchmeldeanlagen
☐ Erprobung Wiederanlaufszenarien / Datenwiederherstellung
☐ In Hochwassergebieten: Serverräume über der Wassergrenze
☐ Regelmäßige Datensicherung (Aufbewahrung an sicherem, ausgelagertem Ort)
☐ Getrennte Aufbewahrung der Sicherungen
☐ Notfallplan (z.B. unterbrechungsfreie Stromversorgung, Backups)
☐ Feuerlöschgeräte in Serverräumen
☐ Serverräume nicht unter Sanitäranlagen
☐

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

- Datenschutz-Management

☐ Datenschutzfreundliche Voreinstellungen (Privacy by default)
☐ Incident-Response-Management (IT-Störungsmanagement)
☐ regelmäßige Revision des Sicherheitskonzeptes
☐
☐ Festlegung der Kriterien zur Auswahl von Auftragnehmern
☐ Eindeutige Vertragsgestaltung
☐ Regelmäßige Kontrolle der Vertragsausführung von Auftragnehmern
☐