## Vereinbarung zur Datenverarbeitung im Auftrag

## zwischen

## dem Land Niedersachsen, vertreten durch die Schulleiterin/ den Schulleiter

*Verantwortlicher (Auftraggeber)*

und

*Auftragsverarbeiter (Auftragnehmer)*

## 1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

*(Gegenstand des Auftrags, konkrete Beschreibung der Dienstleistungen)*

Der Auftragsverarbeiter verarbeitet dabei personenbezogene Daten für den Verantwortlichen im Sinne von Art. 4 Nr. 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 Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

### Dauer des Auftrags

Der Vertrag beginnt am       und endet am

oder

wird auf unbestimmte Zeit geschlossen. Kündigungsfrist ist      .

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

## 2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

*(nähere Beschreibung, ggf. Verweis auf Leistungsverzeichnis als Anlage etc.)*

### Art der Verarbeitung:

*(entsprechend der Definition von Art. 4 Nr. 2 DSGVO kommen zum Beispiel in Betracht: Das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung)*

### Art der personenbezogenen Daten:

*(entsprechend der Definition von Art. 4 Nr. 1 und Nr. 15 DSGVO z.B. Name, Anschrift, Daten zur Leistungsbewertung, Gesundheitsdaten, etc.)*

### Kategorien betroffener Personen:

*(entsprechend der Definition von Art. 4 Nr. 1 DSGVO zum Beispiel: Lehrer, Schüler, Eltern)*

## 3. Rechte und Pflichten sowie Weisungsbefugnisse des Verantwortlichen

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 Verantwortliche verantwortlich. Gleichwohl ist der Auftragsverarbeiter verpflichtet, alle solchen Anfragen, sofern sie erkennbar ausschließlich an den Verantwortlichen gerichtet sind, unverzüglich an diesen weiterzuleiten.

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

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

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

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

## 4. Weisungsberechtigte des Verantwortlichen, Weisungsempfänger des Auftragsverarbeiters

Weisungsberechtigte Personen des Verantwortlichen sind:

*(Vorname, Name, Organisationseinheit, Telefon)*

*Weisungsempfänger beim Auftragsverarbeiter sind:*

*(Vorname, Name, Organisationseinheit, Telefon)*

Für Weisung zu nutzende Kommunikationskanäle:

*(genaue postalische Adresse/ E-Mail/ Telefonnummer)*

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 Auftragsverarbeiters

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Verantwortlichen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter 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 Auftragsverarbeiter 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 Verantwortlichen nicht erstellt.

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

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

Der Auftragsverarbeiter hat über die gesamte Abwicklung der Dienstleistung sicherzustellen, dass die im Anhang genannten technischen und organisatorischen Maßnahmen getroffen werden.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Verantwortlichen, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Verantwortlichen hat der Auftragsverarbeiter im notwendigen Umfang mitzuwirken und den Verantwortlichen soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO). Er hat die dazu erforderlichen Angaben dem Verantwortlichen unverzüglich an folgende Stelle weiterzuleiten:

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

Der Auftragsverarbeiter hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Verantwortliche dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragsverarbeiters dem nicht entgegenstehen. Unabhängig davon hat der Auftragsverarbeiter personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Weisung des Verantwortlichen ein berechtigter Anspruch des Betroffenen aus Art. 16, 17 und 18 DSGVO zugrunde liegt.

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

Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Verantwortliche - 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 Verantwortlichen 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 Verantwortliche kann die Einhaltung eines genehmigten Zertifizierungsverfahrens gem. Art. 42 DSGVO durch den Auftragsverarbeiter als Faktor heranziehen, um die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen zu beurteilen.

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

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragsverarbeiters) ist nur mit Zustimmung des Verantwortlichen 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 Auftragsverarbeiter bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind.

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

Der Auftragsverarbeiter 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 lit. b und Art. 29 DSGVO).

Der Auftragsverarbeiter überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Beim Auftragsverarbeiter ist als Beauftragte(r) für den Datenschutz Herr/Frau

 *(Vorname, Name, Organisationseinheit, Telefon)*

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

oder

Ein betrieblicher Datenschutzbeauftragter ist beim Auftragsverarbeiter nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.

Sofern einschlägig:

Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO unverzüglich zu informieren.

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

Der Auftragsverarbeiter teilt dem Verantwortlichen unverzüglich Störungen, Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen sowie 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 Verantwortlichen nach Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter sichert zu, den Verantwortlichen 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 Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

## 7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Verantwortlichen ist dem Auftragsverarbeiter nur mit Genehmigung des Verantwortlichen gestattet, Art. 28 Abs. 2 DSGVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragsverarbeiter dem Verantwortlichen Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragsverarbeiter dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Verantwortlichen auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragsverarbeiter hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Verantwortlichem und Auftragsverarbeiter auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragsverarbeiters und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Verantwortliche berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragsverarbeiter im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragsverarbeiter die in Anlage ......... mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Verantwortliche einverstanden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO).

## 8. Technische und organisatorische Maßnahmen (insbesondere Art. 28 Abs. 3 Satz 2 lit. c und e DSGVO)

Der Auftragsverarbeiter hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen und das Ergebnis samt vollständigem Auditbericht dem Verantwortlichen mitzuteilen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Verantwortlichen abzustimmen.

Soweit die beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen den Anforderungen des Verantwortlichen nicht genügen, benachrichtigt er den Verantwortlichen unverzüglich.

Die Datensicherheitsmaßnahmen beim Auftragsverarbeiter können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Sicherheitsstandards nicht unterschreiten.

Wesentliche Änderungen hat der Auftragsverarbeiter mit dem Verantwortlichen in dokumentierter Form (schriftlich, elektronisch) abzustimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

## 9. Verpflichtungen des Auftragsverarbeiters nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragsverarbeiter sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen.

## 10. Haftung

Die Haftung der Parteien untereinander richtet sich nach den gesetzlichen Vorschriften.

## 11. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Für Nebenabreden ist grundsätzlich die Schriftform erforderlich.

Der Auftragsverarbeiter übereignet dem Verantwortlichen zur Sicherung die Datenträger, auf denen sich Dateien befinden, die Daten des Verantwortlichen enthalten. Diese Datenträger sind besonders zu kennzeichnen.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Verantwortlichen beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Verantwortlichen verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Für diesen Vertrag gilt deutsches Recht mit Ausnahme der Bestimmungen des internationalen Privatrechts.

Für alle Streitigkeiten aus diesem Vertrag ist, soweit nicht gesetzlich zwingend etwas anderes bestimmt ist, der Sitz des Auftraggebers als Gerichtsstand vereinbart.

### Datum:

### Unterschriften:

………………………………………………………….. …………………………………………………………..

Verantwortlicher Auftragsverarbeiter

**Anhang Technische und organisatorische
Maßnahmen nach Art. 32 DSGVO**

**1. Zugangskontrolle**

*Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.*

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

Beispiele

* Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
* Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
* Einrichtung eines Benutzerstammsatzes pro User
* Verschlüsselung von Datenträgern

**2. Datenträgerkontrolle**

*Das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Datenträgern ist zu verhindern.*

Beispiele

* Verschlüsselung von Datenträgern
* Inventarisierung aller Datenträger
* Regeln und Festlegen von Befugnissen für den Zugriff auf Datenträger

**3. Speicherkontrolle**

*Die unbefugte Dateneingabe, Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten ist zu verhindern.*

Beispiele

* Regeln und Festlegen von Befugnissen
* Installieren von Zugriffsschutzsystemen

**4. Benutzerkontrolle**

*Es ist zu verhindern, dass unbefugte Personen Datenverarbeitungssysteme, in denen personenbezogene Daten gespeichert werden, mit Hilfe von Einrichtungen der Datenübertragung nutzen können.*

Beispiele

* Festlegung der nutzungsberechtigten Personen
* Identifikation und Authentifizierung der Benutzer
* Verschlüsselung der zu übertragenden Daten

**5. Zugriffskontrolle**

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

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

Beispiele

* Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
* Auswertungen
* Kenntnisnahme
* Veränderung
* Löschung

**6. Übermittlungskontrolle**

*Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle ...*

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

Beispiele

* Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network)
* Elektronische Signatur
* Protokollierung
* Transportsicherung

**7. 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:

Beispiel

* Protokollierungs- und Protokollauswertungssysteme

**8.** **Verfügbarkeitskontrolle**

*Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.*

Maßnahmen zur Datensicherung (physikalisch / logisch):

Beispiele

* Backup-Verfahren
* Spiegeln von Festplatten, z.B. RAID-Verfahren
* Unterbrechungsfreie Stromversorgung (USV)
* Getrennte Aufbewahrung
* Virenschutz / Firewall
* Notfallplan

**9.** **Auftragskontrolle**

*Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.*

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

Beispiele

* Eindeutige Vertragsgestaltung
* Formalisierte Auftragserteilung (Auftragsformular)
* Kriterien zur Auswahl des Auftragnehmers
* Kontrolle der Vertragsausführung

**10. Transportkontrolle**

*Es ist zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können.*

Beispiele

* Festlegung der für die Übermittlung oder den Transport Berechtigten
* Verwendung sicherer Transportbehälter
* Verbindliche Festlegung eines sicheren Transportweges

**11. Organisationskontrolle**

*Die innerbetriebliche Organisation ist so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.*

Beispiele

* Bestellung eines Datenschutzbeauftragten
* Schulung der Beschäftigten
* Erlass von Datenschutzrichtlinien
* Erstellung eines Notfallkonzeptes
* Erstellung von Benutzeranweisungen