Auftragsverarbeitungsvertrag

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag
gemäß Art. 28 Abs. 3 DSGVO

Zwischen

Schulträger:	
Schule (Schulname):	
Schulort:	
Anschrift:	

– nachfolgend „**Verantwortlicher**“ genannt –

und

Land Niedersachsen, vertreten durch das
Landesinstitut für schulische Qualitätsentwicklung (NLQ) Hildesheim

– nachfolgend „**Auftragsverarbeiter**“ genannt –

- Verantwortlicher und Auftragsverarbeiter gemeinsam auch die „**Parteien**“ genannt -

Präambel

Im Rahmen der Erfüllung der Nutzungsvereinbarung, nach welcher der Auftragsverarbeiter der Schule eine Wordpress-Plattform kostenfrei zur Nutzung zur Verfügung stellt, verarbeitet das NLQ im Auftrag der verantwortlichen Schule personenbezogene Daten. Hierfür schließen die Parteien den nachfolgenden Auftragsverarbeitungsvertrag ab:

Begriffsbestimmungen

In diesem Vertrag verwendete Begriffe, die in der DSGVO definiert werden, sind im Sinne dieser gesetzlichen Definition zu verstehen.

Vertragsgegenstand

1.1 Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen im Zusammenhang mit der Überlassung einer Wordpress-Plattform zur Nutzung.

1.2 Dabei erhält der Auftragsverarbeiter Zugriff auf personenbezogene Daten und verarbeitet diese nur im Rahmen des Hostings, im Auftrag und nach Weisung des Verantwortlichen, sofern der Auftragsverarbeiter nicht durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist.

1.3 Die Weisungen des Verantwortlichen werden anfänglich durch diesen Vertrag festgelegt und können vom Verantwortlichen danach in schriftlicher Form oder in einem dokumentierten elektronischen Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Verantwortliche ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Regelungen über eine etwaige Vergütung von Mehraufwendungen, die durch ergänzende Weisungen des Verantwortlichen an den Auftragsverarbeiter entstehen, bleiben unberührt.

1.4 Alle erteilten Weisungen sind sowohl vom Verantwortlichen als auch vom Auftragsverarbeiter zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für weitere drei volle Kalenderjahre aufzubewahren.

1.5 Die jeweiligen Weisungsbefugten bzw. die Empfangsberechtigten einer Weisung sowie die jeweiligen Datenschutzbeauftragten werden in der **Anlage A** aufgeführt

Betroffene Personen, Art und Zweck und Umfang der Verarbeitung

1.5.1 Der Auftragsverarbeiter verarbeitet im Auftrag personenbezogene Daten von folgenden betroffenen Personen:

- Lehrerinnen, Lehrer
- Schülerinnen, Schüler

1.5.2 Der Auftragsverarbeiter verarbeitet im Auftrag folgende personenbezogenen Daten:

- IP-Adressen
- Benutzernamen und Passwörter (Zugangsdaten)
- Logfiles, Metadaten, technische Daten

1.5.3 Der Auftragsverarbeiter verarbeitet keine besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO im Auftrag.

1.6 Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten im Auftrag zu folgenden Zwecken:

- Bereitstellung der Wordpress-Plattform wie vereinbart, hierzu gehören Login-Möglichkeiten und Nutzung der Wordpress-Plattform für und durch Mitarbeitende der Schule oder durch die Schule beauftragte Personen.

1.7 Der Auftragsverarbeiter nimmt folgende Verarbeitungen im Auftrag vor (Art der Verarbeitung):

- Erheben/Auslesen/Verwendung: Bereitstellungs- und Support-Leistungen

- Verwendung/Organisation/Löschen/Vernichtung: Verwaltung und Bereitstellung der Wordpress-Plattform.

1.8 Der Umfang der Verarbeitung ergibt sich aus den Vereinbarungen zum Hosting.

Rechte und Pflichten des Verantwortlichen

1.9 Dem Verantwortlichen obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO.

1.10 Der Verantwortliche hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er bei Nutzung der Dienste Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

1.11 Der Verantwortliche ist für die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten Art. 30 Abs. 1 DSGVO zuständig.

1.12 Dem Verantwortlichen obliegt die Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten. Der Auftragsverarbeiter wird unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten unterstützen.

1.13 Dem Verantwortlichen obliegen die aus den Artikeln 15-21 DSGVO resultierenden Pflichten gegenüber den Betroffenen, insbesondere über Auskunft, Berichtigung und Löschung. Der Auftragsverarbeiter wird den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, die Pflichten des Verantwortlichen zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO (Betroffenenrechte) genannten Rechte der betroffenen Person nachzukommen. Macht eine betroffene Person ihre Rechte nach Kapitel III DSGVO gegenüber dem Auftragsverarbeiter geltend, so reagiert dieser nicht selbstständig, sondern verweist die betroffene Person unverzüglich an den Verantwortlichen und wartet dessen Weisungen ab.

Rechte und Pflichten des Auftragsverarbeiters

1.14 Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisungen des Verantwortlichen. Dies gilt auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtliche Anforderung vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

1.15 Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen. Der Auftragsverarbeiter verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt.

1.16 Der Auftragsverarbeiter unternimmt zudem Schritte, um sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Europäischen Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

1.17 Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Das Datengeheimnis und/oder die Verpflichtung zur Vertraulichkeit bestehen auch nach Beendigung der Tätigkeit fort.

1.18 Der Auftragsverarbeiter stellt dem Verantwortlichen die für die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO notwendigen Angaben zur Verfügung. Ferner erstellt der Auftragsverarbeiter selbst ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung nach Art. 30 Abs. 2 DSGVO. Dieses Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann. Der Auftragsverarbeiter stellt der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

1.19 Der Auftragsverarbeiter teilt dem Verantwortlichen die Kontaktdaten des betrieblichen bzw. behördlichen Datenschutzbeauftragten mit. Der für den Auftragsverarbeiter benannte Datenschutzbeauftragte wird in **Anlage A** mitgeteilt. Sofern ein Wechsel stattfindet, wird die Anlage unverzüglich aktualisiert und den in Anlage A festgelegten Empfangsberechtigten übersendet.

1.20 Datensicherungen sind vom Auftragsverarbeiter sorgfältig zu verwahren, sodass sie Dritten nicht zugänglich sind. Der Auftragsverarbeiter ist verpflichtet, dem Verantwortlichen jederzeit Auskünfte zu erteilen, soweit dessen Daten und Unterlagen betroffen sind. Die datenschutzkonforme Vernichtung von Datensicherungen übernimmt der Auftragsverarbeiter in regelmäßigen Abständen, mindestens alle fünf Jahre ab Vertragsbeginn.

1.1 Die Verarbeitung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den europäischen Wirtschaftsraum statt. Jede Verlagerung von Teilleistungen oder der gesamten Dienstleistung in ein Drittland

bedarf der vorherigen Zustimmung des Verantwortlichen in Schriftform oder in einem dokumentierten elektronischen Format und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

1.21 Der Auftragsverarbeiter ist berechtigt, personenbezogene Daten außerhalb des Bürogebäudes des Auftragsverarbeiters (z.B. bei der Heimarbeit durch Mitarbeiter des Auftragsverarbeiters) zu verarbeiten,

- sofern der Auftragsverarbeiter den Verantwortlichen vorher schriftlich oder elektronisch darüber informiert hat, an welchen sonstigen Orten eine Datenverarbeitung stattfindet. Der Verantwortliche ist berechtigt, nach billigem Ermessen der Verarbeitung von personenbezogenen Daten außerhalb der Hauptniederlassung des Auftragsverarbeiters zu widersprechen. Bei der Verarbeitung von personenbezogenen Daten im Rahmen von Heimarbeit hat der Verantwortliche das Recht, gemäß dem Verfahren in Ziffer 7 dieses Vertrags, Kontrollen durchzuführen. Ferner sind spezielle technische und organisatorische Maßnahmen für die Heimarbeit implementiert.

- sofern ein entsprechender Auftrag des Verantwortlichen im Einzelfall vorliegt (z.B. zur Untersuchung und Behebung von Störungen).

- sofern der Verantwortliche hierzu generell seine vorherige schriftliche oder elektronisch dokumentierte Zustimmung erteilt hat. Der Verantwortliche ist berechtigt, nach billigem Ermessen der Verarbeitung von personenbezogenen Daten außerhalb der Hauptniederlassung des Auftragsverarbeiters zu widersprechen. Bei der Verarbeitung von personenbezogenen Daten im Rahmen von Heimarbeit hat der Verantwortliche das Recht, gemäß dem Verfahren in Ziffer 7 dieses Vertrags, Kontrollen durchzuführen. Ferner sind spezielle technische und organisatorische Maßnahmen für die Heimarbeit implementiert.

Hierfür werden Regelungen zum mobilen Arbeiten in Form von Richtlinien beim Auftragsverarbeiter eingesetzt, welche die Verarbeitungsvorgänge des Verantwortlichen im Rahmen dieses Auftragsverarbeitungsvertrags absichern. Die Richtlinien sind vom Auftragsverarbeiter und seinen Mitarbeitern zu beachten und dem Verantwortlichen auf Anfrage vorzulegen.

Technische und organisatorische Maßnahmen

1.22 Der Auftragsverarbeiter hat angemessene technische und organisatorische Maßnahmen zu ergreifen und aufrechtzuerhalten, um die Daten vor dem Zugriff Dritter oder Datenverlust zu schützen. Der Auftragsverarbeiter wird daher in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. So trifft er alle

technischen und organisatorischen Maßnahmen zur angemessenen Sicherung der Daten des Verantwortlichen (Art. 32 DSGVO).

1.23 Diese technischen und organisatorischen Maßnahmen sind in **Anlage B** geregelt.

1.24 Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellungen grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen zugesichert sind, dass diese Daten nicht ohne aktives Eingreifen einer unbestimmten Zahl von natürlichen anderen Personen zugänglich gemacht werden.

1.25 Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verwaltung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird. Änderungen an den technischen und organisatorischen Maßnahmen sind dem Verantwortlichen vorher so rechtzeitig anzuzeigen, dass diesem genügend Zeit bleibt, um auf Änderungen entsprechend reagieren zu können. Die jeweils aktuelle Fassung der technischen und organisatorischen Maßnahmen wird dem Verantwortlichen zur Zustimmung übersandt.

Kontrollrechte und -pflichten

1.26 Der Verantwortliche überzeugt sich in regelmäßigen Abständen von den technischen und organisatorischen Maßnahmen des Auftragsverarbeiters und kann sich dazu vom Auftragsverarbeiter deren Einhaltung schriftlich bestätigen lassen. Der Verantwortliche oder dessen Beauftragter kann sich hierfür auch vor Ort selbst überzeugen. Der Auftragsverarbeiter räumt dem Verantwortlichen oder dessen Beauftragten insofern ein Zutrittsrecht während der üblichen Arbeitszeit für die Räumlichkeiten und Einrichtungen des Auftragsverarbeiter ein.

1.27 Der Nachweis dafür, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Vorgaben der DSGVO erfolgt, kann der Auftragsverarbeiter auch durch Vorlage einer Bestätigung eines anerkannten lizenzierten Auditors, dass genehmigte Verhaltensregeln gemäß Art. 40 DSGVO oder ein genehmigtes Zertifizierungsverfahren gemäß Art. 42 DSGVO durch den Auftragsverarbeiter eingehalten werden, erbringen.

1.28 Der Auftragsverarbeiter muss dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur

Verfügung stellen sowie Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und dazu beitragen.

Unterauftragsverhältnisse

1.2 Dem Auftragsverarbeiter wird allgemein gestattet, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) in Anspruch zu nehmen. Der Auftragsverarbeiter muss dies gegenüber dem Verantwortlichen innerhalb von vier Wochen vor Beginn der Verarbeitung durch einen Unterauftragsverarbeiter schriftlich anzeigen. Der Verantwortliche kann dagegen Einspruch erheben. Mit dem Unterauftragsverarbeiter ist eine Vereinbarung nach Maßgaben des Art. 28 Abs. 2-4 DSGVO abzuschließen. Jede Verlagerung von Teilleistungen oder der gesamten Dienstleistung auf einen Unterauftragsverarbeiter in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen in Schriftform oder in einem dokumentierten elektronischen Format und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

1.29 Nimmt der Auftragsverarbeiter die Dienste eines Unterauftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diese dem weiteren Auftragsverarbeiter eben Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrumenten zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Art. 28 Abs. 3 DSGVO festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

1.30 Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes weiteren Auftragsverarbeiters.

1.31 Die Kundenbetreuung und die technische Betreuung erfolgen direkt über den Auftragsverarbeiter.

Informationspflichten des Auftragsverarbeiters

1.32 Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes (z.B. technischer Art), im Falle einer Verletzung des Schutzes personenbezogener Daten oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen (Art. 33 Abs. 2 DSGVO). Der Auftragsverarbeiter trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen Person(en), informiert hierüber den Verantwortlichen und ersucht diesen um weitere Weisungen.

1.33 Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Auftragsverarbeiter auf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

1.34 Sollten die Daten des Verantwortlichen beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich darüber zu informieren. Der Auftragsverarbeiter wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Verantwortlichen als „verantwortliche Stelle“ im Sinne der DSGVO liegen.

Haftung

1.35 Sofern nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrags der des Hostings.

Laufzeit und Kündigung

1.36 Die Vertragsdauer entspricht der Dauer des Hostings.

1.37 Eine Kündigung des Hostings bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen. Das Recht der Parteien zur außerordentlichen Kündigung dieses Vertrags sowie des Hostings aus wichtigem Grund bleibt hiervon unberührt.

1.38 Das Hosting darf im Falle einer Beendigung dieses Vertrags nur fortgeführt werden, wenn ausgeschlossen ist, dass der Auftragsverarbeiter personenbezogene Daten des Verantwortlichen verarbeitet. Im Zweifel gilt eine Kündigung des Hostings auch als eine Kündigung dieses Vertrags und gilt eine Kündigung dieses Vertrags auch als Kündigung des Hostings, sofern die Parteien nichts anderes vereinbaren.

1.39 Nach Ende des Vertragsverhältnisses sind vom Auftragsverarbeiter alle Daten des Verantwortlichen spätestens innerhalb eines Monats zu löschen. Der Auftragsverarbeiter hat dem Verantwortlichen die Löschung unverzüglich schriftlich oder in elektronischem Format zu bestätigen. Der Auftragsverarbeiter muss auf Wunsch des Verantwortlichen diesem alle personenbezogenen Daten zurückgeben.

Sonstiges

1.40 Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hostings vor.

1.41 Änderungen oder Ergänzungen und die Aufhebung dieses Vertrags bedürfen nach Art. 28 Abs. 9 DSGVO der elektronisch dokumentierten Formen oder der Schriftform. Gleiches gilt für die Aufhebung des Schriftformerfordernisses selbst.

1.42 Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragsverarbeiter i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der dazugehörigen Datenträger ausgeschlossen ist.

1.43 Sollte eine Regelung dieses Vertrags nichtig sein oder werden oder sich eine Lücke herausstellen, bleibt der Vertrag im Übrigen gültig. Es soll das gelten, was die Parteien vereinbart hätten, wenn die Unwirksamkeit oder die Lücke bekannt gewesen wäre. Die Vertragsparteien prüfen dann gemeinsam, ob Änderungen oder Ergänzungen dieses Vertrags erforderlich sind. Kommen Sie zu dem Ergebnis, dass eine Änderung oder Ergänzung des Vertrags erforderlich ist, oder wird von einer Vertragspartei eine Änderung oder Ergänzung dieses Vertrags beantragt, so nehmen Sie unverzüglich Verhandlungen auf.

1.44 Diese Vereinbarung unterliegt deutschem Recht.

Datum und Unterschriften

_____	_____
Für die Schule	Für das NLQ

Anlage A: Weisungsberechtigte und Empfangsberechtigte; Datenschutzbeauftragte

Für die Schule als Weisungsberechtigter

Schulträger:	
Schule:	
Schulort:	
Weisungsberechtigter (Name):	
Weisungsberechtigter (E-Mail-Adresse):	

Für das NLQ als Empfangsberechtigter

Land Niedersachsen, vertreten durch das

Landesinstitut für schulische Qualitätsentwicklung (NLQ)

Empfangsberechtigter (Name):	Martin Gembus
Empfangsberechtigter (E-Mail-Adresse):	gembus@nibis.de

Datenschutzbeauftragter der Schule

Datenschutzbeauftragter der Schule (Name):	
Datenschutzbeauftragter Schule (E-Mail-Adresse):	

Datenschutzbeauftragter des NLQ:

Den/Die Datenschutzbeauftragte/n erreichen Sie unter:	datenschutz@nlq.niedersachsen.de

Anlage B: Technische und Organisatorische Maßnahmen

A. Vertraulichkeit (Art. 32 (1) lit. b DSGVO, Art 5 (1) lit. f DSGVO)

1. Zutrittskontrolle

Technische Maßnahmen

- **Alarmanlage**
- **Zutrittssicherung Serverraum**
- **Manuelles Schließsystem (z.B. Türschlösser)**

Organisatorische Maßnahmen

- **Schließordnung (Regelung betreffend Öffnen und Verschließen von Gebäuden und Räumen)**
- **Richtlinie/ Anweisung für Zutritt Externer**

2. Zugangskontrolle

Technische Maßnahmen

- **Benutzer-Authentifikation (Name und Passwort)**
- **Firewall**
- **Zugangssicherung des WLAN**

Organisatorische Maßnahmen

- **Passwortrichtlinie**
- **Richtlinie zur Löschung/Vernichtung von Dokumenten mit personenbezogenen Daten**

3. Zugriffskontrolle

Technische Maßnahmen

- **Verwaltung der Zugriffsrechte durch wenige notwendige Administratoren**
- **Zugriffsprotokolle (Datenverarbeitungsanlagen)**

Organisatorische Maßnahmen

- **Verwaltung von Benutzerberechtigungen (Berechtigungskonzept)**
- **Vertraulichkeitsverpflichtung**

- **Formaler Prozess für Erteilung von Zugriffsberechtigungen**

4. Trennungskontrolle

Technische Maßnahmen

- **Mandantenfähigkeit von Anwendungen**
- **Physikalische Trennung von Unterlagen (z.B. Ordner)**
- **Physikalische Trennung von Datenbanken/ Datenträgern**

Organisatorische Maßnahmen

- **Verwaltung von Benutzerberechtigungen für Datenbanken/ Anwendungen**
- **Verzeichnis von Verarbeitungstätigkeiten**
- **Anweisung zur Trennung privater und betrieblicher Daten**
- **Keine private Nutzung betrieblicher Geräte**

B. Integrität (Art. 32 (1) lit. b DSGVO, Art 5 (1) lit. f DSGVO)

1. Weitergabekontrolle

Technische Maßnahmen

- **Verschlüsselung**

Organisatorische Maßnahmen

- **Sorgfältige Auswahl der Auftragsverarbeiter**

Sonstige Maßnahmen

- **SSL-/TLS-Verschlüsselung aller elektronisch übertragenen Daten (bis auf die IP-Adresse)**
- **Umleitung des Datenverkehrs über NLQ-eigenen Server, um zu gewährleisten, dass keine IP-Adressen von privaten Endgeräten an Microsoft übermittelt werden**

2. Eingabekontrolle

Organisatorische Maßnahmen

- **Zuständigkeit für Löschung definiert**
- **Berechtigungskonzept**

C. Verschlüsselung personenbezogener Daten (Art. 32 (1) lit. a DSGVO)

Technische Maßnahmen

- **Verschlüsselung von Laptops/ Tablets**
- **Verschlüsselung von Festplatten**
- **SSL-Verschlüsselung auf Website(s)**

Sonstige Maßnahmen

- **Automatische Verschlüsselung der eingesetzten Datenbanken**

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

Technische Maßnahmen

- **Unterbrechungsfreie Stromversorgung**
- **Regelmäßiges Back-Up**

Organisatorische Maßnahmen

- **Planung von Kapazität und Betriebsmitteln**

E. Wiederherstellbarkeit (Art. 32 (1) lit. c DSGVO)

Technische Maßnahmen

- **Regelmäßiges Back-Up in angemessenen Zeitabständen**
- **Virtualisierung von Back-Ups**

F. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 (1) lit. d. DSGVO)

1. Datenschutz-Management

Technische Maßnahmen

- **Aktualisierung des Betriebssystems durch regelmäßige Updates oder Patches**

Organisatorische Maßnahmen

- **Sensibilisierung der Beschäftigten bzgl. Datenschutz, insb. zur Vermeidung von Cyberangriffen mittels Social-Engineerings**

- **Bestellung Datenschutzbeauftragte/r**
- **Jährliche Überprüfung technischer und organisatorischer Maßnahmen**
- **Regelmäßige dokumentierte Überprüfung von Auftragsverarbeitern**

2. Datenschutz-Prozesse

Organisatorische Maßnahmen

- **Definierter Prozess zur Meldung von Datenpannen**
- **Löschkonzept**

3. Auftragskontrolle

Organisatorische Maßnahmen

- **Vorherige Prüfung der TOM jedes (weiteren) Auftragsverarbeiters**
- **Sorgfältige Auswahl von Auftragsverarbeitern**
- **Schriftliche/elektronisch dokumentierte Weisungen an Auftragsverarbeiter**
- **Abschluss von AVV**
- **Einsatz von EU-Standard-Vertragsklauseln**

G. Privacy by design (Art. 25 (1) DSGVO)

Technische Maßnahmen

- **Software ermöglicht eine Verschlüsselung der Daten**
- **Software ermöglicht die Löschung von Daten**

H. Privacy by default (Art. 25 (2) DSGVO)

Technische Maßnahmen

- **Es wird ausschließlich die minimal notwendige Menge an personenbezogenen Daten erhoben, nämlich IP-Adressen und pseudonyme Anmeldedaten**

I. TOM im Homeoffice

Im Homeoffice gelten die folgenden zusätzlichen bzw. ergänzenden technischen und organisatorischen Maßnahmen:

Vertraulichkeit

- **Passwörter oder sonstige Zugangsmöglichkeiten für Laptops sind geheim zu halten und Dritten nicht zugänglich zu machen.**
- **Unterlagen mit personenbezogenen oder sonst vertraulichen Daten sind unter Verschluss zu halten, sodass Dritte keinen Zugriff hierauf haben können.**

Integrität

- **Es ist untersagt, Sicherheitsmaßnahmen zu deaktivieren oder zu umgehen oder sonstige technische Veränderungen an den durch das Unternehmen zur Verfügung gestellten Geräten vorzunehmen. Software darf nur nach vorheriger Absprache mit dem IT-Verantwortlichen installiert werden.**
- **Ausdrucke mit vertraulichen Informationen (z. B. personenbezogenen Daten) müssen sicher vernichtet werden, wenn sie nicht mehr benötigt werden und keine gesetzlichen Aufbewahrungspflichten einzuhalten sind.**
- **Alle Störungen oder Auffälligkeiten bei der EDV-Nutzung sind unverzüglich bei dem IT-Verantwortlichen zu melden.**
- **Alle Mitarbeiter wurden zur Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet.**

Verfügbarkeit (inkl. schneller Wiederherstellbarkeit bei einem Zwischenfall) und Belastbarkeit

- **Der Systemzugriff erfolgt cloudbasiert, d.h. sollte aus dem Homeoffice kein Zugriff möglich sein (z.B. wegen Laptopverlust oder -beschädigung), ist es möglich, aus dem Büro weiterzuarbeiten.**

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- **Ein Datenschutzmanagementsystem ist eingerichtet:**
  - **Es wurde ein DSB bestellt**
  - **Datenschutzrichtlinien sind eingeführt; Mitarbeiter bestätigen die Kenntnisnahme der DS-Richtlinien**
- **Es ist ein Prozess bei Datenschutzvorfällen etabliert, dieser wird regelmäßig geprüft**