

Datenschutzrechtliche Vereinbarung (nachfolgend auch Vertrag genannt) über die Verarbeitung personenbezogener Daten im Auftrag (Auftragsverarbeitung gemäß Art. 28 DS-GVO)

Zwischen

- „Auftraggeber“ -

und

Namaco UG (haftungsbeschränkt)

Kirchturmsweg 6

31840 Hessisch Oldendorf

- „Auftragsverarbeiter“ –

1. Gegenstand und Dauer der Vereinbarung

Der Gegenstand der Leistungen ergibt sich aus dem Software as a Service (SAAS) Vertrag zur Nutzung der Software Diplomify (Hauptvertrag).

1. Der Auftragsverarbeiter verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.
2. 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 darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Dauer des Auftrags:

- Die Vertragslaufzeit richtet sich nach der Laufzeit des Hauptvertrages.

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

Die Verarbeitung personenbezogener Daten im Auftrag erfolgt ausschließlich zweckgebunden. Der Zweck, der Umfang und die Art ergeben sich (gemäß der Definition von Art. 4 Nr. 2 DS-GVO) aus der Leistungsvereinbarung des Hauptvertrages und dem Verzeichnis der Verarbeitungstätigkeiten (Anlage 3).

Kategorien betroffener Daten (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):

- Beschäftigtendaten (Lehrkräfte)
- Schüler*innendaten

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DS-GVO):

Stammdaten

Schüler*innen: Name, Vorname, Namenszusatz, Geschlecht, Alter, Geburtsort/-land/-datum

Lehrkräfte: Name, Vorname, Namenszusatz, Email-Adresse

personenbezogene Daten

Schüler*innen: Abschlüsse, Arbeitsgemeinschaften, Arbeitsverhalten, besuchter Unterricht, Bemerkungen, erhaltene Abschlüsse, Fächer, Jahrgangsstufe, Klasse, Kompetenzbereiche, Kompetenzen, Konferenzdaten, Kurse, Niveaustufen, Schüler, Schulformen, Schuljahre, Sozialverhalten, Unterrichtsarten, übernommene Ämter, Versetzungsstatus, (un) entschuldigte Fehltage, Zeugnisse (PDF)

Lehrkräfte: Benutzername, Klassenleitung, unterrichtete Fächer, IP-Adresse der letzten Anmeldung, letzte Änderungen an Schüler*innen und Noten, Prüfsumme des Kennwortes, technische Angaben zu Browser und Betriebssystem

Bewertungen und Zeugnisdaten

Schüler*innen: Bewertungen in den Fächern, Bewertung von Arbeits- und Sozialverhalten, Kompetenzbewertungen, Noten

Förderbedarfe

Schüler*innen: Förderbedarf, Bedarfsausgangslage, Förderziele/-maßnahmen, Förderdauer, Förderkurse

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

1. Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinn. Gleichwohl ist der Auftragsverarbeiter verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.
2. Sollten Dritte gegen den Auftragsverarbeiter aufgrund der Verarbeitung von Auftraggeber-Daten nach Maßgabe dieses Vertrages Ansprüche geltend machen, wird der Auftraggeber den Auftragsverarbeiter von allen solchen Ansprüchen auf erstes Anfordern freistellen.
3. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
4. 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. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragsverarbeiters und erfolgen in Textform.
5. Der Auftraggeber ist berechtigt, sich wie unter Nr. 11 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.
6. Der Auftraggeber informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
7. Der Auftraggeber 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 Auftraggebers, Weisungsempfänger des Auftragsverarbeiters

Weisungsberechtigte Funktionen des Auftraggebers sind:

Ansprechpartner Auftraggeber

Weisungsempfänger beim Auftragsverarbeiter sind:

- Christoph Müller, Geschäftsführer Namaco UG (haftungsbeschränkt),
- Michael Perk (Hauptentwickler)

Für Weisung zu nutzende Kommunikationskanäle:

- postalisch an folgende Anschrift: Kirchturmsweg 6, 31840 Hessisch Oldendorf
- per Email an folgende Adresse: info@diplomify.de

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

1. Der Auftragsverarbeiter 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 Auftragsverarbeiter unterliegt, verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen/Auftraggeber 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 DS-GVO).
2. 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 Auftraggebers nicht erstellt.
3. Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragsverarbeiter im notwendigen Umfang gegen Erstattung der dem Auftragsverarbeiter hierdurch entstehenden nachzuweisenden Aufwände und Kosten mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils an die in Ziffer 4 genannte weisungsberechtigte Funktion des Auftraggebers weiterzuleiten.
4. Der Auftragsverarbeiter 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 DS-GVO). Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.
5. Der Auftragsverarbeiter 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 Auftragsverarbeiters dem nicht entgegenstehen.

6. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.
7. Der Auftragsverarbeiter sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.
8. Der Auftragsverarbeiter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.
9. Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter 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 DS-GVO). Der Auftragsverarbeiter überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.
10. Der Auftraggeber und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
11. Der Auftraggeber ist unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde zu informieren, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
12. Soweit der Auftraggeber seinerseits einer Kontrolle der 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 ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
13. Beim Auftragsverarbeiter ist als Beauftragte(r) für den Datenschutz bestellt:

Name, Vorname:	Dr. Sebastian Kraska
Organisationseinheit:	IITR Datenschutz GmbH Marienplatz 2, 80331 München
Kontaktdaten:	email@iitr.de

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

6. Rechte der betroffenen Person

1. Der Auftragsverarbeiter wird den Auftraggeber mit technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.
2. Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragsverarbeiter geltend macht, wird der Auftragsverarbeiter dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.
3. Der Auftragsverarbeiter wird dem Auftraggeber Informationen über die gespeicherten Auftraggeber-Daten, die Empfänger von Auftraggeber-Daten, an die der Auftragsverarbeiter sie auftragsgemäß weitergibt, und den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen oder er sie sich selbst beschaffen kann.
4. Der Auftragsverarbeiter wird es dem Auftraggeber ermöglichen, im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragsverarbeiter hierdurch entstehenden nachzuweisenden Aufwände und Kosten, Auftraggeber-Daten zu berichtigen, zu löschen oder

ihre weitere Verarbeitung einzuschränken oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Einschränkung der weiteren Verarbeitung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

5. Soweit die betroffene Person gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit bezüglich der Auftraggeber-Daten nach Art. 20 DSGVO besitzt, wird der Auftragsverarbeiter den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei der Bereitstellung der Auftraggeber-Daten unterstützen, wenn der Auftraggeber sich die Daten nicht anderweitig beschaffen kann.

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

1. Der Auftragsverarbeiter teilt dem Auftraggeber 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 Auftraggebers nach Art. 33 und Art. 34 DS-GVO.
2. Der Auftragsverarbeiter sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

8. Unterauftragsverhältnisse mit Subunternehmern für Kerndienstleistungen (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

1. Die zukünftige Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragsverarbeiter ohne gesonderte Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 Satz 2 DS-GVO. Der Auftragsverarbeiter muss 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 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen. In diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen zudem immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter.
2. Eine Beauftragung von Subunternehmern in Drittstaaten erfolgt nicht.
3. Der Auftragsverarbeiter hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber 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 Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.
4. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

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

Der Auftragsverarbeiter hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen:

- Regelmäßige Prüfung des beim Subunternehmer eingerichteten Datenschutzkonzeptes (mindestens alle 2 Jahre)
- Regelmäßige Prüfung der beim Subunternehmer eingerichteten technischen und organisatorischen Maßnahmen (mindestens alle 2 Jahre)

Das Ergebnis der Überprüfungen ist zu dokumentieren.

Zurzeit sind für den Auftragsverarbeiter die in der Anlage 1 dokumentierten Subunternehmer mit der Verarbeitung von personenbezogenen Daten beschäftigt.

6. Der Auftragsverarbeiter informiert den Verantwortlichen über jede Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer.

9. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

1. Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird. Für die auftragsgemäße Verarbeitung personenbezogener Daten wird eine angemessene und nachvollziehbare Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten der von der Verarbeitung Betroffenen berücksichtigt.
2. Das in Anlage 2 beschriebene Datenschutzkonzept stellt die Mindestanforderungen der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragsverarbeiter dar. Hierbei ist auch das Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung beschrieben.
3. 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 (Art. 32 Abs. 1 lit. d DS-GVO).
4. Die Maßnahmen beim Auftragsverarbeiter können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

10. Verpflichtungen des Auftragsverarbeiters nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

1. Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig löschen. Eine Löschung darf ausschließlich im Rahmen der Vertragsbeendigung oder nach dokumentierter Weisung des Auftraggebers erfolgen.
2. Löschanfragen, die eine betroffene Person an den Auftragsverarbeiter heranträgt, werden vom Auftragsverarbeiter unverzüglich an den Auftraggeber weitergeleitet.
3. Der Auftragsverarbeiter wird die Auftraggeber-Daten nach Beendigung dieses Vertrages datenschutzgerecht vernichten, sofern nicht gesetzlich eine Verpflichtung des Auftragsverarbeiters zur weiteren Speicherung der Auftraggeber-Daten besteht. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
4. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung von Auftraggeber-Daten dienen, dürfen durch den Auftragsverarbeiter auch nach Vertragsende aufbewahrt werden.

11. Nachweise und Überprüfungen

1. Der Auftragsverarbeiter wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragsverarbeiter vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.
2. Der Auftraggeber ist berechtigt, den Auftragsverarbeiter bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen.
3. Zur Durchführung von Inspektionen nach § 11 Abs. 2 ist der Auftraggeber berechtigt, im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 09 bis 17 Uhr) nach rechtzeitiger Vorankündigung gemäß § 11 Abs. 5 auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragsverarbeiters die Geschäftsräume des Auftragsverarbeiters zu betreten, in denen Auftraggeber-Daten verarbeitet werden.
4. Der Auftragsverarbeiter ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Überprüfungs-zwecke sind, zu erhalten.
5. Der Auftraggeber hat den Auftragsverarbeiter rechtzeitig (mindestens zwei Wochen vorher) über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragnehmer.
6. Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser § 11 dieses Vertrags gegenüber dem Auftragsverarbeiter verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung un-

terliegt. Auf Verlangen des Auftragsverarbeiters hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Wettbewerber des Auftragsverarbeiters mit der Kontrolle beauftragen.

7. Nach Wahl des Auftragsverarbeiters kann der Nachweis der Einhaltung der Pflichten nach diesem Verträge zusätzlich zu Inspektionen auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit — z.B. nach BSI-Grundschutz — („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

12. Haftung

1. Für die Haftung des Auftragsverarbeiters nach diesem Vertrag gelten die Haftungsausschlüsse und -begrenzungen gemäß dem Hauptvertrag oder den jeweils geltenden Nutzungsbedingungen. Soweit Dritte Ansprüche gegen den Auftragsverarbeiter geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragsverarbeiter von diesen Ansprüchen auf erstes Anfordern frei.
2. Der Auftraggeber verpflichtet sich, den Auftragsverarbeiter auch von allen etwaigen Geldbußen, die gegen den Auftragsverarbeiter verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

13. Sonstiges

1. 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.
2. Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich. Als Gerichtsstand wird das für den Auftraggeber örtlich zuständige Gericht vereinbart.
3. Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers 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 Auftraggeber unverzüglich zu verständigen.
4. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
5. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Für den Auftraggeber:

Datum:

Name:

Position:

Schule:

Straße:

PLZ, Ort:

Unterschrift

Für den Auftragsverarbeiter:

Name: Christoph Müller

Position: Geschäftsführer



Unterschrift

Anlage 1 - Unterauftragsverhältnisse

Aktuell bestehen die nachfolgenden Unterauftragsverhältnisse im Zusammenhang mit der Auftragsverarbeitung:

Name	Adresse	Leistungen
Hetzner Online GmbH	Industriestraße 25 91710 Gunzenhausen	• Infrastruktur- und Plattformdienstleistungen, • Rechenkapazität, • Speicherplatz und Datenbankdienste, • Sicherheitsleistungen • technische Wartungsleistungen

Anlage 2 – Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter sichert zu, dass er die nachfolgend beschriebenen Mindestanforderungen im Rahmen seines Datenschutzkonzeptes einhält. Es beschreibt die im Rahmen der Auftragsverarbeitung erforderlichen Maßnahmen beim Auftragsverarbeiter zum sicheren Umgang mit personenbezogenen Daten. Die Grundlage für dieses Datenschutz-Konzept bilden die EU-Datenschutzgrundverordnung DS-GVO und ggf. weitere von den interessierten Parteien geforderten Maßnahmen. Hierbei orientiert sich der Auftragsverarbeiter im Wesentlichen an den Vorgaben der Artikel 24, 25 und 32 DS-GVO.

1. Vertraulichkeit

1.1 Zutrittskontrolle

Der Betrieb der technischen Einrichtungen obliegt ausschließlich dem Unterauftragsverarbeiter für das Hosting. Der Anbieter setzt die entsprechenden Maßnahmen um und weist dies unter anderem in Form einer Zertifizierung nach ISO 27001 nach.

1.2 Zugriffskontrolle & Sitzungssicherheit

Für die Zugriffe auf personenbezogene Daten ist ein rollenbasiertes Berechtigungskonzept vorhanden, welches die Zugriffe in der Form einschränkt, dass nur berechtigte Personen auf die personenbezogenen Daten zugreifen können. Die administrativen Tätigkeiten müssen auf einen kleinen Kreis von Administratoren eingeschränkt sein.

Der Zugang zu Diplomify erfordert die Eingabe einer Benutzerkennung und eines Passwortes, zudem erfolgt der Login wahlweise erst nach zusätzlicher Authentifizierung per Email.

Die Passwörter werden mittels Einwegverschlüsselung (Hash) gespeichert. Kryptographische Verfahren wie Salting ermöglichen eine kollisionsresistente Speicherung. Passwörter werden bei der Eingabe nie im Klartext angezeigt.

Benutzer können ihre Passwörter jederzeit ändern; Passwörter, die dabei unterhalb geeigneter Entropiegüte liegen, werden vom System abgelehnt.

Sitzungen, die nicht aktiv vom Benutzer beendet werden, werden nach einer vom Serverbetreiber konfigurierbaren Anzahl von Minuten (Standard: 15) Inaktivität automatisch geschlossen.

1.3 Pseudonymisierung

Auswertungen werden pseudonymisiert, sofern der Personenbezug für das Ergebnis nicht zwingend erforderlich ist.

1.4 Trennungskontrolle

Die personenbezogenen Daten der Schulen (Mandanten) werden strikt voneinander getrennt. Benutzer und Administratoren können ausschließlich auf die Daten der eigenen Schule zugreifen.

2. Integrität

2.1 Weitergabekontrolle

Im Rahmen der Weitergabekontrolle wird sichergestellt, dass nur berechtigte Personen die personenbezogenen Daten zur Kenntnis nehmen können. Bei einer Übermittlung per E-Mail sind entsprechende Schutzmaßnahmen (z.B. Verschlüsselung der Kommunikation zwischen den Mail-Servern) zu ergreifen. Mobile Geräte oder mobile Speichermedien müssen verschlüsselt werden, wenn auf ihnen personenbezogene Daten dauerhaft gespeichert werden.

2.2 Auftragskontrolle

Im Rahmen der Auftragskontrolle wird sichergestellt, dass die im Auftrag durchgeführten Datenverarbeitungsvorgänge ausschließlich auf Weisung des Auftraggebers erfolgen. Hierzu werden die mit der Datenverarbeitung Beschäftigten geschult und unterwiesen. Unterauftragsverarbeiter dürfen nur auf Basis der mit dem Auftraggeber vereinbarten Regelungen beauftragt werden.

3. Verfügbarkeit und Belastbarkeit

Im Rahmen eines umfassenden Monitorings wird die Betriebsinfrastruktur hinsichtlich ihrer Leistungsdaten durch den Unterauftragsverarbeiter für das Hosting rund um die Uhr überwacht.

Die Verarbeitung von personenbezogenen Daten erfolgt auf Datenverarbeitungssystemen, die einem regelmäßigen und dokumentierten Patch-Management unterliegen. Es dürfen im Netz keine Systeme verbunden sein, die außerhalb der Wartungszyklen der Hersteller sind (insb. kein Windows XP, Windows Server 2003 etc.). Sicherheitsrelevante Patches werden kurzfristig nach Bekanntgabe eingespielt.

Die durchgängige Verfügbarkeit von personenbezogenen Daten wird mittels redundanten Speichermedien und Datensicherungen gemäß dem Stand der Technik gewährleistet.

4. Weitere verfahrensspezifische Maßnahmen:

Die Kommunikation zwischen dem Client (dem Benutzer) und dem Diplomify Server erfolgt zwingend über das TLS-Protokoll (SSL, HTTPS). Dazu wird serverseitig eine permanente Umleitung des Traffics auf den Port 443 und client-seitig durch die Direktive HTTP Strict Transport Security sichergestellt.

Um Cross Site Request Forgery, Cache Poisoning und Link Poisoning Attacken zu verhindern, validiert Diplomify den Host Header des Clients bevor eine Anfrage bearbeitet wird. Um die Datensicherheit der Benutzer zu verbessern und vor Cross-Origin Attacken zu schützen wird außerdem die Referrer Policy, und Cross-Origin Opener Policy auf „same-origin“ gesetzt.

Eine Sitzung wird mit einer Kennung (zufällige Zeichenkette) versehen. Die Sitzungsdauer kann über die Diplomify Einstellungen für den Server konfiguriert werden. Die Übertragung der Sitzungskennung erfolgt ausschließlich mittels Cookies und dem HTTPS Protokoll. Unbekannte Sitzungskennungen werden vom System abgelehnt. SQL-Anfragen im Backend werden ausschließlich mittels Query-Parameterization konstruiert, wodurch SQL Injections verhindert werden.

Cross-Site-Scripting (XSS) Attacken werden durch die im Backend verwendete Template-sprache unterbunden. Cross-Site Request Forgery wird durch die Erstellung sogenannter CSRF-Tokens verhindert. Diese werden bei jeder POST-Anfrage mitgesendet und überprüft. Dieses Feature verhindert es unter anderem, dass Angreifer eine Anfrage zu einem späteren Zeitpunkt „wiederholen“ können. Die http Direktive X-Frame-Options stellt sicher, dass nur Inhalte der schuleigenen Domain durch den Browser erlaubt werden und verhindert so Click Jacking Angriffe.

Anlage 3 – Verzeichnis der Verarbeitungstätigkeiten

Angelegt: 05.10.2022		Letzte Änderung: -/-	
Bezeichnung der Verarbeitungstätigkeit		Diplomify - Zeugniserstellung	
Zweck der Verarbeitung		Verwaltung von Schulnoten, Schülerbeobachtungen und Erstellung von Zeugnissen; Dokumentation der Lernentwicklung	
Betroffene Personen		- Schüler*innen - Lehrkräfte	
Datenkategorien		<u>Stammdaten</u> Schüler*innen: Name, Vorname, Namenszusatz, Geschlecht, Alter, Geburtsort/-land/-datum Lehrkräfte: Name, Vorname, Namenszusatz, Email-Adresse <u>personenbezogene Daten</u> Schüler*innen: Abschlüsse, Arbeitsgemeinschaften, Arbeitsverhalten, besuchter Unterricht, Bemerkungen, erhaltene Abschlüsse, Fächer, Jahrgangsstufe, Klasse, Kompetenzbereiche, Kompetenzen, Konferenzdaten, Kurse, Niveaustufen, Schüler, Schulformen, Schuljahre, Sozialverhalten, Unterrichtsarten, übernommene Ämter, Versetzungsstatus, (un)entschuldigter Fehltage, Zeugnisse (PDF) Lehrkräfte: Benutzername, Klassenleitung, unterrichtete Fächer, IP-Adresse der letzten Anmeldung, letzte Änderungen an Schüler*innen und Noten, Prüfsumme des Kennwortes, technische Angaben zu Browser und Betriebssystem <u>Bewertungen und Zeugnisdaten</u> Schüler*innen: Bewertungen in den Fächern, Bewertung von Arbeits- und Sozialverhalten, Kompetenzbewertungen, Noten <u>Förderbedarfe</u> Schüler*innen: Förderbedarf, Bedarfsausgangslage, Förderziele/-maßnahmen, Förderdauer, Förderkurse	
Zugriffsberechtigte Personen		Lehrkräfte: - Zur Dokumentation aller zeugnisrelevanten Informationen, Zeugnisdruck Administratoren (Auftraggeber): - Zur Konfiguration des Systems im Sinne seiner Funktion Administration (Auftragsnehmer): - Zur Fehlerbehebung/Wartung (nur mit Erlaubnis des Auftraggebers)	
Unterauftragnehmer		Gemäß Anlage 1	
Datenübermittlung		-/-	

Löschfristen	Löschung nach Kündigung des Hauptvertrages mit der Schule gemäß der vereinbarten Fristen oder unmittelbar auf schriftliche Anweisung durch den Auftraggeber.
--------------	--