Auftragsverarbeitungsvereinbarung nach Art. 28 DSGVO

Dienstnutzer:

Christian-von-Dohm-Gymnasium
Bornhardtstr.16
38644 Goslar

nachfolgend kurz „Dienstnutzer“ genannt.

Auftragsverarbeiter:

Matheretter, Kai Noack
Bogenstraße 6
D-15366 Hoppegarten

nachfolgend kurz „Auftragsverarbeiter“ genannt.

Dienstnutzer und Auftragsverarbeiter zusammen auch als „Parteien“ bezeichnet.

Präambel

Der Dienstnutzer hat den Auftragsverarbeiter mit den in Ziffer 1 genannten Leistungen beauftragt. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten, für die der Dienstnutzer als verantwortliche Stelle im Sinne des Art. 4 Nr. 7 DSGVO gilt. Dieser Auftragsverarbeitungsvereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien gemäß Art. 28 Abs. 3 Datenschutzgrundverordnung (DSGVO) im Zusammenhang mit dem Umgang des Auftragsverarbeiters oder von ihm unterbeauftragte Dritte mit personenbezogenen Daten zur Durchführung des Hauptvertrages. Die Erfüllung der Auftragsverarbeitungsvereinbarung wird nicht gesondert vergütet.

Es werden die Begriffsdefinitionen der DSGVO zugrunde gelegt.

1. Vertragsgegenstand und Dauer

1.1 Der Auftragsverarbeiter erbringt für den Dienstnutzer Leistungen im Bereich der Cloud-Dienste auf Grundlage des geschlossenen Hauptvertrages.

Dabei erhält der Auftragsverarbeiter Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Dienstnutzers, sofern der Auftragsverarbeiter nicht durch das Recht der Union oder der Mitgliedsstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist. Umfang und Zweck der Datenverarbeitung durch den Auftragsverarbeiter ergeben sich aus dem Hauptvertrag (und sofern vorhanden aus der dazugehörigen Leistungsbeschreibung). Dem Dienstnutzer obliegt die alleinige Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO.

1.2 Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

1.3 Die Bestimmungen dieser Vereinbarung finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragsverarbeiter und seine Beschäftigten

oder durch den Auftragsverarbeiter Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Dienstnutzer stammen oder für den Dienstnutzer erhoben wurden oder auf sonstige Weise in dessen Auftrag verarbeitet (nachfolgend Dienstnutzer-Daten“ genannt) werden.

1.4 Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

1.5 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der europäischen Union oder einem anderen Vertragsstaat des Abkommens über den europäischen Vertragsraum (Beschluss 94/1/EG) statt. Jede Verlagerung von Teilleistungen oder der gesamten Dienstleistung in ein Drittland bedarf der vorherigen Zustimmung des Dienstnutzers in Schriftform oder dokumentiertem elektronischen Format und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

2. Art der verarbeiteten Daten, Kreis der betroffenen Personen

Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragsverarbeiter Zugriff auf die in Anlage 1 näher spezifizierten personenbezogenen Daten der ebenfalls in Anlage 1 näher spezifizierten betroffenen Personen. Diese Daten umfassen keine besonderen Kategorien personenbezogener Daten.

3. Weisungsrecht

3.1 Der Auftragsverarbeiter darf Dienstnutzer-Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Dienstnutzers erheben, nutzen oder auf sonstige Weise verarbeiten. Dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragsverarbeiter durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Dienstnutzer diese rechtlichen Anforderungen vor der Verarbeitung mit.

3.2 Die Weisungen des Dienstnutzers werden anfänglich durch diesen Vertrag festgelegt und können vom Dienstnutzer danach in schriftlicher Form oder in dokumentiertem elektronischen Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Dienstnutzer ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigte Person ist: Dirk Sudmann (Niedersächsisches Kultusministerium).

Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

3.3 Alle erteilten Weisungen sind sowohl vom Dienstnutzer als auch vom Auftragsverarbeiter zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für drei weitere volle Kalenderjahre aufzubewahren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

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

4. Pflichten des Auftragsverarbeiters

4.1 Der Auftragsverarbeiter ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Dienstnutzers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

4.2 Beim Auftragsverarbeiter ist Ansprechpartner für den Datenschutz (sofern ein Datenschutzbeauftragter nach Art. 37 Abs. 1 DS-GVO nicht bestellt werden muss): Kai Noack, service@matheretter.de

4.3 Den bei der Datenverarbeitung durch den Auftragsverarbeiter beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu nutzen oder auf sonstige Weise zu verarbeiten. Der Auftragsverarbeiter wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (nachfolgend „Beschäftigte“ genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und über die sich aus diesem Vertrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehren sowie mit der gebotenen Sorgfalt die Einhaltung der vorgenannten Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Beschäftigten und dem Auftragsverarbeiter bestehen bleiben. Dem Dienstnutzer sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

4.4 Die Verarbeitung von Dienstnutzer-Daten, die Gegenstand dieser Vereinbarung sind, in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragsverarbeiters) ist nur gestattet, sofern die Einhaltung Verpflichtungen dieser Vereinbarung sowie der Maßgaben des Art. 32 DS-GVO auch in diesem Fall sichergestellt sind. Der Auftragsverarbeiter hat den Dienstnutzer über die Verarbeitung von Dienstnutzer-Daten in Privatwohnungen sowie die getroffenen Sicherheitsmaßnahmen in Textform zu unterrichten.

4.5 Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragsverarbeiters, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragsverarbeiter den Dienstnutzer unverzüglich in Schriftform oder dokumentiertem elektronischen Format informieren. Dasselbe gilt für Prüfungen des Auftragsverarbeiters durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält soweit möglich folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze,
b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung und
c) eine Beschreibung der vom Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Der Auftragsverarbeiter trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Person(en), informiert hierüber den Dienstnutzer und ersucht diesen um weitere Weisungen. Der Auftragsverarbeiter ist darüber hinaus verpflichtet, dem Dienstnutzer jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

4.6 Der Auftragsverarbeiter unterstützt den Dienstnutzer erforderlichenfalls bei der Erfüllung der Pflichten des Dienstnutzers nach Art. 33 und 34 DS-GVO in angemessener Weise (Art. 28 Abs. 3 S. 2 lit. f DS-GVO). Meldungen für den Dienstnutzer nach Art. 33 oder 34 DS-GVO darf der Auftragsverarbeiter nur nach vorheriger Weisung seitens des Dienstnutzers gemäß § 4 dieser Vereinbarung durchführen.

4.7 Sollten die Daten des Dienstnutzers 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 Dienstnutzer unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Dienstnutzer als „Verantwortlichem“ im Sinne der DS-GVO liegen.

4.8 Ein Wechsel in der Person des Ansprechpartners für den Datenschutz ist dem Dienstnutzer unverzüglich mitzuteilen.

4.9 Der Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Dienstnutzers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gemäß Art. 30 Abs. 2 DS-GVO enthält. Das Verzeichnis ist dem Dienstnutzer auf Anforderung zur Verfügung zu stellen.

4.10 An der Erstellung des Verfahrensverzeichnisses durch den Dienstnutzer sowie bei der Erstellung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden gemäß Art. 36 DS-GVO hat der Auftragsverarbeiter im angemessenen Umfang mitzuwirken. Er hat dem Dienstnutzer die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

5. Technische und organisatorische Sicherheitsmaßnahmen

Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Dienstnutzers gemäß Art. 32 DS-GVO, insbesondere mindestens die in Anlage 2 angekreuzten oder ergänzten Maßnahmen getroffen hat. Sofern auch besondere Kategorien personenbezogener Daten verarbeitet werden, trifft der Auftragsverarbeiter zusätzlich die sich aus § 22 Absatz 2 BDSG ergebenden angemessenen und spezifischen Maßnahmen. Der Auftragsverarbeiter legt auf Anforderung des Dienstnutzers die näheren Umstände der Festlegung und Umsetzung der Maßnahmen offen. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Sämtliche Anpassungen sind vom Auftragsverarbeiter zu dokumentieren und dem Dienstnutzer regelmäßig (mindestens jährlich) schriftlich oder in Textform mitzuteilen. Der Dienstnutzer kann jederzeit eine aktuelle Fassung der vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen anfordern. Über wesentliche Änderungen der Sicherheitsmaßnahmen hat der Auftragsverarbeiter den Dienstnutzer unverzüglich in Textform zu unterrichten.

6. Fernzugriff

6.1 Für die Durchführung von Fernzugriffen auf die IT-Systeme des Dienstnutzers gelten ergänzend folgende Regelungen:

6.2 Fernzugriffe werden, sofern und soweit hierbei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, ausschließlich mit Einwilligung der zuständigen Mitarbeiter des Dienstnutzers ausgeführt.

6.3 Der Auftragsverarbeiter verwendet angemessene Identifizierungs- und Verschlüsselungsverfahren.

6.4 Fernzugriffe werden vom Auftragsverarbeiter dokumentiert und protokolliert. Der Dienstnutzer ist berechtigt Fernzugriffe bei und nach Durchführung zu kontrollieren. Dabei hat er die in § 5 dieser Vereinbarung aufgeführten Bestimmungen zu beachten. Bei Fernzugriffen ist der Dienstnutzer - soweit

technisch möglich und im Hinblick auf die Art der erbrachten Leistungen realisierbar - berechtigt, diese von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen.

6.5 Fernzugriffe zu den relevanten Systemen des Dienstnutzers erfolgen nur nach dem Need-to-know-Prinzip.

6.6 Der Auftragsverarbeiter darf Dienstnutzer-Daten im Wege eines Filetransfers oder Downloads für Zwecke der Leistungserbringung nur dann von den Datenverarbeitungssystemen des Dienstnutzers abziehen und auf sein eigenes kopieren, wenn er dafür jeweils zuvor und für den Einzelfall die Einwilligung des Dienstnutzers eingeholt hat. Dienstnutzer-Daten dürfen nur zum Zweck der Leistungserbringung nach dem Hauptvertrag verwendet werden und dürfen zudem nicht ohne angemessene Verschlüsselung auf mobile Speichermedien (PDAs, USB- Speichersticks oder ähnliche Geräte) kopiert werden.

6.7 Software-Aktualisierungen dürfen in Abstimmung mit dem Dienstnutzer nur nach vorheriger Genehmigung auf den IT-Systemen des Dienstnutzers eingespielt werden. Es ist sicherzustellen, dass eine hinreichende Datensicherung der Dienstnutzer-Daten gewährleistet ist.

6.8 Personenbezogene Daten, die der Auftragsverarbeiter beim Fernzugriff erhalten hat, wird der Auftragsverarbeiter dem Dienstnutzer unverzüglich zurückgeben, wenn diese Daten für die Durchführung der Leistungen des Auftragsverarbeiters nach dem Hauptvertrag nicht mehr erforderlich sind, oder mit Einwilligung des Dienstnutzers löschen. Etwaige dem Auftragsverarbeiter übergebene Papierausdrucke mit personenbezogenen Daten muss der Auftragsverarbeiter nach Abschluss des Hauptvertrages unverzüglich zurückgeben oder mit Zustimmung des Dienstnutzers datenschutzgerecht vernichten.

7. Kontrollrechte des Dienstnutzers

7.1 Der Dienstnutzer überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von der Einhaltung der in diesem Vertrag niedergelegten Pflichten durch den Auftragsverarbeiter, insbesondere der technischen und organisatorischen Maßnahmen. Hierfür kann er vom Auftragsverarbeiter alle erforderlichen Informationen z.B. Auskünfte des Auftragsverarbeiters einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragsverarbeiter steht. Der Dienstnutzer wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragsverarbeiters dabei nicht unverhältnismäßig stören.

7.2 Der Auftragsverarbeiter verpflichtet sich, dem Dienstnutzer auf dessen mündliche, schriftliche oder elektronische Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle des Einhaltung der in diesem Vertrag niedergelegten Pflichten sowie der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters erforderlich sind und Vor-Ort-Kontrollen zuzulassen.

7.3 Der Dienstnutzer dokumentiert das Kontrollergebnis und teilt es dem Auftragsverarbeiter mit. Bei Fehlern oder Unregelmäßigkeiten, die der Dienstnutzer insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragsverarbeiter unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Dienstnutzer dem Auftragsverarbeiter die notwendigen Verfahrensänderungen unverzüglich mit.

7.4 Der Auftragsverarbeiter stellt dem Dienstnutzer auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

7.5 Der Auftragsverarbeiter weist dem Dienstnutzer die Verpflichtung der Mitarbeiter nach Ziffer 4.3 auf Verlangen nach.

8. Einsatz von Subunternehmern

8.1 Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in **Anlage 3** genannten Subunternehmer durchgeführt. Der Auftragsverarbeiter ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt, soweit er den Dienstnutzer hiervon vorab in Kenntnis setzt und dieser der Beauftragung des Subunternehmers vorab schriftlich oder in dokumentiertem elektronischen Format zugestimmt hat. Der Auftragsverarbeiter ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragsverarbeiter hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Dienstnutzer seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, bedarf dies der gesonderten Zustimmung des Dienstnutzers und der Auftragsverarbeiter hat sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragsverarbeiter wird dem Dienstnutzer auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

8.2 Eine weitere Auslagerung durch den Subunternehmer bedarf der ausdrücklichen Zustimmung des Dienstnutzers.

8.3 Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragsverarbeiter Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragsverarbeiter für den Dienstnutzer erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Dienstnutzer genutzt werden.

9. Anfragen und Rechte betroffener Personen

9.1 Der Auftragsverarbeiter unterstützt den Dienstnutzer nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DSGVO.

9.2 Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragsverarbeiter geltend, so reagiert dieser nicht selbstständig, sondern verweist die betroffene Person unverzüglich an den Dienstnutzer und wartet dessen Weisungen ab.

10. Haftung

10.1 Dienstnutzer und Auftragsverarbeiter haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung. Der Auftragsverarbeiter stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Dienstnutzer ab.

10.2 Der Auftragsverarbeiter stellt den Dienstnutzer auf erstes Anfordern von sämtlichen Ansprüchen frei, die betroffene Personen gegen den Dienstnutzer wegen der Verletzung einer dem Auftragsverarbeiter durch die DSGVO auferlegten Pflicht oder der Nichtbeachtung oder Verletzung

einer vom Dienstnutzer in dieser AV-Vereinbarung oder einer gesondert erteilten Anweisung geltend machen.

10.3 Die Parteien stellen sich jeweils von der Haftung frei, wenn und soweit eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist. Im Übrigen gilt Art. 82 Absatz 5 DS-GVO.

11. Außerordentliches Kündigungsrecht

Der Dienstnutzer kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragsverarbeiter seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO oder sonstige anwendbare Datenschutzvorschriften vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Dienstnutzers nicht ausführen kann oder will oder der Auftragsverarbeiter sich den Kontrollrechten des Dienstnutzers auf vertragswidrige Weise widersetzt. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

12. Beendigung des Hauptvertrags

12.1 Der Auftragsverarbeiter wird dem Dienstnutzer nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Dienstnutzers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragsverarbeiter. Der Auftragsverarbeiter hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

12.2 Der Dienstnutzer hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragsverarbeiter in geeigneter Weise zu kontrollieren bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragsverarbeiter steht.

12.3 Der Auftragsverarbeiter ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragsverarbeiter über personenbezogene Daten verfügt, die ihm vom Dienstnutzer zugeleitet wurden oder die er für diesen erhoben hat.

13. Schlussbestimmungen

13.1 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 zugehörigen Datenträger ausgeschlossen ist.

13.2 Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform oder eines dokumentierten elektronischen Formats. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

13.3 Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

13.4 Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Hoppegarten.

Folgende Dokumente sind untrennbarer Bestandteil dieser Vereinbarung:

- Anlage 1: Beschreibung der betroffenen Personen/Betroffenengruppen sowie der – ggf. besonders schutzbedürftigen - Daten/Datenkategorien
- Anlage 2: Technische und organisatorische Maßnahmen des Auftragsverarbeiters zum Datenschutz gemäß Art. 32 DSGVO (Sicherheitskonzept)
- Anlage 3: Unterauftragsverhältnisse beim Auftragsverarbeiter

Für den Dienstnutzer:

Für den Auftragsverarbeiter:

Datum und Unterschrift

Unterschrift

Christian-von-Dohm-Gymnasium
Bornhardtstr.16
38644 Goslar

Anlage 1: Beschreibung der betroffenen Personen/Betroffenengruppen sowie der ggf. besonders schutzbedürftigen Daten/Datenkategorien

Die folgenden Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- Identifikationsdaten: Vor- und Nachname
- Verifikationsdaten: Passwörter
- Identifikationsdaten: Schulzugehörigkeit
- Identifikationsdaten: Rolle (Lehrer oder Schüler)

Folgende Kategorien von betroffenen Personen sind hiervon betroffen:

- Berechtigter Nutzer mit Single-Sign-On
- Manuell durch Admin-Accounts angelegte Nutzer

Anlage 2: Technische und organisatorische Maßnahmen des Auftragsverarbeiters zum Datenschutz gemäß Art. 32 DSGVO

Der Auftragnnehmer betreibt einen Server bei dem Unternehmen Hetzner. Der Datacenter-Park des Server-Betreibers befindet sich in Falkenstein/Vogtland, Deutschland.

1. Vertraulichkeit gemäß Art. 32 Abs. 1 lit. b DSGVO

1.1 Zutrittskontrolle

- elektronisches Zutrittskontrollsystem mit Protokollierung
- Hochsicherheitszaun um den gesamten Datacenter-Park
- dokumentierte Schlüsselvergabe an Mitarbeiter
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
- Der Zutritt für betriebsfremde Personen zu den Räumen ist nur in Begleitung eines Hetzner-Mitarbeiters gestattet
- Verwaltung: elektronisches Zutrittskontrollsystem mit Protokollierung
- Videoüberwachung an den Ein- und Ausgängen

1.2 Zugangskontrolle

- Das Passwort zur Administrationsoberfläche wird vom Auftragsverarbeiter vergeben - die Passwörter erfüllen vordefinierte Richtlinien. Zusätzlich steht eine Zwei-Faktor-Authentifizierung zur Absicherung zur Verfügung.
- Der Zugang ist passwortgeschützt, Zugriff besteht nur für berechtigte Mitarbeiter, verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert.

1.3 Zugriffskontrolle

- Der Auftragsverarbeiter stellt durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) sicher, dass unberechtigte Zugriffe verhindert werden.
- Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter.
- Für übertragene Daten/Software ist der Auftragsverarbeiter in Bezug auf Sicherheit und Updates zuständig.

1.4 Datentrennungskontrolle

- Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
- Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt im Rechenzentrum Falkenstein zerstört (geschreddert).
- Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
- Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

- Das Anlegen von Nutzeraccounts erfolgt mit einem Pseudonym und einer Pseudo-E-Mail-Adresse.
- Echtname oder Kennungsname werden von den Nutzern selbst eingetragen und können von diesen jederzeit wieder geändert oder gelöscht werden.

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

2.1. Weitergabekontrolle

- Alle Mitarbeiter sind im Sinne des Art. 32 Abs.4 DSGVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
- Möglichkeiten zur verschlüsselten Datenübertragung werden entsprechend der Leistungsbeschreibung des Vertrages zur Verfügung gestellt.

2.2. Eingabekontrolle

- Die Daten werden vom Auftragsverarbeiter selbst eingegeben bzw. erfasst.
- Änderungen der Daten werden protokolliert.

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

3.1 Verfügbarkeitskontrolle

- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
- Ein Backup aller Daten erfolgt täglich per Datenbank-Dump.
- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
- Dauerhaft aktiver DDoS-Schutz.
- Monitoring des Servers.

3.2 Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

- Eine Sicherung kann kurzfristig auf den Server eingespielt werden.

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

4.1 Datenschutz-Management

- Ein Datenschutz-Managementsystem ist vorhanden.

4.2 Incident-Response-Management

- Ein Incident-Response-Management ist vorhanden.

4.3 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

- Datenschutzfreundliche Voreinstellungen werden bei unseren Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DSGVO).

4.4 Auftragskontrolle

- Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung.

- Der Auftragsverarbeiter hat einen Ansprechpartner für den Datenschutz.

Anlage 3: Unterauftragsverhältnisse beim Auftragsverarbeiter

Unterauftragnehmer (Firmenname mit Rechtsform):

Hetzner Online GmbH

Beschreibung der Leistungen:

Hosting eines Servers

Anschrift/Ort der Leistungserbringung:

Hetzner Online GmbH

Industriestrasse 25

D-91710 Gunzenhausen

Rechenzentrum:

Falkenstein/Vogtland, Deutschland