Vertrag über die Verarbeitung von Daten im Auftrag nach Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO)

Zwischen

Musterschule
Manu Musterperson
Musterstraße 1
12345 Musterstadt
Deutschland

- Auftraggeber -

und

Thielicke IT Solutions
Tom Thielicke
Christburger Str. 46
10405 Berlin
Deutschland

- Auftragnehmer -

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand des Auftrags

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

Der Auftragnehmer stellt die Lernplattform „Tipp10“ zum Erlernen des Zehnfingersystems zur Verfügung.

Folgende Datenarten sind regelmäßig Gegenstand der Datenverarbeitung:

2.1 Zugriffsdaten

Unabhängig von der Intention beim Besuch dieser Internetseite wird jeder Zugriff in sogenannten Server-Logdateien protokolliert. Die Speicherung dient internen systembezogenen Zwecken, sowie dem Schutz und der Vorsorge gegen Missbrauch und Angriffen. Protokolliert werden:

- Name der abgerufenen Datei
- Datum und Uhrzeit des Abrufs
- übertragene Datenmenge
- Meldung über erfolgreichen Abruf
- Webbrowser und anfragende Domain
- IP-Adresse

2.2 Cookies

Um Ihnen auf unserer Website bestimmte Funktionen bieten zu können, verwenden wir so genannte Session Cookies. Dies sind kleine Textdateien, die auf Ihrem Computer für die Dauer einer Browser-Sitzung gespeichert werden. Nach dem Ende der Browser-Sitzung werden die von uns verwendeten Session Cookies wieder gelöscht. Der ausschließliche Zweck der Session Cookies besteht also darin, die vollständige Funktion unserer Website zu ermöglichen und Ihren Loginstatus festzuhalten. Sie haben die Möglichkeit, die Installation von Cookies auf Ihrem Computer zu verhindern, indem Sie die Browsereinstellungen verändern. Allerdings ist in diesem Fall die Nutzung unserer Website stark eingeschränkt.

2.3 Webtracking

Wir weisen ausdrücklich darauf hin, dass bei der Nutzung von Tipp10 keinerlei Werbung oder Webtracking wie z.B. Google Analytics oder eingebetteter Code von Drittanbietern wie z.B. Facebook verwendet wird.
Eine Weitergabe jeglicher personenbezogener Daten durch Tom Thielicke IT Solutions an Dritte erfolgt grundsätzlich nicht.

2.4 Nutzung der Schulversion

Der Betrieb einer Schulplattform setzt voraus, dass diese durch eine verantwortliche Person (Administrator:in) eingerichtet und verwaltet wird. Folgende personenbezogenen Daten werden hierfür erhoben:

Zugangsdaten des:der Administrator:in
- E-Mail-Adresse
- Vor- und Zuname (optional)
- Geburtsdatum (optional)
- Lernstatistik
- Nutzungsdaten (Zeitpunkte von Registrierungs- und Loginprozessen)

Plattformdaten
- Titel und Subdomain der Plattform
- Einführungstext der Plattform (optional)
- Individueller Notenschlüssel (optional)
- Individuelle Beschriftungen für Urkunden (optional)
- Plattformeinstellungen

Rechnungsdaten der Schule oder des Unternehmens
- Name der Schule oder des Unternehmens
- Anschrift
- UID-Nr. (optional)
- Zusätzliche E-Mail-Adresse (optional)

Single-Sign-On (optional)
- Provider
- Url
- Client-ID
- Client Secret

Daten der angelegten Lehrpersonen und Schüler:innen
- Rolle (Administrator:in, Lehrer:in oder Schüler:in)
- Benutzername (kann in anonymisierter Form hinterlegt werden)
- Vor- und Zuname (optional)
- E-Mail-Adresse (optional)
- Passwort (optional bei Single-Sign-On)
- SUB-Kennung (nur bei Single-Sign-On)
- Klassennamen
- Aufgabennamen und -beschreibungen
- Lernstatistik
- Nutzungsdaten (Zeitpunkte von Registrierungs- und Loginprozessen)

Bei Abschluss eines Auftragsverarbeitungsvertrags
- Weisungsberechtigte Personen
- Name der Schule oder des Unternehmens
- Anschrift
- E-Mail-Adresse (optional)

2.5 Nutzung des Ticketsystems (Supportanfragen)

- E-Mail-Adresse
- Betriebssystem (optional)
- Browser (optional)
- Kurzbeschreibung
- Erläuterungen
- Veröffentlichung der Supportanfrage ohne personenbezogene Daten (optional)

2.7 Kreis der von der Datenverarbeitung Betroffenen

Auftraggeber
Schüler:innen
Lehrer:innen

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber auf seiner Meinung nach rechtlich unzulässige Datenverarbeitungen hinzuweisen.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte im Zusammenhang mit dieser Verarbeitung von Daten im Auftrag gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen per E-Mail erfolgen.

(4) Der Auftraggeber kann weisungsberechtigte Personen benennen. Weisungsberechtigte Personen des Auftraggebers sind:

Max Mustermann
Mara Musterfrau
Didi Divers

Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer per E-Mail mitteilen.

(5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch

den Auftragnehmer feststellt.

(6) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen für den Auftraggeber geltenden gesetzlichen Grundlage besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

(3) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften.

(4) Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesem Vertrag festgelegten oder sich unmittelbar aus der DSGVO ergebenden Pflichten erforderlich sind. Auf Verlangen des Auftraggebers gestattet der Auftragnehmer ebenfalls die Prüfung der unter diesen Vertrag fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Auftraggeber einschlägige Zertifizierungen im Sinne des Art. 28 Abs. 5 DSGVO des Auftragnehmer berücksichtigen. Der Auftraggeber kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können gegebenenfalls auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragnehmer umfassen und werden mit angemessener Vorankündigung und unter Einhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragsverarbeiters sowie nach Möglichkeit ohne Störung des Betriebsablaufs durchgeführt.

(5) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

(6) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.

(7) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(8) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(9) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei entsprechenden Meldepflichten unterstützen.

(10) Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder Subunternehmern ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform zulässig. Eine Verarbeitung von Daten für den Auftraggeber in Privatwohnungen ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform im Einzelfall zulässig.

(11) Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

(12) An der Erstellung der Verfahrensverzeichnisse bzw. Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber hat der Auftragnehmer mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen. Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

(13) Weisungsempfangsberechtigt ist der Auftragnehmer als Einzelunternehmer selbst. Sollten weitere Personen während der Laufzeit dieses Vertrages Weisungsempfangsberechtigung erlangen, teilt der Auftragnehmer dies dem Auftraggeber unverzüglich mit.

(14) Die Pflicht des Auftragnehmers zur Benennung eines Datenschutzbeauftragten nach Art. 37 DSGVO entfällt aufgrund der Stellung des Auftragnehmers als Einzelunternehmer. Der Auftragnehmer versichert die Einhaltung der gesetzlichen Vorschriften, der Regelungen des vorliegenden Vertrages sowie etwaiger weiterer geltender rechtlichen Weisungen des Auftraggebers bei der Verarbeitung personenbezogener Daten des Auftraggebers.

5. Datengeheimnis / Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

6. Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers in Textform zulässig. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der Anlage 1 zu diesem Vertrag angeben.

(2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.

(3) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Unterauftragnehmer benannt worden ist, hat der Auftragnehmer den Auftraggeber hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unterauftragnehmer gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen.

(4) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

(5) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die gesetzlich bestehenden Kontrollbefugnisse des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

7. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung nach Art. 12-23 DSGVO - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen.

8. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

9. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als „Anlage 2“ zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

(3) Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

10. Dauer des Auftrags

(1) Der Vertrag beginnt am

26-04-2024

und wird auf unbestimmte Zeit geschlossen.

(2) Der Vertrag verliert seine Gültigkeit automatisch mit Ablauf der Dauer des Hauptvertrages.

(3) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

11. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Auftraggeber unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

(3) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

12. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

13. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

_____ , den _____

_____

- Auftraggeber -

Berlin, den 26-04-2024

MUSTER

- Auftragnehmer -

Anlage 1
Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“) und mit denen ein Vertrag zur Auftragsverarbeitung besteht.

Dabei handelt es sich um nachfolgendes Unternehmen:

Keyweb AG
Neuwerkstr. 45/46
99084 Erfurt

Aufgabenbereich: Serverhosting

Anlage 2
Technische und organisatorische Maßnahmen des Auftraggebers nach Art. 32 DSGVO

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Auftragnehmer:

- Manuelles Schließsystem
- Sicherheitsschloss
- Schlüsselregelung
- Personenkontrolle; Besucher dürfen sich nur in Begleitung des Auftragnehmers im Gebäude bewegen
- Sorgfältige Auswahl des Reinigungspersonals

Keyweb AG:

-Verdeckte und standortgetrennte Rechenzentren
- Alarmanlage mit Ausschaltung zum Wachschutz
- Zutrittskontrollsystem/Schließsystem über Chipkarte
  - Nur berechtigte Mitarbeiter erhalten Zugang zu den Rechenzentren des Auftragnehmers
  - Die Vergabe der Zutrittsberechtigung erfolgt uhrzeitabhängig basierend auf den jeweiligen Dienstzeiten der Mitarbeiter
- Zutritt von Dritten nur mit Voranmeldung
- Protokollierung der Besucher
  - Ständige Begleitung von Besuchern durch einen Mitarbeiter des Auftragnehmers
  - Tragepflicht von Besucherausweisen
- Sorgfältige Auswahl von Reinigungspersonal
- Videoüberwachung
  - Überwachung besonderer Gefahrenbereiche wie Eingangsbereich, Standort wichtiger Netzwerkkomponenten
  - Aufzeichnung der Videoüberwachung mit Speicherung für 3 Monate
- Regelmäßige Kontrollgänge

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Auftragnehmer:

- Automatische, passwortgeschützte Bildschirmsperre (nach 15 Minuten)
- Manuelle Bildschirmsperre beim Verlassen des Arbeitsplatzes
- Einsatz einer Software-Firewall
- Einsatz einer Hardware-Firewall
- Authentifikation mit Benutzername / Passwort (mindestens acht Zeichen, Sonderzeichen, Ziffern, 90 Tage Gültigkeitsdauer)
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle
- Sorgfältige Auswahl von Reinigungspersonal
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Verschlüsselung von Backups
- Verschlüsselung von mobilen Datenträgern
- Verschlüsselung von Smartphone-Inhalten
- Verschlüsselung von Datenträgern in Laptops / Notebooks

Keyweb AG:

- konkrete Verarbeitungsvorgänge sind dem Auftragnehmer nicht bekannt. Insofern muss der Auftraggeber durch softwaretechnische Gestaltung dafür Sorge tragen, dass die Benutzung der Datenverarbeitungssysteme von Unbefugten nicht möglich ist
- Zugang zum Serversystem des Auftragsgebers nur mittels Usernamen und Passwort bzw. SSH-Keys, welche den Zugriff nur von bestimmten IPs des Auftragnehmers erlauben
- Mitteilung der Zugangsdaten durch den Auftraggeber
- nur für einen konkreten Auftrag über das SSL-geschützte Ticketsystem des Auftragnehmers
- Das Ticket zur Beauftragung muss über den Kundenaccount des Auftraggebers erstellt werden
- Eine Verbindung zum Server zwecks Wartung erfolgt ausschließlich direkt über die lokale Konsole oder über eine verschlüsselte Verbindung , z.B. SSH
- Protokollierung der Logins und Kennwortfehleingaben
- Besucher – und Zugangsprotokollierung
- keine Nutzung von WLAN

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems

Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Auftragnehmer:

- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel (Passwort mit mindestens acht Zeichen, Sonderzeichen, Ziffern, 90 Tage Gültigkeitsdauer)
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Einsatz von Aktenvernichtern
- Verschlüsselung von Datenträgern

Keyweb AG:

- Verpflichtungserklärung aller Mitarbeiter auf Datengeheimnis
- Sorgfältige Auswahl der Mitarbeiter
- Zugriff erfolgt nur nach konkreter Beauftragung durch den Auftraggeber über das Ticketsystem des Auftragnehmers
- Das Ticket zur Beauftragung muss über den Kundenaccount des Auftraggebers erstellt werden
- Bearbeitender Mitarbeiter auf Seiten des Auftragnehmers ist durch eine persönliche Benutzerkennung im Ticketsystem identifizierbar
- Arbeiten erfolgen nur im Rahmen dessen, was zur Lösung des vom Auftraggebers geschilderten Problems notwendig ist
- Weitergehende Arbeiten erfolgen nur in Abstimmung mit dem Auftraggeber
- Daten auf Festplatten, welche endgültig aus einem Server entfernt werden, werden umgehend durch Verwendung der Gutmann Löschmethode (35-maliges Überschreiben) dauerhaft und unwiederbringlich entfernt.
- Protokollierung der Datenlöschung

4. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Auftragnehmer:

- Verschlüsselter Transfer über SSL

Keyweb AG:

- Verpflichtung aller Mitarbeiter auf das Datengeheimnis
- Eine Weitergabe von personenbezogenen Daten ist nicht Bestandteil des Auftrages. Eine weitergehende Weitergabekontrolle muss insoweit vom Auftraggeber gewährleistet werden.

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Auftragnehmer:

- Eingabe, Änderung und Löschung von Daten erfolgt nur nach konkreter Beauftragung durch den AuftraggeberNachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Keyweb AG:

- Verpflichtung aller Mitarbeiter auf das Datengeheimnis
- Eingabe, Veränderung oder Löschung erfolgt nur nach konkreter Beauftragung durch den Auftraggeber über das SSL-gesicherte Ticketsystem des Auftragnehmers
- Das Ticket zur Beauftragung muss über den Kundenaccount des Auftraggebers erstellt
- werden Bearbeitender Mitarbeiter auf Seiten des Auftragnehmers ist durch eine persönliche Benutzerkennung im Ticketsystem identifizierbar

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Auftragnehmer:

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

- vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

Keyweb AG:

- Der Auftragnehmer schließt mit evtl. Unterauftragsnehmern bei Bedarf einen Vertrag zur Auftragsverarbeitung

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Auftragnehmer:

- Feuer- und Rauchmeldeanlagen
- Erstellen eines Backup- & Recoverykonzepts
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

Keyweb AG:

- Feuerlöschgeräte in den Rechenzentren
- CO2 Handfeuerlöscher
- Feuer- und Rauchmeldeanlage mit Brandfrüherkennungssystemen an Decke und Boden
- Direkte Aufschaltung zur Feuerwehr
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Unterbrechungsfreie Stromversorgung (USV)
- Dieselnotstromaggregat
- Generatoren mit einer Spitzenleistung von 500kVA
- Klimaanlagen in den Rechenzentren
- Kühlinfrastruktur ist N+1 redundant
- Alarmmeldung bei unberechtigten Zutritten zu den Rechenzentren
- 80 GBit Außenanbindung ein hochleistungsfähiges, multiredundantes Internet-Backbone
- TÜV Geprüftes Hochverfügbarkeits-Rechenzentrum Stufe 2 tekPlus
- mehrstufiges DDOS-Erkennungs- und Schutzsystem
- Access-Listen, welche vergangene Angriffsmuster und UDP- Traffic auf normalerweise durch TCP-Dienste belegte Ports filtern
- permanente Überwachung des ein- und ausgehenden Datenverkehrs mithilfe von Netflow

- Nullrouting und Blackholing der Ziel-IP
- über Service-Level-Agreements garantierte Hardware- und Netzwerkverfügbarkeit

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Auftragnehmer:

- Logische Mandantentrennung (softwareseitig)
- Festlegung von Datenbankrechten

Keyweb AG:

- Die Daten des Auftraggebers sind physikalisch oder logisch von anderen Kundendaten getrennt
- Dem Auftragnehmer sind die Zwecke der Erhebung unbekannt, die Trennungskontrolle muss insoweit vom Auftraggeber gewährleistet werden