

Vertrag über die Verarbeitung von Daten im Auftrag für die Kroschke SIGN Academy

zwischen

_____ (Firma)

- Auftraggeber -

und

Kroschke sign-international GmbH, Kroschkestr. 1, 38112 Braunschweig

- 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 Gegenstand des Auftrags ergibt sich aus dem jeweiligen Vertrag zwischen den Parteien (im Folgenden „Vertrag“).

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 darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte 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 können in Textform (z.B. E-Mail) erfolgen.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(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 Meldepflicht 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

Vertrag über die Verarbeitung von Daten im Auftrag für die Kroschke SIGN Academy

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 ansonsten 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 sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

(4) 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.

(5) 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.

(6) 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.

(7) 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.

5. Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer wird dem Auftraggeber den Namen und die Kontaktdaten seines Datenschutzbeauftragten gesondert in Textform mitteilen.

(2) Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 1 kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu bestellen und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

6. Meldepflichten des Auftragnehmers

(1) 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.

(2) 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.

Vertrag über die Verarbeitung von Daten im Auftrag für die Kroschke SIGN Academy

(3) 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 der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.

(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) 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.

8. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

(4) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

9. Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers in Textform zulässig. Der Auftragnehmer nennt alle bestehenden Unterauftragsverhältnisse gem. **Anlage 2**. Ein Wechsel der Unterauftragnehmer sind dem Auftraggeber unverzüglich mitzuteilen

(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

Vertrag über die Verarbeitung von Daten im Auftrag für die Kroschke SIGN Academy

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 Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 8 dieses Vertrages) 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) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogene Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

10. 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.

11. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen

Vertrag über die Verarbeitung von Daten im Auftrag für die Kroschke SIGN Academy

Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

12. 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.

13. 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 1** 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.

14. Dauer des Auftrags

(1) Der Vertrag beginnt mit Unterzeichnung und wird auf unbestimmte Zeit geschlossen.

(2) Er ist mit einer Frist von drei Monaten zum Quartalsende kündbar.

(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.

15. 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

Vertrag über die Verarbeitung von Daten im Auftrag für die Kroschke SIGN Academy

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.

16. 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.

17. 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 _____
Ort Datum

- Auftraggeber -

Braunschweig, den 07.05.2024



Kroschke sign-international GmbH
Michael Essner
Datenschutzkoordinator
Geschäftsleitung Recht & Compliance

Vertrag über die Verarbeitung von Daten im Auftrag für die Kroschke SIGN Academy

Anlage 1: Technische und organisatorische Maßnahmen

Art. 32 DSGVO: Sicherheit der Verarbeitung

Art. 32 DS-GVO bestimmt, dass die verantwortliche Stelle technische und organisatorische Maßnahmen treffen muss. Diese müssen unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen getroffen werden. Diese Maßnahmen müssen die Pseudonymisierung, die Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit als auch die Fähigkeit, Systeme nach einem Zwischenfall rasch wiederherstellen zu können, mit einbeziehen. Weiter muss ein Verfahren implementiert werden, was die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen Maßnahmen gewährleistet. Die folgenden technischen und organisatorischen Maßnahmen wurden durch die Kroschke sign-international GmbH getroffen.

I. Vertraulichkeit

Vertraulichkeit bedeutet, dass die Daten nur von befugten Personen erhoben, verarbeitet, genutzt usw. werden dürfen. Die Vertraulichkeit der Datenverarbeitung wird durch die folgenden Maßnahmen gesichert:

1. Zutrittskontrolle

Unbefugten ist der Zutritt zu den Datenverarbeitungsanlagen (→ Rechenzentrum), mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

<input checked="" type="checkbox"/> Alarmanlage	<input checked="" type="checkbox"/> Chip-/Transponder-Schließsystem
<input type="checkbox"/> Videoüberwachung Zugänge	<input checked="" type="checkbox"/> Sicherheitsschlösser
<input type="checkbox"/> Besetzter Empfang / Pfortner	<input type="checkbox"/> Protokollierung Besucher
<input type="checkbox"/> Ausweisregelung für Besucher (→ Zutritt haben nur: IT, GF, GL, US)	
<input checked="" type="checkbox"/> Schlüsselkonzept Serverraum	<input type="checkbox"/> verschlossener Serverschrank
<input checked="" type="checkbox"/> Notstromaggregat	<input checked="" type="checkbox"/> USV (unterbrechungsfreie Stromversorgung)
<input checked="" type="checkbox"/> Klimaanlage	
<input type="checkbox"/> sorgfältige Auswahl Reinigungspersonal	<input type="checkbox"/> sorgfältige Auswahl Wachpersonal
Weitere:	

Vertrag über die Verarbeitung von Daten im Auftrag für die Kroschke SIGN Academy

2. Zugangskontrolle

Durch die Zugangskontrolle soll verhindert werden, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Auf die Serverumgebung selbst können nur die IT zugreifen.

<input checked="" type="checkbox"/> Zuordnung von Benutzerrechten	<input checked="" type="checkbox"/> Erstellen von Benutzerprofilen
<input checked="" type="checkbox"/> Passwortvergabe	<input checked="" type="checkbox"/> Anmeldung mit Benutzername/Passwort
<input checked="" type="checkbox"/> Sperren von USB-Ports	<input checked="" type="checkbox"/> Sperren bestimmter Ports
<input checked="" type="checkbox"/> Einsatz von VPN-Verbindungen	<input checked="" type="checkbox"/> Einsatz von Intrusion-Detection-Systemen
<input checked="" type="checkbox"/> Verschlüsselung von Datenträgern	<input type="checkbox"/> Verschlüsselung von Smartphone-Inhalten
<input checked="" type="checkbox"/> Mobile Device Management	<input checked="" type="checkbox"/> Antivirensoftware
<input checked="" type="checkbox"/> Verschlüsselung von Datenträgern/ Laptops	<input checked="" type="checkbox"/> Einsatz einer Hardwarefirewall
<input type="checkbox"/> Einsatz einer Softwarefirewall	
weitere:	

3. Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, 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.

<input type="checkbox"/> Rollenbegriffungskonzept	<input checked="" type="checkbox"/> Rechteverwaltung durch Admin
<input checked="" type="checkbox"/> Anzahl Adminrollen so gering wie möglich	<input checked="" type="checkbox"/> Passwortrichtlinie (→ folgt ab Windows 10) (inkl. Passwortlänge, Passwortwechsel)
<input checked="" type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen (insbesondere bei Eingabe, Änderung, Löschung von Daten)	<input checked="" type="checkbox"/> Sichere Aufbewahrung von Datenträgern (→ Tresor)
<input type="checkbox"/> physische Löschung von Datenträgern vor Wiederverwendung	<input checked="" type="checkbox"/> ordnungsgemäße Vernichtung von Datenträgern
<input checked="" type="checkbox"/> Einsatz von Aktenvernichtern/Dienstleister	<input type="checkbox"/> Protokollierung der Vernichtung (z.B. Vernichtungszertifikat durch Dienstleister)
<input type="checkbox"/> Verschlüsselung von Datenträgern	<input type="checkbox"/> Automatisches Ausloggen bei Inaktivität (z.B. Bildschirmsperre bei Abwesenheit)
weitere:	

Vertrag über die Verarbeitung von Daten im Auftrag für die Kroschke SIGN Academy

4. Trennungsgebot

Durch das Trennungsgebot wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

<input type="checkbox"/> physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern	<input checked="" type="checkbox"/> logische Mandantentrennung
<input type="checkbox"/> Verschlüsselung von Datensätzen, die zum demselben Zweck verarbeitet werden	<input type="checkbox"/> Datensätze werden mit Zweckattributen versehen
<input checked="" type="checkbox"/> Festlegung von Datenbankrechten	<input checked="" type="checkbox"/> Trennung Produktiv- und Testsystem
weitere:	

5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer bestimmten betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugeordnet werden. (Art. 4 Nr. 5 DS-GVO).

Prozesse, die mit personenbezogenen Daten arbeiten, sind bereits von Anfang an datenschutzfreundlich zu gestalten; die Pseudonymisierung kann hierfür ein wichtiger Bestandteil sein.

<input type="checkbox"/> Trennung von Zuordnungsdatei und Aufbewahrung auf anderem, getrennten System	<input type="checkbox"/> Pseudonym / Talent-ID bei Skilldatenbanken
<input checked="" type="checkbox"/> Pseudonymisierte Nutzung von Tracking-Tools	<input type="checkbox"/> Pseudonymisierung bei Analysedatenbanken
weitere:	

Vertrag über die Verarbeitung von Daten im Auftrag für die Kroschke SIGN Academy

II. Integrität

Integrität bedeutet, dass die Systeme und die dort hinterlegten Daten korrekt, unverändert, und verlässlich sind. Die Integrität der Daten wird durch folgende Maßnahmen sichergestellt:

1. Eingabekontrolle

Durch die Eingabekontrolle wird gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind.

<input type="checkbox"/> Protokollierung von Stammdatenänderungen	<input checked="" type="checkbox"/> Logfilekontrolle
<input type="checkbox"/> Vergabe von Änderungs-, Lösch- und Bearbeitungsrechten aufgrund eines Rollenbegriffungskonzeptes	<input checked="" type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung, Löschung von Daten durch individuelle Nutzer
<input checked="" type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen (insbesondere bei Eingabe, Änderung, Löschung von Daten)	<input checked="" type="checkbox"/> Protokollierung der Serveraktivitäten
<input checked="" type="checkbox"/> Protokollierung gescheiterter Zugriffsversuche	
weitere:	

2. Weitergabekontrolle

Bei der Weitergabekontrolle wird gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports, ihrer Speicherung auf Datenträgern 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.

<input checked="" type="checkbox"/> VPN-Tunnel bei externen Geräten	<input type="checkbox"/> Weitergabe in anonymisierter oder pseudonymisierter Form
<input type="checkbox"/> E-Mail-Verschlüsselung	<input type="checkbox"/> Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
<input type="checkbox"/> Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung	<input checked="" type="checkbox"/> Vereinbarte Löschrufen
<input checked="" type="checkbox"/> sichere Transportbehälter	<input checked="" type="checkbox"/> Sorgfältige Auswahl Transportpersonal
weitere:	

Vertrag über die Verarbeitung von Daten im Auftrag für die Kroschke SIGN Academy

3. Auftragskontrolle

Durch die Auftragskontrolle wird gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

<input checked="" type="checkbox"/> Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten	<input checked="" type="checkbox"/> vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
<input checked="" type="checkbox"/> schriftliche Weisungen an den Auftragnehmer	<input checked="" type="checkbox"/> Verpflichtung Mitarbeiter des Auftragnehmers auf den Datenschutz/Verschwiegenheitspflichten
<input checked="" type="checkbox"/> Auftragnehmer hat Datenschutzbeauftragten bestellt (wenn gesetzlich vorgeschrieben)	<input checked="" type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Vertragsende
<input checked="" type="checkbox"/> Kontrollrechte gegenüber dem Auftragnehmer	<input checked="" type="checkbox"/> laufende Kontrolle des Auftragnehmers
<input type="checkbox"/> Vereinbarung von Vertragsstrafen	
weitere:	

III. Verfügbarkeit und Belastbarkeit

Verfügbarkeit bedeutet, dass Daten zur Verfügung stehen, wenn sie gebraucht werden.

Das Schutzziel „Belastbarkeit“ wird nicht in der DS-GVO legaldefiniert und hat auch keine Entsprechung im IT-Grundschutz. Nach gegenwärtiger Auffassung ist unter „Belastbarkeit“ die Widerstandsfähigkeit von Systemen gemeint, wie sie im Bereich des Notfallmanagements eine Rolle spielt.

Diese Schutzziele werden durch die folgenden Maßnahmen sichergestellt:

1. Verfügbarkeitskontrolle

Durch die Verfügbarkeitskontrolle wird gewährleistet, dass personenbezogene Daten gegen den zufälligen Verlust geschützt sind.

<input checked="" type="checkbox"/> USV	<input checked="" type="checkbox"/> Klimaanlage in Serverräumen
<input checked="" type="checkbox"/> Temperaturüberwachung / Feuchtigkeitsüberwachung in Serverräumen	<input type="checkbox"/> Videoüberwachung im Serverraum
<input checked="" type="checkbox"/> Schutzsteckdosenleisten in Serverräumen	<input checked="" type="checkbox"/> Feuer- und Rauchmeldeanlagen
<input type="checkbox"/> Alarmmeldung bei unberechtigten Zutritten zu den Serverräumen	<input checked="" type="checkbox"/> Backup- und Recoverykonzept
<input checked="" type="checkbox"/> Testen von Datenwiederherstellung	<input checked="" type="checkbox"/> Erstellen eines Notfallplans
<input checked="" type="checkbox"/> Aufbewahrung von Datensicherungen im anderem Brandabschnitt	<input checked="" type="checkbox"/> Serverräume nicht unter sanitären Anlagen
<input checked="" type="checkbox"/> Regelmäßige Erstellung von Sicherheitskopien	<input checked="" type="checkbox"/> Spiegelung der Systeme
weitere:	

Vertrag über die Verarbeitung von Daten im Auftrag für die Kroschke SIGN Academy

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Die getroffenen Maßnahmen müssen einer regelmäßigen Kontrolle unterzogen werden. Auch sind sie dem jeweils entsprechendem Stand der Technik anzupassen und aktuell zu halten. Im Unternehmen wird ein solches regelmäßiges Kontroll- und Evaluierungskonzept wie folgt umgesetzt:

- Auftragskontrolle der Dienstleister in regelmäßigen Intervallen
- Regelmäßige Mitarbeiterschulungen- und Prüfungen
- Regelmäßige Prüfung der technischen Komponenten und des Backup- und Recoverykonzepts
- Wartungsprotokolle technischer Komponenten
- Regelmäßiges Einspielen von Patches und Softwareupdates
- Zertifizierungen:

weitere:

Schriftliche Dokumentation

<input checked="" type="checkbox"/> interne Verhaltensregeln
<input checked="" type="checkbox"/> Risikoanalyse
<input type="checkbox"/> Allgemeine Datensicherheitsbeschreibung
<input checked="" type="checkbox"/> Umfassendes Datensicherheitskonzept
<input checked="" type="checkbox"/> Notfallplan & Backupsystem
<input type="checkbox"/> Zertifikat: Zertifizierungsstelle:
<input type="checkbox"/> Sonstiges:

Vertrag über die Verarbeitung von Daten im Auftrag für die Kroschke SIGN Academy

Anlage 2

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“).

Es handelt sich um nachfolgende Unternehmen:

AuA24 AG
Südportal 3
22848 Norderstedt