



IT schafft
Vorsprung!

Auftragsverarbeitung nach DSGVO

CEMA Gruppe



CEMA GmbH Spezialisten
für Informationstechnologie
Dortmund



IT schafft Vorsprung!

Vereinbarung zum Datenschutz

- nachfolgend **Auftraggeber** genannt -

und

der in Anlage 3 genannte Auftragsverarbeiter

CEMA Gruppe (gemäß Artikel 26 DSGVO)

Vertreten durch

CEMA GmbH

Spezialisten für Informationstechnologie

Freie-Vogel-Str. 369

44269 Dortmund

- nachfolgend **Auftragnehmer**
genannt –

treffen für die in der Anlage 1 genannten Verträge die nachfolgenden Vereinbarungen zur Wahrung des Datenschutzes gemäß Artikel 28 Abs. 3 Datenschutzgrundverordnung (DSGVO) (wirksam ab 25. Mai 2018) bzw. §11 BDSG (wirksam bis Mai 2018) im Rahmen einer Auftrags(daten)verarbeitung.



IT schafft Vorsprung!

Inhaltsverzeichnis

1. Präambel	4
2. Definitionen	4
3. Anwendungsbereich und Verantwortlichkeit	5
4. Umfang, Art und Zweck der Datenverwendung, Art der Daten und Kreis der Betroffenen Umfang	6
5. Umfang der Weisungsbefugnis	7
6. Pflichten des Auftragsverarbeiters	7
7. Pflichten des Auftraggebers	12
8. Anfragen und Auskunfts-, Sperrungs- oder Löschanforderungen Betroffener	12
9. Kontrollpflicht des Auftraggebers	12
10. Subunternehmer	13
11. Haftung, Sonstiges	14



IT schafft Vorsprung!

1. Präambel

(1) Gemäß Art. 28 DSGVO / § 11 BDSG werden an die Durchführung einer Auftragsverarbeitung sowie an Form und Inhalt der Vereinbarung über die Auftragsverarbeitung bestimmte gesetzliche Anforderungen gestellt.

(2) Die Anforderungen müssen ebenso erfüllt werden, wenn automatisierte Verfahren oder Datenverarbeitungsanlagen durch andere Stellen im Auftrag gewartet oder geprüft werden und dabei der Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

(3) Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus den in der Anlage 1 bezeichneten Verträgen ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem/den Hauptvertrag/Hauptverträgen in Zusammenhang stehen und bei denen Mitarbeiter des Auftragsverarbeiters oder durch den Auftragsverarbeiter beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können bzw. ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

2. Definitionen

(1) Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Dabei kommt es nicht darauf an, wer diese Zuordnung vornehmen kann, sondern nur darauf, ob eine solche überhaupt möglich ist.

(2) Im Zweifelsfall gelten alle Daten, mit denen der Auftragsverarbeiter oder seine Mitarbeiter bzw. von ihm Beauftragte in Berührung kommen oder kommen können, als personenbezogene Daten im Rahmen dieser Vertragsdurchführung.

(3) Für diesen Vertrag kommen die weiteren Begriffsdefinitionen in Artikel 4 DSGVO zur Anwendung.



IT schafft Vorsprung!

3. Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragsverarbeiter führt alle Arbeiten im Auftrag und nach den Weisungen des Auftraggebers durch. Dies umfasst jene Tätigkeiten, die im Hauptvertrag konkretisiert sind.

(2) Gegenstand und Dauer des Auftrags ergeben sich aus dem/den Hauptvertrag/Hauptverträgen gemäß Anlage 1.

(3) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich.

(4) Soweit eine der Vertragsparteien nicht in der Union niedergelassen ist, benennt der Verantwortliche oder der Auftragsverarbeiter schriftlich, gem. Artikel 27 DSGVO, einen Vertreter in der Union. Dieser vertritt den Verantwortlichen oder den Auftragsverarbeiter in allen nach der DSGVO obliegenden Pflichten. Die Vertragsparteien informieren sich gegenseitig in einem Fall der Bestellung über die Kontaktdaten des Vertreters und den Umfang seiner Beauftragung.

(5) Soweit eine Vertragspartei einen Datenschutzbeauftragten benannt hat, informiert sie die jeweils andere Vertragspartei über den Namen und die Kontaktdaten.

(6) Der Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung (Art. 30 Abs. 2 DSGVO), die Folgendes enthält:

- a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und des Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
- b) die Kategorien von Verarbeitungen, die im Auftrag des Verantwortlichen durchgeführt werden;
- c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Abs. 1 Unterabsatz 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- d) eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DSGVO.



IT schafft Vorsprung!

(7) Die Pflichten in Absatz 6 bestehen nur, soweit der Auftragsverarbeiter zur Führung eines solchen Verzeichnisses nach der DSGVO verpflichtet ist. Es bleiben insbesondere die Ausnahmetatbestände des Art. 30 Abs. 5 DSGVO unberührt.

(8) Der Auftragsverarbeiter führt das Verzeichnis schriftlich, was auch in einem elektronischen Format erfolgen kann. Der Auftraggeber übermittelt dem Auftragsverarbeiter die zur Führung des Verzeichnisses erforderlichen Informationen in Anlage 2 vor Vertragsbeginn. Der Auftragsverarbeiter stellt dem Auftraggeber und seinem bestellten Datenschutzbeauftragten einen Abdruck des Verzeichnisses auf Anforderung zur Verfügung.

(9) Verlangt eine Aufsichtsbehörde von einer der Vertragsparteien die Herausgabe des Verzeichnisses, informieren sich die Vertragsparteien gegenseitig unverzüglich hierüber und über den Inhalt der Auskunft. Soweit die Pflicht zum Führen eines Verzeichnisses für eine der Vertragsparteien nicht gilt, bleiben hiervon die Informationspflichten unberührt.

(10) Soweit der Auftraggeber nicht selbst Verantwortlicher im Sinne des Artikel 4 Nummer 7 DSGVO ist, führt er das Verzeichnis der Verarbeitungen als Auftragnehmer im Auftrag des Auftragnehmers, teilt dem Auftragnehmer zur Erfüllung dessen Pflichten nach Art. 30 Absatz 3 DSGVO auf Anforderung das Verzeichnis mit und unterstützt diesen bei allen weiteren Pflichten gegenüber dem Verantwortlichen.

4. Umfang, Art und Zweck der Datenverwendung, Art der Daten und Kreis der Betroffenen Umfang

(1) Der Auftragsverarbeiter wird die Auswahl und Gestaltung seiner Datenverarbeitungssysteme an dem Ziel ausrichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Er wird, sofern dies nach dem Auftrag möglich ist, personenbezogene Daten anonymisieren oder pseudonymisieren. Er wird den Auftraggeber auf technische Möglichkeiten zur Datenvermeidung und Datensparsamkeit hinweisen. Er wird Maßnahmen zur Gewährleistung des Rechts auf Datenportabilität gem. Art. 20 DSGVO und der Rechenschaftspflichtigkeit gem. Art. 5 (2) DSGVO treffen. Der Auftragsverarbeiter hat hierzu insbesondere sicherzustellen, dass

- a) er auf Anforderung des Auftraggebers, diesem die im Auftrag verarbeiteten Daten in einem gängigen maschinenlesbaren Format innerhalb einer Woche nach Eingang der Aufforderung zur Verfügung stellen kann und
- b) die Ausführung der Weisungen des Auftraggebers sowie die Durchführung der Auftragsverarbeitung dokumentiert.



IT schafft Vorsprung!

(2) Der Umfang, der Zweck, die Rechtsgrundlage und die Erfüllung der sonstigen rechtlichen Zulässigkeitsanforderungen sowie die Art der Daten und der Kreis der betroffenen Personen wird in den Anlagen ausführlich dokumentiert und verbindlich vereinbart.

5. Umfang der Weisungsbefugnis

(1) Der Auftraggeber behält sich umfassende Weisungsbefugnis für die Durchführung des Auftrages gegenüber dem Auftragsverarbeiter und alle durch ihn zur Verarbeitung von personenbezogenen Daten befugten Personen vor. Sollten über den Hauptvertrag oder diese Zusatzvereinbarung hinaus konkrete Weisungen erforderlich sein, wird der Auftraggeber dem Auftragsverarbeiter Einzelweisungen erteilen. Hierfür werden eine oder mehrere weisungsbefugte Personen benannt.

(2) Der Auftraggeber ist verpflichtet, die Einzelweisung schriftlich oder elektronisch ausschließlich an die vom Auftragsverarbeiter benannte weisungsbefugte Personen zu erteilen. Der Auftraggeber dokumentiert alle Weisungen.

6. Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter darf Daten nur gemäß und im Umfang der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Zur Entgegennahme von Weisungen werden eine oder mehrere befugte Weisungsempfänger benannt. Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, wenn er der Meinung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder eines Mitgliedstaates verstößt und soweit eine mitgliedstaatliche Bestimmung auf den Auftragsverarbeiter anwendbar ist. Ein solcher Hinweis berechtigt den Auftragsverarbeiter zur Aussetzung der Befolgung der Weisung, bis diese nach dem Hinweis vom Auftraggeber nochmals schriftlich bestätigt wird.

(2) Wenn personenbezogene Daten verarbeitet oder genutzt werden, so ist die Organisation auf der Seite des Auftragsverarbeiters so zu gestalten, dass die besonderen Anforderungen des Datenschutzes umgesetzt werden. Der Auftragsverarbeiter garantiert daher, die notwendigen technischen und organisatorischen Maßnahmen zu ergreifen, um die Verarbeitung der personenbezogenen Daten des Auftraggebers zu schützen. Dies beinhaltet insbesondere folgende Maßnahmen:



IT schafft Vorsprung!

a) Zutrittskontrolle

Unbefugten wird der Zutritt zu Räumlichkeiten, in denen personenbezogene Daten lagern oder verarbeitet werden, verwehrt. Während der Dienstzeit wird dies durch die Mitarbeiter des Auftragsverarbeiters gewährleistet. Außerhalb der Dienstzeiten sind diese Räumlichkeiten verschlossen zu halten. Ausschließlich autorisierte Personen, welche zutrittsberechtigt sind, haben einen Schlüssel zu diesen Räumlichkeiten.

b) Zugangskontrolle

Im Rahmen der Zugangskontrolle wird verhindert, dass Unbefugte die Verarbeitungssysteme nutzen. Die logische Zugangskontrolle wird durch ein umfassendes Rechte- und Rollenkonzept erreicht.

c) Zugriffskontrolle

Im Rahmen der Zugriffskontrolle stellt der Auftragsverarbeiter sicher, dass ausschließlich die Berechtigten auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Die Rollen der Benutzer, die auf die personenbezogenen Daten des Auftraggebers zugreifen können, sind fest definiert.

d) Weitergabekontrolle

Eine Weitergabe der Daten an Dritte erfolgt nicht. Datentransfer zwischen Auftraggeber und Auftragsverarbeiter erfolgt über eine dem aktuellen Stand der Technik entsprechende verschlüsselte Verbindung.

Der Auftragsverarbeiter verpflichtet sich ferner ausdrücklich, dafür Sorge zu tragen, dass Daten des Auftraggebers während ihrer Speicherung und Verarbeitung beim Auftragsverarbeiter nicht unbefugt kopiert, gelöscht, gelesen oder verändert werden können.

e) Eingabekontrolle

Im Rahmend der Eingabekontrolle stellt der Auftragsverarbeiter sicher, dass für alle Eingaben überprüft werden kann, ob und von wem personenbezogene Daten eingegeben, gelöscht oder verändert worden sind. Die Eingabekontrolle erfolgt über die systeminterne Protokollierung. Auf Verlangen des Auftraggebers ist diesem der aktuelle Stand der Protokollierungsdaten zugänglich zu machen.



IT schafft Vorsprung!

f) Auftragskontrolle

Der Auftragsverarbeiter stellt sicher, dass personenbezogene Daten des Auftraggebers ausschließlich nach dessen Weisungen verarbeitet werden können. Der Auftragsverarbeiter ist daher verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit diese Auskünfte Daten und Unterlagen des Auftraggebers betreffen. Ferner verpflichtet sich der Auftragsverarbeiter, die Kontrolle der Datenverarbeitung durch den Auftraggeber jederzeit zu dulden und zu unterstützen.

g) Verfügbarkeitskontrolle

Der Auftragsverarbeiter schützt die personenbezogenen Daten im Umfang und gemäß den Vereinbarungen des zwischen Auftragsverarbeiter und Auftraggeber geschlossenen Hauptvertrags vor zufälliger Zerstörung oder Verlust. Er gewährleistet die rasche Wiederherstellung der Verfügbarkeit personenbezogener Daten und des Zugangs zu diesen auch bei einem technischen Zwischenfall oder einer ungewöhnlichen Belastung der Systeme.

h) Trennungskontrolle

Der Auftragsverarbeiter hat durch Organisation seiner Arbeitsprozesse sicherzustellen, dass die Daten des Auftraggebers nicht mit den Daten anderer Kunden vermischt werden oder anderen Kunden bekannt werden können. Innerhalb von Datenverarbeitungsanlagen kann dies durch Zugriffsberechtigungen sichergestellt werden.

i) Wirksamkeitskontrolle

Der Auftragsverarbeiter hat ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzuführen und die Ergebnisse zu dokumentieren. Dazu gehört die Sicherstellung der Benachrichtigungspflichten gegenüber Aufsichtsbehörden und Betroffenen bei Verletzungen des Schutzes personenbezogener Daten durch die Einführung von Überwachungsmaßnahmen, die geeignet sind, Schutzverletzungen und deren Auswirkungen rechtzeitig festzustellen und deren mögliche Auswirkungen zu bestimmen. Die Dokumentation ist dem Auftraggeber auf Verlangen zur Verfügung zu stellen.

(3) Der Auftragsverarbeiter stellt dem Auftraggeber die für das Verzeichnis nach Art. 30 Abs. 1 DSGVO notwendigen Angaben ohne gesonderte Aufforderung vor Vertragsbeginn in Anlage 3 zur Verfügung.

(4) Der Auftragsverarbeiter stellt sicher, dass die zur Verarbeitung der Daten des Auftraggebers befugten Personen gemäß Art. 28 Abs. 3 Satz 2 lit. b DSGVO oder aufgrund einer gesetzlichen Regelung zur Verschwiegenheit verpflichtet sind und in die Schutzbestimmungen des



IT schafft Vorsprung!

Datenschutzrechtlich eingewiesen worden sind. Auf Verlangen, weist der Auftragsverarbeiter dem Auftraggeber die wirksame Verpflichtung seiner Mitarbeiter auf das Datengeheimnis nach. Der Auftragsverarbeiter gibt dem Datenschutzbeauftragten des Auftraggebers zu diesem Zweck die Verpflichtungserklärungen zur Kenntnis.

(5) Der Auftragsverarbeiter teilt dem Auftraggeber die Kontaktdaten eines eventuell bestellten betrieblichen Datenschutzbeauftragten in Anlage 3 mit und informiert den Auftraggeber bei jeder Änderung.

(6) Stellt der Auftragsverarbeiter fest, dass eine der in der Anlage 5 beschriebenen und festgelegten Schutzmaßnahmen nicht oder nicht mehr wirksam ist und hierdurch, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führen kann teilt er dies dem Auftraggeber unverzüglich mit. Die Mitteilung muss folgende Informationen enthalten:

- a) 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;
- b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- d) eine Beschreibung der von dem Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Auftragsverarbeiter diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

(7) Der Auftragnehmer - unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen - unterstützt den Auftraggeber bei der Einhaltung seiner Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung. Er unterstützt den Auftraggeber bei der Erfüllung seiner Benachrichtigungs- und Auskunftspflichten gegenüber Aufsichtsbehörden und Betroffenen. Er trägt hierfür durch die Einführung von Überwachungsmaßnahmen Sorge, die geeignet sind,



IT schafft Vorsprung!

Schutzverletzungen und deren Auswirkungen rechtzeitig festzustellen und deren mögliche Auswirkungen zu bestimmen. Er trägt durch geeignete technische und organisatorische Maßnahmen dafür Sorge, dass der Auftraggeber seine Pflicht zur Benachrichtigung aller Empfänger von Daten über eine Berichtigung oder Löschung der personenbezogenen Daten oder der Einschränkung der Verarbeitung sowie seine Pflicht zur Übermittlung von bereitgestellten personenbezogenen Daten an den Betroffenen oder an einen anderen Verantwortlichen in einem strukturierten, gängigen und maschinenlesbaren Format (Recht auf Datenübertragbarkeit) erfüllen kann.

(8) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragsverarbeiter hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragsverarbeiter wird bei Beendigung des Vertragsverhältnisses alle vom Auftraggeber überlassenen Datenträger sowie gefertigte Kopien vollständig an den Auftraggeber zurückgeben, es sei denn, der Auftraggeber verlangt eine Löschung der Daten. Der Auftragsverarbeiter weist dem Auftraggeber in diesem Fall die ordnungsgemäße Löschung der Daten durch ein Löschartokoll, oder durch ein anderes zum Nachweis geeignetes Dokument, nach. Der Auftragsverarbeiter wird in diesem Dokument die Art der Löschung konkret beschreiben.

(9) Die vom Auftragsverarbeiter konkret getroffenen technischen und organisatorischen Maßnahmen sind in der Anlage 2 verbindlich festgelegt. Änderungen dieser Maßnahmen sind nach Mitteilung an den Auftraggeber und dessen Genehmigung oder bei Maßnahmen, die ausschließlich zu einer Erhöhung des Sicherheitsniveaus führen, nach Mitteilung an den Auftraggeber zulässig.

(10) Jedwede Übermittlung personenbezogener Daten in ein Drittland, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Auftragsverarbeiter die, in der DSGVO niedergelegten, Bedingungen einhält; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation. Soweit sich die Übermittlung auf geeignete Garantien gem. Art. 46 DSGVO stützt, sind diese gegenüber dem Auftraggeber nachzuweisen. Stützt sich die Übermittlung auf eine Ausnahmeregel des Art. 49 DSGVO so hat der Auftragsverarbeiter die Garantien und die von ihm vorgenommene Beurteilung schriftlich ausführlich dokumentiert, nach Genehmigung durch den Auftraggeber, im Verzeichnis gem. Art. 30 DSGVO aufzunehmen.



IT schafft Vorsprung!

7. Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Der Auftraggeber trägt die Verantwortung für die Zulässigkeit der Verarbeitung und die Information der Betroffenen gem. Art. 12-14 DSGVO.

(3) Über die Herausgabe oder Löschung der Daten nach Vertragsende muss der Auftraggeber bis zum Vertragsende entschieden haben. Trifft der Auftraggeber bis zu diesem Zeitpunkt keine Entscheidung, werden die Daten ordnungsgemäß nach dem Stand der Technik gelöscht. Der Auftragsverarbeiter ist verpflichtet, den Auftraggeber zwei Wochen vor Vornahme der endgültigen Löschung hiervon zu unterrichten.

8. Anfragen und Auskunfts-, Sperrungs- oder Löschverlangen Betroffener

(1) Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragsverarbeiter ihn dabei unterstützen, diese Informationen innerhalb des gesetzlichen Zeitraumes von einem Monat nach Antragstellung bereit zu stellen, wenn der Auftraggeber den Auftragsverarbeiter hierzu unter Fristnennung schriftlich auffordert.

(2) Der Auftraggeber ist auch für die Berichtigung, Sperrung und Löschung der Daten Betroffener verantwortlich. Der Auftragsverarbeiter unterstützt ihn bei den dabei anfallenden Arbeiten und wird die Weisungen des Auftraggebers unverzüglich durchführen und den Auftraggeber über die erfolgte Berichtigung, Sperrung und Löschung informieren.

(3) Stellt ein Betroffener eine Anfrage oder einen Antrag an den Auftragsverarbeiter, wird dieser die Anfrage bzw. den Antrag unverzüglich unter Angabe des Zeitpunkts des Zugangs der Anfrage beim Auftragsverarbeiter an den Auftraggeber weiterleiten.

9. Kontrollpflicht des Auftraggebers

(1) Der Auftraggeber kann sich von den vom Auftragsverarbeiter getroffenen Maßnahmen vor Vertragsbeginn und sodann in regelmäßigen Abständen überzeugen. Hierzu ist er berechtigt, vom Auftragsverarbeiter aussagekräftige Zertifikate unabhängiger Dritter, die für den Auftragsverarbeiter



IT schafft Vorsprung!

erteilt worden sind, anzufordern, den Auftragsverarbeiter aufzufordern, Auskünfte in Form einer übersandten Checkliste oder eines Online-Audits zu erteilen, interne Prüfdokumente zu übersenden oder nach rechtzeitiger Anmeldung Kontrollen in den Betriebsstätten des Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs vorzunehmen.

(2) Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Prüfung in den Betriebsstätten des Auftragsverarbeiters im erforderlichen Umfang und wird die Kontrollen des Auftraggebers dulden.

10. Subunternehmer

(1) Der Auftragsverarbeiter kann auch Subunternehmer mit der Durchführung der Dienstleistungen beauftragen. Wenn der Auftragsverarbeiter Subunternehmer beauftragt, führt der Auftragsverarbeiter eine Liste der Subunternehmer, die die personenbezogenen Daten des Verantwortlichen verarbeiten dürfen, und stellt dem Verantwortlichen auf Anfrage eine Kopie dieser Liste zur Verfügung.

Leistungen, die der Auftragsverarbeiter von Dritten als reine Nebenleistungen zur Durchführung der Geschäftstätigkeit in Anspruch nimmt, gelten nicht als Unterauftragsverhältnisse im Rahmen dieser Vereinbarung. Dazu gehören z.B. Reinigungsdienste, reine Telekommunikationsdienste ohne besondere Bezugnahme auf Dienstleistungen des Auftragsverarbeiters für den Verantwortlichen, Post- und Kurierdienste, Transportdienste oder Sicherheitsdienstleistungen.

(2) Wenn weitere Subunternehmer durch den Auftragsverarbeiter eingeschaltet werden sollen, so werden die vertraglichen Vereinbarungen so gestaltet, dass sie allen Anforderungen zwischen den Vertragspartnern aus diesem Vertrag entsprechen. Dem Auftraggeber sind Kontroll- und Überprüfungsrechte entsprechend dieser Zusatzvereinbarung auch gegenüber den Subunternehmern/Unterauftragsverarbeitern einzuräumen. Ebenso ist der Auftraggeber berechtigt, auf schriftliche Anforderung von dem Auftragsverarbeiter Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

Der Antrag hat mindestens fünf Tage vor dem geplanten Einsatz zu erfolgen, um eine vorherige Prüfung durch den Auftraggeber zu ermöglichen.

(3) Der Verantwortliche genehmigt die Verwendung der in Anlage 4 genannten Subauftragnehmer bei der Erbringung der Dienstleistungen gemäß den Bedingungen dieser Vereinbarung.

(4) Der Auftragsverarbeiter teilt dem Verantwortlichen jeden neuen Subunternehmer mit, bevor er den Subunternehmer beauftragt, personenbezogene Daten im Zusammenhang mit der Erbringung der betreffenden Dienstleistungen zu verarbeiten. Der Verantwortliche kann der Verwendung eines neuen



IT schafft Vorsprung!

Subunternehmens widersprechen, indem er den Auftragnehmer unverzüglich innerhalb von zehn (10) Werktagen nach Erhalt der Mitteilung des Auftragnehmers schriftlich benachrichtigt. Der Widerspruch soll auf datenschutzrechtliche Gründe oder Zweifel am Schutzniveau der Datenverarbeitung durch den Subunternehmer gestützt werden. Für den Fall, dass der Verantwortliche einem neuen Subunternehmer widerspricht, wird der Auftragsverarbeiter angemessene Anstrengungen unternehmen, um dem Verantwortlichen eine Änderung der Dienste zur Verfügung zu stellen oder eine wirtschaftlich sinnvolle Änderung der Konfiguration des Verantwortlichen oder der Nutzung der Dienste zu empfehlen, um die Verarbeitung personenbezogener Daten durch den betreffenden Subunternehmer zu vermeiden, ohne den Verantwortlichen unangemessen zu belasten. Wenn der Auftragsverarbeiter nicht in der Lage ist, diese Änderung innerhalb einer angemessenen Frist, die dreißig (30) Tage nicht überschreiten darf, zur Verfügung zu stellen, kann der Verantwortliche die anwendbaren Verträge nur in Bezug auf die Dienstleistungen kündigen, die vom Auftragsverarbeiter nicht ohne die Verwendung des Subunternehmens erbracht werden können, indem er den Auftragsverarbeiter schriftlich benachrichtigt. Der Auftragsverarbeiter erstattet dem Verantwortlichen alle vorausbezahlten Gebühren für den Rest der Laufzeit solcher Verträge nach dem Wirksamwerden der Kündigung in Bezug auf diese gekündigten Dienste, ohne dem Verantwortlichen eine Strafe für diese Kündigung aufzuerlegen.

(5) Im Rahmen der Bearbeitung des Auftrages, können Leistungen durch Mitglieder der CEMA Gruppe bzw. deren Mitarbeiter erfüllt werden. Diese sind jedoch als Teil der gemeinsam verantwortlichen Gruppe gemäß Artikel 26 DSGVO keine Subunternehmer. Die Vereinbarung nach Artikel 26 DSGVO kann beim Auftragnehmer eingesehen werden.

11. Haftung, Sonstiges

(1) Jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine, nicht dieser Verordnung entsprechende, Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den, durch eine Verarbeitung verursachten Schaden, nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat. Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Der Auftragsverarbeiter unterstützt den Auftraggeber bei den erforderlichen Nachweisen. Ist mehr als ein



IT schafft Vorsprung!

Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß Art. 82 Abs. 2 und 3 DSGVO für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadenersatz für die betroffene Person sichergestellt ist. Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Art. 82 Abs. 4 DSGVO vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten, für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern, der unter den in Art. 82 Abs. 2 DSGVO festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.

(2) Liegen die hinreichenden Garantien gem. Art. 28 Abs. 1 DSGVO nicht mehr vor oder zeigt sich ein Mangel erst nach Begründung des Auftragsverhältnisses und wird dieser nicht innerhalb einer vom Auftraggeber gesetzten Frist abgestellt, haftet der Auftragsverarbeiter für den hierdurch entstehenden Schaden.

(3) Stellt der Auftraggeber im Rahmen seiner regelmäßigen Kontrolle einen Verstoß gegen die gesetzlichen oder vertraglichen Regelungen fest, hat der Auftragsverarbeiter diese innerhalb einer angemessenen Frist zu beseitigen.

(4) Im Fall eines vom Auftragsverarbeiter zu verantwortenden Verstoßes gegen eine Verpflichtung aus diesem Vertrag kann der Auftraggeber vom Auftragsverarbeiter für jeden Einzelfall eine angemessene Vertragsstrafe verlangen. Ein Einzelfall liegt dann vor, wenn eine einzige Handlung kausal ist für einen oder zeitgleich auch mehrere Verstöße gegen die o.g. Verpflichtungen oder wenn mehrere selbständige Handlungen vorliegen, diese aber immer dieselbe(n) Verpflichtung(en) verletzen und darüber hinaus in einem engen, räumlichen und zeitlichen Zusammenhang stehen. Die Verpflichtung zur Zahlung einer Vertragsstrafe besteht nicht, wenn der Auftragsverarbeiter nachweist, dass er oder ein von ihm beauftragter Subunternehmer den Verstoß nicht zu vertreten hat. Hierbei gilt der gesetzliche Haftungsmaßstab des § 276 BGB, wobei eine Verletzung der zugesicherten technisch-organisatorischen Maßnahmen als eine übernommene Garantie gewertet wird. Im Falle der Geltendmachung der Vertragsstrafe wird die Vertragsstrafe auf einen Schadenersatzanspruch angerechnet. Der Anspruch auf Erstattung eines die Vertragsstrafe übersteigenden Schadens bleibt unberührt.

(5) Der Auftragsverarbeiter haftet für ein Verschulden seines Subunternehmers sowie dessen weitere Subunternehmer wie für eigenes Verschulden.

(6) Sollten die Daten des Auftraggebers beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder



IT schafft Vorsprung!

Maßnahmen Dritter, auch soweit es sich um staatliche Maßnahmen handelt, gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich darüber zu informieren. Der Auftraggeber wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt. Die Einrede des Zurückbehaltungsrechts nach § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(7) Die Unwirksamkeit einer Bestimmung dieser Vereinbarung berührt die Gültigkeit der übrigen Bestimmungen nicht. Sollte sich eine Bestimmung als unwirksam erweisen, werden die Parteien diese durch eine neue ersetzen, die dem von den Parteien Gewollten am nächsten kommt.

(8) Sämtliche Vereinbarungen, die eine Änderung, Ergänzung oder Konkretisierung dieser Vereinbarung beinhalten, sowie besondere Zusicherungen und Abmachungen oder eine Änderung dieser Regel selbst sind schriftlich oder elektronisch niederzulegen.

(9) Es besteht zwischen den Parteien Einigkeit darüber, dass eventuelle "Allgemeine Geschäftsbedingungen" des Auftragsverarbeiters auf diese Vereinbarung keine Anwendung finden.

(10) Es gilt deutsches Recht.

(11) Im Fall von Widersprüchen von Regelungen dieser Vereinbarung und Regelungen aus sonstigen Vereinbarungen gehen die Regelungen dieser Vereinbarung und ihrer Anlagen vor.

(12) Die Anlagen 1 und 2 sind verbindlicher Bestandteil dieser Vereinbarung.

Ort, Datum

Ort, Datum

Unterschrift Auftraggeber

Unterschrift Auftragnehmer