Vertrag zur Auftragsverarbeitung

.
.
.
.

im Folgenden: Auftraggeber (kann auch ein lesbarer Stempeleindruck sein)

und
Backens Systems GmbH
Max-Volmer-Straße 14
40724 Hilden
vertreten durch den Geschäftsführer Dirk Backens
im Folgenden: Auftragnehmer

1. Gegenstand und Dauer der Verarbeitung

a) Der Auftragnehmer erbringt Leistungen für den Auftraggeber. Diese ergeben sich aus der laufenden Geschäftsbeziehung zwischen den Parteien über die (Dienst-) Leistungen. Im Rahmen dieser Leistungen verarbeitet der Auftragsnehmer personenbezogene Daten für den Auftraggeber und seine weiteren Unternehmensstandorte auf Basis der Geschäftsbeziehung.

b) Die Laufzeit dieses Vertrages zur Auftragsverarbeitung ist an die Laufzeit der bestehenden Geschäftsbeziehung zwischen Auftraggeber und Auftragnehmer über die (Dienst-) Leistungen des Auftragnehmers gekoppelt.

2. Ort der Leistungserbringung

a) Der Auftragnehmer erbringt die Leistungen nach diesem Vertrag ausschließlich in der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum.

b) Eine Verlagerung der Tätigkeit oder von Teilen der Tätigkeit in ein Drittland i.S.v. Art 44 DSGVO darf nur nach vorheriger schriftlicher Zustimmung des Auftraggebers erfolgen und muss zudem die Vorgaben des Artikel 44 DSGVO erfüllen. Die Zustimmung muss in Schriftform (§ 126 BGB) erteilt werden.

3. Art und Zweck der Verarbeitung

a) Die Verarbeitung der Daten meint Verarbeitung im Sinne von Artikel 4 Nr. 2 DSGVO.

b) Die Verarbeitung der Daten erfolgt zum Zweck der Vertragserfüllung (Artikel 6 b DSGVO).

4. Art der Daten und Kategorien der betroffenen Personen

a) Folgende Arten personenbezogener Daten im Sinne von Artikel 4 Nr.1,13,14 und 15 DSGVO werden verarbeitet:

- Name, Vorname
- Kommunikationsdaten wie Telefon-, Fax- und Handynummer, E-Mailadresse
- Vertragsstammdaten
- Vertragsabrechnungs- und Zahlungsdaten
- Kundenhistorie
- Sonstige, nämlich: .....

b) Folgende Personenkategorien sind betroffen:

- Kunden, sowie deren Mitarbeiter
- Interessenten, sowie deren Mitarbeiter
- Sonstige, nämlich: .....

5. Verantwortlicher; Weisungsbefugnis des Auftraggebers

a) Der Auftraggeber ist Verantwortlicher im Sinne von Artikel 28 und Artikel 4 Nr. 7 DSGVO. Er ist allein verantwortlich für die Wahrung der Rechte der betroffenen Personen nach den Artikeln 12 bis 22 DSGVO.

b) Der Auftraggeber ist berechtigt dem Auftragnehmer Weisungen in Bezug auf die Auftragsverarbeitung im Rahmen dieses Vertrages zu erteilen. Diese sind in Textform (§ 126b BGB) zu erteilen. Mündliche Weisungen sind unverzüglich in Textform nachzureichen.

c) Weisungsberechtigte Personen des Auftraggebers sind:

.....

d) Weisungsempfänger beim Auftragnehmer sind: Mitarbeiter des Auftragnehmers

e) Der Auftragnehmer ist verpflichtet, den Auftraggeber unverzüglich auf Weisungen, welche er für datenschutzrechtswidrig hält, hinzuweisen. Er hat sodann mit der Ausführung der Weisung abzuwarten bis der Auftraggeber ausdrücklich eine neue Weisung erteilt oder an der bisherigen festhält.

f) Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt, der unter datenschutz@backens-systems.de zu erreichen ist.

6. Verschwiegenheitspflicht

Der Auftragnehmer gewährleistet, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7. Sicherheit der Verarbeitung

a) Auftraggeber und Auftragnehmer treffen technische und organisatorische Maßnahmen, welche geeignet sind, das Risiko für die Verletzung von Rechten und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen zu minimieren und ein dem Risiko angemessenes Schutzniveaus zu schaffen. Dabei sind der Stand der Technik, die Implementierungskosten, die Art, der Zweck, die Umstände und der Umfang der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere des Risikos zu berücksichtigen.

b) Die Maßnahmen nach Ziffer 7 a) schließen unter anderem Folgendes ein:
   - die Pseudonymisierung und Verschlüsselung personenbezogener Daten
   - die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
   - die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu diesen bei einem physischen oder technischen Zwischenfall zügig wiederherzustellen
   - ein Verfahren zur regelmäßigen Überprüfung, Bewertungen und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

c) Die konkreten Maßnahmen ergeben sich aus Anlage 1 zu diesem Vertrag.

d) Der Auftragnehmer kann die Maßnahmen jederzeit anpassen oder verändern, sofern sichergestellt ist, dass das bisherige Schutzniveau nicht unterschritten wird. Insbesondere

kann er die Maßnahmen an technische wie organisatorische Weiterentwicklungen anpassen.

8. Beauftragung von Subunternehmen

a) Der Auftraggeber erteilt die allgemeine Genehmigung für den Einsatz von Subunternehmen durch den Auftragnehmer, soweit diese in Bezug auf die Auftragsverarbeitung vertraglich unter Berücksichtigung der jeweiligen Dienstleistung in vergleichbarem Maße verpflichtet sind wie der Auftragnehmer gegenüber dem Auftraggeber und die datenschutzrechtlichen Vorgaben nach DSGVO gewährleisten.

b) Der Auftragnehmer setzt nur in der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum ansässige Subunternehmen ein. In einem Drittland i.S.v. Art 44 DSGVO ansässige Subunternehmen dürfen nur nach vorheriger Zustimmung des Auftraggebers erfolgen; diese müssen zudem die Vorgaben des Artikel 44 DSGVO erfüllen.

c) Der Auftragnehmer kann weitere Subunternehmen, welche zur zweckmäßigen Durchführung seiner Tätigkeit erforderlich sind, zusätzlich zu den bereits beauftragten einsetzen.

d) Der Auftragnehmer informiert den Auftraggeber über den beabsichtigten Einsatz neuer oder zusätzlicher Subunternehmen. Der Auftraggeber kann gegen den Einsatz des neuen Subunternehmens Einspruch erheben. Der Einspruch ist, sofern in dem Informationsschreiben keine Einspruchsfrist genannt ist, binnen sieben Tagen in Textform nach Zugang der Information zu erheben. Wird der Einspruch nicht frist-und/ oder formgerecht erhoben, gilt der Einsatz des betreffenden Subunternehmens als genehmigt.

e) Erhebt der Auftraggeber frist- und formgerecht Einspruch, kann der Auftragnehmer den Vertrag mit dem Auftraggeber kündigen. Die Kündigung muss zu ihrer Wirksamkeit in Schriftform (§ 126 BGB) erfolgen und binnen einer Frist von vier Wochen nach Zugang des Einspruchs erfolgen. Alternativ kann der Auftragnehmer nach seinem Ermessen anbieten, den Vertrag unter Einsetzung des bisherigen Subunternehmens fortzuführen, sofern dieses keinen unverhältnismäßigen Aufwand erfordert. Der Auftraggeber hat sodann mögliche Mehrkosten zu tragen. Der Auftragnehmer ist nicht verpflichtet, die Fortführung anzubieten.

9. Mitteilungspflicht bei Störungen und Verletzung des Schutzes personenbezogener Daten

a) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Verstöße gegen datenschutzrechtliche Bestimmungen oder die Festlegungen dieses Vertrages mit, welche von ihm oder von ihm beschäftigten Personen hervorgerufen wurden.

b) Der Auftragnehmer teilt dem Auftraggeber unverzüglich mit, wenn Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten auftreten.

c) Der Auftragnehmer unterstützt den Auftraggeber soweit möglich bei der Erfüllung dessen Melde- und Benachrichtigungspflichten nach Artikeln 33 und 34 DSGVO.

10. Sonstige Pflichten des Auftragnehmers

a) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit technischen und organisatorischen Maßnahmen dabei, dass dieser seiner Pflicht zur Beantwortung von Anträgen von Betroffenen auf Wahrnehmung ihrer Rechte nach Abschnitt III der DSGVO nachkommen kann.

b) Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle erforderlichen Informationen zur Verfügung und erteilt Auskünfte, welche für den Nachweis, dass er sich an die vertraglichen und gesetzlichen Vorgaben hält, erforderlich sind.

c) Der Auftragnehmer ermöglicht dem Auftraggeber oder von dessen beauftragten Prüfern nach Absprache Kontrollen.

d) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten nach Artikel 32 bis 36 DSGVO.

12. Datenlöschung bei Vertragsende

Der Auftragnehmer ist verpflichtet, alle personenbezogenen Daten zu löschen, wenn dieser Vertrag endet. Diese Verpflichtung besteht nicht, sofern eine gesetzliche Pflicht zur Speicherung der Daten besteht.

13. Sonstiges

a) Sollte das Eigentum des Auftraggebers oder die zu verarbeitenden personenbezogenen Daten beim Auftragnehmer durch Maßnahmen Dritter wie Pfändung oder Beschlagnahme, durch ein Insolvenzverfahren oder durch Vergleichbares gefährdet werden, hat der Auftragnehmer den Auftraggeber zu informieren.

b) Anlagen sind Bestandteil dieses Vertrages.

c) Änderungen oder Ergänzungen dieses Vertrages und seiner Anlagen bedürfen zu ihrer Wirksamkeit der Schriftform (§ 126 BGB). Dies gilt auch für die Änderung dieses Formerfordernisses selbst.

d) Für Streitigkeiten aus und im Zusammenhang mit diesem Vertrag gilt der Gerichtsstand, welcher in dem Hauptvertrag (vgl. Ziffer 1b) zwischen den Parteien bestimmt ist.

Anlagen:

Anlage 1: Technisch organisatorische Maßnahmen

....., den	Hilden, den ……
.....	.....
Auftraggeber (Kunde)	Auftragnehmer (Backens Systems GmbH)
(Name + Unterschrift + Stempel)	

Anlage 1 „technische und organisatorische Maßnahmen“ zum Vertrag über Auftragsverarbeitung

In Erfüllung der Verpflichtungen aus Ziffer 7 des Vertrages zur Auftragsverarbeitung sind folgende technischen und organisatorischen Maßnahmen getroffen:

Organisationskontrolle

Die innerbetriebliche Organisation ist so zu gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Folgende Maßnahmen bestehen:

- Schulung und Sensibilisierung der Mitarbeiter
- Regelungen von Verantwortlichkeiten
- Verschiedene Richtlinien für Mitarbeiter
- Einbruchmeldeanlage und Brandmeldeanlage
- Datenschutzbeauftragter extern

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu den Räumlichkeiten der Auftragnehmerin zu erhalten. Folgende Maßnahmen bestehen:

- Schließanlage mit Sicherungsschein und Gruppenschlüssel
- Schlüsselausgabelisten für Mitarbeiter
- Mietbereichseingangstür Bürotrakt: mit Zutrittskontrolle und Codeschlüssel gesichert, sind während der Bürozeit aber freigeschaltet
- Mietbereichseingangstür Techniktrakt: mit Zutrittskontrolle und Codeschlüssel gesichert, sind während Anwesenheitszeit von Technikern oder Kunden aber freigeschaltet
- Eingangstüre Technikraum: mit Zutrittskontrolle und Codeschlüssel gesichert, Türe mit Türschließer und Knauf ausgestattet
- Besucher werden an der Zugangstür abgeholt und in den Räumlichkeiten begleitet

Zugangskontrolle

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

- Zugang zu technischen Systemen und Anwendungen ist nur mit Benutzerkonto + Kennwort möglich
- Passwortrichtlinie
- Schutz vor Schadsoftware durch zentrale Firewall/Antiviren-Appliance
- Softwarepflege-Vertrag für zentrale Firewall/Antivieren-Appliance zur Sicherstellung der Aktualität
- Server im verschlossenen Serverschrank, zu welchem nur ein eingeschränkter Personenkreis Zugang hat; die Tür ist mit einem Schloss der Schließanlage gesichert

Zugriffs- und Speicherkontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung entsprechenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Folgende Maßnahmen bestehen:

- Zweckgebundenes Berechtigungskonzept nach dem Prinzip „need-to-do“
- Protokollierung von Änderungen
- Dokumentation der Benutzerprofile innerhalb des Datenverarbeitungssystems ES-Office
- Genehmigung von Benutzerkonten durch Geschäftsführung

Weitergabekontrolle

Maßnahmen, mit welchen gewährleitet werden kann, dass personenbezogene Daten bei der elektronischen Übertragung, während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft werden kann, an welchen Stellen eine Übermittelung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Plausibilitätsprüfungen innerhalb der DV-Systemen und DV-Anwendungen
- SSL-Verschlüsselung auf unserer Webseite
- Virensoftware über zentrale Security-Appliance
- VPN-Technologie über SSL-VPN und IPsec
- Verschlüsselung von externen Datenträgern
- Kontrollierte Vernichtung von Datenträgern durch Formatierung und anschließende mechanische Zerstörung

Übertragungskontrolle

Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welchen Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können. Folgende Maßnahmen bestehen:

- VPN-Technologie

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Folgende Maßnahmen bestehen:

- Protokollierung von Eingaben und Änderungen in ES-Office und Dokumentenmanagement
- Protokollierung von Änderungen in den internen Systemen
- Sperrung der Protokolle für die weitere Verarbeitung nur in Dokumentenmanagement-System

Auftragskontrolle

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

- Vertragliche Regelungen mit Subdienstleistern
- Vertrag zur Auftragsverarbeitung

Verfügbarkeitskontrolle und Wiederherstellbarkeit, Datenintegrität

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind sowie Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können und nicht durch Fehlfunktionen des Systems beschädigt werden können. Folgende Maßnahmen bestehen:

- Dreifaches Backup-Konzept
- Test der Wiederherstellbarkeit der Systeme
- aktueller Virenschutz auf allen betriebenen Systemen mithilfe zentraler Appliance
- redundante Systemsicherung auf gespiegelten Festplatten und 2x abgesetzte NAS-Systeme