AUFTRAGSDATENVERARBEITUNG BEI VOM KUNDEN BEAUFTRAGTEN LEISTUNGEN

der eurodata AG, Großblittersdorfer Str. 257-259, 66119 Saarbrücken (Stand: 07.09.2015)

Diese Vertragsbedingungen konkretisieren die datenschutzrechtlichen Rechte und Pflichten des Kunden (Auftraggeber - AG) und der eurodata (Auftragnehmer - AN) in Bezug auf die Auftragsdatenverarbeitung bzw. nach § 11 Abs. 5 des Bundesdatenschutzgesetzes (BDSG) gleich gestellte Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, wie sie dem Vertrag, der auf diese Anlage Bezug nimmt, zugrunde liegt.

I. FESTLEGUNGEN GEMÄß § 11 BDSG:

1. GEGENSTAND UND DAUER DES AUFTRAGS:

a) Gegenstand des Auftrags ist die Regelung der Datenverarbeitung im Auftrag im Rahmen der Erbringung von Leistungen nach dem Vertrag durch AN für AG als „verantwortliche Stelle“ i.S.v. § 3 Abs. 7 BDSG.

b) Er endet mit der Beendigung des Vertrages und Erfüllung der Pflichten nach Ziffer I.10.

2. UMFANG, ART UND ZWECK DER VORGESEHENEN ERHEBUNG, VERARBEITUNG ODER NUTZUNG VON DATEN, ART DER DATEN UND KREIS DER BETROFFENEN:

a) Der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen sind in dem Vertrag, der auf diese Anlage Bezug nimmt, und nachfolgend bestimmt.

b) Bei der Erbringung von Leistungen nach dem Vertrag im Auftrag des AG kann AN auch personenbezogene Daten verarbeiten, insbesondere von:

aa) Mitarbeitern (einschließlich Organen, Beschäftigten i.S.v. § 3 Abs. 11 BDSG und freien Mitarbeitern) des Kunden (wie Stammdaten (wie Name, Titel, Geburtsdatum, ferner Kommunikationsdaten wie Adressdaten, Telefon-, Fax-, E-Mail-Daten, außerdem Bankverbindungsdaten) sowie Abrechnungsdaten (einschließlich Zahlungsdaten) und Sozialversicherungs- und Steuerdaten) sowie ggf. von Angehörigen solcher Mitarbeiter;

bb) Lieferanten und Dienstleistern (z.B. Vermietern, Beratern, IT-Dienstleistern, Lizenzgebern, Handwerkern, Reinigungsfirmen) des Kunden und von deren Mitarbeitern (einschließlich Vertragsstamm-, Abrechnungs- und Steuerungsdaten);

cc) Kunden und Mitarbeitern von Kunden des Kunden (wie Vertragsstamm-, Abrechnungs- und Steuerungsdaten);

dd) Interessenten und Mitarbeitern von Interessenten des Kunden (einschließlich Stammdaten (wie Name, Titel, Anschrift, Geburtsdatum, Art und Umfang des Interesses));
ee) sonstigen Geschäftspartnern des Kunden und von deren Mitarbeitern (z.B. von Kammern, Versicherungen, Verbänden und Behörden).

3. NACH § 9 BDSG ZU TREFFENDEN TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN:

a) AN hält in seinem Verantwortungsbereich die vereinbarten technischen und organisatorischen Maßnahmen gemäß § 9 BDSG ein und hat seine innerbetriebliche Organisation gemäß datenschutzrechtlichen Anforderungen gestaltet.

b) Dies beinhaltet im Zeitpunkt des Abschlusses der Vereinbarung zur Auftragsdatenverarbeitung folgende Maßnahmen:

aa) Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (**Zutrittskontrolle**):

Der unbefugte Zutritt zu den Räumen, in denen die personenbezogenen Daten verarbeitet und aufbewahrt werden, wird verhindert. AN wird hierzu Sicherungsbereiche und den Kreis der zutrittsberechtigten Personengruppen (einschließlich Regelungen für den Umgang mit Erfüllungsgehilfen oder sonstigen Dritten) festlegen. Der Zutrittskontrolle zu den Geschäftsräumen des AN dient den Empfang als Eingangskontrolle. Außerdem werden die folgenden technischen Maßnahmen insbesondere auch zur Legitimation der Berechtigten getroffen: (i) Zutrittskontrollsystem unter Einsatz von Schlüsseln sowie Ausweisen (Magnet-/Chipkarte) und Ausweislesern, insbesondere für Serverräume; (ii) Regelung und Kontrolle der Vergabe von Schlüsseln, Ausweisen und Codes; (iii) Türsicherung (insbes. elektronische Türöffner); (iv) Schutz von Verkabelungsschränken vor Fremdzugriffen (z. B. mit Sicherheitsschlössern) (v) Gebäudesicherung und Überwachungseinrichtungen, insbesondere Alarmanlage (Alarmdeaktivierung mit Zwei-Faktor-Authentifizierung (z. B. Ausweisleser und PIN)) und optisch-elektronische Überwachung (z.B. Video-/Fernsehmonitor); (vi) Kontrolle und Protokollierung der Zutrittsvergabe (z.B. über eine Schlüssel- oder ID-Kartenliste); (vii) Aufbewahrung von Vergabe- und Anwesenheitsprotokollen für Serverräume.

bb) Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**):

Zugang zu den Datenverarbeitungssystemen erhalten ausschließlich berechtigte Personen. Das Eindringen Unbefugter in Datenverarbeitungssysteme wird verhindert durch technische Maßnahmen (z.B. Vergabe von Zugangsdaten (Passwortschutz)) und organisatorische Maßnahmen zur Benutzeridentifikation und Authentifizierung.

cc) Maßnahmen, um zu 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 (**Zugriffskontrolle**):

Jede unbefugte Nutzung von Datenverarbeitungssystemen ist durch AN zu verhindern, unabhängig davon, ob der Zugriff lokal oder per Fernzugriff erfolgt.

Der Zugriff wird administrativ mittels Benutzerauthentifizierung geregelt. Die Anmeldung erfolgt über ein individuelles Benutzerkonto mittels Benutzernamen und Passwort. Alle Kontoänderungsaktivitäten werden protokolliert (z.B. Anlegen eines Kontos, Ändern des Passwortes, Ändern von Gruppenmitgliedschaften, fehlerhafte Passworteingabe sowie Kontosperrungen und - entsperrungen).

Zugangsdaten für Nutzer, d.h. Nutzername und Passwort, sind an den individuellen Nutzer gebunden und dürfen nicht an Dritte weitergegeben werden. Der Zugriff auf das Produktivsystem erfordert zwingend eine VPNVerbindung (Kombination aus Zertifikat und Zwei-Faktor-Authentifizierung mit einer Gültigkeit von 60 Sekunden). Passwörter werden stets verschlüsselt gespeichert, ein ausgedrucktes Initialkennwort für neue Mitarbeiter muss bei der Erstanmeldung geändert werden. Passwörter sind mindestens acht Zeichen lang und werden nur akzeptiert, wenn sie Sonderzeichen und Ziffern enthalten. AN stellt sicher, dass Nutzer das Passwort spätestens nach 180 Tagen ändern. Bei Offenlegung oder Abhandenkommen eines Passwortes ist dieses umgehend zu ändern. AN belehrt die Nutzer über den datenschutzgerechten Umfang mit Zugangsdaten und Passwörtern.

Der Verhinderung unerlaubter Tätigkeiten in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen dient die bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung durch: (i) Differenzierte Berechtigung (insbesondere Rollen- und Rechtekonzept, Profile, Rollen, Transaktionen und Objekte); (ii) Protokollierung der Vergabe von Zugriffsberechtigungen über das Rollen- und Rechtekonzept (z.B. ID-Nummer oder Kontoname, Gruppenmitgliedschaften und deren Berechtigungen, sowie davon abweichende individuelle Berechtigungen); (iii) Protokollierung des Zugriffs auf personenbezogene Daten, z.B. in Bezug auf deren Kenntnisnahme, Veränderung und Löschung.

dd) Maßnahmen, um zu 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 (**Weitergabekontrolle**):

Die Aspekte der Weitergabe personenbezogener Daten werden durch Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträgern (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung geregelt: (i) Transportsicherung, z.B. zur Verhinderung des Zugriffs Unbefugter auf dem Transport- bzw. Übertragungsweg und während des Transport- bzw. Übertragungsvorgangs; (ii) Protokollierung, wer zu welchem Zeitpunkt welche Daten an wen weitergegeben hat (Nachvollziehbarkeit der Weitergabe von Daten); (iii) Einsatz elektronischer Signaturen, um das Verändern oder Löschen von personenbezogenen Daten zu erkennen; (iv) Verschlüs-

selung, z.B. Tunnelverbindung (Einsatz von dem Stand der Technik entsprechenden asymmetrischen oder hybriden Verschlüsselungstechniken).

ee) Maßnahmen, um zu gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**):

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege wird durch Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt bzw. gelöscht worden sind, gewährleistet.

ff) Maßnahmen, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen von AG verarbeitet werden können (**Auftragskontrolle**):

AN wählt den Unterauftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus und schließt Verträge, deren Inhalt den Anforderungen des § 11 BDSG genügt und den Anforderungen zu Datenschutz und Datensicherheit zwischen den Vertragsparteien dieses Vertrages entsprechen. In dem Vertrag mit dem jeweiligen Unterauftragnehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des AN und des Unterauftragnehmers deutlich voneinander abgegrenzt werden. Werden mehrere Unterauftragnehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Unterauftragnehmern. AN überzeugt sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Unterauftragnehmer getroffenen technischen und organisatorischen Maßnahmen. Das Ergebnis ist zu dokumentieren. Die weisungsgemäße Auftragsdatenverarbeitung wird durch technische und organisatorische Maßnahmen zur Abgrenzung der Kompetenzen des AG, des AN und des Unterauftragnehmers gewährleistet.

gg) Maßnahmen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**):

Die Daten werden gegen zufällige Zerstörung oder Verlust durch regelmäßige Sicherung geschützt. Personenbezogene Daten, die im Rechenzentrum des AN gespeichert werden, sind an zwei physikalisch unterschiedlichenOrten vorhanden. Insbesondere werden folgende Maßnahmen zur Datensicherung ergriffen: (i) Backup-Verfahren; (ii) Spiegeln von Festplatten (z.B. RAID-Verfahren); (iii) Unterbrechungsfreie Stromversorgung (USV) mit Notstromgeneratoren; (iv) Schutz gegen Schadsoftware (u.a. Viren); (v) Firewall; (vi) Klimatisierung der Serverräume durch eine n+1-redundante Auslegung der Klimaanlage, Temperaturkontrolle mittels Sensoren, Prüfung und Wartung der Klimaanlagen in regelmäßigen Abständen durch qualifiziertes Fachpersonal; (vii) Branderkennungs-, Brandmelde- und Löschanlage; (viii) Notfallplan, (ix) Datensicherungskonzept unter Verwendung separater Backup-Medien.

hh) Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (**Trennungskontrolle**):

Daten, die zu unterschiedlichen Zwecken erhoben werden, werden auch getrennt verarbeitet. Der getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken dienen die Zweckbindung und Funktionstrennung sowie die physische und logische Trennung von Daten.

c) AN kann, soweit technisch möglich und wirtschaftlich vertretbar, für Maßnahmen nach Ziffer I.3 b) bb) bis dd) dem Stand der Technik entsprechende Verschlüsselungsverfahren verwenden.

d) AN ist berechtigt, im Interesse von Datenschutz und Datensicherheit, insbesondere zur Gewährleistung der IT-Sicherheit, die Offenlegung von Sicherheitsvorkehrungen zu verweigern, soweit dies erforderlich ist, oder auf Kosten des AG deren Prüfung von einem berufsmäßig zur Verschwiegenheit verpflichteten Dritten vornehmen zu lassen, der gegenüber dem AG lediglich mitteilt, ob die jeweiligen technischen und organisatorischen Maßnahmen den gesetzlichen Anforderungen genügen oder nicht.

e) Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. AG ersetzt AN den durch die Anpassung der technischen und organisatorischen Maßnahmen nach § 9 BDSG an den technischen Fortschritt entstehenden Mehraufwand, soweit AG diese veranlasst hat.

4. BERICHTIGUNG, LÖSCHUNG UND SPERRUNG VON DATEN:

AN ist nach Maßgabe der gesetzlichen Bestimmungen sowie – soweit dem keine berechtigten Interessen des AN entgegenstehen – nach Weisung des AG im Rahmen des Vertrages zur Berichtigung, Löschung und Sperrung von personenbezogenen Daten verpflichtet. Aufgrund der Verantwortlichkeit von AG kann AG unter diesen Voraussetzungen insbesondere jederzeit die Berichtigung, Löschung oder Sperrung der personenbezogenen Daten verlangen. AG trägt die Verantwortung für das Löschen personenbezogener Daten, wenn deren Speicherung unzulässig ist oder ein sonstiger Fall einer Löschungspflicht vorliegt. AN kann im Rahmen seines Leistungsangebots bereits bei Auftragserteilung eine Regelfrist für die Datenlöschung vorgeben. Entstehen dem AN Kosten durch die Berichtigung, Löschung und Sperrung von Daten von AG, so zahlt AG 5,- EUR zzgl. USt. je Berichtigung, Löschung oder Sperrung, soweit diese Kosten nicht bereits mit dem Vertrag abgegolten sind. Für die Vernichtung, Löschung oder Sperrung von Auftragsdaten zum oder nach Vertragsende gilt Ziffer I.10.

5. NACH § 11 ABS. 4 BDSG BESTEHENDE PFLICHTEN DES AN, INSBESONDERE DIE VON IHM VORZUNEHMENDEN KONTROLLEN:

AN erfüllt die Pflichten nach § 11 Abs. 4 BDSG, insbesondere die sich für ihn aus §§ 4f, 4g, 5, 38 BDSG ergebenden Pflichten. AN stellt sicher, dass die mit der Verarbeitung der vom AG weitergegebenen personenbezogenen Daten befassten Mitarbeiter gemäß § 5 BDSG (Datengeheimnis) verpflichtet und in die Schutzbestimmungen des BDSG eingewiesen worden sind. AN setzt für die Verarbeitung der personenbezogenen Daten nur solche Mitarbeiter ein, die gemäß § 5 BDSG auf das Datengeheimnis verpflichtet worden sind. AG bleibt zur Führung des öffentlichen Verfahrensverzeichnisses gemäß § 4g Abs. 2 Satz 2 BDSG verpflichtet; AN stellt AG die für die Übersicht nach § 4g Abs.2 Satz 1 BDSG notwendigen Angaben gegen Kostenerstattung zur Verfügung; AG ist verpflichtet, den AN über etwaige Mängel unverzüglich und vollständig zu unterrichten. AN wird der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte nach Maßgabe von § 38 Abs. 3 BDSG unverzüglich erteilen; die Kosten trägt AG.

6. BERECHTIGUNG ZUR BEGRÜNDUNG VON UNTERAUFTRAGSVERHÄLTNISSEN:

a) AG ist damit einverstanden, dass AN zur Erfüllung seiner vertraglichen Leistungen jeweils verbundenen Unternehmen (§ 15 AktG) und Dritten Unteraufträge erteilt.

b) AG ist berechtigt, dieses Einverständnis in Bezug auf einen Unterauftragnehmer aus wichtigem Grund zu widerrufen.

c) Die Auftragskontrolle richtet sich nach Ziffer I.3 b) ff).

d) AG ist zur Kontrolle und Überprüfung der Unterauftragnehmer entsprechend Ziffer I.7 berechtigt.

e) AN erteilt AG auf dessen schriftliche Aufforderung hin gegen Kostenerstattung Auskunft über Name bzw. Firmierung und Anschrift des jeweiligen Unterauftragnehmers sowie den wesentlichen Vertragsinhalt (Leistungen ausschließlich Preise) und die Umsetzung der datenschutzrelevanten Pflichten durch den jeweiligen Unterauftragnehmer.

f) Die Weiterleitung oder Zugänglichmachung von personenbezogenen Daten an bzw. für den jeweiligen Unterauftragnehmer ist erst zulässig, wenn der Unterauftragnehmer die Verpflichtungen nach § 11 BDSG erfüllt hat.

7. KONTROLLRECHTE DES AG UND ENTSPRECHENDE DULDUNGS- UND MITWIRKUNGSPFLICHTEN DES AN:

AN ermöglicht AG, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim AN getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. AN ist verpflichtet, die Kontrollen des AG nach diesem Vertrag zu dulden und Mitwirkungsleistungen zu erbringen, soweit für die Kontrolle des AG nach diesem Vertrag erforderlich, und dem AG auf schriftliche Anforderung innerhalb angemessener Frist Auskünfte zu geben, die zur Durchführung der Kontrolle erforderlich sind. Sollte es im Ausnahmefall erforderlich sein, kann sich AG nach rechtzeitiger schriftlicher Anmeldung während der üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs in den Betriebsstätten des AN von der Einhaltung der getroffenen technischen und organisatorischen Maßnahme persönlich überzeugen. AG wird das Ergebnis seiner Prüfung dokumentieren. AG erstattet AN die durch Kontrollen und Auskünfte nach Ziffer I.7 entstehenden Kosten.

8. MITZUTEILENDE VERSTÖßE DES AN ODER DER BEI IHM BESCHÄFTIGTEN PERSONEN GEGEN VORSCHRIFTEN ZUM SCHUTZ PERSONENBEZOGENER DATEN ODER GEGEN DIE IM AUFTRAG GETROFFENEN FESTLEGUNGEN:

AN unterrichtet AG innerhalb angemessener Frist bei Verstößen des AN oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen, auch bei schwerwiegenden Störungen des Betriebsablaufes oder bei Verdacht auf schwerwiegende Datenschutzverletzungen i.S.v. §§ 42a BDSG, 15a TMG (z.B. unter den gesetzlichen Voraussetzungen bei Fehlversendungen, verlorengegangenen Datenträgern, unterschlagenen Daten, Datenhacking oder Zugangsberechtigungs-/Passwort-Offenlegungen).

9. UMFANG DER WEISUNGSBEFUGNISSE, DIE SICH AG GEGENÜBER AN VORBEHÄLT:

a) AG ist im Rahmen des Vertrages zur Erteilung von Weisungen an AN berechtigt. AG und AN teilen sich wechselseitig rechtzeitig, spätestens jedoch vor Erteilung der ersten Weisung durch AG, die jeweils weisungsberechtigten Personen und deren Vertreter mit. Bei einem Wechsel oder einer längerfristigen Verhinderung der jeweiligen Person ist der jeweils anderen Vertragspartei unverzüglich deren Nachfolger bzw. deren Vertreter mitzuteilen.

b) Der Umfang der Weisungsbefugnis ist auf die Erhebung, Verarbeitung und Nutzung personenbezogener Daten beschränkt. Sie umfasst insbesondere nicht technische bedingte Verarbeitungen oder technische und organisatorische Einzelmaßnahmen, soweit deren Zweck auch auf andere Weise erreicht werden kann.

c) AN erhebt, verarbeitet und nutzt Daten im Rahmen des Vertrages und der Weisungen von AG. Weisung ist die auf einen bestimmten datenschutzrelevanten Umgang des AN mit personenbezogenen Daten gerichtete schriftliche Anordnung des AG. Weisungen bedürfen zu ihrer Wirksamkeit der Schriftform, es sei denn, es besteht Gefahr im Verzug oder die Umsetzung der Weisung duldet aus anderen Gründen keinen Aufschub. In diesen Fällen hat AG dem AN die Weisung unaufgefordert unverzüglich schriftlich zu bestätigen.

d) Ist AN der Ansicht, dass eine Weisung des AG gegen Vorschriften über den Datenschutz verstößt, hat er AG unverzüglich darauf hinzuweisen.

e) Erteilt AG Einzelweisungen, die über den Vertrag, die Anforderungen des BDSG oder über die Anforderungen von anderen datenschutzrechtlichen Gesetzen hinausgehen, trägt AG sämtliche dem AN dadurch verursachten Kosten.

f) Ist AG aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird AN den AG dabei unterstützen, diese Informationen bereit zu stellen, vorausgesetzt AG hat AN hierzu schriftlich aufgefordert und AG erstattet AN die durch diese Unterstützung entstehenden Kosten.

g) AG erfüllt die Informationspflichten gemäß § 42a BDSG und § 15a TMG.

10. RÜCKGABE ÜBERLASSENER DATENTRÄGER UND LÖSCHUNG BEIM AN GESPEICHERTER DATEN NACH BEENDIGUNG DES AUFTRAGS:

a) Vorbehaltlich abweichender Weisungen oder Vereinbarungen und vorbehaltlich gesetzlicher oder satzungsmäßiger Pflichten ist AN nach Vertragsende verpflichtet, ihm überlassene Datenträger wahlweise unverzüglich dem AG zurück zu geben oder diese zu vernichten und ihm in Zusammenhang mit dem Auftrag überlassene und noch nicht gelöschte personenbezogene Daten datenschutzgerecht zu löschen. Über die Herausgabe oder Löschung nach Vertragsende muss AG innerhalb einer vom AN gesetzten angemessenen Frist entscheiden. Wenn AG nicht innerhalb angemessener Frist entscheidet, ist AN berechtigt, nach seiner Wahl die Rückgabe oder Löschung gemäß Satz 1 vorzunehmen.

b) Wenn AN zu vernichtende Unterlagen oder Datenträger mit personenbezogenen Daten dem AG nicht zurückgibt, so ist AN verpflichtet, die Unterlagen oder Datenträger datenschutzrechtsgerecht zu entsorgen.

c) Zur Vernichtung von personenbezogenen Daten, die sich auf Datenträgern befinden, genügt deren physikalische Zerstörung (Schreddern).

d) Zur Löschung von personenbezogenen Daten, die sich auf Festplatten, USB-Sticks und anderen wiederbeschreibbaren Datenträgern befinden, genügt es, diese Datenträger im jeweils erforderlichen Umfang mehrfach mit Nullen und Zufallszahlen zu überschreiben. Nicht geeignet sind das Löschen mittels der Delete-Funktion, das Verschieben der Datei mit den Daten in den Papierkorb oder das Umbenennen der Datei mit den personenbezogenen Daten.

e) Soweit und solange AN personenbezogene Daten aufgrund technisch und organisatorisch sachdienlicher routinemäßiger Datensicherungen elektronisch speichert (z.B. als temporäre Datensicherung oder als Backup), ist AN berechtigt, anstelle einer Löschung der personenbezogenen Daten den Zugriff auf die personenbezogenen Daten zu sperren. Die Vereinbarung zur Auftragsdatenverarbeitung gilt in Bezug auf die elektronische Speicherung dieser personenbezogenen Daten solange fort, bis die personenbezogenen Daten gelöscht sind.

f) Auf Verlangen des AG, welches zu seiner Wirksamkeit der Schriftform bedarf, bestätigt AN dem AG die jeweilige Entsorgung oder Vernichtung von Unterlagen oder Datenträgern oder die Löschung, auf Verlangen auch unter Angabe des Datums, in Textform.

g) Entstehen dem AN mit oder nach Vertragsbeendigung Kosten durch die Herausgabe, Entsorgung, Vernichtung, Löschung oder Sperrung der Daten des AG, so trägt diese Kosten der AG (5,- EUR zzgl. USt. je Auftrag).

II. ERHEBUNG, VERARBEITUNG UND NUTZUNG PERSONENBEZOGENER DATEN IM AUFTRAG VON AG AUßERHALB DES EWR:

Die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten findet - soweit von AN nicht anders angezeigt - ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

Damit AG Dritte in anderen als den unter Ziffer II. Satz 1 genannten Gebieten („Drittländer“) mit der Erhebung, Verarbeitung oder Nutzung von Daten im Zusammenhang mit der Erbringung von Leistungen nach dem Vertrag zwischen AG und AN beauftragen kann, bevollmächtigt AG hiermit AN, Vereinbarungen nach Maßgabe der EU-Standardvertragsklau-seln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG (veröffentlicht im Amtsblatt der Europäischen Union L 39, vom 12.02.2010, S. 10 ff.) in Vertretung - d.h. im Namen und in Vollmacht - für AG abzuschließen. AG erteilt AN auf dessen Aufforderung hin unverzüglich eine Vollmachtsurkunde. AN erteilt AG auf dessen schriftliche Aufforderung hin gegen Kostenerstattung Auskunft über diese Drittlandverträge. Die Drittlandverträge gelten mit folgender Maßgabe auch für AN, der diesen insoweit beitritt. Da AG als Datenexporteur einen Vertrag, der auf diese Anlage Bezug nimmt, mit AN geschlossen hat (als Auftragsdatenverarbeitung i.S.v. § 11 BDSG bzw. i.S.v. Art. 2e, 17 Abs. 3 der Richtlinie 95/46/EG und den hierzu erlassenen nationalen Vorschriften) und die Datenimporteure als Drittlandsubunternehmer für AN fungieren, ist AN gegenüber AG primär verantwortlich, dass die Drittlandsubunternehmer die Pflichten gemäß den EU-Standardvertragsklauseln erfüllen. AN hat zu diesem Zweck entsprechende abgeleitete Kontrollpflichten gegenüber den Drittlandsubunternehmern und kann hierfür die in den Drittlandverträgen beschriebenen Kontrollbefugnisse des AG wahrnehmen. AG bleibt verpflichtet, die Ausübung der Kontrollbefugnisse zu überwachen, und kann jederzeit auch selbst diese Kontrolle gegenüber den Drittlandsubunternehmern ausüben.