VERTRAG ZUR VERARBEITUNG PERSONENBEZOGENER DATEN IM AUFTRAG

zwischen

Name
und Adresse
des Kunden

(„Auftraggeber“/„Verantwortlicher“)

und

Emarsys Interactive Services GmbH
Stralauer Platz 34
10243 Berlin
Deutschland
(„Auftragnehmer“/„Auftragsverarbeiter“)

1. PRÄAMBEL

Der Auftragnehmer erbringt gegenüber dem Auftraggeber im Rahmen eines gesonderten Vertrages und/oder auf Grundlage gesonderter Einzelaufträge (im Folgenden insgesamt als „**Hauptvertrag**“ bezeichnet) verschiedene Marketing-Dienstleistungen, insbesondere im Zusammenhang mit der Planung, Durchführung und Analyse von E-Mail-Kommunikation (im Folgenden insgesamt als „**Leistungen**“ bezeichnet). Die Leistungen sind im Hauptvertrag und den jeweiligen Leistungsbeschreibungen näher beschrieben.

2. GEGENSTAND

2.1. Verarbeitung personenbezogener Daten

Diese Vereinbarung („**Vertrag**“) regelt die Verarbeitung der personenbezogenen Daten, die der Auftragnehmer im Rahmen der Erbringung der Leistungen für den Auftraggeber verarbeitet („**Daten**“). Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Die Daten umfassen insbesondere die Namen, E-Mail-Adressen und Interessengebiete der Empfänger von E-Mail-Newslettern des Auftraggebers; weitere Einzelheiten zur Art der personenbezogenen Daten und den Kategorien betroffener Personen sind im Hauptvertrag und den jeweiligen Leistungsbeschreibungen geregelt.

2.2. Inhalt der Auftragsverarbeitung

Gegenstand, Dauer, Art und Zweck der Verarbeitung der Daten ergeben sich aus dem Hauptvertrag und den jeweiligen Leistungsbeschreibungen.

3. PFLICHTEN DES AUFTRAGGEBERS (VERANTWORTLICHER)

3.1. Auftraggeber als Verantwortlicher

Der Auftraggeber bleibt für die Daten der alleinige Verantwortliche im Sinne des Datenschutzrechts und ist für die Rechtmäßigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der betroffenen Personen verantwortlich. Soweit erforderlich, hat der Auftraggeber die betroffenen Personen über die Verarbeitung ihrer Daten zu informieren oder deren Einwilligung einzuholen.

3.2. Weisungen

Soweit die Datenverarbeitung durch den Auftragnehmer im Rahmen einer dem Auftraggeber zur Online-Nutzung zur Verfügung gestellten Standard-Software erfolgt, übt der Auftraggeber sein Weisungsrecht (siehe Ziffer 4.1) in der Regel durch die eigene Benutzung der Online-Schnittstelle dieser Software aus. Im Übrigen sind Weisungen des Auftraggebers entweder über die dem Auftraggeber vom Auftragnehmer zur Verfügung gestellte Web-Oberfläche oder in Textform zu erteilen; mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Dem Auftraggeber bleiben solche Weisungen jederzeit vorbehalten. Geht der Inhalt von Weisungen des Auftraggebers über dasjenige hinaus, was der Auftragnehmer dem Auftraggeber nach dem Hauptvertrag schuldet, hat der Auftraggeber die entsprechenden Leistungen gesondert zu beauftragen und zu vergüten.

3.3. Meldepflicht

Gelangen im Verantwortungsbereich des Auftraggebers die vom Auftragnehmer gemäß dieser Vereinbarung verarbeiteten Daten des Auftraggebers ungeplant zur Kenntnis eines unbefugten Dritten, informiert der Auftraggeber den Auftragnehmer hierüber rechtzeitig, sodass der Auftragnehmer notwendige technische und organisatorische Maßnahmen auf seiner Seite vornehmen kann.

3.4. Pflicht zur Freistellung

Machen Dritte (einschließlich staatlicher Stellen) gegenüber dem Auftragnehmer Ansprüche bzw. Rechtsverletzungen geltend, die darauf beruhen, dass der Auftraggeber gegen seine Pflichten verstoßen hat, so gilt Folgendes: Der Auftraggeber wird den Auftragnehmer von diesen Ansprüchen freistellen, dem Auftragnehmer bei der Rechtsverteidigung angemessene Unterstützung bieten und den Auftragnehmer von den angemessenen Kosten der Rechtsverteidigung freistellen. Voraussetzung für diese Freistellungspflicht ist, dass der Auftragnehmer den Auftraggeber über geltend gemachte Ansprüche unverzüglich in Textform informiert, keine Anerkenntnisse oder gleichkommende Erklärungen abgibt und es dem Auftraggeber ermöglicht, auf Kosten des Auftraggebers – soweit verfahrensrechtlich möglich – alle gerichtlichen und außergerichtlichen Verhandlungen über die Ansprüche zu führen.

4. PFLICHTEN DES AUFTRAGNEHMERS (AUFTRAGSVERARBEITER)

4.1. Weisungsgebundenheit

Der Auftragnehmer verarbeitet die Daten ausschließlich im Rahmen und zum Zwecke der Erbringung der Leistungen für den Auftraggeber und nach dessen dokumentierten Weisungen. Der Auftragnehmer verarbeitet die personenbezogenen Daten auf keine andere Weise und für keine anderen Zwecke, sofern er nicht durch das Recht der EU oder der EU-Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist; 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.

4.2. Hinweispflicht

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen anwendbare Vorschriften über den Datenschutz verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Eine Pflicht zur rechtlichen Prüfung von Weisungen besteht für den Auftragnehmer nicht.

4.3. Unterstützungspflicht

Sofern der Auftraggeber seinen Pflichten gegenüber den betroffenen Personen (insbesondere der Pflicht, einer betroffenen Person Auskunft über die Verarbeitung ihrer personenbezogenen Daten zu geben) nur mit Hilfe des Auftragnehmers erfüllen kann, wird der Auftragnehmer den Auftraggeber hierbei auf dessen Anforderung angemessen unterstützen. Der Auftragnehmer

Initialen des Kunden

leitet im Fall der Geltendmachung von Betroffenenrechten ihm gegenüber diese Anträge an den Auftraggeber weiter. Ebenso unterstützt der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Auftraggeber auf Anforderung bei der Einhaltung von dessen Verpflichtungen hinsichtlich der Sicherheit personenbezogener Daten (Sicherheit der Verarbeitung, Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person) sowie einer ggf. erforderlichen Datenschutz-Folgenabschätzung und vorherigen Konsultationen. Den entstehenden und über das gesetzlich geforderte Ausmaß hinausgehenden Aufwand hat der Auftraggeber gesondert zu beauftragen und zu vergüten.

4.4. Berichtigung, Löschung und Sperrung

Sind personenbezogene Daten zu berichtigen, zu löschen oder zu sperren, nimmt dies der Auftraggeber durch Nutzung der entsprechenden Funktionen der bereitgestellten Software selbst vor. Ist dies nicht möglich, übernimmt der Auftragnehmer die Berichtigung, Löschung oder Sperrung nach den Weisungen des Auftraggebers. Für die Löschung der Daten am Ende der Vertragslaufzeit gilt Ziffer 7.2.

4.5. Ort der Datenverarbeitung

Die Verarbeitung der Daten findet ausschließlich im Gebiet der Europäischen Union (EU) und/oder in Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt, sofern der Auftraggeber dem Auftragnehmer nicht in diesem Vertrag oder in sonstiger dokumentierter Weise eine Verarbeitung in einem Land außerhalb der EU und des EWR gestattet.

4.6. Datenschutzbeauftragter

Der Auftragnehmer hat einen Datenschutzbeauftragter zu bestellen. Auf Anforderung teilt der Auftragnehmer dem Auftraggeber die Kontaktdaten seines Datenschutzbeauftragten mit.

4.7. Datengeheimnis

Der Auftragnehmer wird seine Beschäftigten, die mit der Verarbeitung personenbezogener Daten betraut sind, mit den maßgebenden Bestimmungen des Datenschutzes vertraut machen und sie schriftlich zur Vertraulichkeit und auf das Datengeheimnis verpflichten. Insbesondere gilt diese Verschwiegenheitspflicht der mit der Verarbeitung der Daten betrauten Personen auch für die Daten von juristischen Personen oder Personenvereinigungen und bleibt auch nach der Beendigung ihrer Tätigkeit für den Auftragnehmer bestehen.

4.8. Meldepflicht

Gelangen die Daten des Auftraggebers unrechtmäßig, d.h. unter Verstoß gegen anwendbares Datenschutzrecht, diesen Vertrag oder Weisungen des Auftraggebers, zur Kenntnis eines unbefugten Dritten, informiert der Auftragnehmer den Auftraggeber hierüber unverzüglich.

4.9. Technische und organisatorische Maßnahmen

Unter Berücksichtigung des Stands 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 trifft der Auftragnehmer alle erforderlichen technischen und organisatorischen Maßnahmen, die geeignet sind, ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Der Auftragnehmer trifft in seinem Verantwortungsbereich insbesondere die in der Anlage 1 zu diesem Vertrag genannten technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. Ebenso unternimmt der Auftragnehmer Schritte, um sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Auftraggebers verarbeiten, es sei denn, sie sind nach dem Recht der EU oder der EU-Mitgliedstaaten zur Verarbeitung verpflichtet.

4.10. Versicherung

Der Auftragnehmer verpflichtet sich, während der Laufzeit dieser Vereinbarung angemessenen Versicherungsschutz für eventuelle Haftpflichtschäden aus oder im Zusammenhang mit dieser Vereinbarung vorzuhalten.

4.11. Pflicht zur Freistellung

Machen Dritte (einschließlich staatlicher Stellen) gegenüber dem Auftraggeber Ansprüche bzw. Rechtsverletzungen geltend, die darauf beruhen, dass der Auftragnehmer gegen seine Pflichten verstoßen hat, so gilt Folgendes: Der Auftragnehmer wird den Auftraggeber von diesen Ansprüchen freistellen, dem Auftraggeber bei der Rechtsverteidigung angemessene Unterstützung bieten und den Auftraggeber von den angemessenen Kosten der Rechtsverteidigung freistellen. Voraussetzung für diese Freistellungspflicht ist, dass der Auftraggeber den Auftragnehmer über geltend gemachte Ansprüche unverzüglich in Textform informiert, keine Anerkenntnisse oder gleichkommende Erklärungen abgibt und es dem Auftragnehmer ermöglicht, auf Kosten des Auftragnehmer – soweit verfahrensrechtlich möglich – alle gerichtlichen und außergerichtlichen Verhandlungen über die Ansprüche zu führen.

5. KONTROLLRECHTE DES AUFTRAGGEBERS

5.1. Zertifizierung

Der Auftragnehmer verpflichtet sich, während der Laufzeit dieser Vereinbarung ein nach ISO 27001 zertifiziertes Information Security Management System zu verwenden und dies dem Auftraggeber auf Anforderung nachzuweisen.

5.2. Kontrollen

Der Auftraggeber ist berechtigt, die Einhaltung a) der gesetzlichen Vorschriften über den Datenschutz, b) der vertraglichen Vereinbarungen der Parteien und c) der Weisungen des Auftraggebers im erforderlichen Umfang beim Auftragnehmer zu kontrollieren oder durch einen vom Auftraggeber beauftragten Prüfer kontrollieren zu lassen. Der Auftragnehmer wird zu solchen Kontrollen beitragen und alle erforderlichen Informationen zum Nachweis der Einhaltung zur Verfügung stellen. Kontrollen in den Betriebsstätten des Auftragnehmers muss der Auftraggeber mindestens zwei Wochen vorher schriftlich ankündigen. Kontrollen sind zu den üblichen Geschäftszeiten und ohne wesentliche Beeinträchtigung des Geschäftsbetriebs des Auftragnehmers durchzuführen. Jede Partei trägt ihre eigenen, im Rahmen von Kontrollen entstehenden Kosten.

5.3. Schutzwürdige Interessen des Auftragnehmers

Soweit durch Kontrollen Betriebs- und Geschäftsgeheimnisse des Auftragnehmers offenbart oder geistiges Eigentum des Auftragnehmers gefährdet werden kann, hat der Auftraggeber die Kontrollen auf eigene Kosten durch einen fachkundigen und unabhängigen Dritten vornehmen zu lassen, der sich gegenüber dem Auftragnehmer zur Verschwiegenheit verpflichtet.

6. UNTERAUFTRAGSVERHÄLTNISSE

6.1. Einschaltung von Subunternehmern

Der Auftragnehmer darf Subunternehmer zur Verarbeitung der Daten einschalten, wenn der Auftragnehmer mit dem Subunternehmer einen schriftlichen oder elektronischen Vertrag über die Verarbeitung von Daten im Auftrag schließt, dessen Schutzniveau mindestens demjenigen dieses Vertrages entspricht, und der Auftraggeber der Einschaltung des Subunternehmers vorher schriftlich oder elektronisch zustimmt. Der Auftragnehmer informiert den Auftraggeber schriftlich oder elektronisch über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Die Zustimmung des Auftraggebers gilt als erteilt, wenn der Auftraggeber nicht innerhalb eines Monats nach Erhalt dieser Information schriftlich oder elektronisch widerspricht.

6.2. Genehmigte Subunternehmer

Der Auftraggeber stimmt hiermit der Einschaltung der in der Anlage 2 genannten Subunternehmer zu.

6.3. Haftung für Subunternehmer

Kommt ein Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Subunternehmers.

7. LAUFZEIT

7.1. Laufzeit

Die Laufzeit dieses Vertrages entspricht der Laufzeit des Hauptvertrages zuzüglich weiterer 30 Tage. Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt.

7.2. Daten bei Vertragsende

Nach Ablauf von 30 Tagen nach dem Ende des Hauptvertrags wird der Auftragnehmer die Daten des Auftraggebers von seinen Datenträgern löschen und entsprechende Unterlagen bei sich vernichten, sofern der Auftragnehmer nicht gesetzlich zur weiteren Aufbewahrung verpflichtet ist. Der Auftraggeber ist selbst dafür verantwortlich, Daten rechtzeitig vor Ablauf dieser Frist zu exportieren und zur weiteren eigenen Verwendung zu sichern. Eine Herausgabe oder ein Export von Daten, der nicht über die im Rahmen der Leistungen enthaltenen Standardfunktionen möglich ist (z.B. Download von Dateien), hat der Auftraggeber rechtzeitig gesondert zu beauftragen und zu vergüten.

7.3. Sicherungskopien

Die vorstehenden Löschungspflichten gelten nicht für Datenkopien, die in regelmäßig erstellten Sicherungskopien von umfassenden Datenbeständen des Auftragnehmers enthalten sind, deren isolierte Löschung für den Auftragnehmer einen erheblichen Aufwand bedeuten würde und die im Rahmen des vom Auftragnehmer angewandten Sicherungs-Zyklus spätestens nach 14 Tagen automatisch gelöscht oder ersetzt werden. Die Wiederherstellung und jede sonstige Nutzung solcher Kopien bis zu ihrer automatischen Löschung bzw. Überschreibung ist nach Vertragsbeendigung unzulässig. Der Auftraggeber kann vom Auftragnehmer auch die sofortige Löschung solcher Sicherungskopien verlangen, wenn der Auftraggeber dem Auftragnehmer die hierdurch verursachten angemessenen Kosten erstattet; dies umfasst auch eine Aufwandsentschädigung für die Arbeitszeit des vom Auftragnehmer beanspruchten Personals.

8. SCHLUSSBESTIMMUNGEN

8.1. Anwendbares Recht

Soweit sich nicht aus dem Hauptvertrag eine andere Rechtswahl ergibt, findet auf diesen Vertrag ausschließlich deutsches Recht Anwendung (ohne eventuelle

Verweisungen auf andere Rechtsordnungen und unter Ausschluss des UN Kaufrechts).

8.2. Gerichtsstand

Soweit sich nicht aus dem Hauptvertrag ein anderer Gerichtsstand ergibt, ist ausschließlicher Gerichtsstand für Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag Berlin, Deutschland.

8.3. Teilunwirksamkeit

Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden, so wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Statt der unwirksamen Bestimmung gilt dasjenige, was die Parteien nach dem ursprünglich angestrebten Zweck unter wirtschaftlicher Betrachtungsweise redlicherweise vereinbart hätten. Das Gleiche gilt im Falle einer Vertragslücke.

Auftraggeber / Verantwortlicher:		**Auftragnehmer / Auftragsverarbeiter:**	**Emarsys Interactive Services GmbH**
Unterschrift:		**Unterschrift:**	
Name:		**Name:**	Holger Behnsen
Position/Funktion:		**Position/Funktion:**	General Manager
Ort, Datum:		**Ort, Datum:**	Wien, 7. Mai 2018

Initialen des Kunden

ANLAGE 1: TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER VERARBEITUNG

1. PSEUDONYMISIERUNG UND VERSCHLÜSSELUNG PERSONENBEZOGENER DATEN

Maßnahmen, um eine unzulässige Verarbeitung personenbezogener Daten allgemein zu verhindern:

- Personenbezogene Daten werden verschlüsselt übermittelt.
- Soweit zumutbar und möglich (ohne das Erbringen der vereinbarten Leistungen zu verhindern) werden personenbezogene Daten durch Hashen oder Verweis auf eine Datenbank, wo personenebezogene Daten gespeichert sind, anonymisiert und/oder pseudonymisiert.

2. FÄHIGKEIT, DIE VERTRAULICHKEIT, INTEGRITÄT, VERFÜGBARKEIT UND BELASTBARKEIT DER SYSTEME UND DIENSTE IM ZUSAMMENHANG MIT DER VERARBEITUNG AUF DAUER SICHERZUSTELLEN

ZUTRITTSKONTROLLE

Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

- Realisierung des Zutrittschutzes:
  - Der zu schützende Bereich ist durch eine geeignete Bauweise abgesichert.
  - Alle möglichen Zugänge wurden gegen unbefugten Zugang gesichert.
  - Es besteht eine für alle verbindliche Zugangs-Authentisierung (Schlüssel oder Chipkarte).
  - Es ist ein Zutrittskontrollsystem eingerichtet.
- Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen:
  - Es gibt organisatorische Regelungen über Zutrittsberechtigungen zum Geschäftsbereich.
  - Es gibt eine Dokumentation über die Vergabe der Schlüssel.
- Begleitung von Besuchern und Fremdpersonal:
  - Es existieren Richtlinien für die Überwachung von Besuchern und Fremdpersonal (Begleitung, Besucherausweis, Protokollierung etc.).
  - Es existieren Regelungen für die Überwachung von Wartungspersonal (Begleitung, vorhergehende Anmeldung, Prüfung der Identität etc.).

ZUGANGSKONTROLLE

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (einschließlich Verschlüsselungsverfahren):

- Zugangsschutz (Authentisierung):
  - Es besteht Zugangsschutz zu allen Datenverarbeitungssystemen durch Benutzer-Authentisierung.
  - Die Umsetzung der Maßnahmen zum Zugangsschutz wird kontrolliert.
  - Es wird ein Passwort-Generator für Zufalls-Passwörter genutzt.
- Gesicherte Übertragung von Authentisierungs-Geheimnissen (Credentials) im Netzwerk:
  - Die Übertragung der Authentisierungs-Geheimnisse über das Netz erfolgt verschlüsselt.
- Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen:
  - Es existiert ein sicheres Verfahren zur Rücksetzung nach Zugangssperren, z.B. Neuvergabe einer Nutzerkennung.
- Verbot der lokalen Speicherung für Passworte und/oder Formulareingaben:
  - Zugriffspasswörter und/oder Formulareingaben werden nicht auf dem Client selbst oder in seiner Umgebung abgelegt (z.B. Speicherung im Browser oder Haftnotizen).
  - Die Nutzer werden über diese Vorgaben belehrt.
- Festlegung befugter Personen:
  - Es existiert ein Rollenkonzept (vordefinierte Benutzerprofile).
  - Zugangsberechtigungen werden immer individuell (personengebunden) vergeben.
  - Der Kreis der befugten Personen ist auf das betriebsnötige Minimum reduziert.
- Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen:
  - Ein Prozess zur Beantragung, Genehmigung, Vergabe und Rücknahme von Authentifizierungsmedien und Zugangsberechtigungen ist eingerichtet, beschrieben und wird angewendet.
  - Für die Vergabe von Zugangsberechtigungen ist eine verantwortliche Person benannt.
  - Es existiert eine Vertretungsregelung.
- Automatische Zugangssperre:
  - Bei mehr als 30 Minuten Inaktivität einer Arbeitsstation bzw. eines Terminals wird ein kennwortgeschützter Bildschirmschoner mit Hilfe der betriebssystemeigenen Mechanismen automatisch aktiviert.
- Manuelle Zugangssperre:
  - Es existiert eine Richtlinie, Arbeitsstationen und Terminals bei vorübergehendem Verlassen des Arbeitsplatzes gegen unbefugte Nutzung zu schützen, z.B. durch automatische oder manuelle Aktivierung des kennwortgeschützten Bildschirmschoners
  - Die Mitarbeiter werden hinsichtlich der Notwendigkeit der Umsetzung dieser Maßnahmen geschult.

ZUGRIFFSKONTROLLE

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 (einschließlich Verschlüsselungsverfahren):

- Berechtigungskonzept/Umsetzung von Zugriffsbeschränkungen:
  - Es gibt Regelungen zum Anlegen, Ändern und Löschen von Berechtigungsprofilen.
  - Jeder Zugangsberechtigte kann nur auf die Daten zugreifen, die er zur auftragsgemäßen Bearbeitung des jeweils aktuellen Vorgangs konkret benötigt und die in dem individuellen Berechtigungsprofil eingerichtet sind.
  - Soweit Datenbestände mehrerer Auftraggeber in einer Datenbank gespeichert sind oder mit einer Datenverarbeitungsanlage verarbeitet werden, ist eine logische Zugriffsbeschränkung implementiert, die ausschließlich auf die Datenverarbeitung für den jeweiligen Auftraggeber ausgerichtet ist (Mandantenfähigkeit).
- Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen:
  - Ein Prozess zur Beantragung, Genehmigung, Vergabe und Rücknahme von Zugriffsberechtigungen ist implementiert.
  - Berechtigungen sind an eine persönliche Benutzerkennung und an einen Account geknüpft.
  - Entfällt die Grundlage für eine Berechtigung (z.B. durch Funktionsänderung), wird diese sofort entzogen.
- Protokollierung des Datenzugriffs:
  - Alle Lese-, Eingabe-, Änderungs- und Löschungstransaktionen werden protokolliert.
  - Zur Missbrauchserkennung werden regelmäßig stichprobenartige Auswertungen vorgenommen.

WEITERGABEKONTROLLE

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht von Unbefugten 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 (einschließlich Verschlüsselungsverfahren):

- Protokollierung:
  - Es findet eine Protokollierung der sendenden und empfangenden Stelle statt.
  - Die Festlegung ist dokumentiert und sie ist den betroffenen Mitarbeitern bekannt.
- Sichere Datenübertragung zwischen Server und Client:
  - Die Datenübertragung zwischen Clients und Servern erfolgt verschlüsselt (SSL, SSH, SFTP oder VPN).
- Übertragung im Backend:
  - Die Verbindung zu den Backendsystemen ist geschützt.
  - Daten mit hohem Schutzbedarf werden verschlüsselt.
- Risikominimierung durch Netzsegmentierung:
  - Es wurde eine Netzsegmentierung vorgenommen, die darauf abzielt, dass die Datenübertragung über ein Minimum von Netzelementen stattfindet.
  - Es existiert ein Netzplan.
  - Das relevante System befindet sich in einer DMZ.
- Sicherheitsgateways an Netzübergabepunkten:
  - Es existieren Firewalls an Netzwerk-Übergabepunkten.
  - Die Firewalls sind ständig aktiviert.
  - Die Firewalls sind durch den Nutzer nicht deaktivierbar.
- Härtung der Backend-Systeme:
  - Voreingestellte Dienstkonten/Passworte wurden deaktiviert.
  - Es existieren Handlungsanweisungen bei Missbrauchsverdacht.
  - Es existiert ein aktueller Virenschutz.
- Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder:
  - Es gibt eine dokumentierte Schnittstellenspezifikation.
  - Für die Übermittlung existieren Verfahrensanweisungen.
  - Es gibt eine Beschreibung aller zu übermittelnden personenbezogenen Datenfelder.

Initialen des Kunden

- Mensch-Maschine-Authentisierung:
  - Gegenseitige Authentisierung mittels kryptographischen Verfahren.
- Zugriff auf lokale Zwischenspeicher:
  - Jeder Zugriff auf etwaige lokale Zwischenspeicher oder Datenbanken, die Kundendaten des Auftraggebers enthalten, zu Zwecken bzw. mit Anwendungen, die der Auftraggeber nicht freigegeben hat, ist technisch unterbunden.
- Eine Versendung von personenbezogenen Daten per Post findet nicht statt.
- Prozess zur Sammlung und Entsorgung:
  - Es existieren Regelungen zur datenschutzkonformen Vernichtung von Datenträgern.
  - Es existieren Regelungen zur datenschutzkonformen Vernichtung von Dokumenten.
- Datenschutzgerechtes Lösch-/Zerstörungsverfahren:
  - Datenträger werden vor Wiederbenutzung durch andere Nutzer datenschutzgerecht gelöscht; eine Wiederherstellung der gelöschten Daten ist gar nicht oder nur mit unverhältnismäßigem Aufwand möglich.
  - Hardwarekomponenten oder Dokumente werden so vernichtet, dass eine Wiederherstellung gar nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

EINGABEKONTROLLE

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

- Es existiert eine Dokumentation darüber, welche Personen aufgrund ihrer Aufgabenstellung befugt und verantwortlich sind, personenbezogene Daten in der Datenverarbeitungsanlage einzugeben, zu verändern oder zu entfernen.

AUFTRAGSKONTROLLE

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle):

- Nur der Auftraggeber selbst ist befugt, die Aufträge im System zu steuern.
- Ausübung der Kontrollpflichten:
  - Der Auftragnehmer unterstützt den Auftraggeber bei der Ausübung seiner Kontrollpflichten.
  - Alle auftretenden Vorfälle werden dem Auftraggeber gemeldet.
  - Der Auftragnehmer hat alle Mitarbeiter über die Meldepflicht von Vorfällen informiert.
- Protokollierung der Auftragsdurchführung durch den Auftragnehmer:
  - Es gibt eine Dokumentation, welche die lückenlose Nachvollziehbarkeit der einzelnen im Rahmen der Auftragsausführung erforderlichen Arbeitsschritte gewährleistet. Auf Anforderung kann belegt werden, dass der jeweilige Auftrag strikt nach den Weisungen des Auftraggebers durchgeführt wurde (Mindestangaben: Auftraggeber/Kunde, Aktion/Teilauftrag, genaue Spezifikation der Verarbeitungsschritte/-parameter, Bearbeiter, Termine, ggf. Empfänger).

3. FÄHIGKEIT, DIE VERFÜGBARKEIT DER PERSONENBEZOGENEN DATEN UND DEN ZUGANG ZU IHNEN BEI EINEM PHYSISCHEN ODER TECHNISCHEN ZWISCHENFALL RASCH WIEDERHERZUSTELLEN

VERFÜGBARKEITSKONTROLLE

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

- Backup-Konzept:
  - Es existiert ein Backup-Konzept.
  - Backups finden regelmäßig statt.
  - Eine für das Backup verantwortliche Person und Vertreter sind benannt.
  - Es wird regelmäßig überprüft, ob das Rückspielen eines Backups möglich ist.
- Notfallplan:
  - Es existiert ein Notfallplan, in dem die einzuleitenden Schritte aufgeführt werden und in dem festgelegt ist, welche Personen, insbesondere auch auf Seiten des Auftraggebers, über den Vorfall zu unterrichten sind.
- Prüfung der Notfalleinrichtungen:
  - Es findet eine regelmäßige Prüfung von Notstromaggregaten und Überspannungsschutzeinrichtungen sowie eine permanente Überwachung der Betriebsparameter statt.

ZWECKBINDUNG

Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Die Daten unterschiedlicher Kunden des Auftragnehmers werden in getrennten Dateien und in getrennten Verzeichnissen gespeichert und nicht zusammengeführt.

4. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG DER WIRKSAMKEIT DER TECHNISCHEN UND ORGANISATORISCHEN MAßNAHMEN ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER VERARBEITUNG

ORGANISATIONSKONTROLLE

- Prozessdefinition/-kontrolle:
  - Es gibt Verfahrensanweisungen.
  - Für die Verarbeitung von Daten im Unternehmen sind Prozesse und Arbeitsabläufe definiert.
  - Die Umsetzung und Einhaltung der Prozesse wird kontrolliert.
- Schulung/Verpflichtung:
  - Grundsätze des Datenschutzes, einschließlich technisch-organisatorischer Maßnahmen.
  - Pflicht zur Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse einschließlich den Vorgängen des Auftraggebers.
  - Ordnungsgemäßer und sorgfältiger Umgang mit Daten, Dateien, Datenträgern und sonstigen Unterlagen.
  - Die Schulungen sind dokumentiert.
  - Die Schulungen werden regelmäßig wiederholt, mindestens jedoch alle drei Jahre.
- Schulung/Verpflichtung Betriebsfremder:
  - Firmenfremde erhalten erst dann Zugang zu Datenverarbeitungsanlagen, wenn diese schriftlich auf das Daten- und ggf. auch auf das Fernmeldegeheimnis bzw. weitere Verschwiegenheitsverpflichtungen verpflichtet und geschult wurden, bevor diese die Datenverarbeitungsanlagen in Betrieb nehmen und bedienen dürfen.
- Interne Aufgabenverteilung:
  - Eine Trennung zwischen operativen und administrativen Funktionen ist erfolgt.
- Vertreterregelung:
  - Für alle betriebsnotwendigen Aufgaben/Funktionen ist ein Vertreter festgelegt.

Initialen des Kunden

ANLAGE 2: SUBUNTERNEHMER

Subunternehmer	Vom Subunternehmer erbrachte Leistungen
Emarsys eMarketing Systems AG Märzstraße 1 1150 Wien Österreich	Entwicklung und Bereitstellung der Marketing Plattform.
Emarsys Technologies Kft Kossuth Lajos utca 7-9 First Site Hotel & Business Complex 2. Stock 1053 Budapest Ungarn	Entwicklung und Bereitstellung der Marketing Plattform.
Emarsys UK Ltd Focus Point 21 Caledonian Road London N1 9DX Vereinigtes Königreich	Kundenbetreuung.
LINFORGE Technologies GmbH Brehmstraße 10 1110 Wien Österreich	Servicepartner für die betriebliche Systemadministration.
CloudAMQP / 84codes AB Sveavägen 98 113 50 Stockholm Schweden	Message Broker als Dienstleistung („as a Service“).
CDNetworks Europe, Co. Ltd. 85 Gresham St London EC2V 7NQ Vereinigtes Königreich	Content Delivery Network.
Heroku, Inc. The Landmark @ 1 Market St. Suite 300 San Francisco, CA 94105 USA	Plattform als Dienstleistung („as a Service“). Die Verarbeitung personenbezogener Daten findet ausnahmslos innerhalb der Europäischen Union statt.
Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 USA	Datenspeicher-Engine. Die Verarbeitung personenbezogener Daten findet ausnahmslos innerhalb der Europäischen Union statt.
Compose / IBM Corp. 1 New Orchard Road Armonk, New York 10504-1722 USA	Datenbank als Dienstleistung („as a Service“). Die Verarbeitung personenbezogener Daten findet ausnahmslos innerhalb der Europäischen Union statt.

Initialen des Kunden