RAHMENVEREINBARUNG
ZUR AUFTRAGSDATENVERARBEITUNG

Fischlein & Westphal GbR
z.Hd. Nino Fischlein
Athenstraße 1
D-97424 Schweinfurt
als Verantwortlicher (hier bezeichnet als „**Auftraggeber**“)

und der
The Call International GmbH
The Squaire West 12
60600 Frankfurt
als Auftragsverarbeiter (hier bezeichnet als „**Auftragnehmer**“)

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in § 3 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung.

§ 1 Begriffsbestimmungen

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DS-GVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.
(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DS-GVO 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.
(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DS-GVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DS-GVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DS-GVO, biometrischen

Daten gem. Art. 4 Abs. 14 DS-GVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DS-GVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
(6) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DS-GVO eine von einem Mitgliedstaat gem. Art. 51 DS-GVO eingerichtete unabhängige staatliche Stelle.

§ 2 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich der Telekommunikation auf Grundlage außerhalb dieses Vertrages geschlossenen Vereinbarungen. Hierfür liegen dem Auftraggeber gesonderte Vertragswerke bzw. Auftragsbestätigungen vor (im Folgenden „**Hauptvertrag**“). Zur Klarstellung bzw. Ergänzung dessen dient § 3 dieser Vereinbarung.
Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und der dazugehörigen Leistungsbeschreibung).
Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.
(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die vorliegenden Regelungen gehen im Zweifel den Regelungen des außerhalb dieser Vereinbarung geschlossenen Hauptvertrags vor.
(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.
(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 3 Hauptvertrag

(1) Der Auftragnehmer nimmt im Auftrag des Auftraggebers nach Maßgabe dieser Klausel Datenverarbeitungen vor.
(2) Gegenstand des Auftrages und Zweck der Datenverarbeitung ist

der Versand von Sprachnachrichten per Telefonanruf an Kunden und Mitarbeiter des Auftraggebers.

(3) Die Vertragsdauer gilt

mit Tag der Unterzeichnung bis unbegrenzt

(4) Applikationen mittels derer personenbezogene Daten von dem Auftraggeber verarbeitet werden sind die Folgenden:

NAR-Id	Name der Applikation
	tCALL Communication Technology

(5) Betroffene Personen sind

Bestandskunden und Mitarbeiter des Auftraggebers.

(6) Die folgenden Daten werden verarbeitet:

Telefonnummern der Betroffenen aus Datenbanken des Auftraggebers.

(7) Eine Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 DS-GVO findet nicht statt.
(8) Der Auftragnehmer nutzt die im Rahmen des Vertragsverhältnisses unter (6) aufgeführten personenbezogenen Daten, die vom Auftraggeber stammen oder für diesen erhoben oder erworben wurden, ausschließlich für die Erbringen der unter (2) genannten Dienst- oder Werkleistungen.

§ 4 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.
(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.
(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 Art der verarbeiteten Daten, Kreis der Betroffenen

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in § 3 (6) näher spezifizierten personenbezogenen Daten.
(2) Der Kreis der von der Datenverarbeitung Betroffenen ist in § 3 (5) dargestellt.

§ 6 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.
(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die folgend aufgeführten Maßnahmen der

a) Zutrittskontrolle
b) Zugangskontrolle
c) Zugriffskontrolle
d) Weitergabekontrolle
e) Eingabekontrolle
f) Auftragskontrolle
g) Verfügbarkeitskontrolle
h) Trennungskontrolle

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftragnehmer beschreibt dem Auftraggeber die bei ihm implementierten technischen und organisatorischen Sicherheitsmaßnahmen in der Anlage zu diesem Vertrag.
(3) Beim Auftragnehmer ist als betrieblicher Datenschutzbeauftragter bestellt:

Herr Fabian Sonnenschein,
c/o The Call International GmbH
The Squaire West 12
D-60600Frankfurt am Main
E-Mail: fas@thecallgoup.de

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 7 Informationspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.
(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DS-GVO liegen.
(5) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 6 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.
(6) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
(7) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.
(8) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 8 Einsatz von Subunternehmern

(1) Der Auftragnehmer begründet keine Unterauftragsverhältnisse mit Subunternehmern („Subunternehmerverhältnis“). Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von Subunternehmerverhältnissen befugt, soweit er den Auftraggeber hiervon vorab in Kenntnis setzt und dieser der Beauftragung des Subunternehmers vorab schriftlich zugestimmt hat. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln).
(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen **liegt nicht vor**, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 9 Anfragen und Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DS-GVO.
(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 10 Haftung

(1) Die Parteien haften untereinander sowie gegenüber Dritten nach den gesetzlichen Vorschriften. Insoweit wird insbesondere auf Art. 82 DS-GVO verwiesen.
(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

§ 11 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen. Zu entsorgende Unterlagen sind mit einem Aktenvernichter nach DIN 32757-1 zu vernichten. Zu entsorgende Datenträger sind nach DIN 66399 zu vernichten.
(2) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 12 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.
(2) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.
(3) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Hamburg.

Schweinfurt, den 24. März 2020

Christian Bollstetter
The Call International GmbH

Nino Fischlein
Fischlein & Westphal GbR

The Call International GmbH

Technische und organisatorischen Maßnahmen (TOM)
Beschreibung der implementierten Sicherungsmaßnahmen gem. Artt. 32, 30 Abs. 2 lit. d DS-GVO

1. Zutrittskontrolle

Die Zutrittskontrolle gewährleistet, dass nur berechtigte Personen Zutritt zu bestimmten Gebäuden und Räumen eines Unternehmens haben. Eine Zutrittskontrolle kann sowohl organisatorisch (durch einen Wachdienst, Pförtner etc.) oder technisch (Zutrittskontrollsystem, Vereinzelungsanlagen (Drehkreuz, Personenschleusen), biometrische Zutrittskontrollsysteme, Videoüberwachung, Alarmanlage, Schließanlage, gesondert gesicherter Serverraum, …) umgesetzt werden.

Beschreibung der Umsetzung der Zutrittskontrolle beim Auftragnehmer bzw. Verweis auf eine beim Auftraggeber geltende einschlägige IT-Sicherheitsrichtline:

Die Datenverarbeitungsanlage des Dienstes wird auf den Web Services der Interxion Deutschland GmbH betrieben. Damit wird automatisch der hohe Interxion Web Services bereitgestellt.

2. Zugangskontrolle

Die Zugangskontrolle gewährleistet, dass es Unbefugten nicht möglich ist, Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder gespeichert werden, zu nutzen. Die Zugangskontrolle wird am Computer üblicherweise durch die Eingabe von Benutzerkennung und Passwort realisiert. Sie kann aber auch mit Magnet- oder Chipkarten oder mit biometrischen Merkmalen sichergestellt werden.

Beschreibung der Umsetzung der Zugangskontrolle beim Auftragnehmer bzw. Verweis auf eine beim Auftraggeber geltende einschlägige IT-Sicherheitsrichtline:

Der Zugang zu den Servern der Datenverarbeitungsanlage ist nur durch SSL Zertifikate möglich. Damit ist der höchste Wert an Zugangssicherheit zu der Datenverarbeitungsanlage sichergestellt. Physische Zugänge werden durch Interxion Deutschland GmbH reglementiert.

3. Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, dass Zugriff auf personenbezogene Daten in Verarbeitungssystemen ausschließlich den Personen gewährt werden darf, die die Befugnis zur Einsichtnahme sowie zur Verarbeitung dieser Daten haben. Realisiert wird die Zugriffskontrolle beispielsweise durch Rollenkonzepte sowie Zugriffsberechtigungskonzepte,

regelmäßige Überwachung der Rechtevergabe, 4-Augenprinzip, Firewall, Virenschutz, Log-Files, etc.

Beschreibung der Umsetzung der Zugriffskontrolle beim Auftragnehmer bzw. Verweis auf eine beim Auftraggeber geltende einschlägige IT-Sicherheitsrichtline:

Die Datenverarbeitungsanlage kann nur von Administratoren mit entsprechenden SSL – Zertifikaten betreten werden. Die Infrastruktur ist durch eine Firewall vom Internet getrennt. Die Daten der Datenverarbeitungsanlage können über ein Administrationsinterface bearbeitet werden. Dieses Interface kann nur durch Login mit Username und Passwort und eine explizite Datenzuordnungen zu den jeweiligen Usern genutzt werden. Damit wird sichergestellt, dass nur autorisierte Personen die Daten einsehen können.

4. Weitergabekontrolle

Die Weitergabekontrolle gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden können. Zudem soll überprüft und festgestellt werden können, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen der Datenübertragung vorgesehen ist. Maßnahmen der Weitergabekontrolle sind Verschlüsselung von E-Mails, Transporte in gesicherten Behältnissen, Regelungen zur Nutzung des Internets, gesperrte Seiten im Internet, Firewall, Virenschutz, sichere Protokolle, Sicherung von externen Netzwerkzugängen (beispielsweise von Fernwartungszugängen), Regelung und Verfahren zur Akten- und Datenträgervernichtung, Festlegung sicherer Postversandverfahren, etc.)

Beschreibung der Umsetzung der Weitergabekontrolle beim Auftragnehmer bzw. Verweis auf eine beim Auftraggeber geltende einschlägige IT-Sicherheitsrichtline:

Die Weitergabe der personenbezogenen Daten erfolgt nur in verschlüsselten Dateien. Zugang zur Datenverarbeitungsanlage und den Daten erfolgt nur über oben genannte SSL-Zertifikate und kann somit nicht von unbefugten durchgeführt werden.

5. Eingabekontrolle

Die Eingabekontrolle gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungsanlagen eingegeben, verändert oder entfernt worden sind. Dies geschieht in der Regel durch eine automatische Protokollierung der Eingaben in Logfiles, protokolliert werden in der Regel: betroffener Datensatz, Art der Aktivität (Anlage, Veränderung, Löschung des Datensatzes), Zeitpunkt der Aktivität bzw. des Ereignisses, ausführende Person (Nutzerkennung).

Beschreibung der Umsetzung der Eingabekontrolle beim Auftragnehmer bzw. Verweis auf eine beim Auftraggeber geltende einschlägige IT-Sicherheitsrichtline:

Die Daten der Datenverarbeitungsanlage werden über ein internes Adminstrationsinterface verwaltet. Über dieses Interface kann nach Login eine Verarbeitung der Daten erfolgen. Damit wird in Logfiles dokumentiert wann welche Daten wie verarbeitet wurden.

6. Auftragskontrolle

Die Auftragskontrolle gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur gemäß den Weisungen des Auftraggebers verarbeitet werden können. Hier ist zu beschreiben, welche Regelungen zur Umsetzung und Kontrolle der technischen und organisatorischen Maßnahmen bei einem etwaig eingesetzten Subunternehmer vertraglich vereinbart wurden.

Beschreibung der Umsetzung der Auftragskontrolle beim Auftragnehmer bzw. Verweis auf eine beim Auftraggeber geltende einschlägige IT-Sicherheitsrichtline:

Die The Call International GmbH beschäftigt keine Subunternehmer zur Umsetzung des Dienstes

7. Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle gewährleistet den Schutz personenbezogener Daten gegen zufällige Zerstörung oder Verlust. Die Umsetzung erfolgt durch ein Datensicherungs- und Backupkonzept, Notfallplan, Virenschutz, Firewall, Maßnahmen gegen Brand, Wasser, Blitzschlag, Stromausfall, Diebstahl und Sabotage.

Beschreibung der Umsetzung der Verfügbarkeitskontrolle beim Auftragnehmer bzw. Verweis auf eine beim Auftraggeber geltende einschlägige IT-Sicherheitsrichtline:

Die Interxion Deutschland GmbH bietet per default Vorkehrungen gegen Brand, Wasser, Blitzschlag, Stromausfall, Diebstahl und Sabotage. Des Weiteren sind alle Dienste redundant ausgelegt um einen Datenverlust zu verhindern.

8. Trennungskontrolle

Das Trennungsgebot ist ein Grundsatz, nach dem zu unterschiedlichen Zwecken erhobene Daten auch nur getrennt verarbeitet werden dürfen. Umzusetzen ist das Trennungsgebot durch physikalische und logische Trennung der Daten in Verarbeitungssystemen oder auf Datenträgern, z.B. durch strikte Trennung von Test- und Produktiv-Datenbestand, Einsatz verschiedener Datenbanken, Verschlüsselung einzelner Datensätze, Gewährleistung von sogenannter Mandantentrennung.

Beschreibung der Umsetzung des Trennungsgebots beim Auftragnehmer bzw. Verweis auf eine beim Auftraggeber geltende einschlägige IT-Sicherheitsrichtline:

Die Datenverarbeitungsanlage ist mandantenfähig und somit sind alle Daten immer ihren jeweiligen Mandanten zugeordnet und nur von diesen zu verarbeiten.

Die Umgebungen für die Entwicklung, Tests und die Produktion sind jeweils durch komplett separate Umgebungen (Hardware und Software) voneinander getrennt.