Vereinbarung zur Auftragsverarbeitung
gem. Art. 28 Abs. 3 DS-GVO

Zwischen dem Kunden

als Verantwortlicher (hier bezeichnet als „Auftraggeber“)

und

Solutiness GmbH

Böttgerstraße 17

89231 Neu-Ulm

Deutschland

Vertreten durch die Geschäftsführung Regina Keller-Sylla

als Auftragsverarbeiter (hier bezeichnet als „Auftragnehmer“)

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in § 1 dieses Vertrages genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DSGVO stellt konkrete Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen aufgrund der Allgemeinen Geschäftsbedingungen zur Nutzung von tele-LOOK. 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 den AGBs. 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 Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen der AGB s vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit den AGBs 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 der gebuchten Leisungen, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 2 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen der AGBs 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. Die weisungsberechtigten Personen ergeben sich aus Anlage 5. 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 in den AGBs 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.

§ 3 Art der verarbeiteten Daten, Kreis der Betroffenen

Im Rahmen der Durchführung der AGBs erhält der Auftragnehmer Zugriff auf die in Anlage 1 näher spezifizierten personenbezogenen Daten. Der Kreis der von der Datenverarbeitung Betroffenen ist in Anlage 2 dargestellt.

§ 4 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 DSGVO, insbesondere mindestens die in Anlage 3 aufgeführten Maßnahmen der Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags-, Verfügbarkeits- und Trennungskontrolle. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Beim Auftragnehmer ist

( ) als betrieblicher Datenschutzbeauftragter

(X) als Ansprechpartner für den Datenschutz (sofern gem. Art. 37 DSGVO und § 38 BDSG keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht)

bestellt: Harald Ruf, Solutiness GmbH, Böttgerstr. 17, 89231 Neu-Ulm, E-Mail: harald.ruf@tele-look.de, Tel.: +49 731-85 07 42 20. Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite und teilt sie der Aufsichtsbehörde mit. Veröffentlichung und Mitteilung weist der Auftragnehmer auf Anforderung des Auftraggebers in geeigneter Weise nach. Der Auftragnehmer ist aus folgenden Gründen nicht verpflichtet einen Datenschuztbeauftragten zu bestellen:

- weniger als 10 Mitarbeiter
- keine Verarbeitung von Daten gem. Art. 9/10 DSGVO
- kein Fall des Art. 37 I b DSGVO
- kein Fall des § 38 I 2 BDSG iVm Art 35 DSGVO

(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 IIIb DSGVO) 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. Ein Muster der Belehrung findet sich im Anhang 6 zu diesem Vertrag.

§ 5 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 DSGVO liegen.

(5) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 5 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(6) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten bzw. Ansprechpartners für den Datenschutz 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 II DSGVO 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.

§ 6 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber alle Auskünfte und Informationen zum Nachweis der Einhaltung der gesetzlichen datenschutzrechtlichen Bestimmugen sowie der in diesem Vertrag zum Datenschutz niedergelegten Pflichten zur Verfügung zu stellen, z.B. die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(5) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 4 Abs. 4 auf Verlangen nach.

§ 7 Einsatz von Subunternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 4 genannten Subunternehmer durchgeführt. Für die Einschaltung weiterer als der in Anlage 4 genannten Subunternehmer ist die vorherige schriftliche Zustimmung des Auftraggebers erforderlich. 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) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, ist mitunter Voraussetzung für die Zustimmung seitens des Auftraggebers, dass der Auftragnehmer dem Auftraggeber vorab ein bei dem Subunternehmer als Empfänger personenbezogener Daten angemessenes Datenschutzniveau nachweist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(3) 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.

§ 8 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 bis 22 sowie 32 und 36 DSGVO.

(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.

§ 9 Haftung

(1) Für den Ersatz von Schäden gegenüber einem Betroffenen, der wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung einen Schaden erlitten hat, gelten die gesetzlichen Bestimmungen.

§ 10 Außerordentliches Kündigungsrecht

Der Auftraggeber kann die gebuchten Leistungen fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

§ 11 Beendigung des Vertrages

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Vertrags 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 Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Vertrages hinaus die ihm im Zusammenhang mit dem Vertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Vertrags 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) Es gelten die Begriffsbestimmungen der DSGVO. Der Auftraggeber und der Auftragnehmer und ggf. deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(2) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(3) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(4) 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.

(5) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist der Standort des Auftragnehmers.

Anlagen

Alle Anlagen sind Vertragsbestandteil

Anlage 1 – Beschreibung der Daten/Datenkategorien

Anlage 2 – Beschreibung der Betroffenen/Betroffenengruppen

Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers (TOM)

Anlage 4 – Genehmigte Subunternehmer

Anlage 5 – Weisungsberechtigte Personen

Anlage 6 – Belehrung auf das Datengeheimnis (Muster) (siehe Dokument: Solutiness Merkblatt.docx)

Anlage 1 – Beschreibung der Daten/Datenkategorien

In Bezug genommene personenbezogene Daten sind

1.1 **Teilnehmer eines VideoCalls -** Personen, die keinen Account haben und eingeladener Teilnehmer eines VideoCalls sind:

(a) IP-Adresse – aller Besucher – wird zu log und Fehlersucher verwendet.

(b) Mobile-Telefonnummer (und ggf. weitere Kontaktdaten) Die Mobile-Telefonummer wird zum Versenden der SMS benötigt (MSISDN)

(c) Standbilder die während eines Calls gemacht werden

(d) Weiter Information, die durch einen registrierten Kunden in Form von Notizen erzeugt werden

(e) Dauer, Zeitpunkt eines Video

(f) Gerätekennzeichnung des Smartphones (z.B. Samsung S8) wird anhand des UserAgent – Strings ausgelesen und zur Fehlersuche gespeichert

(g) Operation System des Phones wird anhand des UserAgent-Strings ausgelesen und zur Fehlersuche gespeichert

Nexmo Inc. selbst haben KEINEN Zugriff auf die persönlichen Daten des Services des Auftragnehmers (z.B. Email, Useraccount, Passwort, Mobiletelefonnummer, Vor- und Nachname, Adresse, Notizen, Dauer, Zeitpunkt eines Video), da die Kommunikation zwischen Nexmo Inc. und den Clients während eines Videogesprächs über Sessionid und Tokens geregelt wird.
Nexmo Inc. speichert Informationen wie z.b. die IP-Adresse, Betriebssystem des Clients, Browser, Version des Browser anonym. Diese Informationen werden zur Verbesserung des Services benutzt.

Diese Daten umfassen

(X) keine

( ) die nachstehend aufgeführten besonderen Kategorien personenbezogener Daten.

_____

(z.B. rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit, Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln, genetische oder biometrische Daten, Gesundheitsdaten sowie Daten zum Sexualleben oder der sexuellen Orientierung)

Anlage 2 – Beschreibung der Betroffenen/Betroffenengruppen

Kunden des Auftraggebers, Mitarbeiter des Auftraggebers bzw. Personen, die der Auftraggeber beauftragt und einlädt oder als Benutzer anlegt um den Service des Auftragnehmers zu benutzen.

[z. B. Mitarbeiter, Lieferanten, Kunden etc.]

Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers

Siehe anliegendes Beiblatt (Solutiness TOM.pdf)

Solutiness GmbH

Sicherheitskonzept zum Datenschutz
Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

1. Vorbemerkung

Solutiness ist durch Art. 32 DSGVO sowie insbesondere im Rahmen von Vertragsverhältnissen zur Auftragsverarbeitung verpflichtet, Maßnahmen zur Sicherheit der Datenverarbeitung zu treffen. Im Folgenden werden diese Maßnahmen näher beschrieben. Sie dienen zur Sicherstellung der Erfüllung gesetzlicher und vertraglicher Anforderungen an den Datenschutz unter dem Gesichtspunkt der Sicherheit der Datenverarbeitung. Darüber hinaus gelten die im tele-LOOK SaaS Vertrag geltenden Bestimmungen.

2. Belehrung zum Datengeheimnis

Alle Mitarbeiter unseres Hauses sind auf das Datengeheimnis verpflichtet. Mitarbeiter, die tragbare Geräte (Notebook, Pad, Smartphone) mit Zugriffsmöglichkeiten auf personenbezogene Daten nutzen, werden gesondert über entsprechende Pflichten bei der Nutzung in der Öffentlichkeit und zur Aufbewahrung dieser Geräte unterrichtet.

3. Grundsätzliches

Die nachstehenden technischen und organisatorischen Maßnahmen sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere von Risiken für die Rechte und Freiheiten natürlicher Personen ausgewählt und umgesetzt worden. Die Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

4. Vertraulichkeit

4.1 Zutrittskontrolle

Grundsatz

Unbefugten ist der Zugang zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Regelung bei Solutiness

Der Zugang zum Gebäude des Auftragnehmers wird durch die Erfordernis von Schlüsseln gesichert.

Besucher werden in gesonderten Besprechungsräumen außerhalb der Verarbeitungsräume empfangen.

Der Zugang zu den Rechenzentren in dem der Service des Auftragnehmers läuft wird durch umfangreiche Sicherheitsmassnahmen gesichert (siehe Amazon Webservice: https://aws.amazon.com/de/compliance/data-center/perimeter-layer/)

4.2 Zugangskontrolle

Grundsatz

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Regelung bei Solutiness

Der unbefugte externe Zugriff auf die gespeicherten Daten ist durch ein Firewall-System gesichert. Dieses wird von einem IT-Fachmann betreut, der vertraglich auf das Datengeheimnis verpflichtet ist. Externen IT-Firmen haben einen Vertrag zur Auftragsdatenverarbeitung abgeschlossen.
Der Zugriff auf die IT-Systeme ist geschützt durch anwenderspezifische Kennungen und Passworte. Bei Serversysteme ist der Zugriff nur per SSH- und mit SSH-Zertifikaten möglich.

Es gibt keine Gruppenpasswörter, jeder Mitarbeiter hat ein eigenes, nur ihm bekanntest Passwort.

Administratorpasswörter sind in gesonderten verschlüsselten Dateien abgelegt.

Die Passwörter laufen nach regelmässigen Zeit ab und verfügen über eine Mindestlänge.

4.3 Zugriffskontrolle

Grundsatz

Es ist 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.

Regelung bei Solutiness

Für die eingesetzten IT-Systeme existieren differenzierte persönliche Zugriffsberechtigungen, die auf die Aufgaben der jeweiligen Mitarbeiter abgestimmt sind. Über die Vergabe von Berechtigungen entscheidet die Geschäftsführung.

Die Anzahl der Administratoren ist auf das „Notwendigste“ reduziert.

4.4 Trennungskontrolle

Grundsatz

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

Regelung bei Solutiness

Mandanten sind logisch voneinander getrennt (softwareseitig).
Der Zugriff auf die Datenbank erfolgt mit festgelegten Datenbankrechten.

Trennung von Produktiv und Testsystem.

Es werden keine zu unterschiedlichen Zwecken erhobenen personenbezogenen Daten verknüpft.

4.5 Pseudonymisierung und Verschlüsselung

Grundsatz

Es sind soweit möglich Maßnahmen zur Pseudonymisierung zu treffen, ist zu gewährleisten, dass Datenschutzgrundsätze wie der Grundsatz der Datenminimierung wirksam umgesetzt werden. Personenbezogene Daten sind soweit möglich verschlüsselt aufzubewahren und zu übermitteln.

Regelung bei Solutiness

Personenbezogene Daten werden pseudonymisiert (z.b. Bilder sind nur mit Hilfe der Datenbank einem Person zuordnenbar).

Die Datenübermittlung erfolgt grundsätzlich verschlüsselt mit gängigen Verschlüsselungtechniken aus dem Webbereich (HTTPS, SSH, SSL) .

5. Integrität

5.1 Weitergabekontrolle

Grundsatz

Es ist 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 welchen Stellen eine Übermittlung von personenbezogenen Daten durch Einrichtungen zur Datenübermittlung vorgesehen ist.

Regelung bei Solutiness

Eine weitere Übermittlung personenbezogener Daten von Solutiness zu Dritten findet nicht statt.
Die Server verfügen über verschlüsselte Laufwerke, ebenfalls ist die Datenbank verschlüsselt.

Mitarbeiter, die Notebook, Pad, Smartphones nutzen, werden gesondert über besondere Pflichten bei der Nutzung in der Öffentlichkeit, zur sicheren Aufbewahrung der Geräte und zum Verbot der Weitergabe belehrt.

5.2 Eingabekontrolle

Grundsatz

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind.

Regelung bei Solutiness

Die Verarbeitung der personenbezogenen Daten wird protokolliert.

Schutz vor Schadsoftware durch Einsatz von Virenscannern, Firewall und VPCs.

6. Verfügbarkeit und Belastbarkeit

6.1 Verfügbarkeitskontrolle

Grundsatz

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Regelung bei Solutiness

Es werden regelmäßige Datensicherungen durchgeführt.

Die Serverräume sind mit unterbrechungsfreier Stromversorgung (USV) ausgestattet.

Schutz vor Schadsoftware durch Einsatz von Virenscannern, Firewall und VPCs.

6.2 Rasche Wiederherstellbarkeit

Grundsatz

Es ist zu gewährleisten, dass personenbezogene Daten und der Zugang zu ihnen bei einem technischen Zwischenfall rasch wiederherstellbar sind.

Regelung bei Solutiness

Es werden regelmäßige Datensicherungen durchgeführt, die sich in unmittelbarem Zugriff der zuständigen Mitarbeiter befinden.

Die Datenbanken und Volumes werden täglich gebackuped. Die Datenbankbackups werden 7 Tage aufbewahrt. Die Volumes 30 Tage.

Die Backups werden kontrolliert. Die Datenbank ist redundant verfügbar. Backup sind ausschließlich auf Systemen von AWS gespeichert.

7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

7.1 Überprüfung der Maßnahmen

Grundsatz

Es ist ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzuführen.

Regelung bei Solutiness

Die in diesem Katalog festgelegten Maßnahmen werden bei Solutiness in regelmäßigen Zeitabständen auf ihre Einhaltung und ihre Wirksamkeit überprüft. Dies geschieht durch Geschäfts- und IT-Leitung.

7.2 Auftragskontrolle

Grundsatz

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag erhoben, verarbeitet oder genutzt werden, nur entsprechend den Weisungen des Auftraggebers erhoben, verarbeitet oder genutzt werden können.

Regelung bei Solutiness

Die Pflichten von Solutiness und die Rechte des jeweiligen Auftraggebers einer Auftragsverarbeitung werden in einer Vereinbarung zur Auftragsverarbeitung mit dem Auftraggeber detailliert und einvernehmlich geregelt.

Anlage 4 – Genehmigte Subunternehmer

Die nachfolgenden Unternehmen sind genehmigte Subunternehmer im Sinne des § 7:

1. root360 GmbH: Universitätsstrasse 14, 04109 Leipzig
   Ansprechpartner: Steffen Drya, EMail: steffen.drya@root360.de
   Zweck: IT-Administration und Wartung der AWS-Server

2. Nexmo Inc.: 23 Main Street, Holmdel, NJ, 07733 USA

   Ansprechpartner: Privacy Team, EMail: privacy@nexmo.com

   Zweck: WebRTC Provider

Name, Rechtsform, Vertretungsberechtigter, Anschrift (nicht: Postfach)

DATA PROCESSING ADDENDUM

THIS DATA PROCESSING ADDENDUM is entered into as of the date of the last signature below (the **"Effective Date"**) by and between the customer specified in the table below ("**Customer**") and Nexmo Inc. ("**Nexmo**").

	Customer: Solutiness GmbH	**Nexmo Inc.**
Signature:	Plüher Plüher (Jun 22, 2019)	Nicole Schiereck
Name:	Plüher	Nicole Schiereck
Title:	CEO	Privacy Counsel
Date:	Jun 22, 2019	Jun 24, 2019
Street:	Alte Breisacher Str. 14a	23 Main Street
Suite/Floor:	-	
City:	Freiburg	Holmdel
State/County/Province:	BW	NJ
ZIP/Post Code:	79112	07733
Country:	Germany	USA
Data protection contact		
Name:	Klaus Plueher	Privacy Team
Title:	Herr	
Email:	info@solutiness.com	privacy@nexmo.com

RECITALS

(A) Nexmo provides certain cloud communication services (the **"Services"**) to Customer and in connection with the Services, Nexmo processes certain personal data in respect of which Customer, members of the Customer Group (as defined below), or third parties who interface with Customer's products, services or systems, may be a data controller under the Applicable Data Protection Law (as defined below).

(B) Customer and Nexmo have agreed to enter into this data processing addendum (**"DPA"**) in order to ensure that adequate safeguards are put in place with respect to the protection of such personal data as required by the Applicable Data Protection Law.

(C) For purposes of this DPA, "**Agreement**" shall mean the Nexmo Terms of Use, except where the Parties have mutually executed a Messaging Services Agreement or Master Services Agreement in force as of the Effective Date, then "Agreement" shall mean that agreement. This DPA amends and supplements the Agreement and if there is any conflict between this DPA and the Agreement

regarding the parties' respective privacy and security obligations, the provisions of this DPA shall prevail.

1. Definitions

1.1 The following expressions are used in this DPA:

(a) **"Applicable Data Protection Law"** means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data; and (ii) on and after 25 May 2018, Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**"General Data Protection Regulation"** or **"GDPR"**);

(b) **"Customer Group"** means Customer and any corporate entities which are from time to time: (i) under Common Control with Customer; and (ii) established and/or doing business in the European Economic Area or Switzerland;

(c) **"Data Subject Request"** means a request from a data subject regarding his/her Personal Data, whether in relation to access, rectification, restrictions on processing, erasure or portability in respect of such Personal Data;

(d) **"Nexmo Group"** means Nexmo and any corporate entities which are from time to time under Common Control with Nexmo;

(e) **"Personal Data"** means all data which is defined as 'personal data' in the Applicable Data Protection Law and which is provided by Customer to Nexmo or accessed, stored or otherwise processed by Nexmo in connection with the Services;

(f) **"processing"**, **"data controller"**, **"data subject"**, **"supervisory authority"** and **"data processor"** shall have the meanings ascribed to them in the Applicable Data Protection Law.

1.2 An entity **"Controls"** another entity if it: (a) holds a majority of the voting rights in it; (b) is a member or shareholder of it and has the right to remove a majority of its board of directors or equivalent managing body; (c) is a member or shareholder of it and controls alone or pursuant to an agreement with other shareholders or members, a majority of the voting rights in it; or (d) has the right to exercise a dominant influence over it pursuant to its constitutional documents or pursuant to a contract; and two entities are treated as being in **"Common Control"** if either controls the other (directly or indirectly) or both are controlled (directly or indirectly) by the same entity.

2. Status of the parties

2.1 The type of Personal Data processed pursuant to this DPA and the subject matter, duration, nature and purpose of the processing, and the categories of data subjects, are as described in Annex 1.

2.2 Each of Customer and Nexmo warrant in relation to Personal Data that it will (and will procure that any of its staff and/or sub-processors will) comply with the Applicable Data Protection Law. As between the parties, Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3 In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties hereby acknowledge and agree that either (i) Customer is the Data Controller and Nexmo is the Data Processor, or (ii) Customer is a Data Processor and Nexmo is Customer's sub-processor. Accordingly, Nexmo agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPA.

3. Nexmo obligations

3.1 With respect to all Personal Data, Nexmo warrants that it shall:

(a) only process the Personal Data in order to provide the Services and shall act only in accordance with this DPA and Customer's written instructions as represented by the Agreement and this DPA, except to the extent prohibited by applicable law, in which case Nexmo will notify Customer to the extent allowed;

(b) as soon as reasonably practicable upon becoming aware, inform Customer if, in Nexmo's opinion, any instructions provided by Customer under Clause 3.1(a) infringe the Applicable Data Protection Law;

(c) implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks that are presented by the processing, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data. Such measures include, without limitation, the security measures set out at: https://www.nexmo.com/security-information;

(d) take reasonable steps to ensure that only authorised personnel have access to such Personal Data and that any persons whom it authorises to have access to the Personal Data are under obligations of confidentiality;

(e) as soon as reasonably practicable upon becoming aware, notify Customer of any actual or alleged incident of unauthorised or accidental disclosure of or access to any Personal Data by any of its staff, sub-processors or any other identified or unidentified third party (a **"Security Incident"**);

(f) promptly provide Customer with reasonable cooperation and assistance in respect of the Security Incident and all information in Nexmo's possession concerning the Security Incident, including the following:

(i) the possible cause and consequences of the Security Incident;

(ii) the categories of Personal Data involved;

(iii) a summary of the unauthorised recipients of the Personal Data; and

(iv) the measures taken by Nexmo to mitigate any damage;

(g) not make any announcement about a Security Incident (an **"Incident Notice"**) without:

(i) the prior written consent from Customer; and

(ii) prior written approval by Customer of the content, media and timing of the Incident Notice;

(iii) unless required to make a disclosure or announcement by applicable law;

(h) provide reasonable assistance to Customer to enable Customer to comply with its obligations to respond to any Data Subject Requests received in connection with this DPA, including by notifying Customer of any Data Subject Requests Nexmo receives relating to Customer's obligations under the Applicable Data Protection Law;

(i) as soon as reasonably practicable following, and in any event within sixty (60) days of, termination or expiry of the Agreement or completion of the Services, Nexmo will delete all Personal Data (including copies thereof) processed pursuant to this DPA other than to the

extent Nexmo retains Personal Data to comply with its legal obligations or is otherwise permitted to do so under Applicable Data Protection Law;

(j) provide such assistance to Customer as Customer reasonably requests (taking into account the nature of processing and the information available to Nexmo) in relation to Customer's obligations under the Applicable Data Protection Law with respect to:

(i) data protection impact assessments (as such term is defined in the GDPR);

(ii) notifications to the supervisory authority under the Applicable Data Protection Law and/or communications to data subjects by Customer in response to any Security Incident; and

(iii) Customer's compliance with its obligations under the GDPR with respect to the security of processing.

4. Sub-processing

4.1 Customer grants a general authorisation (a) to Nexmo to appoint other members of the Nexmo Group as sub-processors and (b) to Nexmo and other members of the Nexmo Group to appoint third-party data centre operators and outsourced support and service providers as sub-processors to support the performance of the Services.

4.2 Nexmo will maintain a list of sub-processors at www.nexmo.com/gdpr/sub-processors and the site will contain a mechanism to subscribe to notifications of new sub-processors. Customer shall subscribe, and if Customer subscribes, Nexmo shall provide details of any change in sub-processors as soon as reasonably practicable but not less than ten (10) days prior to any such change. If Customer has a reasonable objection to any new or replacement sub-processor, it shall notify Nexmo of such objections in writing within ten (10) days of the addition or replacement and the parties will seek to resolve the matter in good faith. If Nexmo is able to provide the Services to Customer in accordance with the Agreement without using the sub-processor and decides in its discretion to do so, then Customer will have no further rights under this clause 4.2 in respect of the proposed use of the sub-processor. If Nexmo requires use of the sub-processor and is unable to satisfy Customer as to the suitability of the sub-processor or the documentation and protections in place between Nexmo and the sub-processor within sixty (60) days from Customer's notification of objections, Customer may terminate the Agreement by providing written notice to Nexmo and termination shall be effective upon receipt by Nexmo.

4.3 Nexmo will ensure that any sub-processor it engages to provide the Services on its behalf in connection with the Agreement does so only on the basis of a written contract which imposes on such sub-processor terms substantially no less protective of Personal Data than those imposed on Nexmo in this DPA (the **"Relevant Terms"**). Nexmo shall procure the performance by such sub-processor of the Relevant Terms and shall be liable to Customer for any breach by such sub-processor of any of the Relevant Terms.

4.4 Customer acknowledges that in order to send communications through the Services, Nexmo may need to transmit Customer's communications through existing telecommunications networks, operated by companies bound to comply with applicable telecommunications and privacy laws but who may not all have direct contracts with Nexmo and/or Customer. Customer hereby instructs Nexmo to transmit the communications through existing telecommunications networks as necessary to provide the Services and acknowledges and agrees that such telecommunications networks are not considered sub-processors under either the DPA or the Agreement.

5. Audit and records

5.1 Nexmo shall, in accordance with the Applicable Data Protection Law, make available to Customer such information in Nexmo's possession or control as Customer may reasonably request and

Nexmo can reasonably provide with a view to demonstrating Nexmo's compliance with the obligations of data processors under the Applicable Data Protection Law in relation to its processing of Personal Data.

5.2 Customer may exercise its right of audit under the Applicable Data Protection Law, through Nexmo providing:

(a) an audit report in respect of its data centre not older than 18 months by a registered and independent external auditor demonstrating that Nexmo's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard (such as ISO 27001 or SSAE 16 II SOC1 and SOC2); and

(b) additional information in Nexmo's possession or control to an EU supervisory authority when it requests or requires additional information in relation to the data processing activities carried out by Nexmo under this DPA.

6. Data transfers

6.1 To the extent Nexmo processes Personal Data in a country outside the EEA that is not deemed adequate in accordance with Art. 45 of the GDPR, the parties agree that the standard contractual clauses approved by the EU authorities under Applicable Data Protection Law and set out in Annex 2 will apply in respect of that processing and Nexmo will comply with the obligations of the 'data importer' in the standard contractual clauses and Customer will comply with the obligations of 'data exporter'.

6.2 Customer acknowledges that the provision of the Services under the Agreement may require the processing of Personal Data by sub-processors in countries outside the EEA from time to time.

6.3 If, in the performance of this DPA, Nexmo transfers any Personal Data to a sub-processor (which shall include without limitation any affiliates of Nexmo) and without prejudice to clause 4 where such sub-processor will process the Personal Data outside the EEA, Nexmo shall in advance of any such transfer ensure that a mechanism to achieve adequacy in respect of that processing is in place, such as:

(a) the requirement for Nexmo to execute or procure that the third party execute on behalf of Customer the standard contractual clauses approved by the EU authorities under the Applicable Data Protection Law and set out in Annex 2;

(b) the requirement for the third party to be certified under the Privacy Shield framework; or

(c) the existence of any other specifically approved safeguard for data transfers (as recognised under the Applicable Data Protection Law) and/or a European Commission finding of adequacy.

6.4 The following terms shall apply to the standard contractual clauses set out in Annex 2:

(a) Customer may exercise its right of audit under Clause 5(f) of the standard contractual clauses as set out in, and subject to the requirements of, clause 5.2 of this DPA; and

(b) Nexmo may appoint sub-processors as set out in, and subject to the requirements of, clauses 4 and 6.3 of this DPA.

7. General

7.1 If Customer determines that a Security Incident must be notified to any supervisory authority and/or data subjects and/or the public or portions of the public pursuant to the Applicable Data Protection Law, Customer will notify Nexmo before the communication is made and supply Nexmo with copies

of any written documentation to be filed with the supervisory authority and of any notification Customer proposes to make (whether to any supervisory authority, data subjects, the public or portions of the public) which directly or indirectly references Nexmo, its security measures and/or role in the Security Incident, whether or not by name. Subject to Customer's compliance with any mandatory notification deadlines under the GDPR, Customer will consult with Nexmo in good faith and take account of any clarifications or corrections Nexmo reasonably requests to such notifications and which are consistent with the GDPR.

7.2 The parties acknowledge that Nexmo does not have a direct relationship with Customer's end users whose personal data Nexmo may process in connection with Customer's use of the Services. Customer shall be responsible for ensuring its end users are provided adequate notice of Nexmo's processing activities, including with respect to Customer end user data for which Nexmo acts as a controller (if any), and shall make available to end users a privacy notice that fulfills the requirements of Applicable Data Protection Law. Nexmo agrees to provide Customer with sufficient information regarding its processing activities to allow Customer to provide such notice.

7.3 This DPA is without prejudice to the rights and obligations of the parties under the Agreement which shall continue to have full force and effect, including any limitations and exclusions on liability contained therein which shall apply to this DPA as if fully set forth herein. In the event of any conflict between the terms of this DPA and the terms of the Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data.

7.4 This DPA sets out all of the terms that have been agreed between the parties in relation to the subjects covered by it. Other than in respect of statements made fraudulently, no other representations or terms shall apply or form part of this DPA.

7.5 Members of the Customer Group may enforce the terms of this DPA directly against Nexmo where they are controller in respect of Personal Data under Applicable Data Protection Law.

7.6 This DPA shall be governed by and construed in accordance with the law of the country or territory which governs the Agreement and the dispute resolution and/or jurisdiction provisions of the Agreement shall also apply to this DPA.

Annex 1

Details of the processing activities of Personal Data

(a) The Personal Data comprises:

(i) data that relates to Customer's relationship with Nexmo, including the names and/or contact information of individuals authorized by Customer to access Customer's Nexmo account and billing information of individuals that Customer has associated with its Nexmo account;

(ii) data processed by Nexmo for the purposes of transmitting, distributing or exchanging Customer Content; including data used to trace and identify the source and destination of a communication, such as individual data subjects' telephone numbers, data on the location of the device generated in the context of providing the Services, and the date, time, duration and the type of communication; and

(iii) content exchanged by means of use of the Services, such as text, message bodies, voice and video media, images, and sound

(b) The duration of the processing will be: the duration of the Services under the Agreement (to the extent applicable);

(c) The processing will comprise activities relating to: (i) the provision of the Services (which may include the detection, prevention and resolution of security, fraud and technical issues); (ii) responding to support requests; (iii) compliance with applicable laws, rules and regulations relating to the Services; (iv) the protection of the rights, property and safety of Customer, its customers, end users, Nexmo and others; and (v) fulfilling and enforcing rights and obligations under the Agreement;

(d) The purpose of the processing is the provision of the Services pursuant to the Agreement as initiated by the Customer from time to time;

(e) Data subjects may include Customer's customers, employees, suppliers and end users about whom data is provided to Nexmo via the Services by (or at the direction of) the Customer or by Customer's end users.

Annex 2

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Data transfer agreement between:

Customer who has executed the above DPA,
the "data exporter"

And

Nexmo Inc., 23 Main Street, Holmdel, NJ 07733 USA
Tel: +44 203 865 9460; email: privacy@nexmo.com
the "data importer";
each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) **"personal data"**, **"special categories of data"**, **"process/processing"**, **"controller"**, **"processor"**, **"data subject"** and **"supervisory authority"** shall have the same meaning as in EU Data Protection Laws 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) the **"data exporter"** means the controller who transfers the personal data;

(c) the **"data importer"** means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of EU Data Protection Laws 95/46/EC;

(d) the **"sub-processor"** means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) the **"applicable data protection law"** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established; and

(f) **"technical and organisational security measures"** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4.1(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of EU Data Protection Laws 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub- processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by

operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Co-operation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5.1(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

This agreement has been entered into on the date shown at the beginning of the first page of this agreement.

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Customer who has executed the above DPA,

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Nexmo Inc., a global provider of cloud communication services

Data subjects

The personal data transferred concern the following categories of data subjects (please specify): as set out on Annex 1 to the DPA

Categories of data

The personal data transferred concern the following categories of data (please specify): as set out on Annex 1 to the DPA

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify): None

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify): as set out on Annex 1 to the DPA

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

See https://www.nexmo.com/security-information for information and details regarding technical and organizational measures implemented by Nexmo.

Nexmo DPA

Final Audit Report 2019-06-24

Created:	2019-06-22
By:	Nicole Schiereck (nicole.schiereck@vonage.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAadBcWtqBpwDhmzx7BMhhQsQ4ThL72fM6

"Nexmo DPA" History

Web Form created by Nicole Schiereck (nicole.schiereck@vonage.com)
2019-02-13 - 08:53:11 GMT

Web Form filled in by Plüher (klaus.plueher@solutiness.com)
2019-06-22 - 07:06:50 GMT- IP address: 88.130.62.192

User email address verification waived
2019-06-22 - 07:06:52 GMT- IP address: 88.130.62.192

Document emailed to Nicole Schiereck (nicole.schiereck@vonage.com) for signature
2019-06-22 - 07:06:52 GMT

Email viewed by Nicole Schiereck (nicole.schiereck@vonage.com)
2019-06-24 - 09:53:42 GMT- IP address: 66.249.93.41

Document e-signed by Nicole Schiereck (nicole.schiereck@vonage.com)
Signature Date: 2019-06-24 - 12:35:24 GMT - Time Source: server- IP address: 94.1.186.14

Signed document emailed to Nicole Schiereck (nicole.schiereck@vonage.com) and Plüher (klaus.plueher@solutiness.com)
2019-06-24 - 12:35:24 GMT

Vereinbarung zur Auftragsverarbeitung
gemäß Art. 28 DSGVO

zwischen

Solutiness GmbH

Alte Breisacher Str. 14 a

79112 Freiburg

- Verantwortlicher - nachstehend Auftraggeber genannt -

und

root360 GmbH
Beethovenstraße 35
04107 Leipzig

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand des Auftrags ist die Bereitstellung der Dienstleistung „Managed Cloud Hosting" im Rahmen des mit dem Auftragsverarbeiter vereinbarten Umfangs

(2) Dauer

☑ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum .....

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Gegenstand des Auftrags ist die Bereitstellung der Dienstleistung „Managed Cloud Hosting" im Rahmen des mit dem Auftragsverarbeiter vereinbarten Umfangs.

Der Zugriff von Mitarbeiter der 24/7-Bereitschaft des Auftragnehmers zur Sicherstellung der Serverfunktionen findet in Ausnahmefällen außerhalb von den Betriebsstätten des Auftragsverarbeiters statt. Der Auftraggeber erteilt hierzu seine ausdrückliche Genehmigung.

Der Auftragnehmer verpflichtet sich, die Zugriffe im Rahmen dieser Ausnahmen auf das notwendige Maß zu begrenzen und angemessene Sicherheitsmaßnahmen für die technischen Zugriffe zu implementieren.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Als Datenschutzbeauftragte(r) ist beim Auftragnehmer
Herr Frank Hillmer,
SIKKER Datenschutz & Compliance
Emilienstraße 15
04107 Leipzig
bestellt.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau

- ☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);
- ☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);
- ☑ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO);
- ☐ wird hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);
- ☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☑ Personenstammdaten
- ☑ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☑ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☑ Kundenhistorie
- ☑ Vertragsabrechnungs- und Zahlungsdaten
- ☑ Logfiles mit IP-Adressen
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ ...

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☑ Kunden
- ☑ Kunden der Kunden
- ☑ Interessenten
- ☑ Abonnenten
- ☑ Beschäftigte
- ☑ Beschäftigte der Kunden
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ ...

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO **[Einzelheiten in Anlage 1].**

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
Der Auftraggeber stimmt der Beauftragung der in Anlage 2 genannten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

- ☐ ist nicht gestattet;
- ☑ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
- ☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren), eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Haftung

(1) Auftraggeber und Auftragnehmer haften gegenüber Betroffenen entsprechend der Vorschriften in Art. 82 DS-GVO.

(2) Individuelle Vertragsstrafen über die vereinbarte Haftung hinaus werden nicht vereinbart.

12. Sonstiges

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

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

(3) Es gilt das Recht der Bundesrepublik Deutschland.

	Leipzig 23.5.2018
Ort, Datum	Ort, Datum
Unterschrift (Auftraggeber)	Unterschrift (Auftragnehmer)

Anlage 1 – Technisch-organisatorische Maßnahmen

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

- Der Zugang nur über Hausschließanlage möglich (kein öffentlicher Zugang).
- Eine protokollierte Schlüsselregelung regelt den Zutritt über das manuelle Schließsystem.
- Es sind Sicherheitsschlösser in Einsatz.
- Es ist eine Videoüberwachung der Eingänge außerhalb der Geschäftszeiten aktiv.
- Wachpersonal und Reinigungsdienste werden sorgfältig ausgewählt.

Zugangskontrolle

- Notwendige Benutzerrechte werden explizit zugeordnet.
- Eine Authentifizierung erfolgt mit Benutzername und Passwort und/oder Private-Public-Key-Verfahren.
- Die Verwendung von eindeutige persönliche Benutzerprofilen ist zwingend vorgegeben.
- Ein Einsatz von Anti-Viren-Software und Firewalls findet auf allen Clients Anwendung. Alle Client-Datenträger sind verschlüsselt.
- Freigegebene Sicherheitspatches werden regelmäßig allen Clients sowie Servern eingespielt.
- Eine Fernwartung ist nur zu Wartungszwecken und nicht außerhalb der Geschäftszeiten zugelassen.
- Desktops werden automatisch entsprechend der Richtlinie zum "Nutzung von Telekommunikation (Telefon, E-Mail, Internet) und PC/Laptop" gesperrt und der Zugang zum BIOS mit einem separaten Passwort gesichert.
- Entsprechend einer Passwortrichtlinie werden Vorgaben u.A. zu Passwortlänge, Passwortkomplexität und Änderung bei vermutetem Missbrauch angewendet.

Zugriffskontrolle

Die Einschränkung der Zugriffsmöglichkeit des Berechtigten ausschließlich auf die seiner Zugriffsberechtigung unterliegenden Daten wird durch folgende Maßnahmen gewährleistet:

- Dienste welche personenbezogene Daten verarbeiten werden verschlüsselt.
- Die Anzahl der Administratoren auf das „Notwendigste" reduziert.
- Eine Fernwartung ist nur zu Wartungszwecken und nicht außerhalb der Bürozeiten von 8:00 - 18:00 Uhr zugelassen.
- Zur Dokumentvernichtung wird ausschließlich ein Aktenvernichter der Sicherheitsstufe 3 eingesetzt.

Trennungskontrolle

- Eingesetzte Dienste werden in verschiedene System-Komponenten getrennt (Funktionstrennung).
- Durch softwareseitigen Ausschluss (Mandantentrennung) und eine Separierung durch getrennte Verschlüsselung wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden (Bsp. Trennung von Produktiv- und Testsystemen).

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Beim Einsatz von Kundendatenbeständen für IT-Softwaretests werden personenbezogene Daten (z.B. E-Mail-Adressen) durch eine Phantasieadresse ersetzt - pseudonymisiert.

- Für eine Aufbewahrung nach Ablauf der Löschfrist sind personenbezogene Daten zu anonymisieren bzw. pseudonymisieren.

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

- Die Weitergabe von Daten erfolgt über dedizierten Standleitungen bzw. verschlüsselten VPN-Tunneln.
- Eine E-Mail-Transport-Verschlüsselung wird, sofern beidseitig verfügbar, eingesetzt.
- Der Zugang zu datenverarbeitenden Systemen erfolgt ausschließlich über verschlüsselte Verfahren z.B. OpenSSH oder SSL.
- Eine Bereitstellung von personenbezogen Daten erfolgen über verschlüsselte Verbindungen wie sftp, OpenSSH oder https.
- Beim physischen Transport erfolgt ein sorgfältige Auswahl von Transportpersonal und -fahrzeugen.
- Unbefugtes Lesen, Kopieren Verändern oder Entfernen von Daten bei der Übertragung sowie beim physichen Transport von Datenträgern oder Datentransfer wird durch eine Datenverschlüsselung verhindert.

Eingabekontrolle

- Die Eingabe, Änderung und Löschung von Daten wird protokolliert.
- Eine Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten ist durch die Verwendung individueller Benutzernamen (nicht Benutzergruppen) realisiert.
- Die Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten erfolgt grundsätzlich auf Basis des Minimalprinzips durch den Dienst-Administrator.

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

- Die Speicherung von Kundendaten erfolgt in den dafür vorgesehenen Rechenzentren der Auftragnehmer. Eine Speicherung außerhalb dieser ist nicht vorgesehen.
- Die Sicherung personenbezogene Daten erfolgt nach Datensicherungskonzepts bzw. entsprechend zusätzlicher Anforderungen. Die Sicherungsvorgänge werden regelmäßig kontrolliert.
- Es stehen Feuerlöscher nach den gesetzlichen Vorgaben zur Verfügung.
- Zur unabhängigen Stromversorgung im Störfall ist eine USV implementiert.
- Es ist eine Videoüberwachung der Eingänge außerhalb der Geschäftszeiten aktiv.
- Ein Notfallplan regelt die Maßnahmen zur Aufrechterhaltung des Geschäftbetriebes.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management

- Alle Mitarbeiter werden zur Einhaltung der internen Richtlinie zur Datenschutzorganisation geschult und verpflichtet.
- Darüber hinaus finden regelmäßige Sensibilisierung der Mitarbeiter statt.
- Die Richtlinie zur Datenschutzorganisation schließt regelmäßige interne Audits zur Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen ein.

- Die Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz steht allen Mitarbeitern bei Bedarf zentral zur Verfügung.
- Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt.

Incident-Response-Management

- Der Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde) ist dokumentiert.
- Die Dokumentation Sicherheitsvorfällen und Datenpannen erfolgt nachvollziehbar über ein Ticketsystem.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

- Die Verarbeitung dem Verarbeitungszweck entsprechenden personenbezogene Daten erfolgt durch explizit konfigurierte Systeme.
- Es wird sichergestellt, dass Voreinstellungen der Systemlieferanten dahingehend angepasst werden, dass eine Verarbeitung von personenbezogene Daten nach dem Minimalprinzip nur den notwendigen Personen zugänglich sind und verarbeitet werden.

Auftragskontrolle

- Die Auswahl des Auftragnehmers erfolgt unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit). Das schließt Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen ein.
- Es erfolgt eine schriftliche Weisung an den Auftragnehmer (z.B. durch Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln).
- Der Auftragnehmer hat Datenschutzbeauftragten bestellt sofern rechtlich erforderlich.
- Eine Überprüfung des Auftragnehmers und seiner Tätigkeiten findet im Rahmen der regelmäßigen internen Audits statt.

Anlage 2 – Liste der Subauftragnehmer

Der Auftraggeber genehmigt den Einsatz folgender weiterer (Unter-)Auftragsverarbeiter:

Name/Firma /Anschrift (Unter-) Auftrags-verarbeiter	Ort/e der Datenverarbeitung (Land, Ort)	Art der Daten-verarbeitung	Rechtsgrundlage bei Drittlands-übermittlung
Amazon Web Services, Inc.	Frankfurt, DE Dublin, IE	Cloud Hosting	EU Standard-Vertragsklauseln, EU-U.S. Privacy Shield

Änderung der Subauftragnehmer root360 GmbH

zwischen

Solutiness GmbH

Alte Breisacher Str. 14a

79112 Freiburg

- Verantwortlicher - nachstehend Auftraggeber genannt -

und

root360 GmbH
Beethovenstraße 35
04107 Leipzig

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Entsprechend des bestehenden Auftragsdatenverarbeitungsvertrages informieren wir als Auftragnehmer über Änderungen der Sub-Auftragnehmer (Anlage 2 im ADVV).

Der Auftraggeber stimmt hiermit der Änderung der Sub-Auftragnehmer (Stand 31.05.2018) entsprechend der Anlage 2 zu.

Freiburg 31.5.2018

Ort, Datum

Unterschrift (Auftraggeber)

Anlage 2 – Liste der (Unter-)Auftragsverarbeiter (Stand 31.05.2018)

Der Auftraggeber genehmigt den Einsatz folgender weiterer (Unter-)Auftragsverarbeiter:

Name/Firma /Anschrift (Unter-) Auftrags-verarbeiter	**Ort/e der Datenverarbeitung (Land, Ort)**	**Art der Daten-verarbeitung**	**Rechtsgrundlage bei Drittlands-übermittlung**
Amazon Web Services, Inc. bis einschließlich 30.6.2018	Frankfurt, DE Dublin, IE	Cloud Hosting	EU Standard-Vertragsklauseln EU-U.S. Privacy Shield https://www.privacyshield.gov/participant?id=a2zt0000000TOWQAA4
AWS Europe, Luxemburg ab einschließlich 01.07.2018	Frankfurt, DE Dublin, IE	Cloud Hosting	
FRESHWORKS INC., USA	US	Ticketsystem, Chat: Kommunikations-daten, Fall-beschreibungen	EU Standard-Vertragsklauseln EU-US Privacy Shield https://www.privacyshield.gov/participant?id=a2zt0000000GnbQAAS,
Zestia Ltd., England	UK, US	CRM System: Kommunikations-daten, Vertragsstamm-daten, Kundenhistorie	EU Standard-Vertragsklauseln

Anlage 5 – Weisungsberechtigte Personen

Weisungsberechtigte Personen des Auftraggebers sind:

_____

Weisungsempfänger beim Auftragnehmer sind:

Regina Keller-Sylla, Geschäftsführung, Solutiness GmbH, Böttgerstraße 17, 89231 Neu-Ulm, Deutschland

Anlage 6 – Belehrung auf das Datengeheimnis (Muster)

Siehe anliegend (Solutiness Merkblatt.pdf)

Solutiness GmbH

Merkblatt zum Datenschutz und zur Wahrung von Geschäftsgeheimnissen

I. Datenschutz

Aufgrund Ihrer Aufgabenstellung gilt für Sie das Datengeheimnis nach Datenschutzgrundverordnung (DSGVO) und Bundesdatenschutzgesetz (BDSG). Das Datenschutzrecht regelt im Wesentlichen folgende Punkte:

1. Datengeheimnis

Das Datenschutzrecht untersagt den bei der Datenverarbeitung Beschäftigten, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Hierzu zählen insbesondere auch die unbefugte Erhebung sowie die unbefugte Weitergabe von Daten.

Dieses Datengeheimnis ist von Ihnen auch nach Beendigung Ihrer Tätigkeit in unserem Unternehmen weiterhin zu beachten.

2. Zweck des Datenschutzrechts

Zweck des Datenschutzrechts ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

3. Zulässigkeit der Verarbeitung

Daten natürlicher Personen dürfen nur erhoben, verarbeitet oder genutzt werden, wenn und soweit
- der Betroffene eingewilligt hat
- eine Rechtsvorschrift dies erlaubt oder anordnet oder
- das Gesetz selbst die Verarbeitung gestattet.

Nach der EU-Datenschutzgrundverordnung (DSGVO) und dem BDSG ist das Erheben, Speichern oder Nutzen personenbezogener Daten insbesondere zulässig, wenn und soweit
- dies zur Zweckbestimmung des Vertragsverhältnisses mit dem Betroffenen gehört, z.B. im Rahmen eines Anstellungsvertrages oder zur Abwicklung eines Kundenauftrages, oder
- dies den Zwecken vorvertraglichen Maßnahmen auf Anfrage des Betroffenen dient, beispielsweise bei Bewerbungen oder Angeboten.

Im Übrigen ist eine Verarbeitung nur unter strengen Voraussetzungen und unter Beachtung der schutzwürdigen Interessen des Betroffenen gestattet. Dies gilt auch und gerade für die Übermittlung personenbezogener Daten an Dritte.

Bei der Verarbeitung von personenbezogenen Daten (wie auch von Geschäftsgeheimnissen) in der Öffentlichkeit ist eine Einsichtnahme durch Dritte zu verhindern. Sofern Sie mit z.B. mit einem Notebook auf Reisen arbeiten, ist dieses stets so zu bedienen, dass andere keine Einsicht nehmen können, und darf nicht unbeaufsichtigt bleiben.

4. Rechte der Betroffenen

Der Betroffene kann seine Rechte nur wahrnehmen, wenn er weiß, dass Daten über ihn gespeichert werden. Deshalb ist der für die Datenverarbeitung Verantwortliche gesetzlich verpflichtet, ihn zu benachrichtigen. Die Pflicht zur Benachrichtigung entfällt, wenn der Betroffene auf andere Weise Kenntnis von der Speicherung erhält, was in der Regel bei Vertragsverhältnissen gelten kann.

Jeder Betroffene hat grundsätzlich ein Recht auf unentgeltliche Auskunft über die zu seiner Person gespeicherten Daten. In bestimmten Fällen kann er eine Berichtigung, Sperrung oder Löschung seiner Daten verlangen.

5. Bußgeld- und Strafvorschriften des Datenschutzrechts

§ 42 BDSG Strafvorschriften

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht

und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.
(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.
(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Strafverfahren gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

Art. 83 DSGVO Allgemeine Bedingungen für die Verhängung von Geldbußen
(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.
(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:
a) Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
d) Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;
e) etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;
f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;
g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
h) Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;
i) Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;
j) Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und
k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.
(3) Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.
(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:
s) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;
b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;
c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.
(5) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:
a) die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;
b) die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;
c) die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;

d) alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;
e) Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.
(6) Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 58 Absatz 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.
(7) Unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 2 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.
(8) Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde gemäß diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.
(9) Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, kann dieser Artikel so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie die von Aufsichtsbehörden verhängten Geldbußen haben. In jeden Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. Die betreffenden Mitgliedstaaten teilen der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften mit, die sie aufgrund dieses Absatzes erlassen, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften.

II. Verschwiegenheit

1. Regeln zur Verschwiegenheit

Im Rahmen Ihrer Tätigkeit können Ihnen darüber hinaus Geschäfts- und Betriebsgeheimnisse unseres Unternehmens oder von Geschäftspartnern unseres Unternehmens bekannt werden. Über diese ist Verschwiegenheit zu wahren. Dies gilt grundsätzlich auch nach Beendigung Ihres Arbeitsverhältnisses.

Beachten Sie stets die Gefahren, die in den Fällen von Betriebsspionage und Geheimnishehlerei für unser Unternehmen bzw. unsere Kunden entstehen können. Die Verletzung fremder Geheimnisse kann zu empfindlichen Schadensersatzansprüchen sowie zu strafgerichtlichen Verurteilungen führen.

2. Strafvorschriften des UWG

Eine Reihe von zivil- und strafrechtlichen Vorschriften befassen sich mit Delikten, die die Pflicht zur Verschwiegenheit und den Schutz von Geschäftsgeheimnissen betreffen. Beispielhaft seien Ihnen im Folgenden die Normen des UWG zur Kenntnis gebracht, die aber nur einen Teil der einschlägigen Strafnormen enthalten.

§ 17 Verrat von Geschäfts- und Betriebsgeheimnissen
(1) Wer als eine bei einem Unternehmen beschäftigte Person ein Geschäfts- oder Betriebsgeheimnis, das ihr im Rahmen des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während

der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, mitteilt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen,
1. sich ein Geschäfts- oder Betriebsgeheimnis durch
a) Anwendung technischer Mittel,
b) Herstellung einer verkörperten Wiedergabe des Geheimnisses oder
c) Wegnahme einer Sache, in der das Geheimnis verkörpert ist,
unbefugt verschafft oder sichert oder
2. ein Geschäfts- oder Betriebsgeheimnis, das er durch eine der in Absatz 1 bezeichneten Mitteilungen oder durch eine eigene oder fremde Handlung nach Nummer 1 erlangt oder sich sonst unbefugt verschafft oder gesichert hat, unbefugt verwertet oder jemandem mitteilt.
(3) Der Versuch ist strafbar
(4) In besonders schweren Fällen ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter
1. gewerbsmäßig handelt,
2. bei der Mitteilung weiß, dass das Geheimnis im Ausland verwertet werden soll, oder
3. eine Verwertung nach Absatz 2 Nr. 2 im Ausland selbst vornimmt.
(5) Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.
(6) § 5 Nr. 7 des Strafgesetzbuches gilt entsprechend.

§ 18 Verwertung von Vorlagen
(1) Wer die ihm im geschäftlichen Verkehr anvertrauten Vorlagen oder Vorschriften technischer Art, insbesondere Zeichnungen, Modelle, Schablonen, Schnitte, Rezepte, zu Zwecken des Wettbewerbs oder aus Eigennutz unbefugt verwertet oder jemandem mitteilt, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.
(3) Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.
(4) § 5 Nr. 7 des Strafgesetzbuches gilt entsprechend.

§ 19 Verleiten und Erbieten zum Verrat
(1) Wer zu Zwecken des Wettbewerbs oder aus Eigennutz jemanden zu bestimmen versucht, eine Straftat nach § 17 oder § 18 zu begehen oder zu einer solchen Straftat anzustiften, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs oder aus Eigennutz sich bereit erklärt oder das Erbieten eines anderen annimmt oder mit einem anderen verabredet, eine Straftat nach § 17 oder § 18 zu begehen oder zu ihr anzustiften.
(3) § 31 des Strafgesetzbuches gilt entsprechend.
(4) Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.
(5) § 5 Nr. 7 des Strafgesetzbuches gilt entsprechend.

Ort und Datum der Belehrung sowie der Aushändigung dieses Schriftstückes:

Unterschrift des Arbeitnehmers