

**AGB (Allgemeine Geschäftsbedingungen)
über die Verarbeitung personenbezogener Daten
im Auftrag nach Art. 28 Abs. 3 DSGVO
im Rahmen der Dienstleistungen des Portals Terminland**

1. Gesetzliche Grundlagen der Auftragsdatenverarbeitung

Das Erfordernis zur Formulierung dieses Vertrages ist im datenschutzrechtlichen Teil in dem mit Ihnen geschlossenen Dienstleistungsvertrag nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO) zu entnehmen.

Wenn Sie als Unternehmen personenbezogene Daten (z. B. Kontaktdaten Ihrer Kunden, etc.), die Ihrem Unternehmen zuzurechnen sind, durch ein fremdes Dienstleistungsunternehmen (Auftragnehmer) verarbeiten lassen wollen, so bleiben Sie datenschutzrechtlich dennoch weiterhin in der Verantwortung. Sie haben den Auftragnehmer sorgfältig auszuwählen und dabei besonderes Augenmerk auf seine Sicherheitsvorkehrungen zu legen. Der Auftrag ist schriftlich zu erteilen und muss insbesondere klare Aussagen über folgende Teilbereiche enthalten:

1. Spezifizierung der ausgelagerten Datenerhebung, Datenverarbeitung und Datennutzung
2. Darstellung der beim Auftragnehmer tatsächlich realisierten technisch und organisatorischen Maßnahmen zur Datensicherheit sowie
3. Festlegung etwaiger Unterauftragsverhältnisse (Subunternehmer) und
4. Kontrollrechte

Der Auftragnehmer darf die Daten nur im Rahmen der sogenannten „Weisungen“ des Auftraggebers verarbeiten bzw. nutzen. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen Datenschutzvorschriften verstößt, so hat er den Auftraggeber unverzüglich darauf hinzuweisen.

2. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

Mit den Dienstleistungen des Portals Terminland kann der Auftraggeber seinen Kunden eine Online-Terminbuchung zur Verfügung stellen. Mit der Online-Terminbuchung können seine Kunden mit dem Auftraggeber über das Internet einen Termin vereinbaren.

Weiterhin kann der Auftraggeber mit dem Online-Terminmanager von Terminland seine Kundentermine über das Internet verwalten. Optional hat der Auftraggeber zusätzlich die Möglichkeit, sich kostenfrei in den Branchenführer des Terminland-Portals eintragen zu lassen.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der

Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Die Laufzeit des Vertrages richtet sich nach der Laufzeit des Hauptvertrages.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

3. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

Nähere Beschreibung, ggf. Verweis auf Leistungsverzeichnis als Anlage etc.

Die Leistungen ergeben sich aus dem Hauptvertrag.

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DSGVO):

Der Auftragnehmer ist mit der Bereitstellung und Einrichtung der Online-Terminbuchung beauftragt.

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DS-GVO):

- Personenstammdaten: Vor- und Nachname, vollständige Anschrift
- Kommunikationsdaten: Telefonnummern, E-Mail-Adressen
- für den Termin zusätzlich notwendige Informationen (z. B. Kfz-Kennzeichen, Gesundheitsdaten, etc.)

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO):

Der Kreis der Betroffenen umfasst Kunden/Interessierte des Auftraggebers, die den Online-Terminplaner nutzen.

4. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in

einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Der Auftraggeber kann weisungsberechtigte Personen benennen.

Weisungsempfänger beim Auftragnehmer sind:

Mitarbeiter des Terminland-Supports

Für Weisung zu nutzende Kommunikationskanäle:

Per E-Mail: support@terminland.de
Per Telefon: 0611 - 9 777 3-18
Per Fax: 0611 - 9 777 3-33
Postalisch: Schulz & Löw Consulting GmbH
Geschäftsbereich Terminland
Kreuzberger Ring 44a
65205 Wiesbaden

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für

keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

Der Auftragnehmer führt eine jährliche Kontrolle des Rechenzentrums durch.

Das Ergebnis der Kontrollen ist zu dokumentieren.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO).

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO).

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen:

- Fernmeldegeheimnis
- Sozialgeheimnis
- Berufsgeheimnisse nach § 203 StGB
- Bankgeheimnis

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS- GVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Beim Auftragnehmer ist als Beauftragter für den Datenschutz

Herr Thomas Gutte

Thomas Gutte Datenschutzberatung

Hochstraße 2

65195 Wiesbaden

0611 – 71186990

Thomas.Gutte@gutte-datenschutzberatung.de

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DSGVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragnehmer die in Anlage 1 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO).

8. Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Das im Anhang **Verzeichnis der allgemeinen technisch-organisatorischen Maßnahmen** beschriebene Verzeichnis der technischen und organisatorischen Maßnahmen stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT- Systeme und Verarbeitungsprozesse beim Auftragnehmer dar. Einmal im Jahr findet eine Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung statt.

Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DSGVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber mitzuteilen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen.

Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10. Haftung

Auf Art. 82 DSGVO wird verwiesen.

11. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anlage 1

Unterauftragnehmer

Name	Anschrift	Tätigkeitsgegenstand
Equinix GmbH	Postfach 101121 60011 Frankfurt am Main	Server-Housing
FAX.de GmbH	Bei den Kämpen 10 21220 Seevetal-Ramelsloh	Fax-Versand
GTC TeleCommunication GmbH	Zimmermannstr. 15 70182 Stuttgart	Fax-Versand
GOYYA Marketing KG	Radeberger Str. 26 01099 Dresden	SMS-Versand

Anlage 2

Verzeichnis der allgemeinen technisch-organisatorischen Maßnahmen

nach Artikel 32 Absatz 1 DSGVO und den Hinweisen der Arbeitsgruppe der unabhängigen Datenschutzaufsichtsbehörden (Düsseldorfer Kreis)

Angaben zum Verantwortlichen/Auftragsverarbeiter

Firma	Schulz & Löw Consulting GmbH Geschäftsbereich Terminland
Straße	Kreuzberger Ring 44a
PLZ/Ort	65205 Wiesbaden
Telefon	0611 - 9 777 3-18
E-Mail-Adresse	support@terminland.de
Internet-Adresse	www.terminland.de
Gesetzliche/r Vertreter	Hartwig Schulz
Datenschutzbeauftragter	Thomas Gutte Thomas Gutte Datenschutzberatung
Telefon	0611 – 71186990
E-Mail-Adresse	Thomas.Gutte@gutte-datenschutzberatung.de
Straße (* nur bei Externen)	Hochstraße 2
PLZ/Ort (* nur bei Externen)	65195 Wiesbaden

Verzeichnis der allgemeinen technisch-organisatorischen Maßnahmen	
1 Pseudonymisierung	<ul style="list-style-type: none"> ▪ Es werden keine Echtdaten für Testumgebungen verwendet. ▪ Termine, die in der Vergangenheit liegen, können entsprechend den Anforderungen des Auftraggebers automatisch anonymisiert werden. Dabei werden die Persönlichen Daten in dem Termin gelöscht und die sonstigen Angaben wie Datum, Uhrzeit bleiben bestehen.
2 Verschlüsselung	<ul style="list-style-type: none"> ▪ Verschlüsselungsmethoden werden stets auf dem aktuellen Stand der Technik gehalten ▪ Mobile Datenträger werden auf dem Transportweg stets verschlüsselt ▪ Der Zugriff auf das Terminland-System erfolgt über eine verschlüsselte SSL-Verbindung
3 Vertraulichkeit	<ul style="list-style-type: none"> ▪ Die Terminland-Server befinden sich in einem Rechenzentrum der Firma Equinix. Der Zugang zu dem Rechenzentrum ist nur für autorisierte Mitarbeiter nach vorheriger Anmeldung möglich. ▪ Jeder Mitarbeiter muss sich bei einem Besuch zunächst beim Pförtner anmelden und wird dort in eine Besucherliste eingetragen, in der alle Besuche dokumentiert werden. ▪ Die Räumlichkeiten des Rechenzentrums sind mit einem Zutrittskontrollsystem mit Videoüberwachung ausgestattet. ▪ Termindaten müssen für den Support von dem Kunden explizit freigeschaltet werden, damit der Support diese einsehen kann. ▪ Sensible Daten können in der E-Mail-Kommunikation maskiert oder ausgeblendet werden. ▪ Es bestehen Vorgaben für Länge und Komplexität von Kennwörtern, die nach Möglichkeit technisch erzwungen werden ▪ Terminland verfügt über eine Benutzerverwaltung mit Kennwortschutz. Bei mehr als 10 Falscheingaben des Kennworts wird der Benutzer gesperrt. Die Sperre kann nur durch einen Administrator aufgehoben werden. ▪ Ein Benutzer kann in Terminland mit einem Gültigkeitszeitraum versehen werden. ▪ Des Weiteren verfügt Terminland über eine differenzierte Berechtigungsverwaltung pro Benutzer. Lese- und Schreibrechte können getrennt pro Terminplan vergeben werden. Weiterhin können funktionale Rechte pro Benutzer festgelegt werden. ▪ Es existieren abgestufte Schließkreise mit unterschiedlichen Zutrittsberechtigungen im Rechenzentrum ▪ Die Terminland-Server befinden sich in einem abgeschlossenen Serverschrank. ▪ Zugriffsmöglichkeiten auf Daten werden auf das erforderliche Maß beschränkt
4 Integrität	<ul style="list-style-type: none"> ▪ Die Erfassung und Änderung von Terminen wird protokolliert. Ebenso werden Änderungen an den Einstellungen des Systems protokolliert. ▪ Änderungen an der Terminland-Software werden versioniert. ▪ Produktiv-, Demo- und Testsysteme sind als solche gekennzeichnet.

Verzeichnis der allgemeinen technisch-organisatorischen Maßnahmen	
5 Verfügbarkeit	<ul style="list-style-type: none"> ▪ Die Server von Terminland stehen in einem ISO 27001 und ISO 9001-2008 zertifiziertem Rechenzentrum der Firma Equinix. Die Einhaltung der geforderten Sicherheitsstandards zur Gewährleistung der Verfügbarkeit werden regelmäßig und nachweislich überprüft. ▪ Die Serverhardware ist u. a. redundant ausgelegt. Festplatten und Netzteile sind mit einer n+1-Redundanz ausgelegt. ▪ Es erfolgt ein tägliches Backup der Daten. Die Aufbewahrung des Backups erfolgt räumlich getrennt. ▪ Virenschutz und Firewall-Systeme werden stets aktuell gehalten ▪ Für Systeme mit hohen Verfügbarkeitsanforderungen existieren Stand-By-Systeme ▪ Patches werden zeitnah eingespielt ▪ Daten werden täglich vollumfänglich gesichert ▪ Es werden regelmäßig Rücksicherungstests durchgeführt ▪ Für wichtige IT-Systeme existiert ein SLA-Monitoring
6 Belastbarkeit	<ul style="list-style-type: none"> ▪ Für wichtige IT-Systeme werden ausreichend Ressourcen zur Verfügung gestellt
7 Physischer oder technischer Zwischenfall	<ul style="list-style-type: none"> ▪ Es bestehen Datensicherungs-Konzepte ▪ Für wesentliche Geschäftsprozesse existieren entsprechende Notfallkonzepte und Business-Impact-Analysen ▪ Ein Prozess für den Umgang mit Incidents ist definiert
8 Verfahren zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM	<ul style="list-style-type: none"> ▪ Es gelten folgende Datenschutz-Management-Grundsätze: <ul style="list-style-type: none"> ○ Datenschutz ist Aufgabe des gesamten Unternehmens ○ Es werden datenschutzfreundliche Technologien eingesetzt, wo immer das möglich und wirtschaftlich ist ○ Die IT-Sicherheit muss auf dem aktuellen Stand der Technik sein ▪ Wenn immer das erforderlich ist, werden die eingesetzten Verfahren einer dokumentierten Datenschutz-Folgeabschätzung unterzogen, bestehend aus: <ul style="list-style-type: none"> ○ Schutzbedarfsfeststellung ○ Risikoanalyse ○ Sicherheitskonzept ▪ Weisungen von Kunden im Rahmen der Auftragsverarbeitung werden kundenbezogen dokumentiert. ▪ Ausgeführte Tätigkeiten im Rahmen der Auftragsverarbeitung werden kundenbezogen dokumentiert. ▪ Alle Mitarbeiter werden regelmäßig geschult, um die Einhaltung der Vorschriften der DSGVO und die Einhaltung von Weisungen sicherzustellen. Es erfolgen regelmäßig Nachschulungen. ▪ Es erfolgt ein jährliches Datenschutzaudit durch den externen Datenschutzbeauftragten. ▪ Datenschutzvorfälle werden stets dokumentiert und ausgewertet.