# Technische und organisatorische Maßnahmen des Auftragnehmers (TOM)

## Datenschutzbeauftragter des Auftragnehmers

Der Datenschutzbeauftragte des Auftragnehmers ist:

Andreas Bethke
Papenbergallee 34
25548 Kellinghusen

Fon. +49 48 22 36 63 000
Fax. +49 48 22 36 63 333
Mob. + 49 17 93 21 97 88
http://www.b3-unternehmensgruppe.de

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DS-GVO:

## 1 Zutrittskontrolle

**Der Auftragnehmer verwehrt Unbefugten den Zutritt zu den Büro-, Server- und Archivräumen. Dies geschieht durch:**

- Zutrittskontrollsystem/ Zutritt nur für autorisierte Mitarbeiter mittels eines so genannten „Batch“ und jeweils unter Beachtung nachfolgender Grundsätze: Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen über ihre Identität und Anschrift,in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten, darüber, wie er seine Rechte ausüben kann, und über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.
- Rücknahme von Zugangsmittel (Batch) erfolgt nach Ablauf der Berechtigung und wird von einem Mitarbeiter/einer Mitarbeierin des Vertriebsinnendienstes schriftlich nachgehalten.
- Die Türsicherung erfolgt in Bonn und Hamburg in den Geschäftsräumen mittels eines Sicherheitsschlosses.
- Die Einlasskontrolle erfolgt jeweils am Empfang durch persönliche Kontrolle. Fremde Besucher haben sich einzutraten und werden bei den Besuchen persönlich zu den betreffenden Räumen begleitet. Sofern in den Räumen datenschutzrelevante Informationen einsehbar sind, erfolgt eine persönliche Begleitung des Besuchers.

- Im Alarmfall ist das Gebäude unverzüglich von allen Mitarbeitern zu verlassen. Die Türen sind sowohl in den Büroräumen, als auch in den Rechenzentren selbstschließend, so dass auch nach Verlassen der Räume sichergestellt ist, dass kein unberechtigter Zutritt durch Dritte erfolgen kann.
- Der Zutritt zum Gebäude ist durch Türschlösser gesichert und zusätzlich durch ein so genanntes Batch-System (elektronischer Eingangschip). Die Überwachungseinrichtung der Rechenzentren verfügt ferner über eine Alarmanlage und Videoüberwachung (24/7) unter Beachtung der DS-GVO-Normen. Der Remotezugiff auf die Rechenzentren ist nur ausgewählten Mitarbeiter der Technik gestattet, welche mittels eines gesondert gesicherten virtuellen VPN-Tunnelzugriffs auf die Rechenzentren zugreifen können.

**Besonderheiten:**

## 2 Zugangskontrolle

**Der Auftragnehmer verhindert, dass EDV-Systeme von Unbefugten genutzt werden können. Dies geschieht durch:**

- Es wird ein Kennwortverfahren angewendet (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts), mit welchem sichergestellt wird, dass Passwörter die Mindestanforderungen an die Sicherheit erfüllen. Die Erteilung erfolgt für den IT-Bereich (PC, Drucker, sonstige Hardwareumgebung für die Office-IT durch die Schwestergesellschaft in Berlin – nexnet GmbH, dort durch den Leiter der IT-Abteilung). Für den TK-Bereich erfolgt die Erteilung durch den Leiter der Technik in Hamburg).
- Die Passwörter unterliegen genauen Sicherheitsvorgaben. Die Einzelheiten regelt die Passwort-Richtlinie der dtms GmbH (z.B. Mindestlänge 8 Zeichen, deren Einhaltung technisch überprüft und erzwungen wird). Ferner wird sichergestellt, dass nur Mitarbeiter der dtms GmbH zu den Bereich Zugriff erhalten, welche für ihre Arbeit erforderlich sind. Diese wird durch eine entsprechende Rechtevergabe in der Office-IT und im TK-Bereich sichergestellt.
- Ein Passwortwechsel wird alle 3 Monate erzwungen, indem der Mitarbeiter aufgefordert wird, sein Passwort zu ändern. Erfolgt dies nach wiederholter Aufforderung nicht, wird der Zugang gesperrt.
- Ebenso werden externe USB-Schnittstellen gesperrt und nur für Mitarbeiter freigeschaltet, die aufgrund ihrer beruflichen Tätigkeit dieses Medium benötigen. Der Umgang mit mobilen Geräten ist im Detail in der Richtlinie für mobile Geräte der dtms GmbH geregelt. Personenbezogene Daten dürfen auf mobilen Datenträgern nicht gespeichert werden.
- Die IT-Systeme im Bereich der Office-IT und im Bereich der Telekommunikation sind mittels einer Firewall vor Viren und Schadsoftware geschützt. Hierdurch werden unberechtigte Zugriffe erkannt und entsprechend unterbunden. Im Bereich des E-Mail-Zugangs werden die eingehenden E-Mails auf Viren und Schadsoftware geprüft und erforderlichenfalls in einem Quarantäne-Bereich abgelegt.
- Neben der vorstehend beschriebenne Firewall und dem Virenscanner verfügt die dtms GmbH zusätzlich noch über einen so genannten Schnittstellenschutz
- Es erfolgt die Sperrung des Benutzerkontos nach drei fehlgeschlagenen Anmeldeversuchen.

- Die PC im Bereich der IT- und TK sind durch automatische, passwortgeschützte Bildschirm- und Rechnersperre gesichert
- Es erfolgt eine eindeutige Zuordnung von Benutzerkonten zu den Benutzern
- Sensible Systeme, insbesondere Serversysteme sind nur als Administrator nutzbar
- Die Übertragung von personenbezogenen Daten erfolgt nur im Netzwerk der Unternehmung (SSH, VPN) und somit gesichert.
- Der Zugriff auf das firmeninterne VPN ist nur über zertifikatsbasierte Authentifizierung möglich. Die Vergabe der Authentifizierungen ist in der IT-Richtlinie der dtms GmbH geregelt.
- Die Vernichtung von nicht mehr erforderlichen Datenträgern erfolgt mittels kontrollierter Vernichtung durch ein qualifiziertes Entsorgungsunternehmen
- Bei Ausscheiden eines Mitarbeiters/einer Mitarbeiterin hat der/die Betroffene alle Zugangsberechtigungen unverzüglich mit Ausscheiden zurückzugeben.

**Besonderheiten:**

## 3 Zugriffskontrolle

**Der Auftragnehmer gewährleistet, 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. Dies geschieht durch:**

- Die Office-IT stellt nach Vorgabe der Geschäftsführung sicher, dass eine differenzierte Berechtigungen (z.B. in Form von Profilen, Rollen, Transaktionen, Objekten) erteilt wird. Die Mitarbeiter haben nur Zugriff auf Bereich innerhalb der IT, welche für ihre jeweilige Tätigkeit erforderlich und geboten sind. Diese Berechtigungen werden jeweils zyklsich einer Kontrolle unterzogen. Die genauen Vorgaben regelt die IT-Richtlinie der dtms GmbH.
- Die Auswertungen, Kenntnisnahme, Veränderung, Löschung von personenbezogenen Daten erfolgen kontrolliert und werden protokolliert
- Es erfolgt eine automatische Sperre auf IT-Systeme, sofern eine mehrmalige fehlerhafte Authentifizierung vorgenommen wurde
- Vermeidung der Konzentration von Funktionen – Funktionstrennungvon Administratorentätigkeit auf unterschiedliche qualifizierte Personen
- Bei Ausscheiden eines Mitarbeiters/einer Mitarbeiterin hat der/die Betroffene werden alle Zugangsberechtigungen unverzüglich mit Ausscheiden gesperrt.

**Besonderheiten:**

## 4 Weitergabekontrolle

**Der Auftragnehmer gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist. Dies geschieht durch:**

- Es erfolgt eine Verschlüsselung bei der Datenübertragung mittels SSH oder SSL bzw.je nach Anwendung auch durch eine Tunnelverbindung (VPN = Virtual Private Network)
- Die Schnittstellen von PCs sind vor dem Zugriff und der Koppelung durch unbefugte nicht autorisierte Hardwäre und ander technische Geräte geschützt.
- Bei dem Datenaustrauch wird die Übertragung standardmäßig mittels Transportprotokolle (SSL) gesichert.
- Im Falle von Heimarbeit wird die Datenübertragung im vorgenannten Sinne verschlüsselt; eine Übertragung von Daten ist ausschließlich durch eine Tunnelverbindung möglich
- Die datenschutzgerechte Entsorgung von Papier- und Datenträger erfolgt durch ein hierfür qualifiziertes Unternehmen

**Besonderheiten:**

## 5 Eingabekontrolle

**Der Auftragnehmer gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dies geschieht durch:**

- Die Eingabe wer Daten in die Systeme eingibt erfolgt durch Protokollierungs- und Protokollauswertungssysteme. In sensiblen Bereichen ist erkennbar von welchem PC mit welcher Zugriffsberechtigung die Daten eingegeben, geändert oder gelöscht wurden. Zugriff auf die jeweiligen Protokollen haben für den Bereich der Office-IT der Leiter der Offlice-IT und dessen Stellvertreter/in und die Geschäftsführer, für den Bereich der in der Telekommunikation verwendeten IT der/die Leiter/in Technik und deren/dessen Stellvertreter sowie die Geschäftsführer.
- Sowohl im Bereich der Office-IT als auch im Telekommunikationsbereich gilt das Berechtigungskonzept der dtms GmbH (IT-Richtlinie der dtms GmbH)
- Durch das Berechtigungskonzept ist sichergestellt, dass der Zugriff von Mitarbeitern auf erforderliche Daten nur im Rahmen seiner jeweiligen Funktion im Unternehmen erfolgt und nur in dem Umfang, die für seine Tätigkeit im Unternehmen erforderlich und geboten ist.
- Berechtigungsvergaben auf schützenswerte Ressourcen werden nachhvollziehbar nur durch hierführ autorisierte Personen beantragt und vergeben

**Besonderheiten:**

## 6 Auftragskontrolle

**Der Auftragnehmer gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers und zur Erfüllung des vertraglich definierten Verwendungszweckes verarbeitet werden. Dies geschieht durch:**

- Sicherheitskonzept gemäß § 166 TKG (als **Anlage 6** beiliegend)
- Verpflichtung von Mitarbeitern auf das Datengeheimnis
- Verarbeitung der Daten erfolgt in der Europäischen Union und im Europäischen Wirtschaftsraum

- Vorliegen eines Vertrages zur Auftragsdatenverarbeitung gemäß § 32 DS-GVO

**Besonderheiten:**

# 7 Verfügbarkeitskontrolle

**Der Auftragnehmer gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Dies geschieht durch:**

- Backup-Verfahren / regelmäßige Sicherungskopien
- Überwachung der Computersystem
- Einsatz von unterbrechungsfreier Stromversorgung (USV) und Notstromaggregaten im Rechenzentrum. Vorhandensein von Klima- und Brandmeldeanlage sowie Überspannungsfilter
- Getrennte Aufbewahrung
- Ständig aktualisierte/r Virenschutz/Firewall
- Notfallplan

**Besonderheiten:**

# 8 Pseudonymisierung, Speicherung, Löschung

### 8.1. Allgemeine Verarbeitungsgrundsätze

Das System der dtms GmbH ist auf die Einhaltung der allgemeinen Grundsätze der DS-GVO ausgerichtet. Die folgenden Grundsätze sind einzuhalten.

#### 8.1.1. Erlaubnisvorbehalt und Zweckbindung

Daten dürfen von dtms GmbH bzw. dem Zugriffsberechtigten nur verarbeitet werden, wenn
- dies für den konkreten Zweck **gesetzlich erlaubt** ist
- oder der Endkunde **eingewilligt** hat (**Erlaubnisvorbehalt**).

Eine **Datenverarbeitung für einen bestimmten Zweck ist deshalb nur zulässig**,
- wenn dies in diesen (dem TKG entsprechenden) **Handlungsanweisungen vorgesehen** ist oder
- der **Endkunde** in diese konkrete Datenverarbeitung **wirksam eingewilligt** hat. In diesem Fall ist jeweils im Einzelfall zu prüfen, ob eine ausreichende schriftliche (Art. 7 DS-GVO) oder ausreichende elektronische Einwilligungserklärung des Kunden vorliegt.

Hierbei ist insbesondere das **Zweckbindungsgebot** zu beachten. Eine gesetzliche Erlaubnis zur Datenverarbeitung oder die Einwilligung des Endkunden gilt nur für den konkreten Zweck, den die gesetzliche Erlaubnis oder die Einwilligung des Endkunden ausdrücklich vorsieht. Für die Verarbeitung der Daten für weitere Zwecke ist dem entsprechend ein neuer Erlaubnistatbestand (gesetzliche Erlaubnis oder die Einwilligung des Endkunden) erforderlich. Bei der

konkreten Verarbeitung von Daten ist deshalb auch immer noch zu prüfen, ob die gesetzliche Erlaubnis oder die Einwilligung den vorgesehenen Verarbeitungszweck umfasst.

### 8.1.2. Koppelungsverbot

Die Angebote von dtms GmbH sowie die Angebote der Diensteanbieter beachtet das Koppelungsverbot. Den Betroffenen muss es effektiv frei stehen, in weitere Datenverarbeitung zum Zwecke der Werbung (der Dtms oder der Diensteanbieter) einzuwilligen oder diese Einwilligung zu verweigern.

### 8.1.3. Datenvermeidung und Datensparsamkeit

Das Angebot von dtms GmbH richtet sich an den Zielen der Datenvermeidung und Datensparsamkeit aus, da standardmäßig nur die CLI und/oder die IP-Adresse sowie die zur Abrechnung erforderlichen Daten der Endkunden sowie die erforderlichen Daten der Dienstekunden erhoben werden.

### 8.1.4. Unterrichtung

Die Dienstekunden werden in den AGB sowie in den weiteren u.a. im Internet erhältlichen Informationen über Art, Umfang, Ort und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten unterrichtet.

Die Endkunden werden durch die Diensteanbieter sowie insbesondere ihre TNB informiert. Gestaltungsrechte (z.B. bez. EVN bei der Abrechnung) sind gegenüber dem Teilnehmernetzbetreiber auszuüben und werden von diesem beachtet, auch soweit die Dienste der Diensteanbieter abgerechnet werden.

### 8.1.5. Datenübermittlung

Die Datenübermittlung an Dritte ist nach den nachfolgenden Ablaufplänen an den gesetzlichen Erfordernissen ausgerichtet (z.B. Abrechnung, Übermittlung an Überwachungsbehörden). Eine über die gesetzlichen Erlaubnistatbestände hinausgehende **Weitergabe** von personenbezogenen Daten an **Dritte** ist ohne ausdrückliche Einwilligung der Kunden **nicht zulässig**.

### 8.1.5 Einbindung Dritter

Eine Einbindung Dritter bei der Erhebung und Verarbeitung personenbezogener Daten darf nur aufgrund einer Rechtsgrundlage im Sinne des Datenschutzrechts (TKG) oder aufgrund einer Einwilligung des Betroffenen erfolgen (Verbot mit Erlaubnisvorbehalt [Ziffer 2.1 des Datenschutzkonzepts]).

Eine Einbindung Dritter ist demnach möglich, wenn

- für die Tätigkeit des Dritten eine **gesetzliche Zulässigkeitsregelung des TKG, insbesondere § 9 ff TDDDG**, eingreift oder
- mit dem Dritten eine **Vereinbarung über die Auftragsdatenverarbeitung nach Maßgabe der DS-GVO** geschlossen wurde.

Die Voraussetzungen sind vor der Einbindung in Datenverarbeitung zu prüfen.

### 8.1.6. Besondere Verarbeitungstatbestände

**Vorgabe der Verarbeitungsabläufe**

Das nachfolgende **Datenschutzkonzept** orientiert sich an den Datenverarbeitungsabläufen, wie sie bei der Realisierung der Dienste entstehen und vorzunehmen sind.
**Die folgenden Vorschriften und Regelungen sind zwingend einzuhalten.**

## 8.2. Erhebung der Bestandsdaten des Diensteanbieters im Falle eines Vertragsschlusses

Sofern es durch die Verbindung zu einem **Vertragsschluss** werden die folgenden **Daten des** Dienstekunden zusätzlich zu erheben und zu speichern:

1. Name, Adresse und die dem Dienstekunden zugeteilten Rufnummer(n) bzw. die zu realisierenden Rufnummern bzw. Dienste und ggf. Portierungsdaten. Es sind entweder die dem Dienstekunden von einem anderen Anbieter bereits zugeteilten Rufnummern zu erheben und/oder aber Rufnummern zuzuteilen (im Folgenden „DA-Rufnummern“).
2. Sonstige zum Aufbau und zur Aufrechterhaltung sowie zur Entgeltabrechnung notwendige Bestandsdaten soweit dies für die zukünftige Diensteerbringung und der Abrechnung erforderlich ist (z.B. Art der Dienste, Tarife, IVR-Daten, USt-ID, Steuernummer, Bankleitzahl, Kontonummer, Kontoinhaber, IBAN, BIC/SWIFT usw.).
3. Berücksichtigung des EVN-Wunsches des Endkunden an seinen Diensteanbieter durch die dtms GmbH: Wahlrecht kein EVN, Ja EVN vollständig; Form ggf. elektronisch. EVN wird nur erteilt, wenn formal „Mitnutzererklärung“ nach § 11 Abs. 2 TDDDG vorliegt.
4. Die Bestandsdaten sind nach **Beendigung des Vertrages** mit Ablauf des auf die Beendigung folgenden Kalenderjahres zu **sperren**, da eine weitere Aufbewahrung nach der AO und dem HGB für insgesamt **6 bzw. 10 Jahre** erforderlich ist. Die Daten sind hierzu für die Vertragsbearbeitung zu sperren und sind sowohl elektronisch wie auch physikalisch nur noch durch den Geschäftsführer bzw. seinen Vertreter für Zwecke nach der AO und dem HGB zugänglich und zu verarbeiten. Eine Verarbeitung für andere Zwecke ist unzulässig.
5. Auskunftserteilung über Bestandsdaten erfolgt nur nach Maßgabe der einschlägigen Gesetzes (TDDDG, TKG, DSGVO und BDSG)

## 8.3. Erhebung und Speicherung von Verkehrsdaten zur TK-Leistungserbringung

### 8.3.1. Erhebung der Verkehrsdaten

Durch dtms GmbH dürfen die folgenden **Verkehrsdaten** für die **Dauer der Verbindung** erhoben, verarbeitet und genutzt werden, soweit bzw. weil dies für die Erbringung der TK-Dienstleistungen erforderlich ist (§ 9 ff. TDDDG):

1. die **CLI** des Endkunden (Anrufer-Rufnummer/ANR) und die gewünschte Zielrufnummer(BNR) (bzw. zukünftig bei NGN IP-Adresse des ANR und BNR bzw. der CNR )

2. Beginn und Ende bzw. Beginn und Dauer der jeweiligen Verbindung nach Datum und Uhrzeit
3. ggf. soweit zur Diensterbringung erforderlich, die Art des vom Endkunden in Anspruch genommenen Telekommunikationsdienstes (erfolgt i.d.R. über die Zielrufnummer/BNR)
4. sonstige zum Aufbau und zur Aufrechterhaltung sowie zur Entgeltabrechnung notwendige Verkehrsdaten, soweit diese für die Gesprächsabwicklung erforderlich sind – hierunter fällt auch die Signalisierung der Endkunden-Rufnummer (CLIP) oder die Unterdrückung (CLIR), je nach dem, was der Endkunde fallweise wünscht. Davon unabhängig erfolgt die Signalisierung der Anrufer-Rufnummer immer auf Netzebene.

### 8.3.2. Löschung und weitere Verwendung von Verkehrsdaten nach Verbindungsende

Die vorgenannten Verkehrsdaten dürfen nach § 9 TDDDG über das **Ende der Verbindung** hinaus **nur weiter verarbeitet** oder **genutzt** werden, soweit sie **erforderlich** sind für folgende Zwecke:

1. **Abrechnungsdaten**: Erstellung der Abrechnung ggb. dem Endkunden (Offline-Billing) mit Forderungsersteinzug – im Auftrag der Diensteanbieter

2. **Abrechnungsdaten**: Reklamationsbearbeitung ggb. Diensteanbieter)

3. **Abrechnungsdaten**: Kaufmännisches Mahnwesen im Offline-Billing**.**

4. **Abrechnungsdaten**: Inkasso und gerichtliche Geltendmachung der Forderungen **Abrechnungsdaten**: Rating und Fakturierung sowie Abrechnung ggb. den Diensteanbietern

5. **Verkehrsdaten**: Missbrauchsbekämpfung und Störungserkennung und –beseitigung **Auskunftsanordnungen nach StPO und anderen Gesetzen**

6. **„Überwachung“ nach dem TDDDG und TKG**

7. **Bedarfsgerechtes Gestalten der Dienste sofern nach dem TDDDG und TKG zulässig.**

8. **Fangschaltungen** sofern nach TKG angeordnet.

Ist keine dieser Konstellationen gegeben, sind die Daten unverzüglich nach Verbindungsende zu löschen (§ 96 Abs. 1 TKG).

**Erforderliche Abrechnungsdaten (§ 9 TDDDG)**

Bei den Verbindungen zu telekommunikationsgestützten Diensten sind deshalb im Regelfall für **Abrechnungszwecke** die folgenden Daten (CDR) zu **speichern (§ 9 TDDDG)**:

- die CLI und/oder IP-Adresse der ANR
- BNR oder der angerufene CNR
- Beginn und Ende bzw. Beginn und Dauer der jeweiligen Verbindung nach Datum und Uhrzeit
- Kennzeichnung der Dienstleistung bzw. des Dienstes (erfolgt i.d.R. über die) BNR).

Die nicht zur Abrechnung erforderlichen Daten sind unverzüglich zu löschen, sofern sie nicht aufgrund einer anderen Regelung des TKG oder Fachgesetzen (z. B. StPO) zu speichern sind (gem. TDDDG und TKG).

Diese Abrechnungsdaten erhebt die dtms GmbH in ihren Switchen und sammelt diese in der zentralen Abrechnungsdatenbank. Aus dieser Datenbank exportiert die dtms GmbH die Verkehrsdaten, die für die jeweiligen Diensteanbieter angefallen sind und übermittelt diesen diese Daten mittels einer gesicherten VPN-Verbindung. Die Erlaubnis ergibt sich aus § 9 ff. TDDDG.

Zusätzlich verwendet die dtms GmbH diese Daten für die Abrechnung der eigenen Leistungen mit den Diensteanbietern einschließlich der TDG (siehe Ziffer 9) und für die weiteren in diesem Konzept erlaubten Zwecke (z.B. Störungsbeseitigung nach § 12 TDDDG).

## 9 Trennungskontrolle

**Der Auftragnehmer gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Es besteht keine Notwendigkeit zu einer physischen Trennung; eine logische Trennung der Datenträger ist ausreichend. Dies geschieht durch:**

- Sofern Daten zu verschiedenen Zwecken verarbeitet werden, wird sichergestellt, dass die Verarbeitung jeweils nur mandantenbezogen für den/die jeweils betroffene Person erfolgt. Die Systeme für die Endkundenbearbeitung verfügen über eine interne Mandantenfähigkeit und richten sich nach dem jeweiligen Zweck der Verarbeitung der personenenbezogenen Daten (Zweckbindung)
- Funktionstrennung / Produktion / Test
- Logische Trennung personenbezogener Daten verschiedener Auftraggeber
- Kennzeichung erfasster Daten (Aktenzeichen, CRM- und Abrechnungsnummer)

**Besonderheiten:**

## 10 Organisationskontrolle

**Der Auftragnehmer hat zur Überwachung, Kontrolle und Beratung bei der Umsetzung da-**

**tenschutzrechtlicher Anforderungen einen (externen) betrieblichen Datenschutzbeauftragten schriftlich bestellt. Die Beratungs- und Kontrollaufgaben werden weisungsfrei durchgeführt und Prüfungsergebnisse schriftlich dokumentiert.**

Kontaktdaten des Datenschutzbeauftragten:

Datenschutzbeauftragter des Auftragnehmers (s.o.)

Weiterhin wurden folgende Maßnahmen vom Auftragnehmer umgesetzt:

- Die mit der Datenverarbeitung betrauten Mitarbeiter*innen wurden auf das Datengeheimnis verpflichtet.
- Die mit der Datenverarbeitung betrauten Mitarbeiter*innen wurden auf ihre Pflicht zur Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse hingewiesen.
- Die mit der Datenverarbeitung betrauten Mitarbeiter/-innen wurden in Datenschutzschulungen mit den Vorschriften des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz vertraut gemacht.
- Vier-Augen-Prinzip

## 11 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Die Unternehmensleitung hat Leitlinien zum für Datenschutz und die Informationssicherheit erlassen und im Intranet für die Mitarbeiter veröffentlicht.

Die Beschäftigten werden regelmäßig zum Datenschutz geschult. Mindestens einmal im Kalenderjahr

Die Beschäftigten werden durch ihren zum vertraulichen Umgang mit personenbezogenen Daten und auf das Fernmeldegeheimnis durch ihren Arbeitsvertrag verpflichtet

Technische Maßnahmen zur Umsetzung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO) sind nicht erforderlich, da das TKG diesbezüglich abschließende und restriktivere Regelungen in Bezug auf den Umgang mit Bestands- und Verkehrsdaten trifft

Es gibt Richtlinien für Beschäftigte zum Umgang mit personenbezogenen Daten

Durch unser Fraud-Management-System wird sichergestellt, dass Datenschutzverletzungen erkannt und unverzüglich gemeldet werden

Anfragen von Betroffenen werden an einen für diesen Zweck vorgesehenen Mitarbeiter weitergeleitet, der diese Anfragen zeitnah bearbeitet und mit dem Datenschutzbeauftragten koordiniert.

Die dtms GmbH verfügt für ihre Prozesse im Rahmen derer personenbezogene Daten verarbeitet werden über entsprechende Verzeichnisse von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 und 2 DS-GVO

Die dtms hat ein Datenschutzmanagementsystem (DSMS) implementiert

## 12 Fernwartungskontrolle

**Nur zutreffend, sofern der Auftragnehmer Tätigkeiten via Fernwartungszugang ausführt:**

**Der Auftraggeber stellt durch technische und organisatorische Maßnahmen sicher, dass nur auf die für die Wartung unbedingt erforderlichen personenbezogenen Daten zugegriffen werden kann.**
**Die vom Auftragnehmer mit Wartungsarbeiten betrauten Personen sind zur Wahrung des Datengeheimnisses gemäß DS-GVO, dem TKG und – soweit einschlägig – dem BDSG verpflichtet worden. Bei Wartungsarbeiten ist sicherzustellen, dass der Zugriff auf die Systeme des Auftraggebers und die Übertragung/ Übermittlung von Daten nur in verschlüsselter, pseudonymisierter oder anonymisierter Form erfolgen kann.**

**Folgende Maßnahmen wurden vom Auftragnehmer umgesetzt:**

- Fernwartungszugriff wird über eine verschlüsselte Verbindung realisiert
- Protokollierung von Fernwartungen (Mitarbeiter, Dauer, Grund)
- Ausschluss von Fremdzugriff im Bereich des technisch möglichen

## 13. Standort/e der Datenverarbeitung

Die von dem Auftragnehmer ausgeführte Datenverarbeitung findet an folgenden Standorten statt:

Eine Veränderung der Standorte, in denen Daten des Auftraggebers verarbeitet und/ oder genutzt werden, bedarf der schriftlichen Zustimmung des Auftraggebers.

Standort der Geschäftsräume des Auftragnehmers:

- Taunusstraße 57, 55118 Mainz;
- Konrad-Zuse-Platz 5, 53227 Bonn;
- Haferweg 38, 22769 Hamburg

Standort der Rechenzentren des Auftragnehmers:

- Wendenstraße, 20537 Hamburg;
- Reuchlingstraße, 10553 Berlin;
- Gutleutstraße, 60327 Frankfurt

## 14. Verpflichtungserklärung zur Umsetzung der TOM

Der Auftragnehmer bestätigt, dass er die technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten des Auftraggebers - wie in Anlage 2 beschrieben - vor Beginn der Datenverarbeitung umgesetzt hat. Der Auftragnehmer verpflichtet sich, die Erfüllung dieser Anforderungen für die Dauer der Zusammenarbeit sicherzustellen, regelmäßig zu kontrollieren, zu dokumentieren und auf Nachfrage des Auftraggebers zur Verfügung zu stellen.

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