Die ght ist zertifiziert nach **DIN ISO 27001 ISMS**

ght GmbH
Elektronik im Verkehr
Schafhofstraße 2
90411 Nürnberg
Tel. 09 11/5 27 05-0
Fax 09 11/5 27 05-36
eM@il: kontakt@ght.de
www.ght.de

Geschäftsstelle
Nürnberg

Telematiklösungen
Datenmanagement
Tachographen + Maut
BOS-Digitalfunk
Taxiausrüstung
Tankstellentechnik
Parksysteme
Zutritt- I Zufahrtskontrollen
Videosysteme
Kassenautomaten

Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO

zum Auslesen des Massenspeichers eines digitalen Fahrtenschreibers

§ 1 Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

§ 2 Gegenstand und Dauer der Verarbeitung

(1) **Gegenstand**

Die Verarbeitung beruht auf der zwischen Auftraggeber und ght GmbH Elektronik im Verkehr vereinbarten Supportleistung zum Auslesen des Massenspeichers eines digitalen Tachographen durch einen ght-Servicetechniker vor Ort gemäß schriftlich erteiltem Auftrag, dem dieser AV-Vertrag zugehörig ist.

(2) **Dauer**

Die Laufzeit dieser Vereinbarung richtet sich nach der Dauer der beauftragten Supportleistung durch einen ght-Servicetechniker vor Ort. Das Recht zur außerordentlichen Kündigung bleibt unberührt.

§ 3 Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung

(1) **Art und Zweck der Verarbeitung**

Umfang, Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich aus der beauftragten Supportleistung vor Ort.

(2) **Art der Daten**

Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten können folgende Daten betreffen:

X Personenstammdaten
X Sonstiges
- Zugangsdaten des Kunden und seiner Bediener/Benutzer
- Fahrerdaten
- Fahrzeugdaten und Fahrzeugprofile
- Bewegungsdaten, GPS-Daten
- Aktivitäten von Fahrern und Einsatzprofile, einschließlich Lenk- und Ruhezeiten gemäß Anhang 1B der Verordnung (EG) Nr. 561/2006, Anhang 1C der Verordnung (EG) Nr. 2016/799
- Daten für die Nutzung des Services durch Benutzer
- Daten-Downloads für Fahrerkarte und Tachograph

(3) **Kategorien der betroffenen Personen**

Die Kategorie der durch die Verarbeitung betroffenen Personen umfasst:

X Kunden
X Ansprechpartner
X Mitarbeiter des Kunden, d. h. Fahrer und Benutzer des Service

§ 4 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO).

(2) 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.

(3) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

(4) Ziehen Einzelweisungen Mehrkosten nach sich, insbesondere wenn diese über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind diese dem Auftragnehmer zu vergüten.

§ 5 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikels 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten **(Anlage 1)**.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftraggebers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

Ansprechpartner: Barbara Kraus Kontaktdaten: Datenschutz@ght.de

Als Datenschutzbeauftragter ist beim Auftragnehmer bestellt:

Herr Stephan Hartinger, Coseco GmbH, Telefon: 08232 80988-70, E-Mail: datenschutz@coseco.de

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

(7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe; Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

(9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO obliegt dem Auftragnehmer eine Beweislast nach Art. 82 DSGVO, die Mitwirkungspflichten nach Art. 28 DSGVO sowie die allgemein geltenden Rechenschafts- und Transparenzpflichten nach Art. 5. Der Auftragnehmer verpflichtet sich den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner gesetzlichen Pflichten und im Hinblick auf seine Mithaftung zu unterstützen.

§ 6 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt § 5 Abs. 10 entsprechend.

(3) Der oben genannte Ansprechpartner des Auftraggebers ist für den Auftragnehmer der Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 7 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

(2) Bei der Erbringung der Unterstützungsleistungen nach Abs. 1 dem Auftragnehmer entstehenden und nachzuweisenden Aufwände und Kosten sind vom Auftraggeber zu ersetzen.

§ 8 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

Können auch konkrete Arten von Nachweisen genannt werden bzw. zum Nachweis der Einhaltung der vereinbarten Pflichten, kann der Auftragnehmer, dem Auftraggeber folgende Informationen zur Verfügung vorlegen: >> Durchführung eines Selbstaudits.

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen

Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 9 Subunternehmer

Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist bei Supportleistungen vor Ort nicht vorgesehen. Im Ausnahmefall wird die Zustimmung des Auftraggebers vorher eingeholt.

§ 10 Informationspflichten, Schriftformklausel, Rechtswahl

(1) 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.

Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

Nürnberg, 27.01.2020

Auftragnehmer:

Herbert Werthner

Geschäftsführer der ght GmbH | Elektronik im Verkehr

Anlage 1

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen ist zu reduzieren.

>> Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen, etc.

Technische und organisatorische Maßnahmen:

- Abgestufte Zutrittsregelung.
- Zutrittsrechte werden über Schlüsselregelung dokumentiert.
- Während der Geschäftszeiten ist der Empfang dauerhaft besetzt (Besucheranmeldung).
- Zutritt für Gäste (Wartungstechniker, Lieferanten, Besucher etc.) nur unter Aufsicht.

>> Zugangskontrolle

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern, etc.

Technische und organisatorische Maßnahmen:

- Es existiert eine Passwort- und Benutzerverwaltung.
- Ein vom System vorgegebener Änderungszyklus der Benutzerpasswörter an allen Computerarbeitsplätzen ist eingerichtet (Änderungszyklus).
- An Arbeitsplatzrechnern, an welchen personenbezogene Daten verarbeitet werden, sind Bildschirmschoner eingerichtet, welche nach 15 Minuten aktiviert werden und nur durch erneute Passworteingabe entsperrt werden können.
- An Terminal-Servern, an welchen personenbezogene Daten verarbeitet werden, erfolgt eine Zwangstrennung bei Inaktivität nach zwei Stunden. Ein erneutes Anmelden ist nur durch Passworteingabe möglich.

>> Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen, etc.

Technische und organisatorische Maßnahmen:

- Benutzerprofile sind mit Lese- und teilweise Schreibrechten versehen.
- Datenzugriffe werden protokolliert und im Verdachtsfall ausgewertet.
- Datenzugriffe werden über abgestufte Verzeichnisberechtigungen gewährt.

>> Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing, etc.

Technische und organisatorische Maßnahmen:

- Softwareseitiger Ausschluss (Mandantentrennung)
- Dateiseparierung
- Trennung über Zugriffsregelung (Datenbankprinzip)

>> Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Technische und organisatorische Maßnahmen:

- Als Auftragsverarbeiter trifft die ght GmbH zusätzlich zu Maßnahmen die durch den Verantwortlichen im Rahmen der Beauftragung vorgenommen werden, keine weiteren Maßnahmen zur Pseudonymisierung.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbeabsichtigte oder unbefugte Veränderung oder unrechtmäßiges oder fahrlässiges Handeln von im Auftrag verarbeiteten Daten ist zu reduzieren.

>> Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur, etc.

Technische und organisatorische Maßnahmen:

- Protokollierung der Datenübermittlungsstelle/-wege, welche im Verdachtsfall ausgewertet werden können.
- Externe Zugriffe erfolgen über VPN Clients.

>> Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Dokumentenmanagement, Protokollierung, etc.

Technische und organisatorische Maßnahmen

- Externe Zugriffe erfolgen über VPN Clients.
- Schulungsmaßnahmen für Softwarenutzung
- Zugriffs- und Änderungsprotokollierung auf Datenbankebene.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Nichtverfügbarkeit von im Auftrag verarbeiteten Daten ist zu reduzieren.

>> Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/ offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Meldewege und Notfallpläne; Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO), etc.

Technische und organisatorische Maßnahmen:

- Durchführung von stündlichen, täglichen und wöchentlichen Backups nach definiertem Backupplan
- Einsatz von USV-Geräten
- Einsatz von RAID-Systemen
- Einsatz von Hot-Standby Redundanz-Systemen
- Einsatz von Cold-Standby Redundanz-Systemen

>> Belastbarkeit der Systeme

Datenverarbeitungssysteme & – Dienste müssen auch belastbar sein. Dies bedeutet einerseits, dass etwa ein Webserver auch bei kurzfristig starker Beanspruchung durch viele gleichzeitige Anfragen zuverlässig die angeforderten Daten liefert, als auch die Fähigkeit, externen Angriffen etwa durch Hacker zu widerstehen bzw. diese zu überstehen, z.B. Skalierende Systeme, Denial of Service – Abwehrtechniken, RAID-Systeme, Virenschutz, Firewall.

Technische und organisatorische Maßnahmen:

- Es existieren Sicherheitseinrichtungen wie Firewall, Virenschutz, VPN Zugänge, Netzwerkkennungen.
- Die Firewall verfügt über Erkennungsmechanismen für DoS und DDoS Angriffe.
- Server werden virtualisiert betrieben. CPU und Speicher werden dynamisch zugewiesen.
- Alle Server werden auf RAID Systemen mit einer Fehlertoleranz von mindestens einer HDD pro RAID betrieben.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (DSGVO: Art. 32 Abs. 1 lit. ; Art. 25 Abs. 1)

Es sind Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu betreiben.

>> Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Technische und organisatorische Maßnahmen:

- Es wird keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen durchgeführt.

>> Innerbetriebliche Organisation

a. Prozesse, die zur Einhaltung der technisch- organisatorischen Maßnahmen dienen wie z.B. Interne Verhaltensregeln, Datenschutzmanagementsystem, Audits (ISO 27001) etc.

b. Prozesse der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen im IT-Bereichen wie z.B. Datensicherheitskonzept, Störfallplan, Wiederanlaufplan.

c. Einhaltung des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy by Design/Privacy by Default) z. B. Auswahl datenschutzfreundlicher Technologien bei der Beschaffung

Technische und organisatorische Maßnahmen:

a. <u>Datenschutzmanagement</u>

- Nur Mitarbeiter die auf die Einhaltung der datenschutzrechtlichen Vorgaben verpflichtet wurden, dürfen die für ihren Aufgabenbereich entsprechenden Daten verarbeiten.
- Es existieren interne Verhaltensrichtlinien sowie ein Datenschutz Handbuch.
- Alle Mitarbeiter werden in regelmäßigen Abständen (min. jährlich) zum Thema Datenschutz per E-Learning geschult und sensibilisiert.
- In einem Organigramm sowie in Stellenbeschreibungen sind Verantwortlichkeiten und Befugnisse der einzelnen Mitarbeiter festgelegt und im Unternehmen bekannt gemacht. Dieses wird in regelmäßigen Abständen von der obersten Leitung im Rahmen der ISO 9001 Zertifizierung überprüft.

b. <u>Störfallmanagement</u>

- Die Einhaltung der technisch- organisatorischen Maßnahmen werden jährlich (Audit) durch den Datenschutzbeauftragten überprüft und gegebenenfalls angepasst.

c. <u>Datenschutz durch Technikgestaltung</u>

- Auswahl datenschutzfreundlicher Technologie bei der Beschaffung
- (Fern)zugriffe erfolgen ausschließlich über verschlüsselte Verbindungen