Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen

Firma: _____

Straße und Hausnummer _____

PLZ, Ort _____

- Auftraggeber -

und

Linetec IT Solutions GmbH
Grandweg 64
22529 Hamburg

- Auftragnehmer -

1. Gegenstand des Auftrags

(1) Der Auftragnehmer wird vom Auftraggeber mit der Prüfung, Wartung und Pflege von IT-Systemen beauftragt. Dies erfolgt entweder durch einen Zugriff auf Systeme vor Ort beim Auftraggeber oder per Remote-Zugriff. Hierbei kann ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden.

(2) Die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

2. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

3. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden und dokumentierten Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(3) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

4. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, den Auftraggeber über jede Verletzung des Schutzes personenbezogener Daten gem. Art. 4 Nr. 12 DSGVO bezogen auf diese Vereinbarung nach Kenntniserlangung zu informieren und vorliegende Informationen zur Verfügung zu stellen. Eine solche Meldung ist kein Eingeständnis des Verschuldens oder der Haftung des Auftragnehmers oder dahingehend auszulegen.

(2) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich ab Kenntnis des Zugriffs mitteilen.

5. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.

(2) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

6. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist, die mindestens 14 Tage beträgt, die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören. Die Parteien gehen davon aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Weitere Prüfungen sind vom Auftraggeber unter Angabe des Anlasses zu begründen. Im Falle von Vor-Ort-Kontrollen wird der Auftraggeber dem Auftragnehmer die entstehenden Aufwände inkl. der Personalkosten für die Betreuung und Begleitung der Kontrollpersonen vor Ort in angemessenen Umfang ersetzen. Die Grundlagen der Kostenberechnung werden dem Auftraggeber vom Auftragnehmer vor Durchführung der Kontrolle mitgeteilt.

7. Unterauftragsverhältnisse

(1) Der Auftragnehmer ist berechtigt, die in der **Anlage 2** zu diesem Vertrag angegebenen Unterauftragnehmer für die Verarbeitung von Daten im Auftrag einzusetzen. Der Wechsel von Unterauftragnehmern oder die Beauftragung weiterer Unterauftragnehmer ist unter den in Absatz 2 genannten Voraussetzungen zulässig.

(2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Der Auftragnehmer wird den Auftraggeber im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen Unterauftragnehmers rechtzeitig, spätestens aber 4 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information“). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen drei Wochen nach Zugang der „Information“ zu widersprechen. Der Widerspruch kann vom Auftraggeber jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs kann der Auftragnehmer das Vertragsverhältnis mit dem Auftraggeber mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen. Der Auftragnehmer wird bei der Kündigungsfrist die Interessen des Auftraggebers angemessen berücksichtigen. Wenn kein Widerspruch des Auftraggebers binnen drei Wochen nach Zugang der „Information“ erfolgt gilt dies als Zustimmung des Auftraggebers zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers.

(3) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat, sofern der Unterauftragnehmer zur Benennung eines Datenschutzbeauftragten gesetzlich verpflichtet ist.

(4) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

(5) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 8 dieses Vertrages) des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte des Auftraggebers vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

8. Internationale Datentransfers

Der Auftraggeber erteilt dem Auftragnehmer durch diesen Vertrag die Weisung, dass personenbezogene Daten auch im Drittland verarbeitet werden dürfen, vorausgesetzt der Empfänger der personenbezogenen Daten verfügt über ein angemessenes Datenschutzniveau.

Sollte der Empfänger über kein durch Beschluss der EU-kommission angemessenes Datenschutzniveau verfügen, verpflichtet sich der Auftragnehmer zum Abschluss der EU-Standardvertragsklauseln (Controller-to-Processor) mit dem Empfänger der personenbezogenen Daten.

In diesem Fall ermächtigt der Auftraggeber den Auftragnehmer durch diesen Vertrag, besagten Standardvertrag in seinem Namen abzuschließen. Der Auftraggeber erhält hierdurch die Möglichkeit, sämtliche vertraglichen Bestimmungen gegenüber dem Datenempfänger selbst durchzusetzen. Sämtliche Empfänger personenbezogener Daten im Rahmen einer Unterbeauftragung sind in Anlage 2 dokumentiert.

9. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet.

(2) Der Auftragnehmer hat seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht und zur Vertraulichkeit verpflichtet.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

10. Home-Office Mitarbeiter

(1) Ausgewählte Mitarbeiter des Auftragsnehmers haben das Recht aus Ihren Privatwohnungen zu arbeiten.
(2) Die ausgewählten Mitarbeiter sind geschult und für Telearbeitsplätze zu speziellen Sicherheitsvorkehrungen verpflichtet die insbesondere die Wahrung der Vertraulichkeit, Datenschutz und Datensicherheit von Kundendaten beinhaltet.

11. Berufsgeheimnisträger

(1) Sofern der Auftraggeber ein Berufsgeheimnisträger i.S.d. § 203 StGB (z.B. in seiner/ihrer Funktion als Arzt, Psychologe, Rechtsanwalt, Notar, Steuerberater, Wirtschaftsprüfer etc.) ist, gilt der Auftragnehmer als IT-Dienstleister als sonstige Person, die an der beruflichen oder dienstlichen Tätigkeit mitwirkt.
(2) Der Auftragnehmer bzw. seine Erfüllungsgehilfen fallen damit ebenfalls unter die Schweigepflicht nach § 203 StGB.

12. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

13. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

14. Vergütung

Die Vergütung des Auftragnehmers wird gesondert vereinbart.

15. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 3** zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Der Auftragnehmer ist berechtigt, adäquate Alternativmaßnahmen zu implementieren, sofern das Sicherheitsniveau der Maßnahmen dabei aufrechterhalten wird. Der Auftragnehmer stellt dem Auftraggeber in diesem Zusammenhang die erforderliche Dokumentation der Änderungen und Einstellungen auf Anfrage bereit.

16. Dauer des Auftrags

(1) Der Vertrag beginnt mit Unterzeichnung und läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über die Nutzung der Dienstleistungen des Auftragnehmers durch den Auftraggeber.

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers vertragswidrig verweigert.

17. Beendigung

Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten zur Speicherung der Daten bleiben unberührt.

18. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

19. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

_____, den	_____	_____, den	_____
Ort	Datum	Ort	Datum
_____		_____	
- Auftraggeber -		- Auftragnehmer -	

Anlage 1 - Gegenstand des Auftrags

1. Der vorliegende Vertrag umfasst (ggf. im Zusammenhang mit dem Hauptvertrag) folgende Leistungen:

☐ **Wartung und Pflege der IT-Systeme des Auftraggebers**

☐ **Weitere:**

_____
_____
_____
_____
_____
_____
_____
_____

2. Art(en) der personenbezogenen Daten die im Rahmen des Vertrages Verarbeitet werden oder die Einsichtnahme nicht ausgeschlossen werden kann:

Art der personenbezogenen Daten

☐ Name, Vorname, Anrede

☐ Geburtsdaten

☐ Kontaktdaten

☐ Bank-, Finanz-, Konto-, Transaktionsdaten

☐ Abrechnungsdaten

☐ Gesundheitsdaten

☐ Mitarbeiter- / Personaldaten

☐ Ortungsdaten

☐ Videoaufzeichnungen

☐ Bilddateien, Fotos von Personen

☐ Protokolldateien mit Personenbezug

☐ IP-Adresse

☐ Auskünfte (z.B. von Auskunfteien)

☐ Straftaten, Verurteilungen

☐ Kommunikations- / Verbindungsdaten

Besondere Kategorien von personenbezogenen Daten nach Art. 9 DSGVO

☐ Rassische und/oder ethische Herkunft

☐ Politische Meinungen;

☐ Religiöse und weltanschauliche Überzeugungen

☐ Gewerkschaftszugehörigkeit

☐ Genetische Daten

☐ Biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person

☐ Gesundheitsdaten

☐ Sexualleben und/oder der sexuellen Orientierung

☐ Straftaten (einschließlich Verdachtsmomente) und Strafverfahren, Ausgang und Verurteilungen

Besonders schützenswerte Daten nach § 203 StGB, wenn ja, welche:

_____

☐ Sonstige: _____

3. Kategorien betroffener Personen

Kreis der von der Datenverarbeitung betroffenen Personen:

☐ Mitarbeiter ((einschließlich Arbeitnehmer, Leiharbeitnehmer, zur Berufsbildung beschäftigte, Praktikanten, sonstige Beschäftigte)

☐ Kunden / Interessenten

☐ Patienten, Angehörige

☐ Mitglieder (z.B. von Vereinen)

☐ Lieferanten / Dienstleister (einschließlich der Daten von deren Mitarbeitern)

☐ Berater

☐ Geschäftskontakte

☐ Webseitenbesucher

☐ Mieter

☐ Sonstige: _____

4. Weisungsberechtigte Personen des Auftraggebers

Bitte tragen Sie hier Personen ein, die weisungsbefugt sind und arbeiten an den Systemen beauftragen dürfen:

- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____

Anlage 2 - Unterauftragnehmer

Der *Auftragnehmer* nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten
(„Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende(s) Unternehmen:

- _____
  _____
  _____
- _____
  _____
  _____
- _____
  _____
  _____

Anlage 3
Technische und organisatorische Maßnahmen des Auftragnehmers

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

Datenschutzkonzept, Betroffenenrechte, Technikgestaltung und Datenschutz auf Mitarbeiterebene

Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:

- Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung ständig überwacht wird und welches anlassbezogenen und regelmäßig evaluiert wird.
- Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe & Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.
- Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet.
- Der Schutz von personenbezogenen Daten wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Auswahl von Hard- und Software berücksichtigt. Bei der Einrichtung wird entsprechend berücksichtigt, dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen Folge zu leisten. (Art. 25 DSGVO).
- Sämtliche genutzte Software, Betriebssysteme und Netzwerkgeräte werden stets auf dem aktuell verfügbaren Stand gehalten durch automatische Updates und regelmäßige Prüfung auf Fehler bei den Updates. Ebenso werden die auf allen Client-PCs, Laptops, Mobiltelefonen und Servern vorhandenen Virenschutzprogramme und Firewalls stehts auf dem aktuellen Stand gehalten.
- Mitarbeiter werden im Hinblick auf den Datenschutz auf Verschwiegenheit verpflichtet, belehrt und instruiert, als auch auf mögliche Haftungsfolgen hingewiesen. Sofern Mitarbeiter außerhalb betriebsinterner Räumlichkeiten tätig werden oder Privatgeräte für betriebliche Tätigkeiten einsetzen, existieren spezielle Regelungen zum Schutz der Daten in diesen Konstellationen und der Sicherung der Rechte von Auftraggebern einer Auftragsverarbeitung.
- Es gibt ein Ablaufkonzept bei Ein- und Austritt von Mitarbeiter im Unternehmen, welches sicherstellt, dass die an Mitarbeiter ausgegebene Schlüssel, Zugangskarten oder Codes sowie im Hinblick auf die Verarbeitung personenbezogener Daten erteilte Berechtigungen, nach deren Ausscheiden aus dem Unternehmen, bzw. Wechsel der Zuständigkeiten eingezogen, bzw. entzogen werden.
- Das Reinigungspersonal, Wachpersonal und übrige Dienstleister, die zur Erfüllung nebengeschäftlicher Aufgaben herangezogen werden, werden sorgfältig ausgesucht und es wird sichergestellt, dass es den Schutz personenbezogener Daten beachtet.

Zutrittskontrolle/Zugangskontrolle

Maßnahmen, mit denen Unbefugten der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird

- Die Datenverarbeitungsanlagen befinden sich alle, mit Ausnahme der Arbeitsplatzrechner und Mobilgeräte im Serverschrank im eigenen Gebäude.
- Der Serverschrank ist stets verschlossen und mit einem mechanischen Schloss gesichert
- Es bestehen Zutrittsregelungen für betriebsfremde Personen. Diese dürfen nur unter Aufsicht eines Mitarbeiters die Büroräume betreten.
- Das Gebäude ist durch ein manuelles Schließsystem gesichert

Zugriffskontrolle und Eingabekontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, eingegeben, gelesen, kopiert, verändert oder entfernt werden können sowie Maßnahmen, die es erlauben die Verarbeitungsvorgänge nachträglich nachzuvollziehen:

- Es gibt ein Rechtekonzept, bzw. ein Rollenkonzept, mit dem die Zugriffsberechtigungen der Mitarbeiter, Beauftragter und sonstiger Personen (z.B. Nutzer innerhalb des Systems) festgelegt werden und nur soweit reichen, wie sie für die vorgegebene Nutzung erforderlich sind.
- Protokollierung jedes einzelnen Schrittes der Datenverarbeitung, insbesondere von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten.
- Die Zugriffe der Mitarbeiter auf Daten werden protokolliert. Sofern einzelne Zugriffe nicht protokolliert werden, wird sichergestellt, dass die nachvollziehbar ist, wer auf welche Daten wann Zugriff hatte (z.B. durch Protokollierung der Softwarenutzung oder Rückschluss aus den Zugriffszeiten und dem Berechtigungskonzept).
- Datenträger werden sicher aufbewahrt.
- Es liegt ein Lösch- und Entsorgungskonzept entsprechend der DIN 66399 mit festgelegten Zuständigkeiten und Protokollierungspflichten vor. Mitarbeiter wurden über gesetzliche Voraussetzungen, Löschfristen und Vorgaben für die Datenvernichtung oder Gerätevernichtung durch Dienstleister unterrichtet.
- Die Verarbeitung von Daten die nicht gelöscht werden dürfen (z.B. in Folge der gesetzlichen Archivierungspflichten), wird durch Sperrvermerke und Aussonderung aus dem Produktivsystem eingeschränkt.
- Das Rücksetzen des Passwortes eines Benutzers des Auftraggebers erfolgt ausschließlich an die hinterlegte E-Mail des Benutzers. Lediglich auf Wunsch des

Benutzers/Auftraggebers und durch schriftliche Weisung übernimmt der Verantwortliche das Rücksetzen des Passwortes.

Weitergabekontrolle

Maßnahmen, die 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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Es werden die für die Abgabe von Datenträgern berechtigten Personen und die Empfangsberechtigten bestimmt.
- Im Fall des physischen Transports, werden sichere Transportbehälter oder Transportverpackungen gewählt, bzw. die Sicherheit der Daten durch eine persönliche Aufsicht gewährleistet, sofern diese angesichts der für die Daten bestehenden Gefahren ausreichend ist.
- Im Fall des Fernzugriffs auf Daten wird durch Protokollmaßnahmen gesichert, dass Datenübermittlungen oder Offenlegungen nachvollziehbar sind.
- Sofern erforderlich, möglich und zumutbar, werden Daten in anonymisierter Form bzw. in pseudonymisierter Form weitergegeben.

Gewährleistung der Zweckbindung/Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeiten werden können:

- Die Daten werden logisch getrennt, z.B. in Unterschiedliche Datenbanken
- Ein Übergriff durch nichtberechtigte Personen oder Prozesse wird durch ein Berechtigungskonzept verhindert.
- Im Fall pseudonymisierter Speicherung, werden die Zuordnungsschlüssel getrennt von den Daten gespeichert und gegen eine unberechtigte oder nicht vom Verarbeitungsprozess vorgesehene Verknüpfung gesichert.
- Produktiv- und Testsysteme werden getrennt.

Verfügbarkeit und Belastbarkeit

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Es werden Standardsysteme genutzt, die nicht an bestimmte Hardware gebunden sind, sodass im Notfall die Software auf jeden beliebigen Computer genutzt werden kann
- Es wird ein RAID-System genutzt, um die Ausfallsicherheit der Festplatten zu erhöhen

- Es werden Serversysteme und Dienste eingesetzt, die ein zuverlässiges und kontrolliertes Backupkonzept & Recovery-konzept bieten. Backups erfolgen täglich. Die Backups werden verschlüsselt.
- Backups werden ebenfalls für die Datenverarbeitung auf Mobilgeräten erstellt und kontrolliert. Backups erfolgen regelmäßig, mindestens wöchentlich. Die Backups werden verschlüsselt.
- Backupdatenträger werden mindestens wöchentlich für den Katastrophenfall außerhalb des Gebäudes aufbewahrt oder zumindest in einem anderen Brandabschnitt im Gebäude sicher gelagert
- Die Verfügbarkeit der Datenverarbeitungssysteme wird permanent überwacht.
- Es werden USV-Systeme eingesetzt