AUFTRAGSVERARBEITUNGSVERTRAG NACH ART. 28 ABS. 3 DS-GVO

Auftraggeber (Verantwortlicher):

Auftragnehmer (Auftragsverarbeiter):

TCC GmbH
Buchholzstr. 89-101

51469 Bergisch Gladbach

Geschäftsführer: Rolf Schiefer

1. Gegenstand und Dauer der Vereinbarung:

Der Auftrag umfasst Folgendes: (Gegenstand des Auftrags, konkrete Beschreibung der Dienstleistungen)

- Technische Administration der EDV/TK-Anlage
- Support und Service von Kommunikationssoftware

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO 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. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Dauer des Auftrags

Der Vertrag beginnt am ..... und endet am .....

oder

wird auf unbestimmte Zeit geschlossen. Kündigungsfrist ist .....

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 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

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

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DS-GVO):

- das Erheben,
- das Erfassen,
- die Organisation,
- das Ordnen,
- die Speicherung,
- die Anpassung oder Veränderung,
- das Auslesen,
- das Abfragen,
- die Verwendung,
- die Offenlegung durch Übermittlung,
- Verbreitung oder eine andere Form der Bereitstellung,
- den Abgleich oder die Verknüpfung,
- die Einschränkung,
- das Löschen oder die Vernichtung;

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

- Personendaten: Vorname, Nachname
- Adressdaten
- Kontaktdaten: Telefonnummer, E-Mail, Faxnummer, Mobilfunknummer
- Nutzungsdaten: Daten zu Kommunikationsverhalten, Nutzung von Kommunikationsanlagen
- Vertragsdaten: Vertragsstammdaten, Vertragsbeziehungen
- Schadensdaten: Daten über Ausfälle und Serviceunterbrechungen

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):

- Kunden
- Mitarbeiter
- Interessenten
- Mandanten
- Bewerber
- Partner
- Berater

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO 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

Weisungsberechtigte Personen des Auftraggebers sind:

Weisungsempfänger beim Auftragnehmer sind:

Für Weisung zu nutzende Kommunikationskanäle:

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 DS-GVO).

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 Überprüfungen in seinem Bereich durchzuführen. Das Ergebnis der Kontrollen ist zu dokumentieren.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO 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 DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an folgende Stelle des Auftraggebers weiterzuleiten:

– **Weisungsbefugter (s.o.)**

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 DS-GVO). 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 lö-

schen 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 DS-GVO).

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

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.

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

–

–

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:
Dipl.-Ing. Dragan Stanković

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 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO 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 DS-GVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, 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 diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO 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. DS-GVO 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 Auf-

tragnehmers 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 DS-GVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO 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 2 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 DS-GVO).

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

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 DS-GVO, 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.

Für die auftragsgemäße Verarbeitung personenbezogener Daten wird folgende Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt:

– BSI-Standard 200-3

Das im Anhang 1 beschriebene Datenschutzkonzept 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.

Das im Anhang 1 beschriebene Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung wird als verbindlich festgelegt.

Folgende Möglichkeiten für den Nachweis durch Zertifizierung bestehen:

Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maß- nahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). 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 DS-GVO

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, wie folgt datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen:

– BSI Baustein: „M 2.13 Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln“

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

10. Haftung

Auf Art. 82 DS-GVO 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.

Datum:

Unterschriften

Auftraggeber	Auftragnehmer

ANHANG 1 – TECHNISCH-ORGANISATORISCHE MAßNAHMEN

Festlegung der technischen und organisatorischen Maßnahmen zum Datenschutz

Beschreibung der Arbeitsplatzumgebung in den Geschäftsräumen der TCC GmbH.

1. TECHNISCHE AUSSTATTUNG / IT-INFRASTRUKTUR

Clients (fat-client, thin-client und notebook) in Niederlassungen verbinden sich über einen verschlüsselten VPN-Tunnel mit dem Rechenzentrum in Bergisch Gladbach. Durch diese Anbindung wird ein Höchstmaß an Netzwerksicherheit gewährleistet.

Die innerbetriebliche Organisation ist so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei werden insbesondere folgende Maßnahmen getroffen:

2. ZUTRITTSKONTROLLE

Maßnahmen, damit Unbefugte keinen Zutritt zu den Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden.

- Nachfolgender Personenkreis hat Zugang zu den Geschäftsräumen:
  - Besucher befinden sich stets in Begleitung/unter Aufsicht eines Mitarbeiters der TCC GmbH
  - Mitarbeiter der Kooperationspartner
  - freiberufliche Mitarbeiter, mit denen Geschäftsbeziehung bestehen
  - Gäste/Besucher/Dienstleister in Begleitung / unter Aufsicht eines Mitarbeiters der TCC GmbH
  - Innerhalb der Geschäftszeiten:
    - freiberufliche Mitarbeiter, mit denen Geschäftsbeziehung bestehen
    - Gäste/Besucher/Dienstleister in Begleitung/unter Aufsicht eines Mitarbeiters
  - Außerhalb der Geschäftszeiten:
    - Mitarbeiter des Sicherheitsdienstes
- Dokumentation, wer Schlüssel zu den Geschäftsräumen hat (Ausgabe von Schlüsseln nur gegen Empfangsquittung).
- Beschreibung wie die Zugänge zu den Geschäftsräumlichkeiten gesichert sind:
  - Haupteingänge:
    - Sicherheitsschlosssystem

        - Gegensprechanlage
    - Nebeneingänge:
        - Sicherheitsschlosssystem
- Sonstiges:
    - Einbruchmeldeanlage
    - Anbindung an Eingangstüren
    - Bewegungsmelder in Gängen und Büros
    - Die Zugänge werden auch während der Geschäftszeiten stets geschlossen gehalten; außerhalb der Geschäftszeiten ist der Zugang zu den Räumlichkeiten nur mit Schlüssel und/oder anderen Sicherungseinrichtungen möglich. Alle Außentüren sind in dieser Zeit stets abzuschließen und alle Fenster geschlossen zu halten.
    - Die Server sind in einem abgeschlossenen Rechenzentrum untergebracht. Der Zutritt wird in Listen protokolliert.
    - Notebooks sind durch geeignete Maßnahmen gegen Diebstahl geschützt. Die Mitarbeiter sind insbesondere auch verpflichtet, die Notebooks nicht im Fahrzeug zu lassen.

3. ZUGANGSKONTROLLE

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Gemeint ist hiermit im Gegensatz zur Zutrittskontrolle das Eindringen in das EDV-System seitens unbefugter Personen.

- Das Netzwerk / die Clients sind durch ein NG-Firewall-System gegenüber unberechtigten Zugriffen von außen geschützt. Eine Aktualisierbarkeit ist gegeben; es erfolgt eine regelmäßige Überprüfung auf Aktualität. Im Bereich der Hardware-Ausstattung ist eine Hardware-Firewall durch einen dezidierten Router gegeben. Es werden Desktop-Firewalls auf allen Clients eingesetzt.

- Der Zugriff auf die Client/Serverumgebung von außen ist nur über eine Verschlüsselte Kommunikation (VPN-Tunnel) möglich.
- Die Anmeldung im Netzwerk/Client darf nur mit einem gültigen Account erfolgen, die Nutzerkennung ist personifiziert.
- Für die Verwendung eines sicheren Passwortes gelten folgende Regelungen:

- Alphanumerisch-klein-groß, mindestens acht Zeichen lang, muss mindestens ein Sonderzeichen und eine Ziffer enthalten,
- darf niemanden mitgeteilt werden,
- ist mindestens alle 90 Tage zu ändern,
- Mindestgültigkeit eines geänderten Passworts 1 Tag.

- Auf allen Clients ist ein Bildschirmschoner installiert, welcher zur Reaktivierung des Systems nach 15 Minuten ein Kennwort benötigt.
- Nicht mehr benötigte Berechtigungen werden im Rahmen eines NutzerIdentifikationsmanagements (Pflege der Berechtigungen) zeitnah eingezogen / gelöscht.

4. ZUGRIFFSKONTROLLE

Maßnahmen, damit die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogen Daten zugreifen können und dass bei der Verarbeitung solche Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Auf allen Rechnersysteme ist ein Virenscanner installiert. Die Aktualisierung der Signaturen erfolgt über einen zentralen Aktualisierungsdienst.
- Alle aktive Systeme im TCC GmbH – Netzwerk werden nach Herstellerangaben auf dem aktuellstem Patch-Stand gehalten.
- Alle mobilen Arbeitsgeräte sind nach dem aktuellem Stand der Technik voll verschlüsselt.
- Die Zugriffs-/Administrationsrechte für Clients und/oder Server werden dokumentiert. Durch die Arbeitstätigkeit bedingt haben einige Techniker lokale Adminstrationsrechte auf ihren Arbeitsgeräten.
- Durch das aktivierte Berechtigungssystem ist jedem Mitarbeiter nur der Zugriff auf die im Rahmen seiner Rolle/Funktion notwendigen Verzeichnisse und Informationen möglich.
- Die Zuteilung der Berechtigungen erfolgt namentlich durch definierte Berechtigungen einer Gruppe.
- Alle anvertrauten Daten, Datenträger und Ausdrucke mit schutzwürdigem Inhalt (gemäß Datenschutzgesetz oder Geheimhaltungsvereinbarungen mit Kunden) werden unter Verschluss gehalten, wenn nicht unmittelbar damit gearbeitet wird.

- Personenbezogene Daten, die physisch oder auf Datenträger aufbewahrt werden, werden nach Geschäftsschluss in einem abschließbaren Schrank aufbewahrt.
- Die Mitarbeiter wurden auf die drei letztgenannten Punkte explizit verpflichtet.

5. WEITERGABEKONTROLLE

Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transportes oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Ein Transport von Datenträgern mit personenbezogenen Daten zu einem Aktenvernichter darf nur in geschlossenen Behältnissen und in geschlossenen Fahrzeugen durchgeführt werden, so dass kein Material verloren gehen kann.

- Grundsätzlich hat die Kommunikation personenbezogener Daten verschlüsselt zu erfolgen; der Zugriff ist derzeit nur über VPN möglich
- Webanwendungen, in denen personenbezogene Daten verarbeitet oder gespeichert werden, werden verschlüsselt; es gelten die unter Punkt 3.) definierten Zugriffskontrollen.
- Nicht mehr benötigte Datenträger und Ausdrucke werden durch einen DIN-gemäßen internen Reißwolf oder einer spezialisierten Firma (unter Verwendung von verschlossenen Sammelbehältern) so vernichten, dass eine missbräuchliche Verwendung unmöglich ist. Ausgemusterte Hardware, auf welcher personenbezogene Daten gespeichert sind oder verarbeitet wurden, werden datenschutzgerecht vernichtet.
- Die unautorisierte Weitergabe von Daten ist nicht gestattet.
- Der Versand/Übermittlung von personenbezogenen Daten erfolgt dokumentiert.
- Die Übergabe von Datenträgern mit personenbezogenen Daten hat nur mit Lieferschein/Empfangsbestätigung zu erfolgen.
- Zwischen Auftraggeber und Auftragnehmer sind feste Übertragungswege schriftlich zu vereinbaren.
- Die Nutzung von geschäftlichen PCs und Datenträgern zu privaten Zwecken jedweder Art ist untersagt.

6. EINGABEKONTROLLE

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Administrator-Aktionen werden von den Systemen der Auftraggeber in Protokolldateien mitgeschrieben.
- Datenänderungen und Datenlöschung werden ebenfalls, falls technisch möglich, in einer Änderungs-Log-Datei mitgeschrieben.
- Die Auswertung erfolgt zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage und ggf. zur Missbrauchskontrolle.

7. AUFTRAGSKONTROLLE

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Die Verarbeitung von personenbezogenen Daten der Auftraggeber erfolgt nur wenn ein schriftlicher Vertrag zur Auftragsdatenverarbeitung gem. Art 28 DSGVO vorliegt . Dieser enthält dezidierte Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers.
- Alle zugriffsberechtigten Mitarbeiter werden regelmäßig auf Datenschutz geschult. Die Schulung wird jährlich wiederholt.
- Alle zugriffsbefugten Mitarbeiter sind auf das Datengeheimnis gem. Art. 28 Abs. 3 lit b und das Fernmelde-Geheimnis nach § 88 TKG verpflichtet.
- Ein Datensicherheitskonzept im Hinblick auf die getroffenen technisch-organisatorischen Maßnahmen zum Datenschutz gem. Art. 28 DSGVO liegt vor.
- Ein Datenschutzaudit wird regelmäßig durchgeführt.
- Es werden keine Subunternehmen mit der Verarbeitung personenbezogener Daten beauftragt.

8. VERFÜGBARKEITSKONTROLLE

Maßnahmen, die sicherstellen, dass personenbezogen Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Die nachfolgenden Maßnahmen beziehen sich ausschließlich auf die personenbezogene Daten der TCC GmbH. Die personenbezogene Daten des Auftraggebers werden durch den Auftraggeber zu sichern und sind nicht Bestandteil des Auftrages.

- Es existiert ein Backup Verfahren mit regelmäßig extern sicher hinterlegten Datenträgern.
- Es existiert im Rechenzentrum eine unterbrechungsfreie Stromversorgung (USV) mit gesteuertem Herunterfahren der Systeme bei Stromausfall.
- Der Virenschutz auf den Serversystemen ist durch eine geeignete und regelmäßig aktualisierte Virenschutzsoftware und entsprechenden Hardwarekomponenten sichergestellt (aktueller Virenschutz durch laufenden Servicevertrag).
- Geeignete Archivierungsräumlichkeiten für physische personenbezogene Daten sind vorhanden.

9. TRENNUNGSGEBOT

Es ist sicherzustellen, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können. Es besteht keine Notwendigkeit zu einer physischen Trennung. Eine logische Trennung genügt. Die personenbezogene Daten des Auftraggebers befinden sich auf Systemen des Auftraggebers, auf die Mitarbeiter der TCC GmbH lediglich Zugriff haben.

- Eine Mandantenfähigkeit nach Auftraggeber ist somit nicht erforderlich.

ANGANG 2 UNTERAUFTRAGNEHMER

Firmenname	Anschrift	Unterauftragstätigkeit