Vertrag zur Auftragsverarbeitung gem. Art. 28 DSGVO

Vertrag
zwischen dem/der

.....
- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

synaforce GmbH, IT-Zentrum 1, 94544 Hofkirchen (Zentrale)
inkl. weiterer Standorte der synaforce GmbH
- Auftragnehmer - nachstehend Auftragnehmer genannt –

1. Gegenstand und Dauer des Vertrags

1.1. Gegenstand

Der Gegenstand des Vertrags ergibt sich

aus der Leistungsvereinbarung/dem SLA ..... vom .....,

auf die/das hier verwiesen wird (im Folgenden Leistungsvereinbarung) sowie alle im Zusammenhang mit der Leistungsvereinbarung stehenden ergänzenden Aufträge.

1.2. Dauer

☐ Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

Oder

☐ Der Vertrag wird für unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von ..... zum ..... gekündigt werden.

Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

1.3. Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

1.4. Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn die Parteien vereinbaren ausdrücklich etwas anderes.

2. Konkretisierung des Vertragsinhalts

2.1. Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Vertragsgegenstandes im Hinblick auf Art und Zweck der Aufgabe des Auftragnehmers:

- Art der Verarbeitung (entsprechend der Definition von Art. 4, Nr. 2 DSGVO)
- Art der personenbezogenen Daten (entsprechend der Definition von Art. 4, Nr. 1, 13, 14, 15 DSGVO)
- Kategorien betroffener Personen (entsprechend der Definition von Art. 4, Nr. 1 DSGVO)

2.2. Art der Daten
Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien oder aus öffentlichen Verzeichnissen)
- ☐ _____

2.3. Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ _____

3. Technisch-organisatorische Maßnahmen

3.1. Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorische Maßnahmen gem. Art. 32 DS-GVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung [**Anlage 1**]. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags.

3.2. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

3.3. Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber unverzüglich schriftlich in Kenntnis zu setzen.

4. Rechte von betroffenen Personen

4.1. Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4.2. Soweit vom Leistungsumfang umfasst, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

5.1. Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Als Datenschutzbeauftragter ist beim Auftragnehmer bestellt:

Herr Thomas Irlinger, Tel.: +49 (0)8545 969930, E-Mail: dsb@synaforce.com

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich mitzuteilen.

b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die berechtigterweise Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

d) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

e) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch oder einem Informationsersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

f) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

g) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrags.

h) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Artt. 33, 34 DS-GVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.

i) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zu Verfügung.

j) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen.
Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

5.2. Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DS-GVO.

6. Unterauftragsverhältnisse

6.1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

6.2. Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragnehmer) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

- ☐ Eine Unterbeauftragung ist unzulässig.

- ☐ Der Auftraggeber stimmt der Beauftragung der in [**Anlage 2**] bezeichneten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO mit dem Unterauftragnehmer zu. Die vertragliche Vereinbarung wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

Weitere, nach Vertragsschluss, beabsichtigte Auslagerungen auf Unterauftragnehmer (Ergänzungen) oder der Wechsel der gemäß [**Anlage 2**] bestehenden Unterauftragnehmer sind zulässig, soweit:

a) der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, vorab schriftlich oder in Textform anzeigt und
b) der Auftraggeber schriftlich oder in Textform der geplanten Auslagerung zustimmt und
c) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

6.3. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

6.4. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

6.5. Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Internationale Datentransfers

7.1. Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DS-GVO.

☑ Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. **([Anlage 4] entfällt in diesem Fall)**

☐ Der Auftraggeber gestattet eine Datenübermittlung in ein Drittland an die in [**Anlage 4 – muss ergänzt werden**] genannten Empfänger. In der Anlage werden, die vom Auftraggeber genehmigten Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus aus Art. 44 ff. DS-GVO im Rahmen der Unterbeauftragung spezifiziert.

7.2. Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DS-GVO verantwortlich.

8. Kontrollrechte des Auftraggebers

8.1. Der Auftraggeber ist berechtigt, einmal pro Kalenderjahr anlasslos die ordnungsgemäße Vertragserfüllung durch den Auftragnehmer zu überprüfen und entsprechende Audits auf eigene Kosten und unter Ersatz der dem Auftragnehmer durch die Überprüfung und entsprechende Audits entstehenden Kosten sowie nach vorheriger rechtzeitiger Anmeldung zu geschäftsüblichen Zeiten in angemessenem Umfang durchzuführen. Der Auftraggeber wird dabei das Interesse des Auftragnehmers an einem ungestörten Betriebsablauf wahren. Der Auftraggeber erhält in diesem Zusammenhang vom Auftragnehmer alle relevanten Informationen und Unterlagen, die zur Prüfung der ordnungsgemäßen Vertragserfüllung durch den Auftragnehmer erforderlich sind, sowie Zugang zu den Standorten, in denen die Services erbracht werden. Die Informationen werden kurzfristig, spätestens aber innerhalb von zehn (10) Arbeitstagen ab Anforderung des Auftraggebers, in Abstimmung zwischen dem Aufraggeber und dem Auftragnehmer zur Verfügung gestellt. Der Auftraggeber kann auf eigene Kosten zur Verschwiegenheit verpflichtete Dritte (z.B. Wirtschaftsprüfer oder andere kraft Berufsrechts zur Verschwiegenheit verpflichtete Dienstleister) für die Audits hinzuziehen, wobei der Auftragnehmer aus sachlichem Grund (z.B. wenn der Dritte ein unmittelbarer oder mittelbarer Wettbewerber des Auftragnehmers ist) berechtigt ist, der Hinzuziehung zu widersprechen; im Falle des Widerspruchs ist der Auftraggeber nicht zur Hinzuziehung des jeweiligen Dritten berechtigt. Der Auftragnehmer verpflichtet sich, diese Audits in angemessenem Maß zu unterstützen. Sollten sich beim Audit Mängel herausstellen, so wird der Auftraggeber den Auftragnehmer hierüber unterrichten und ihn zur Stellungnahme auffordern. Der Auftraggeber ist nicht berechtigt, eine Installation von Audit- oder Analyse-Software auf den Systemen des Auftragnehmers oder auch externen Zugriff für solche Analyse-Tools vorzunehmen oder vornehmen zu lassen. Die gesetzlichen und vertraglichen Bestimmungen über die Geheimhaltung und den Datenschutz werden durch die vorstehenden Bestimmungen weder eingeschränkt noch ausgeschlossen.

8.2. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

8.3. Der Nachweis der technisch-organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den Auftrag betreffen, kann erfolgen durch

- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragte, IT-Sicherheitsabteilung, Datenschutz- oder Qualitäts-Auditoren)
- eine geeignete Zertifizierung durch IT-Sicherheits- und/oder Datenschutzaudit (ISO27001, ISO9001, DIN EN 50600, ISAE3402).

8.4. Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, sind kostenpflichtig

9. Weisungsbefugnis des Auftraggebers

9.1. Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.

9.2. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

9.3. Weisungsberechtigte Personen sind in [**Anlage 3**] angegeben oder entsprechen den festgelegten Ansprechpartnern lt. SLA / Leistungsvereinbarung.

10. Löschung und Rückgabe von personenbezogenen Daten

10.1. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.2. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens aber mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

10. Haftung

Die Haftung ist gem. Art. 82 DSGVO und Erwägungsgrund 146 (Schadenersatz) festgelegt und geregelt.

11. Schlussbestimmungen

Änderungen und Ergänzungen dieses Vertrages einschließlich dieser Klausel, bedürfen der Wirksamkeit der schriftlichen Vereinbarung. Sollte eine Bestimmung dieses Vertrages unwirksam oder lückenhaft sein oder werden, berührt dieser Umstand die Wirksamkeit oder Vollständigkeit des Vertrages im Übrigen nicht. Die Vertragspartner werden anstelle der unwirksamen oder lückenhaften Bestimmung eine Regelung vereinbaren, die wirtschaftlich oder rechtlich den mit dem Vertrag verfolgten Zwecken und den Vorstellungen der Vertragspartner in gesetzlich erlaubter Weise am nächsten kommt.

_____, _____	Hofkirchen, _____
Ort, Datum,	
_____	_____
Unterschrift Auftraggeber	Unterschrift Auftragnehmer
_____	_____
Name in Druckbuchstaben	Name in Druckbuchstaben

Anlage 1 – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Zutrittskontrolle**
  Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.
    - Eingangstür/Zufahrtstor immer verschlossen, Zutritt nur mittels RFID-Chip oder Schließanlagenschlüssel
    - Empfang ist während der Arbeitszeiten besetzt
    - Bürotüren sind mit elektronischen Türschlössern gesichert und können nur mit entsprechender Berechtigung geöffnet werden
    - Rechenzentrum durch Sicherheitsschleuse und Stahltüren mit elektronischem Fingerprintleser gesichert
    - Gebäude durch Alarmanlage gesichert
    - Gebäude und Gelände wird per Video überwacht
    - Dokumentation und Beschreibung in SOP Zutrittskontrolle

- **Zugangskontrolle**
  Unbefugten ist die Nutzung von Datenverarbeitungssystemen zu verwehren.
    - AD-Authentifizierung an allen DV-Systemen
    - Verschlüsselung von mobilen Geräten
    - regelmäßiger Passwortwechsel mit Windows - Kennwortrichtlinie
    - Externer Zugriff ausschließlich über Zwei-Faktor-Authentifizierung

- **Zugriffskontrolle**
  Berechtigten ist ausschließlich der Zugriff auf die ihrer Zugriffsberechtigung entsprechenden Daten zu gewähren.
    - Berechtigungskonzept mit regelmäßiger Kontrolle durch internes Audit
    - Rechtesteuerung durch die Personalverwaltung
    - Dokumentation und Beschreibung in SOP Zugriffskontrolle

- **Trennungskontrolle**
  Daten die zu unterschiedlichen Zwecken erhoben wurden, müssen getrennt verarbeitet werden können.
    - Einsatz von Standardsoftware und -datenbanksystemen
    - getrennte IT-Netzwerke (Kunden, Management, Test, usw.)

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- **Weitergabekontrolle**
  Daten dürfen während der elektronischen Übertragung oder während ihres Transportes nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
    - Regelungen zur Nutzung von Internet und E-Mail
    - verschlüsselte Datenübermittlung
    - Netzwerksicherheit durch Hard- und Software Sicherheitskomponenten
    - Verschlüsselung von mobilen Geräten und Datenträgern
    - Geheimhaltungserklärung intern / extern
    - Dienstanweisung

- **Eingabekontrolle**
  Es muss feststellbar sein, ob und von wem personenbezogene Daten in DV-Anlagen eingegeben, geändert oder entfernt wurden.
    - AD-Authentifizierung an allen DV-Systemen
    - Log-Datei Erstellung mit zentraler Archivierung
    - Change Management System gem. ISO 27001
    - werktägliche Datensicherung gemäß SLA-Vereinbarung
    - Netzwerküberwachung

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Verfügbarkeitskontrolle**

Daten müssen vor zufälliger Zerstörung und Verlust geschützt werden.

- werktägliche Datensicherung gemäß SLA-Vereinbarung
- Gebäude durch Alarmanlage gesichert
- Zutrittsschutz
- Brandfrüherkennung und Löschanlage im Rechenzentrum
- Notfallpläne gemäß ISO 27001
- unterbrechungsfreie Stromversorgung und Diesel-Notstromaggregat
- ständige Netzwerküberwachung
- regelmäßige Kontrollen durch interne und externe Audits

- **Rasche Wiederherstellbarkeit:**
    - werktägliche Datensicherung gemäß SLA-Vereinbarung
    - regelmäßige Wiederherstellungstests

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- **Datenschutz-Management**
- **Incident-Response-Management:**
  Wird über die Meldezentrale (Sicherheitsvorfälle) im SharePoint erfasst, durch die Verantwortlichen kategorisiert und dann über das Ticketsystem abgearbeitet.
- **Datenschutzfreundliche Voreinstellungen** (Art. 25 Abs. 2 DS-GVO)
- **Auftragskontrolle**
  Daten, die im Auftrag verarbeitet werden dürfen nur den Weisungen des Auftraggebers entsprechend verarbeitet werden.
    - Verfahrensanweisungen gem. ISO 27001 und ISO 9001
    - Vertraglich fixierte Auftragsdatenverarbeitung
    - Regelmäßige Weiterbildung der Mitarbeiter
    - regelmäßige Kontrollen durch interne und externe Audits

Eine ausführliche Beschreibung unserer technischen und organisatorischen Maßnahmen wird im Dokument „Ausführliche Beschreibung TOMs der synaforce GmbH“ in unserem Downloadbereich unter https://www.synaforce.com/downloads zur Verfügung gestellt.

Anlage 2 – Unterauftragnehmer

# 1 Unterauftragnehmer	**Core-Backbone GmbH, Hans-Sachs-Straße 14, 93138 Lappersdorf** (Colocation- Rack für synchronen, geschützten und verschlüsselten Backupspeicher der synaforce GmbH)
Auftragsgegenstand	Betreuung des Colocation-Racks mit der geschützten und verschlüsselten Backup-Sicherheitsspeicherung und anderen Archivierungen zur synchronen (gespiegelten) Datenhaltung
Zweck	Die Backups werden von dem Auftragnehmer auf einen hochverfügbaren, vor unbefugter Manipulation durch Dritte (z.B. durch Ransomware) geschützten und verschlüsselten Backupspeicher geschrieben und in einem vom Auftragnehmer angemieteten und ausschließlich für ihn zugänglichen Rack im Data Center des Unterauftragnehmers (Colocation bzw. Server Housing) mit einer Distanz von mindestens 150 km synchron gehalten. Der Unterauftragnehmer nimmt ausschließlich im Auftrag des Auftragnehmers notwendige Wartungsarbeiten an der im Rack befindlichen Hardware des Auftragnehmers vor. Ein Zugriff auf die Daten ist ausschließlich für den Auftragnehmer möglich, nicht für den Unterauftragnehmer.
Datenarten, Datenkategorien und Kreis der Betroffenen	Das Backup kann Informationen, wie unter **Punkt 2** des AV-Vertrages angegeben ist, enthalten. Dem entsprechend gelten auch die Angaben zum Kreis der Betroffenen entsprechend.
# 2 Unterauftragnehmer	**TeamViewer GmbH, Jahnstraße 30, 73037 Göppingen**
Auftragsgegenstand	Supportlösung für Fernwartung
Zweck	Remote-Supportunterstützung bei Kundenanfragen
Datenarten und Datenkategorien	• Inhaltsdaten, die in der Kommunikation zwischen verschiedenen Nutzern der Software transportiert werden, sowie Daten, die durch Nutzer bei der Planung und Durchführung von Meetings eingegeben werden • Verbindungsdaten, die auf dem Gerät des Nutzers gespeichert werden (Logfiles, txt-Dateien mit den Verbindungen) • Daten, die in Sitzungsaufzeichnungen auf dem Gerät des Nutzers gespeichert werden • Nutzerinformationen, wie Nutzername, Anzeigename, E-Mail, IP-Adresse, Profilbild (optional), Sprachpräferenz, Standort • Informationen zu Freundeslisten und Kontakten • Daten der Unternehmensprofil-Verwaltung und -Organisation
Kreis der Betroffenen	• Nutzer des Kunden • Verbindungspartner des Kunden / der Nutzer des Kunden • Dritte Personen, deren personenbezogene Daten durch den Kunden / die Nutzer des Kunden in der Kommunikationsverbindung geteilt werden

# 3 Unterauftragnehmer	**Microsoft Ireland Operations, Ltd., One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521**
Auftragsgegenstand	SharePoint zur Dokumentenverwaltung und Versionierung
Zweck	Die Kunden betreffend werden ggf. nur Dokumente abgelegt keine expliziten Daten. Die Dokumente können die genannten Daten und Betroffene beinhalten.
Datenarten und Datenkategorien	• Personenstammdaten • Kommunikationsdaten (z.B. Telefon, E-Mail) • Verhaltens- und Nutzungsdaten • Vertragsdaten • Qualifikationsdaten • Leistungsdaten • Akquisedaten
Kreis der Betroffenen	• Kunden • Interessenten • Beschäftigte • Geschäftspartner

Anlage 3 – Weisungsberechtigte Personen

Die Festlegung der weisungsberechtigten bzw. weisungsempfangenden Personen sind wie folgt festgelegt:

- ☐ Die weisungsberechtigten Personen des Auftragnehmers und die weisungsempfangenden Personen des Auftragnehmers entsprechen der Anlage „Ansprechpartner“ des SLA / der Leistungsvereinbarung bzw. der dokumentierten Änderungen (jährliche Aktualisierung → Anstoß AN, schriftliche Info AG)

- ☐ Explizit festgelegt (abweichend von der Leistungsvereinbarung) und nur gültig für Inhalte des AV-Vertrages (Auftragsverarbeitung)

Weisungsberechtigte Personen des Auftraggebers sind:

Name, Vorname	Position	Kontaktinformationen

Weisungsempfangende Personen beim Auftragnehmer sind:

Name, Vorname	Position	Kontaktinformationen

Anlage 4 – Internationaler Datentransfer

Wenn keine Datenübermittlung in Drittländer erfolgt, ist diese Anlage nicht auszufüllen.

Empfänger der Daten	Zweck und Grundlage der Datenüber-mittlung	Datenarten-/kategorien welche übertragen werden	Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus aus Art. 44 ff. DS-GVO
Wie in 7.1 angegeben überträgt die synaforce GmbH keine Daten an Drittländer			