Vereinbarung zur Auftragsverarbeitung

Als Anlage zum Wartungs- und Instandhaltungsvertrag / zur Leistungsbeschreibung der Leistung „Wartung und Instandhaltung der USV-Gesamtanlage im Betriebsgebäude TFT Süd (BG TFT Süd)“

- nachfolgend „Leistungsvereinbarung“ -

zwischen der
Autobahn GmbH des Bundes, Heidestraße 15, 10557 Berlin;

- nachfolgend „Verantwortlicher“ -

und

Auftragnehmer gemäß Zuschlagserteilung

- nachfolgend „Auftragsverarbeiter“ -

- beide nachfolgend gemeinsam „Vertragsparteien“ -

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsverarbeitungsverhältnis eingegangen. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der europäischen Datenschutz-Grundverordnung (*Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG* - DSGVO), und des Bundesdatenschutzgesetzes (BDSG) zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

§ 1 Anwendungsbereich

(1) Die Vereinbarung findet Anwendung auf die Verarbeitung (Art. 4 Nr. 2 DSGVO) aller personenbezogener Daten (im Folgenden: Daten), der Gegenstand der Leistungsvereinbarung sind oder im Rahmen von deren Durchführung anfallen und auf Weisung des Verantwortlichen verarbeitet werden. Nicht unter den Anwendungsbereich fallen Daten von Mitarbeitern des Auftragsverarbeiters, soweit sie ausschließlich das Beschäftigungsverhältnis mit dem Auftragsverarbeiter betreffen.

(2) Dieser Vertrag gilt vorranging vor anderen Vereinbarungen und Abreden zwischen Auftraggeber und Auftragnehmer, es sie denn, zwischen den Parteien wird ausdrücklich etwas anderes vereinbart.

§ 2 Konkretisierung des Auftragsinhalts

(1) Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Dauer des Auftrags, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in Anlage 1 zu diesem Vertrag festgelegt.

(2) Die verarbeiteten personenbezogenen Daten haben einen hohen Schutzbedarf.

§ 3 Verpflichtungen und Weisungsbefugnis

(1) Die Vertragsparteien sind verpflichtet, die Ihnen durch die Datenschutzgesetze (insb. DSGVO) auferlegten Pflichten einzuhalten. Der Verantwortliche kann jederzeit die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.

(2) Zur Gewährleistung des Schutzes der Rechte der betroffenen Personen unterstützt der Auftragsverarbeiter den Verantwortlichen angemessen, insbesondere durch die Gewährleistung geeigneter technischer und organisatorischer Maßnahmen.

(3) Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

(4) Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen verarbeiten, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder des Mitgliedstaates, 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 DSGVO). Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit Daten gerichtete

schriftliche, elektronische oder mündliche Anordnung des Verantwortlichen. Die Anordnungen sind zu dokumentieren. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Verantwortlichen danach in dokumentierter Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

(5) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt oder geändert wird. Die weisungsberechtigten Personen auf Seiten des Verantwortlichen sowie die zum Empfang der Weisungen berechtigten Personen auf Seiten des Auftragsverarbeiters sowie die vorgesehenen Informationswege sind in der Anlage 2 festgelegt.

(6) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

(7) Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher (oder dokumentierter elektronischer) Zustimmung durch den Verantwortlichen erteilen, es sei denn er ist nach dem Unionsrecht oder dem Recht eines Mitgliedstaats zur Herausgabe verpflichtet.

(8) Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben, es sei denn er ist nach dem Unionsrecht oder dem Recht eines Mitgliedstaats zur Herausgabe verpflichtet. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt.

(9) Der Verantwortliche führt das Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 DSGVO. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung. Der Auftragsverarbeiter führt entsprechend den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

(10) Die Verarbeitung der Daten im Auftrag des Verantwortlichen findet ausschließlich auf dem Gebiet *der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraumes (EWR) / der Bundesrepublik Deutschland* statt. Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage schriftlicher (oder dokumentierter elektronischer) Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der DSGVO im Einklang stehen. Die grundlegenden Voraussetzungen für die Rechtmäßigkeit der Verarbeitung bleiben unberührt.

(11) Der Auftragsverarbeiter gewährleistet, dass ihm unterstellte natürliche Personen, die Zugang zu Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten. Eine Verarbeitung von Daten außerhalb der Betriebsräume des Auftragsverarbeiters (z.B. Telearbeit, Heimarbeit, Home Office, mobiles Arbeiten) bedarf der vorherigen ausdrücklichen schriftlichen (oder dokumentierten elektronischen) Zustimmung des Verantwortlichen, die erst nach Festlegung angemessener technischer und organisatorischer Maßnahmen für die Verarbeitungssituation erteilt werden kann.

§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

(1) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und weist dies dem Verantwortlichen auf Wunsch nach. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

(2) Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung einschließlich der Umsetzung der notwendigen technischen und organisatorischen Maßnahmen (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO). Der Auftragsverarbeiter stellt dem Verantwortlichen hierzu bei Bedarf entsprechende Informationen zur Verfügung.

(3) Sofern der Auftragsverarbeiter der gesetzlichen Pflicht zur Benennung einer bzw. eines Datenschutzbeauftragte/n unterliegt sind die Kontaktdaten der/des Datenschutzbeauftragten dem Verantwortlichen zum Zwecke der direkten Kontaktaufnahme mitzuteilen. Unterliegt der Auftragsverarbeiter nicht der Benennungspflicht, teilt er dem Verantwortlichen die Kontaktdaten eines Ansprechpartners für den Datenschutz mit.

(4) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde im Rahmen ihrer Zuständigkeit bei dem Auftragsverarbeiter anfragt, ermittelt oder sonstige Erkundigungen einzieht.

§ 5 Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren die in Anlage 4 „Technisch-organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Die Anlage „Technisch-organisatorische Maßnahmen“ wird Gegenstand dieser Vereinbarung.

(2) Ergibt eine Prüfung des Verantwortlichen einen Anpassungsbedarf der vom Auftragsverarbeiter zu ergreifenden technisch-organisatorischen Maßnahmen gemäß Artikel 32 DSGVO, sind die Anpassungen vom Auftragnehmer umzusetzen.

(3) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in der Anlage „Technisch-organisatorische Maßnahmen“ festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(4) Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind. Er wird insbesondere Überprüfungen/ Inspektionen, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und deren Durchführung unterstützen.

(5) Die Überprüfung kann auch auf der Grundlage vorgelegter aktueller Testate, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer, unabhängige Datenschutzauditoren), durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO, einer Zertifizierung nach Art. 42 DSGVO oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit erfolgen. Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über den Ausschluss von genehmigten Verhaltens-

regeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

(6) Die Überprüfung kann auch durch eine Inspektion vor Ort erfolgen. Der Verantwortliche kann sich hierzu in den Betriebsstätten des Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieses Vertrages erforderlichen technischen und organisatorischen Erfordernisse überzeugen.

(7) Der Auftragsverarbeiter stellt dem Verantwortlichen darüber hinaus alle erforderlichen Informationen zur Verfügung, die er für die Prüfungen nach Absatz 4 sowie für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten (Datenschutz-Folgenabschätzung i.S.d. Art. 35 DSGVO) benötigt.

(8) Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

§ 6 Mitteilung bei Verstößen durch den Auftragsverarbeiter

Der Auftragsverarbeiter unterrichtet den Verantwortlichen umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen diese Vereinbarung sowie gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Abs. 2 DSGVO sowie auf korrespondierende Pflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. § 3 dieses Vertrages durchführen.
Die Unterrichtung des Verantwortlichen erfolgt per e-Mail an datenschutz@autobahn.de. Die Mitteilung hat neben der Unterrichtung die Kontaktdaten eines konkreten Ansprechpartners für Rückfragen zu enthalten.

§ 7 Löschung und Rückgabe von Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen.

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Verantwortlichen, jedoch spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragsverarbeiter sämtliche im Auftrag des Verantwortlichen verarbeitete personenbezogene Daten dem Verantwortlichen zurückzugeben oder nach vorheriger Zustimmung des Verantwortlichen datenschutzgerecht zu löschen bzw. zu vernichten. Dies umfasst insbesondere dem Auftragsverarbeiter überlassene Daten, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen. Eine weitere Speicherung ist nur zulässig, wenn hierzu eine Verpflichtung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats besteht. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Verantwortlichen auf Anforderung vorzulegen.

(3) Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 2.

§ 8 Subunternehmen

(1) Der Auftragsverarbeiter erhält die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Subunternehmen, die gemäß der Anlage 3 in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens vier Wochen im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Subunternehmen und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des betreffenden Subunternehmens Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Wenn Subunternehmen durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden; dies gilt insbesondere auch im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung.

a) Dem Verantwortlichen sind in der vertraglichen Vereinbarung mit dem Subunternehmen Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Verantwortlichen berechtigt, auf schriftliche (oder dokumentierte elektronische) Anforderung vom Auftragsverarbeiter Auskunft über den Inhalt des mit dem Subunternehmen geschlossenen Vertrages und die darin enthaltene Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmens zu erhalten.
b) Der Auftragsverarbeiter beachtet bei der Übermittlung von personenbezogenen Daten die gesamte Leistungskette (samt eventuell weiterer Subdienstleister und Subsubdienstleister) und ist insbesondere bei der Übermittlung von personenbezogenen Daten in Drittländer für Prüfung und Umsetzung der Vorgaben der Art. 44 – 49 DSGVO eigenständig verantwortlich. Dies gilt insbesondere, aber nicht ausschließlich, für den Abschluss von Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c DSGVO).

(3) Kommt das Subunternehmen seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmens. Der Auftragsverarbeiter hat in diesem Falle auf Verlangen des Verantwortlichen die Beschäftigung des Subunternehmens ganz oder teilweise zu beenden oder das Vertragsverhältnis mit dem Subunternehmen zu lösen, wenn und soweit dies nicht unverhältnismäßig ist.

§ 9 Datenschutzkontrolle

Der Auftragsverarbeiter verpflichtet sich, der/dem Datenschutzbeauftragten des Verantwortlichen zur Erfüllung ihrer jeweiligen gesetzlichen zugewiesenen Aufgaben im Zusammenhang mit diesem Auftrag Zugang zu den üblichen Geschäftszeiten zu gewähren. Er duldet insbesondere Betretungs-, Einsichts- und Fragerechte einschließlich der Einsicht in durch Berufsgeheimnisse geschützte Unterlagen. Er wird seine Mitarbeiter anweisen, mit dem/ der Datenschutzbeauftragten zu kooperieren, insbesondere deren Fragen wahrheitsgemäß und vollständig zu beantworten. Die nach Gesetz bestehenden Verschwiegenheitspflichten und Zeugnisverweigerungsrechte der Genannten bleiben davon unberührt.

§ 10 Haftung und Schadenersatz

Auf Artikel 82 DSGVO wird bezüglich der Haftung und des Rechts auf Schadenersatz verwiesen.

§ 11 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragsverarbeiters - bedürfen einer schriftlichen Vereinbarung 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.

(2) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

_____	_____
Datum, Ort	Datum, Ort
_____	_____
Unterschrift (Verantwortlicher)	Unterschrift (Auftragsverarbeiter)
_____	_____
Name, Vorname, Funktion	Name, Vorname, Funktion

Anlage 1 – Auftragsdetails

1. Gegenstand, Dauer und Zweck der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

Der Auftrag umfasst die Wartung, Inspektion, Instandhaltung, Störungsbeseitigung und – soweit vertraglich vorgesehen – Fernwartung der im Betriebsgebäude TFT Süd (BG TFT Süd) installierten USV-Gesamtanlage einschließlich Online-Doppelwandler-USV 60 kVA, externem Wartungs-Bypass, stationärem VRLA-/Reinblei-AGM-Batteriesystem, Batterie-Monitoring, 60-V-DC-Umschalteinrichtung mit Batteriepuffer, USV-Steuerung/Bedieneinheit, Kommunikations- und Meldeschnittstellen sowie Blindleistungskompensationsanlage (ca. 150 kVAr). Zweck der Verarbeitung ist die Durchführung der vertragsgegenständlichen Wartungs- und Entstörungsleistungen einschließlich Zutritts- und Freigabekoordination, Fernanalyse/Fernwartung, Fehlerdiagnose, Arbeits-, Prüf- und Störungsdokumentation sowie der Nachweisführung gegenüber dem Verantwortlichen.

Die Dauer des Auftrages richtet sich nach dem Hauptvertrag, sofern sich aus den Bestimmungen der Vereinbarung zur Auftragsverarbeitung nicht darüberhinausgehende Verpflichtungen ergeben.

2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

Regelmäßig verarbeitet werden – soweit im Einzelfall vorhanden und einer Person zuordenbar – dienstliche Stamm- und Kontaktdaten (Name, Funktion, Organisationseinheit, dienstliche Telefonnummer, dienstliche E-Mail-Adresse), Zutritts- und Freigabedaten (Name, Unternehmen, Berechtigungsstatus, Zeitpunkte von Zutritt, Arbeitsbeginn und Arbeitsende), Betriebs-, Alarm-, Ereignis- und Auditprotokolle mit Personenbezug (Benutzerkennungen, Bedien- und Quittierinformationen, Zeitstempel, IP-Adressen, Remote-Access-, VPN- und Session-Logs) sowie Wartungs-, Prüf-, Störungs-, Freigabe- und Schulungsdokumentationen mit Personenbezug (Name, Funktion, Unterschrift, Kommunikationsinhalte, Qualifikations- und Teilnahmenachweise).

3. Kategorien betroffener Personen

Kreis der von der Datenverarbeitung betroffenen Personen:

Betroffen sind insbesondere Ansprechpartner und Beschäftigte des Verantwortlichen aus Betrieb BG TFT Süd, Leittechnik/WinCC OA, Tunnelleitzentrale Berlin, Elektro-/Anlagenbetrieb, IT und Informationssicherheit, die zur Leistungserbringung eingesetzten Beschäftigten des Auftragnehmers und genehmigter Unterauftragnehmer, soweit deren Daten in Zutritts-, Freigabe-, Remotezugriffs-, Wartungs- oder Störungsprozessen verarbeitet werden, sowie Teilnehmer von Schulungen/Einweisungen und sonstige in Arbeits-, Störungs-, Freigabe- oder Kommunikationsdokumentationen namentlich bezeichnete Personen.

4. Datenschutzbeauftragter des Auftragnehmers

Namen und Kontaktdaten (inkl. E-Mail und Telefonnummer mitteilen)

ODER

Der Auftragnehmer ist aus den folgenden Gründen gesetzlich nicht dazu verpflichtet einen Datenschutzbeauftragten zu bestellen:

Anlage 2 - „Weisungsbefugnis“ zu § 3 (rollenbezogen für die gegenständliche Leistung; personenbezogene Benennung nach Zuschlagserteilung)

zur Vereinbarung zur Auftragsverarbeitung für die Leistung „Wartung und Instandhaltung der USV-Gesamtanlage im Betriebsgebäude TFT Süd (BG TFT Süd)“
zwischen der Autobahn GmbH des Bundes
und dem Auftragnehmer gemäß Zuschlagserteilung

Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt oder geändert wird. Die weisungsberechtigten Personen auf Seiten des Verantwortlichen sowie die zum Empfang der Weisungen berechtigten Personen auf Seiten des Auftragsverarbeiters sowie die vorgesehenen Informationswege sind nachfolgend festgelegt.

Weisungsberechtigte Personen auf Seiten des Verantwortlichen:

Leiter/in des zuständigen Fachbereichs Elektrotechnik/Technische Ausrüstung oder schriftlich benannte weisungsbefugte Person des Verantwortlichen
Schriftlich benannte Stellvertretung des zuständigen Fachbereichs Elektrotechnik/Technische Ausrüstung
Weitere weisungsberechtigte Personen nur nach schriftlicher Benennung durch den Verantwortlichen

Zum Empfang der Weisungen berechtigte Personen auf Seiten des Auftragsverarbeiters:

Projektleiter/in Wartung und Instandhaltung des Auftragsverarbeiters für die gegenständliche Leistung
Servicekoordinator/in bzw. 24/7-Störungsannahme des Auftragsverarbeiters
Schriftlich benannte Stellvertretung des Auftragsverarbeiters
Weitere empfangsberechtigte Personen nur nach schriftlicher Benennung durch den Auftragsverarbeiter

Vorgesehene Informationswege, wenn Weisung nach Meinung des Auftragsverarbeiters gegen datenschutzrechtliche Vorschriften verstößt:
Verbindliche Informationswege bei datenschutzrechtlich bedenklicher Weisung:

[x] schriftliche Information
[x] elektronische Information
[x] mündliche Information nur im Eilfall; unverzügliche schriftliche oder elektronische Nachdokumentation erforderlich

Weisungen (auch mündliche Weisungen) sind durch die Vertragsparteien zu dokumentieren. Änderungen bei den weisungsbefugten Personen, den zum Weisungsempfang berechtigten Personen und bei den vorgesehenen Informationswegen sind dem Vertragspartner entsprechend unverzüglich anzuzeigen.

Anlage 3 - „Subunternehmen“ zu § 8

Nach § 8 Abs. 1 der Vereinbarung sind die zur Erfüllung dieses Vertrages bereits hinzugezogenen Subunternehmen zu bezeichnen. Gem. § 8 Abs. 1 der Vereinbarung erklärt sich der Verantwortliche mit deren Beauftragung einverstanden.

Subunternehmen (Name, Anschrift bzw. Sitz)	Datum des Abschlusses der Vereinbarung zur Auftragsverarbeitung	(Teil-)Leistungsgegenstand im Rahmen der Auftragsverarbeitung	Bei Verarbeitung im Drittland: Angemessenes Schutzniveau hergestellt durch:

Anlage 4 – Technische und organisatorische Maßnahmen (TOMs) des Auftragnehmers i.S.d. Art. 32 DSGVO

An den Auftragnehmer: Anlage 4 ist leistungsspezifisch für die Wartung, Inspektion, Instandhaltung, Störungsbeseitigung und – soweit vertraglich vorgesehen – Fernwartung der USV-Gesamtanlage im Betriebsgebäude TFT Süd (USV 60 kVA, Batterieanlagen, Batterieüberwachung, 60-V-DC-Umschalteinrichtung, externer Wartungsbypass, USV-Steuerung/Kommunikationsschnittstellen und Blindleistungskompensationsanlage) auszufüllen. Soweit einzelne Maßnahmen wegen der konkreten Ausführungsform nicht einschlägig sind, ist dies ausdrücklich zu vermerken.

§ 1 Technische und organisatorische Sicherheitsmaßnahmen
Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist. Der Auftragnehmer trifft die nachfolgenden technischen und organisatorischen Maßnahmen i.S.d. Art. 32 DSGVO.

§ 2 Innerbehördliche oder innerbetriebliche Organisation des Auftragsverarbeiters
Der Auftragsverarbeiter wird seine innerbehördliche oder innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind.

1. Zertifikate

Bitte teilen Sie uns mit welche Zertifikate Ihre Organisation erhalten hat und fügen Sie diese diesem Dokument bei.

Zertifikat	Scope
ISO27001	☐ Rechenzentrum ☐ Entwicklung ☐ SaaS ☐ Klicken oder tippen Sie hier, um Text einzugeben.
ISO27001 auf Basis IT-Grundschutz	☐ Rechenzentrum ☐ Entwicklung ☐ SaaS ☐ Klicken oder tippen Sie hier, um Text einzugeben.
ISO9001	☐ Rechenzentrum ☐ Entwicklung ☐ SaaS ☐ Klicken oder tippen Sie hier, um Text einzugeben.
Weitere: Klicken oder tippen Sie hier, um Text einzugeben.	☐ Rechenzentrum ☐ Entwicklung ☐ SaaS ☐ Klicken oder tippen Sie hier, um Text einzugeben.

2. Durch Ihre Organisation getroffene Maßnahmen

Der Auftragnehmer erbringt die Garantie einer datenschutzkonformen Datenverarbeitung durch folgende Maßnahmen:

2.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen		**Organisatorische Maßnahmen**	
Rechenzentrum			
☐	Alarmanlage	☐	Schlüsselregelung (Schlüsselausgabe etc.)
☐	Automatisches Zugangskontrollsystem	☐	Personenkontrolle beim Pförtner / Empfang
☐	Türen mit Knauf an Außenseite	☐	Protokollierung der Besucher
☐	Sicherheitsschlösser	☐	Besucher in Begleitung von Mitarbeitern
☐	Manuelles Schließsystem	☐	Tragepflicht von Berechtigungsausweisen
☐	Chipkarten-/Transponder-Schließsystem	☐	Sorgfältige Auswahl von Wachpersonal
☐	Schließsystem mit Codesperre	☐	Sorgfältige Auswahl von Reinigungspersonal
☐	Biometrische Zugangssperren	☐	Weitere: *[Bitte eintragen]*
☐	Lichtschranken / Bewegungsmelder		
☐	Absicherung von Gebäudeschächten		
☐	Videoüberwachung der Zugänge		
☐	Klingelanlage mit Kamera		

Technische Maßnahmen		Organisatorische Maßnahmen	
☐	Weitere: *[Bitte eintragen]*		
Generelle Bürogebäude/ Weitere Gebäude			
☐	Alarmanlage	☐	Schlüsselregelung (Schlüsselausgabe etc.)
☐	Automatisches Zugangskontrollsystem	☐	Personenkontrolle beim Pförtner / Empfang
☐	Türen mit Knauf an Außenseite	☐	Protokollierung der Besucher
☐	Sicherheitsschlösser	☐	Besucher in Begleitung von Mitarbeitern
☐	Manuelles Schließsystem	☐	Tragepflicht von Berechtigungsausweisen
☐	Chipkarten-/Transponder-Schließsystem	☐	Sorgfältige Auswahl von Wachpersonal
☐	Schließsystem mit Codesperre	☐	Sorgfältige Auswahl von Reinigungspersonal
☐	Biometrische Zugangssperren	☐	Weitere: *[Bitte eintragen]*
☐	Lichtschranken / Bewegungsmelder		
☐	Absicherung von Gebäudeschächten		
☐	Videoüberwachung der Zugänge		
☐	Klingelanlage mit Kamera		
☐	Weitere: *[Bitte eintragen]*		

2.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.
Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten" Passworts).

Technische Maßnahmen		Organisatorische Maßnahmen	
Hardware			
☐	Login mit Benutzername + Passwort	☐	Verwalten von Benutzerberechtigungen
☐	Login mit biometrischen Daten	☐	Erstellen von Benutzerprofilen
☐	Anti-Viren-Software Server	☐	Zentrale Passwortvergabe
☐	Anti-Virus-Software Clients	☐	Allg. Richtlinie Datenschutz und / oder Sicherheit
☐	Anti-Virus-Software mobile Geräte	☐	Anleitung „Manuelle Desktopsperre"
☐	Firewall	☐	Richtlinie „Sicheres Passwort" (mind. 12 Zeichen sowie hinreichende Komplexität von mindestens Groß/-Klein/Sonderzeichen)
☐	Intrusion Detection Systeme	☐	Weitere: *[Bitte eintragen]*
☐	Automatische Desktopsperre		
☐	BIOS Schutz (separates Passwort)		
☐	Sperre externer Schnittstellen (USB)		

Technische Maßnahmen		Organisatorische Maßnahmen	
☐	Weitere: *[Bitte eintragen]*		
Fester Arbeitsplatz beim Arbeitgeber			
☐	Weitere: *[Bitte eintragen]*	☐	Richtlinie „Clean desk“
		☐	Weitere: *[Bitte eintragen]*
HomeOffice/Remote			
☐	Einsatz VPN bei Remote-Zugriffen nach aktuellem Stand der Technik Welche Verschlüsselungstechnik wird genutzt? *[Bitte eintragen]*	☐	Mobile Device Policy
☐	Verschlüsselung von Notebooks / Tablet Welche Verschlüsselungstechnik wird genutzt? *[Bitte eintragen]*	☐	Weitere: *[Bitte eintragen]*
☐	Verschlüsselung von Datenträgern		
☐	Verschlüsselung Smartphones		
☐	Mobile Device Management		
☐	Weitere: *[Bitte eintragen]*		

2.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen		Organisatorische Maßnahmen	
☐	Aktenschredder (mind. Stufe 4, cross cut)	☐	Richtlinie „Löschen / Vernichten“
☐	Externer Aktenvernichter (DIN 66399 Stufe P4 bei normal / Stufe P5 bei besonders zu schützenden Daten)	☐	Zertifiziertes Löschen von Digitalen und Papierdaten ☐ nach ISO/Zertifikat *[Bitte eintragen]* ☐ durch zertifizierten Dienstleister *[Bitte eintragen]*
☐	Physische Löschung von Datenträgern	☐	Einsatz Berechtigungskonzepte
☐	Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☐	Minimale Anzahl an Administratoren
☐	Weitere:	☐	Verwaltung Benutzerrechte durch Administratoren

Technische Maßnahmen		Organisatorische Maßnahmen	
	[Bitte eintragen]		
		☐	Weitere: *[Bitte eintragen]*

2.4. 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. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen		Organisatorische Maßnahmen	
☐	Technische Protokollierung der Eingabe, Änderung und Löschung von Daten inkl. Benutzerkennung mindestens auf Datenbankebene	☐	„Manuelle oder automatisierte Kontrolle der Protokolle“
☐	Manuelle oder automatisierte Kontrolle der Protokolle	☐	Bei Vorliegen/ Bedarf/ Nutzung: Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
☐	„Manuelle oder automatisierte Kontrolle der Protokolle“ gilt auch bei Zugriff mit Fremdsoftware	☐	Klare Zuständigkeiten für Löschungen
☐	Weitere: *[Bitte eintragen]*	☐	Weitere: *[Bitte eintragen]*

2.5. 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. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen		Organisatorische Maßnahmen	
Digitale Daten			
☐	Einsatz von VPN	☐	Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☐	Protokollierung der Zugriffe und Abrufe	☐	Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☐	Bereitstellung über verschlüsselte Verbindungen wie sftp, https	☐	Keine Weitergabe in anonymisierter oder pseudonymisierter Form
☐	Nutzung von Signaturverfahren	☐	Keine Übermittlung von personenbezogenen Daten via E-Mail oder in Anhängen zu E-Mails
☐	Weitere: *[Bitte eintragen]*	☐	Weitere: *[Bitte eintragen]*
Physische Daten			
☐	Sichere Transportbehälter	☐	Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen

Technische Maßnahmen		Organisatorische Maßnahmen	
☐	Weitere: *[Bitte eintragen]*	☐	Persönliche Übergabe mit Protokoll
		☐	Weitere: *[Bitte eintragen]*

2.6. Datentrennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen		Organisatorische Maßnahmen	
☐	Trennung von Produktiv- und Testumgebung	☐	Steuerung über Berechtigungskonzept
☐	Logische Mandantentrennung (softwareseitig)	☐	Festlegung von Datenbankrechten
☐	Weitere: [Bitte eintragen]	☐	Datensätze sind mit Zweckattributen versehen
		☐	Weitere: *[Bitte eintragen]*

2.7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Daten-sicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Technische Maßnahmen		Organisatorische Maßnahmen	
Rechenzentrum und Serverraum			
☐	Feuer- und Rauchmeldeanlagen	☐	Existenz eines aktuellen und verprobten Backup- & Recovery-Konzepts (ausformuliert)
☐	Feuerlöscher Serverraum	☐	Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☐	Serverraumüberwachung Temperatur und Feuchtigkeit	☐	Existenz eines aktuellen und verprobten Notfallplans (z.B. BSI IT-Grundschutz 100-4)
☐	Serverraum klimatisiert	☐	Getrennte Partitionen für Betriebssysteme und Daten
☐	Unterbrechungsfreie Stromversorgung (USV)	☐	Redundante Vorhaltung von personen-bezogenen Daten (Dokumentation/ Backup/ Wiederherstellung)
☐	Schutzsteckdosenleisten Serverraum	☐	Weitere: *[Bitte eintragen]*
☐	Videoüberwachung Serverraum		
☐	Alarmmeldung bei unberechtigtem Zutritt zu Serverraum		
☐	Weitere: *[Bitte eintragen]*		
Generelle Bürogebäude/ Weitere Gebäude			
☐	Weitere: *[Bitte eintragen]*	☐	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
		☐	Weitere: *[Bitte eintragen]*

2.8. Pseudonymisierung

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 Maßnahmen		Organisatorische Maßnahmen	
☐	Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System (mögl. verschlüsselt)	☐	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/ pseudonymisieren
☐	Weitere: *[Bitte eintragen]*	☐	Weitere: *[Bitte eintragen]*

2.9. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen		Organisatorische Maßnahmen	
Vorbeugung & Erkennung			
☐	Einsatz von Firewall und regelmäßige Aktualisierung	☐	Weitere: [Bitte eintragen]
☐	Einsatz von Spamfilter und regelmäßige Aktualisierung		
☐	Einsatz von Virenscanner und regelmäßige Aktualisierung		
☐	Intrusion Detection System (IDS)		
☐	Intrusion Prevention System (IPS)		
☐	Weitere: [Bitte eintragen]		
Behandlung bei Eintritt			
☐	Weitere: [Bitte eintragen]	☐	Dokumentierter, gelebter Prozess zur Erkennung, Meldung und Behandlung von Sicherheitsvorfällen/ Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber der Aufsichtsbehörde)
		☐	Einbindung von ☐ DSB und ☐ ISB in Behandlungen bei Sicherheitsvorfällen und Datenpannen
		☐	Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
		☐	Weitere: [Bitte eintragen]

2.10. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Technische Maßnahmen		Organisatorische Maßnahmen	
☐	Weitere: *[Bitte eintragen]*	☐	vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
		☐	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
		☐	schriftlicher Auftragsverarbeitungsvertrag (u.U. EU Standard-Vertragsklauseln)
		☐	Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
		☐	Auftragnehmer hat Datenschutzbeauftragten bestellt (bei Vorliegen einer Bestellpflicht)
		☐	Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
		☐	Regelung zum Einsatz weiterer Subunternehmer
		☐	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
		☐	laufende Überprüfung des Auftragnehmers, seines Schutzniveaus und seiner Tätigkeiten
		☐	Vertragsstrafen bei Verstößen
		☐	Weitere: *[Bitte eintragen]*

2.11. Weitere Datenschutzmaßnahmen

2.11.1. Datenschutz-Management

Technische Maßnahmen		Organisatorische Maßnahmen	
☐	Software-Lösungen für Datenschutz-Management im Einsatz	☐	Interner/ externer Datenschutzbeauftragter Name/ Firma/ Kontaktdaten [Bitte benennen]
☐	Zentrale Dokumentation aller Verfahrens-weisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf und Berechtigung (z.B. Wiki, Intranet, etc.)	☐	Mitarbeiter hinsichtl. Vertraulichkeit und Datengeheimnis geschult und verpflichtet.
☐	Sicherheitszertifizierung nach ☐ ISO 27001 ☐ ISO 27001 auf Basis BSI IT-Grundschutz ☐ weiteres: *[Bitte benennen]*	☐	Regelmäßige Sensibilisierung der Mitarbeiter wird min. einmal jährlich durchgeführt.
☐	Anderweitiges dokumentiertes Sicherheitskonzept *[Bitte benennen]*	☐	Interner / externer Informations-sicherheits-Beauftragter Name / Firma Kontakt *[Bitte benennen]*
☐	Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt.	☐	Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt.
☐	Weitere: *[Bitte eintragen]*	☐	Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach.

Technische Maßnahmen		Organisatorische Maßnahmen	
		☐	Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden.
		☐	Weitere: *[Bitte eintragen]*

2.11.2. Datenschutzfreundliche Voreinstellungen

Privacy by Design bedeutet, dass entsprechende Software und Hardware von Grund auf so konzipiert und entwickelt wird, dass relevante Datenschutzmaßnahmen von Anfang an berücksichtigt werden. Die Technikgestaltung orientiert sich in allen Bereichen an den Datenschutzanforderungen.
Privacy by Default bezeichnet „Datenschutz ab Werk" und bedeutet, dass Software, Hardware und Services bei Auslieferung datenschutzfreundlich voreingestellt sein müssen. So wird die Privatsphäre der User respektiert.

Technische Maßnahmen		Organisatorische Maßnahmen	
☐	Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.	☐	Weitere: *[Bitte eintragen]*
☐	Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen		
☐	Weitere: *[Bitte eintragen]*		

3. Anlagen zu Anlage 4

Die Prüfung der oben gemachten Angaben erleichtern Sie uns mit der Zusendung von Anlagen. Fügen Sie gerne Richtlinie, Zertifikate oder ähnliches bei.

Bitte fügen Sie nichts bei, was bei unberechtigter Kenntnisnahme ein Sicherheitsrisiko für Ihre Organisation darstellen kann.

☐	Verzeichnis zu den Kategorien von im Auftrag durchgeführten Verarbeitungstätigkeiten (Art. 30 Abs. 2 DSGVO)
☐	Liste der eingesetzten Subunternehmer mit Tätigkeiten für Sie als Auftraggeber
☐	Richtlinie Datenschutz
☐	Richtlinie Umgang mit Datenpannen
☐	Übersicht der Sensibilisierungs- und Schulungsmaßnahmen der letzten 24 Monate
☐	Weitere: *[Bitte eintragen]*
☐	Weitere: *[Bitte eintragen]*
☐	Weitere: *[Bitte eintragen]*

Organisation	*Name des Auftragsverarbeiters*
Ausgefüllt durch	*Name, Funktion, Kontakt*
Hiermit bestätige ich die Richtigkeit der gemachten Angaben	Ort, Datum, Unterschrift des Auftragsverarbeiters
Datum	*[Datum]*

4. durch den Auftraggeber auszufüllen - Prüfung und Freigabe

Geprüft durch	*[Namen eintragen]*
Datum der Prüfung	*[Datum]*
Ergebnis	☐ Es besteht noch Klärungsbedarf: *[Bitte eintragen]* ☐ TOMs sind für die angestrebte Datenverarbeitung ausreichend. ☐ Vereinbarung Auftragsverarbeitung kann geschlossen werden.