Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO mit Fernwartung

Verantwortlicher (Auftraggeber / Datenverantwortlicher):

Landeshauptstadt Dresden
Eigenbetrieb Sportstätten
vertreten durch die Amtsleitung
Freiberger Straße 31
01067 Dresden

Vertrags-Nr.:

Auftragsverarbeiter (Auftragnehmer):

Firma
Straße
PLZ Ort

Vertrags-Nr.:

1. Gegenstand, Ort und Dauer der Vereinbarung

1.1 Gegenstand der Verarbeitung

Diese Vereinbarung umfasst folgende vom Auftragsverarbeiter durchzuführende Fernwartungsarbeiten:

☒ Hardware- Diagnose: für folgende(s) Hardwareprodukt(e)
☒ Software-Wartung: für folgende(s) Softwareprodukt(e)

Software-Wartung:
Die Fernwartung erfolgt über eine VPN-Verbindung / FW-to-FW-Kopplung / mittels TeamViewer....
zur Behebung von Fehlerzuständen in der Anwendung xyz in der Abteilung N.
Damit verbunden sind folgende Zugriffe:

- schreibender Zugriff auf die Konfigurationsdateien ..... der Anwendung xyz
- lesender Zugriff auf die anderen Dateien im Programmverzeichnis ..... der Anwendung xyz
- lesender Zugriff auf die Anwendungsdaten in den Verzeichnissen .....
- Zugriff auf die Datei .... wird, soweit erforderlich, nach Rücksprache ermöglicht

Der Auftragsverarbeiter verarbeitet dabei auf Grundlage dieses Vertrages personenbezogene Daten für den Verantwortlichen im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO.

1.2 Ort der Verarbeitung

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 in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standard-Datenschutzklauseln, genehmigte Verhaltensregeln).

1.3 Dauer des Auftrags

Der Vertrag beginnt am Tag.Monat.Jahr und endet nach 2 Jahren am Tag.Monat.Jahr.
Er ist mit einer Frist von 4 Wochen zum Monatssende kündbar.

Der Verantwortliche kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragsverarbeiter eine Weisung des Verantwortlichen nicht ausführen kann oder will oder der Auftragsverarbeiter Kontrollrechte des Verantwortlichen vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

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

2.1 Zweck der Verarbeitung:

(nähere Beschreibung ggf. Verweis auf Leistungsverzeichnis als Anlage etc.)

2.2 Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DSGVO):

2.3 Art der personenbezogenen Daten (entspr. der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO):

2.4 Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO):

3. Rechte und Pflichten sowie Weisungsbefugnisse des Verantwortlichen

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Verantwortliche zuständig. Gleichwohl ist der Auftragsverarbeiter verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Verantwortlichen gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und des Verfahrens sind gemeinsam zwischen Verantwortlichem und Auftragsverarbeiter abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

In der Regel erteilt der Verantwortliche alle Aufträge, Teilaufträge und Weisungen schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
Der Verantwortliche ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen (siehe Ziffer 5).

Im System des Verantwortlichen werden alle Zugriffe im Rahmen der Wartungsarbeiten protokolliert. Die Protokollierung muss so erfolgen, dass sie in einer Revision nachvollzogen werden kann. Sie darf vom Auftragsverarbeiter nicht abgeschaltet werden.

Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Er ist außerdem dazu verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiters vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Verantwortlichen, Weisungsempfänger des Auftragsverarbeiters

Weisungsberechtigte Personen des Verantwortlichen sind:

(Vorname, Name, Organisationseinheit, E-Mail, Telefon)

Weisungsempfänger des Auftragsverarbeiters sind:

(Vorname, Name, Organisationseinheit, E-Mail, Telefon)

Für Weisungen zu nutzende Kommunikationskanäle:

(genaue postalische Adresse / E-Mail / Telefonnummer)

Der Auftragsverarbeiter nimmt Supportanfragen über eine zentrale Hotline / Fernwartungszentrale oder eine zentrale E-Mail-Adresse entgegen. Weisungsempfänger beim Auftragsverarbeiter ist daher im konkreten Fall diejenige Person, die die Supportanfrage entgegennimmt und bearbeitet.

Der Auftragsverarbeiter richtet geeignete technische und organisatorische Maßnahmen ein, durch welche nachvollzogen werden kann, welche natürliche Person die Fernwartung vorgenommen hat.

Der Beginn der Fernwartung ist telefonisch (oder in anderweitig geeigneter und spezifizierter Form) anzukündigen, um dem Beauftragten des Verantwortlichen die Möglichkeit zu geben, die Maßnahmen der Fernwartung zu verfolgen. Zu Zwecken der Fernwartung notwendige Datenübertragungen müssen in hinreichend verschlüsselter Form erfolgen.

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 Auftragsverarbeiters

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Verantwortlichen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, 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).

Der Auftragsverarbeiter verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden nicht ohne Wissen des Verantwortlichen erstellt.

Der Auftragsverarbeiter stellt im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen sicher. Ebenfalls stellt er sicher, dass die für den Verantwortlichen verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Die Datenträger, die vom Verantwortlichen stammen bzw. für den Verantwortlichen genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Bei der Erfüllung der Rechte der betroffenen Personen durch den Verantwortlichen nach Art. 12 bis 22 DSGVO, bei der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgenabschätzungen des Verantwortlichen hat der Auftragsverarbeiter im notwendigen Umfang mitzuwirken und den Verantwortlichen soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO). Auf Weisung hat er dem Verantwortlichen die dazu erforderlichen Angaben unverzüglich weiterzuleiten.

Neben der Verpflichtung des Auftragsverarbeiters, selbst ein Verzeichnis der Verarbeitungstätigkeiten zu führen (Art. 30 Abs. 2 DSGVO), muss dieses dem Verantwortlichen bei Bedarf oder auf Wunsch vorgelegt werden.

Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine vom Verantwortlichen erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie nach Überprüfung durch den Verantwortlichen bestätigt oder geändert wird.

Der Auftragsverarbeiter hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Verantwortliche dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragsverarbeiters dem nicht entgegenstehen.
Unabhängig davon hat der Auftragsverarbeiter personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Weisung des Verantwortlichen ein berechtigter Anspruch des Betroffenen aus Art. 16, 17 oder 18 DSGVO zugrunde liegt.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger Weisung oder Zustimmung durch den Verantwortlichen erteilen.

Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Verantwortliche - 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 Verantwortlichen beauftragte Dritte zu kontrollieren. Die Kontrollen sollen insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort realisiert werden (Art. 28 Abs. 3 Satz 2 lit. h DSGVO).

Der Verantwortliche kann die Einhaltung eines genehmigten Zertifizierungsverfahrens durch den Auftragsverarbeiter gem. Art. 42 DSGVO als Faktor heranziehen, um die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen zu beurteilen.

Der Auftragsverarbeiter stellt sicher, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.
Hierzu wird bis auf Weiteres Folgendes vereinbart:

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragsverarbeiters) ist 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 DSGVO sind auch in diesem Fall umzusetzen. Der Ausschluss der unbefugten Einsichtnahme als auch weiterführender Verarbeitungen personenbezogener Daten durch Dritte, welche sich in der Privatwohnung aufhalten, ist sicherzustellen.

Der Auftragsverarbeiter bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Der Auftragsverarbeiter stellt sicher, 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.

Der Auftragsverarbeiter sichert zu, alle für diesen Auftrag relevanten Geheimnisschutzregeln, die dem Verantwortlichen obliegen, zu beachten. Dazu zählen beispielsweise Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis und weitere.

Berufsgeheimnisträger haben zu gewährleisten, dass die durch den Auftragsverarbeiter zur Verarbeitung der personenbezogenen Daten befugten Personen zusätzlich zu diesem Vertrag zur Geheimhaltung nach § 203 Abs. 4 StGB verpflichtet werden.

Der Auftragsverarbeiter verpflichtet sich, bei der Auftragsverarbeitung in sensiblen Bereichen, beispielsweise bei Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, nur festangestellte Mitarbeiter für Auftragsverarbeitungsarbeiten einzusetzen, die nach dem Verpflichtungsgesetz verpflichtet sind.

Bei der auftragsgemäßen Verarbeitung der personenbezogenen Datenverarbeitung des Verantwortlichen hat er die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragsverarbeiter stellt sicher, 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 DSGVO). Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Beim Auftragsverarbeiter ist als Beauftragte(r) für den Datenschutz Herr / Frau

(Vorname, Name, Organisationseinheit, Telefon)

benannt. Ein Wechsel des Datenschutzbeauftragten ist dem Verantwortlichen unverzüglich mitzuteilen.

Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen unverzüglich über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO zu informieren.

Der Verantwortliche hat das Recht, die Fernwartung zu unterbrechen, insbesondere, wenn er den Eindruck gewinnt, dass unbefugt auf Dateien zugegriffen wird. Die Unterbrechung kann erfolgen, wenn eine Fernwartung mit nicht vereinbarten Hard- und Softwarekomponenten festgestellt wird.

6. Mitteilungspflichten des Auftragsverarbeiters bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter teilt dem Verantwortlichen unverzüglich Störungen, eigene Verstöße oder solche der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen mit. Des Weiteren informiert er den Verantwortlichen über den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.
Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Verantwortlichen gemäß Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter sichert zu, den Verantwortlichen zur Erfüllung dieser Pflichten angemessen zu unterstützen, wenn es erforderlich ist (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO darf der Auftragsverarbeiter für den Verantwortlichen nur nach vorheriger Weisung durchführen (siehe Ziffer 4).

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Verantwortlichen ist dem Auftragsverarbeiter gestattet. Der Auftragsverarbeiter trägt dafür Sorge, dass er den / die Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die diesbezüglich relevanten Prüfunterlagen sind dem Verantwortlichen auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragsverarbeiter hat vertraglich sicherzustellen, dass die zwischen ihm und dem Verantwortlichen vereinbarten Regelungen auch gegenüber Subunternehmern gelten. Im Vertrag mit dem jeweiligen Subunternehmer sind die Angaben so konkret festzulegen, dass die

Verantwortlichkeiten deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen. Insbesondere muss der Verantwortliche berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen bei den Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen (auch vor Ort).

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn dieser die Verpflichtungen bezüglich seiner Beschäftigten nach Art. 29 und Art. 32 Abs. 4 DSGVO erfüllt hat.

Der Auftragsverarbeiter hat die Einhaltung der Pflichten des / der Subunternehmer(s) auf geeignete Weise zu überprüfen.

Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Verantwortlichen auf Verlangen zugänglich zu machen.

Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragsverarbeiter im Einklang mit dem vorliegenden Vertragsabschnitt auferlegt wurden.

Zurzeit werden durch den Auftragsverarbeiter die in Anlage X mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Der Verantwortliche erklärt sich mit deren Beauftragung einverstanden.

Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Hinzuziehung neuer oder Ersetzung bisheriger Subunternehmer. Der Verantwortliche erhält hierdurch die Möglichkeit, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO).

8. Technische und organisatorische Maßnahmen (insbesondere Art. 28 Abs. 3 Satz 2 lit. c und e DSGVO)

Für die konkrete Auftragsverarbeitung wird ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Niveau der Sicherheit der Verarbeitung gewährleistet. Dazu werden einerseits mindestens die Schutzziele von Art. 32 Abs. 1 DSGVO wie Vertraulichkeit, Verfügbarkeit und Integrität 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 (Art. 28 Abs. 3 lit. c). Die Formulierung in Art. 32 Abs. 1 DSGVO „diese Maßnahmen schließen unter anderem Folgendes ein“ verdeutlicht andererseits, dass die dort vorgenommene Aufzählung nicht

abschließend ist. Für die Auftragsverarbeitung sind auch technische und organisatorische Maßnahmen umzusetzen, die die in Kapitel III der DSGVO genannten Rechte der betroffenen Personen wahren (Art. 28 Abs. 3 lit. e). Diese Maßnahmen sollen u. a. sicherstellen,

- dass Daten nur für den Zweck verarbeitet und ausgewertet werden können, für den sie erhoben werden (Zweckbindung),
- dass Betroffene, Verantwortliche und Kontrollinstanzen u. a. erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden und welche Systeme und Prozesse dafür genutzt werden (Transparenz) und
- dass den Betroffenen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam gewährt werden (Intervenierbarkeit).

Entsprechend sind auch die Maßnahmenbereiche zu berücksichtigen, die vorrangig der Minimierung der Eingriffsintensität in die Grundrechte Betroffener dienen.

In Anlage 1 wird die Auswahl der technischen und organisatorischen Maßnahmen passend zum Datensicherheitsrisiko unter Berücksichtigung der Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität, Zweckbindung, Transparenz und Intervenierbarkeit detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragsverarbeiter beschrieben. Die in der Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung werden als verbindlich festgelegt.

Der Auftragsverarbeiter hat bei gegebenem Anlass, mindestens aber alle 2 Jahre, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Verarbeitungssicherheit durchzuführen (siehe Ziffer 8). Das Ergebnis samt vollständigem Auditbericht ist dem Verantwortlichen mitzuteilen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Verantwortlichen abzustimmen.

Soweit die beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen den Anforderungen des Verantwortlichen nicht genügen, benachrichtigt er den Verantwortlichen unverzüglich.

Die Datensicherheitsmaßnahmen des Auftragsverarbeiters können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Sicherheitsstandards und den Grundsatz *Best Practice* nach dem Stand der Technik nicht unterschreiten.
Wesentliche Änderungen sind zwischen Auftragsverarbeiter und Verantwortlichem in dokumentierter Form (schriftlich oder elektronisch) abzustimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragsverarbeiters nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragsverarbeiter sämtliche in seinen Besitz (sowie an Subunternehmen) gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu löschen bzw. zu vernichten / vernichten zu lassen.

Die Löschung bzw. Vernichtung ist dem Verantwortlichen mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
Diese Löschanforderung gilt nicht für Daten, die zur Dokumentationskontrolle und für Revisionsmaßnahmen der Fernwartung benötigt werden.

10. Haftung

Auf Art. 82 DSGVO wird verwiesen.

Im Übrigen wird folgendes vereinbart:
Für Schäden an der Gesundheit, dem Körper oder dem Leben haftet der Auftragsverarbeiter uneingeschränkt.
Sollten Verantwortlicher oder Auftragsverarbeiter gesamtschuldnerisch von einem Dritten in Haftung genommen werden, so stellen sie sich im Innenverhältnis gegenseitig nach dem jeweiligen Verschulden von der Haftung frei.

11. Vertragsstrafe

Bei Verstoß des Auftragsverarbeiters gegen die Regelungen dieses Vertrages, insbesondere zur Einhaltung des Datenschutzes, wird eine Vertragsstrafe von 5% der Summe des jährlichen Wartungsvertrages vereinbart. Berechnungsgrundlage für die Vertragsstrafe bilden die zum Zeitpunkt des Schadenseintrittes gültigen Pflegegebühren (brutto).

12. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie zu 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.

Sollten das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Verantwortlichen beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Verantwortlichen verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Als Gerichtsstand wird Dresden vereinbart.

13. Wirksamkeit der Vereinbarung

Die Unwirksamkeit und / oder Nichtigkeit einzelner Bestimmungen des Vertrages berührt nicht die Gültigkeit der anderen Bestimmungen. Soweit die Vertragspartner an Stelle der unwirksamen oder nichtigen Bestimmungen keine wirksamen, zulässigen und zweckdienlichen Regelungen vereinbaren, soll gelten, was dem gewollten Zweck im Sinne des gesetzlich erlaubten am nächsten kommt. Im Fall von Lücken soll gelten, was nach dem Sinn und dem Zweck dieses Vertrages vernünftigerweise vereinbart worden wäre, wenn die Vertragspartner diese Lücken von vornherein erkannt hätten.

Unterschriften

Verantwortlicher (federführende OE – Auftraggeber)	Auftragsverarbeiter (Auftragnehmer)
Dresden, den	Stadt XYZ, den
.....	.....
Dr. ABC Amtsleiter ABC-Amt Landeshauptstadt Dresden	Herr / Frau ABC Funktion (z.B. Geschäftsführung etc.) Auftragnehmer GmbH
.....	

IT-Dienstleister

Dresden, den

.....

Prof. Dr. Breidung
Betriebsleiter
Eigenbetrieb IT- Dienstleistungen
Landeshauptstadt Dresden

Anlagen

Anlage 1	Technisch-organisatorische Maßnahmen zu Gewährleistung der Schutzziele nach Art. 32 DSGVO des Auftragsverarbeiters
ggf. Anlage X	Beauftragung von Subunternehmen (Inhalte gemäß Ziffer 7)
ggf. Anlage X	Nutzung TeamViewer

Muster-Anlage 1

Technische und Organisatorische Maßnahmen (TOM) zur Gewährleistung der Schutzziele nach Art. 32 DS-GVO

Diese Anlage dient der Auflistung einer Auswahl an technischen und organisatorischen Maßnahmen passend zum Datensicherheitsrisiko zur Gewährleistung der nachfolgend aufgelisteten Schutzziele. Der Auftragsverarbeiter (Auftragnehmer) beschreibt hierbei unter Benennung der eingesetzten IT-Systeme und Verarbeitungsprozesse, wie die jeweiligen Schutzziele durch diese Maßnahme gewährleistet werden. Einige der Schutzziele und Maßnahmen überschneiden sich in ihren Auswirkungen und Aufgaben und wirken damit unweigerlich positiv auf andere Schutzziele ein. Die Auflistung der Maßnahmen stellt nur eine grobe Darstellung und kein vollständiges Informationssicherheitskonzept des Auftragsverarbeiters dar, da dies anderenfalls eine Veröffentlichung interner sicherheitsrelevanter Informationen wäre, welche die Informationssicherheit, als auch den Datenschutz wieder konterkarieren würde. Nach Art. 32 Abs. 1 DS-GVO sind unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der mit ihr verbundenen Risiken geeignete technische und organisatorische Maßnahmen zu treffen, um insbesondere Folgendes sicherzustellen:

1. **Vertraulichkeit**
   Vertraulichkeit ist dann gewährleistet, wenn verarbeitete Daten nur von dem Personenkreis eingesehen und verarbeitet werden kann, welcher auch als Empfängerkreis angedacht ist. Personenbezogene, sensible (z. B. Credentials/Zugangsdaten, Infrastrukturkenntnisse...) oder auch interne (NfD) Daten dürfen somit nicht in die Hände Unbefugter geraten.

   <u>Beispiele zur Gewährleistung:</u>

   - Rechte- und Rollenkonzepte/Berechtigungskonzepte
   - Nutzung von personengebundenen Chipkarten und PIN
   - 4-Augen-Prinzip
   - Firewalls, Intrusion Prevention Systeme, Malware-Erkennung
   - Tresore
   - Auswahl und Nutzung geeigneter kryptographischer Verfahren
   - aktives Patchmanagement
   - Festlegung von Löschfristen und entsprechende datenschutzkonforme Vernichtung/Löschung von Datenträgern
   - Schulung und Sensibilisierung der Mitarbeiter

2. **Verfügbarkeit**
   Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust von Daten, Infrastruktur/Hardware, als auch weiteren Assets, um den ungestörten IT-Betrieb zur täglichen Aufgabenerfüllung aufrecht zu erhalten.

Beispiele zur Gewährleistung:

- Redundanz von Hard- und Software, sowie weiteren kritischen Infrastrukturelementen
- Backup-Strategie, Notfall-/Wiederanlauf-Pläne
- Turnusmäßige Übung der Wiederherstellungsszenarien (Durchführung von Notfallübungen und Erprobung von Wiederanlaufszenarien)
- Unterbrechungsfreie Stromversorgungen (USV)
- physische Sicherungsmaßnahmen (Klimatisierung, Brandschutz)
- Raid-Systeme
- Vertreterregelungen

3. Integrität

Bei der Verhinderung unautorisierter Modifikation von Information wird die Korrektheit (unversehrt, vollständig und aktuell) von Daten und der korrekten Funktionsweise von Systemen und Diensten gewährleistet.

Beispiele zur Gewährleistung:

- Plausibilitätsprüfung der Daten und Zugriffsrechte
- Semantik- und Konsistenzprüfung der Daten / Datenbanken
- Checksummenprüfung/Prüfsummen
- Integritätstests beim Start von Systemen
- Error-Correction-Code-Mechanismen bei Arbeitsspeichern, Festplatten, SSDs etc.
- digitale Signaturen
- Logmechanismen und Kontrolle

4. Zutrittskontrolle

Ergreifung von Maßnahmen zur Verhinderung unbefugter Zutritte(physisch) zu Datenverarbeitungsanlagen.

Beispiele zur Gewährleistung:

- Einteilung in Sicherheitszonen
- elektronisches Zutrittskontrollsystem (Magnet- oder Chipkarten)
- Gebäudesicherheit (Alarmanlagen, Einbruchmeldeanlage mit Aufschaltung zu Sicherheitsfirmen, einbruchhemmende Türen)
- Videoüberwachung

5. Zugangskontrolle

Verhinderung von unbefugter Nutzung von Datenverarbeitungssysteme.

Beispiele zur Gewährleistung:

- automatische Sperrung des Betriebssystems nach einer festgelegten Zeit bei Verlassen des Platzes, als auch Sperrung durch organisatorische Regelungen
- Passwortrichtlinien

6. Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines Datenverarbeitungssystems (Zugriff auf personenbezogene Daten, Programme, und Dokumente) Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass somit personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden

können. Die Berechtigungen ergeben sich aus der Aufgabenzuweisung und der Organisation des Betriebes.

Beispiele zur Gewährleistung:

- Protokollierung von Zugriffen
- Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte
- personengebundene Zugriffsrechte nach aktueller Aufgabenzuweisung
- Zugriffsmatritzen und feingliedrige Berechtigungsvergaben
- Identitätsmanagementsysteme
- klare gelebte Prozesse zu Berechtigungsworkflows
- zeitnahes und bedarfsgerechtes Löschen von Zugriffsrechten

7. Weitergabekontrolle

Gewährleistung, 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.

Beispiele zur Gewährleistung:

- Verschlüsselungstechnologien
- Virtual Private Networks (VPN)
- elektronische Signaturen

8. Eingabekontrolle

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

Beispiele zur Gewährleistung:

- Protokollierung und anlassbezogen Auswertung der Protokolle
- Dokumentenmanagement
- granulare / personengebundene Zugriffsrechte

9. Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
Beispiele zur Gewährleistung:

- eindeutige Vertragsgestaltungen, insbesondere Abgrenzung der Verantwortlichkeiten zwischen Auftraggeber und Auftragnehmer und Festlegung der durchzuführenden Kontrollmaßnahmen
- schriftliche Erteilung von Weisungen (klar und eindeutig)
- Logging und Kontrolle der Logs von Fernwartungsarbeiten
- klare Festlegung von Weisungsempfängern und Weisungsberechtigten Personen
- Kontrolle der Einhaltung der TOMs
- Verpflichtung der Beschäftigten des Auftragnehmers auf das Datengeheimnis gemäß § 53 BDSG (neu)
- soweit erforderlich, Bestellung eines Datenschutzbeauftragten beim Auftragsverarbeiter

- Vereinbarung von angemessenen Vertragsstrafen für Verstöße gegen erteilte Weisungen, insbesondere bei Verstoß gegen die Einhaltung des Datenschutzes

10. Authentizität

Die Authentizität ist dann gewährleistet, wenn ein Dokument bzw. Datum zweifelsfrei seinem Ursprung zugeordnet werden kann.

Beispiele zur Gewährleistung:

- Einsatz von Signaturverfahren, bei denen rechtsverbindlich festgestellt werden kann, ob die Daten von den betroffenen Personen autorisiert (z. B. digital signiert) sind oder wer Urheber der Daten ist, die nicht von den betroffenen Personen stammen (z. B. bei Datenübermittlung)
- Credentials in Verbindung mit Protokollierung und Auswertung

11. Trennungsgebot

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Beispiele zur Gewährleistung:

- physische oder strikt softwaretechnisch (separate Datenbank-Instanzen, virtuelle Container, Trennung auf Schemata-/Nutzerebene, Table Spaces) umgesetzte getrennte Verarbeitung von Daten auf, die zu unterschiedlichen Zwecken erhoben wurden
- Mandantenfähigkeit von Systemen

12. Transparenz

Transparenz bezeichnet die Anforderung, dass sowohl betroffene Personen, als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme hat. Zur Herstellung von Transparenz sind automatisierte Verfahren in aktueller Form nachvollziehbar zu dokumentieren. Die einzelnen Verfahrensschritte müssen dabei so beschrieben werden, dass die Systematik der Prozesse ohne erheblichen zusätzlichen Aufwand nachvollziehbar ist.

Beispiele zur Gewährleistung:

- etablierte Prozesse zu Auskunftspflichten
- Dokumentation der Freigabe oder Vorabkontrolle
- ordnungsgemäßes Führen der Verzeichnisse der Verarbeitungstätigkeiten
- Dokumentation von wesentlichen Programmänderungen
- laufende Fortschreibung der Programmdokumentation (Betriebshandbücher, Schnittstellendokumentationen, Übersichtspläne, Administratorenhandbücher etc.), welche schnell und unkompliziert von neuem Personal überblickt und verwendet werden können müssen
- Dokumentation von Verfahren insbesondere mit den Bestandteilen Geschäftsprozesse, Datenbestände, Datenflüsse, dafür genutzte IT-Systeme, Betriebsabläufe, Verfahrensbeschreibungen, Zusammenspiel mit anderen Verfahren

13. Speicherbegrenzung (Datensparsamkeit/Datenminimierung)

Bereits im Vorfeld der Entwicklung und Auswahl von Datenverarbeitungssystemen und bei der Ausgestaltung der konkreten Datenverarbeitungsprozesse ist darauf hinzuwirken, dass keine oder möglichst wenig personenbezogenen Daten verarbeitet werden. Es sind somit über die Zweckbindung hinaus nur solche personenbezogenen Daten zu verarbeiten, die für die Erfüllung des jeweils zugrundeliegenden Zwecks nötig sind (Erforderlichkeit).

Beispiele zur Gewährleistung:

- Verzicht auf die Erfassung bestimmter Arten von Daten, z. B. sensitive personenbezogene Daten
- minimalistische Abfrage-Gestaltung von Fragebögen oder Erhebungsformularen
- Sicherstellung der frühestmöglichen Löschung von Daten und Festlegung von automatischen Verfallsdaten für Datensätze
- Festlegung von Löschfristen und Überwachung der Einhaltung dieser
- anonyme Erhebungs-/Verarbeitungstechnologien
- Verzicht auf Identifizierungsverfahren bei der Nutzung von Webseiten (Achtung: Konterkarierung der Informationssicherheit möglich)
- Filtertechnologogien

14. Revisionsfähigkeit

Revisionsfähigkeit bedeutet, dass nachprüfbar ist, wie Daten in einen Datenbestand gelangt sind und welche Veränderungen sie im Laufe der Zeit durch wen erfahren haben. Nachprüfbar muss sein, wer für das Aufnehmen bestimmter Daten in einen Datenbestand oder ihr Entfernen daraus die Verantwortung trägt.

Beispiele zur Gewährleistung:

- Protokollierung der Zugriffe auf und Änderungen im Verfahren (Achtung: Diese Daten bergen jedoch selbst ein datenschutzrechtliches Risiko und unterliegen deshalb einer engen Zweckbindung.)
- regelmäßige Auswertung von Protokolldateien, als auch deren Funktion
- Deaktivierung der Schreibrechte auf Protokolldateien (Unveränderbarkeit)
- Nutzung von Dokumentenmanagementsystemen

15. Belastbarkeit

Im Einklang mit der Verfügbarkeit bedeutet die Belastbarkeit ein zeitgerechtes zur Verfügung Stellen von Daten und Systemen, um eine ordnungsgemäße Verarbeitung in einem angemessenen Zeitrahmen gewährleisten zu können, wenn diese benötigt werden.

Beispiele zur Gewährleistung:

- Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage z. B. DDOS, höhere Gewalt)
- Redundante und potente Auslegung von Hard- und Software, sowie der zugehörigen Infrastruktur
- Umsetzung von Reparaturstrategien und Ausweichprozessen

16. Intervenierbarkeit

Bezeichnet die Sicherstellung, dass den betroffenen Personen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam gewährt werden können.

Beispiele zur Gewährleistung:

- etablierte Prozesse zu Auskunftspflichten und Rechte der Betroffenen (Auskunftsrecht, Berichtigung der Daten, Löschen und Sperren, Widerspruchsrecht)
- Einrichtung eines Single Point of Contact (SPoC) für betroffene Personen
- operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten
- Schaffung differenzierter Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten und der damit einhergehenden notwendigen Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen
- Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem
- Implementierung standardisierter Abfrage- und Dialogschnittstellen für betroffene Personen zur Geltendmachung

17. Zweckbindung (Nichtverkettung)

Das Gewährleistungsziel Nichtverkettbarkeit bezeichnet die Anforderung, dass Daten nur für den Zweck verarbeitet und ausgewertet werden, für den sie erhoben werden. Die Verarbeitung muss nach Zwecken getrennt ermöglicht (Funktionstrennung) bzw. die Daten je nach Verarbeitungszweck voneinander getrennt gespeichert werden (Datentrennung). Gegebenenfalls muss der Datenbestand durch Duplizierung und Reduzierung auf den für den neuen Zweck erforderlichen Umfang angepasst werden.

Beispiele zur Gewährleistung:

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten
- programmtechnische Unterlassung bzw. Schließung von Schnittstellen in Verfahren und Verfahrenskomponenten
- qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung
- Trennung nach Organisations-/Abteilungsgrenzen
- Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentisierungsverfahrens
- Verarbeitung pseudonymer bzw. anonymisierter Daten
- geregelte Zweckänderungsverfahren

18. Pseudonymisierung (ggf. Anonymisierung) (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Gesonderte Aufbewahrung und Zugänglichkeit für den verarbeitenden Personenkreis unter Nutzung entsprechender technischer und organisatorischer Maßnahmen.

Beispiele zur Gewährleistung:

- Festlegung der zu pseudonymisierenden Daten
- geregelte Rechtetrennung zwischen Verarbeiter der pseudonymisierten Daten und der „Kreuz-/Zuordnungstabellen“ zur Rückführung (Festlegung der Personen, die zur Verwaltung der Pseudonymisierungsverfahren, zur Durchführung der Pseudonymisierung und ggf. der Depseudonymisierung berechtigt sind)
- Festlegung der zulässigen Anlässe für Pseudonymisierungs- und Depseudonymisierungsvorgänge
- zufällige Erzeugung der Zuordnungstabellen oder der in eine algorithmische Pseudonymisierung eingehenden geheimen Parameter

- Schutz der Zuordnungstabellen bzw. geheimen Parameter sowohl gegen unautorisierten Zugriff als auch gegen unautorisierte Nutzung

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

Beispiele zur Gewährleistung:

- Incident-Response-Management (Nachweis über ein Ticketsystem)
- regelmäßige Information über auftretende Schwachstellen und andere Risiken
- Möglichkeit der regelmäßigen Überprüfungen durch den/die Datenschutzbeauftragte/n und weitere Prüfinstanzen (z.B. Wirtschaftsprüfer, Rechnungsprüfungsamt)
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- Auftragskontrolle
- keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z. B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.
- regelmäßige Revision des Vertrages und der technischen und organisatorischen Maßnahmen anhand der sich ändernden eingesetzten Technik und des Vertragsgegenstandes, der aktuellen Bedrohungslage und dem Stand der Technik -> automatisches Ablaufdatum der Verträge nach 2 Jahren
- externe Prüfungen, Audits, Zertifizierungen

Anlage X zum Vertrag Nr. xxx

Nutzung von TeamViewer

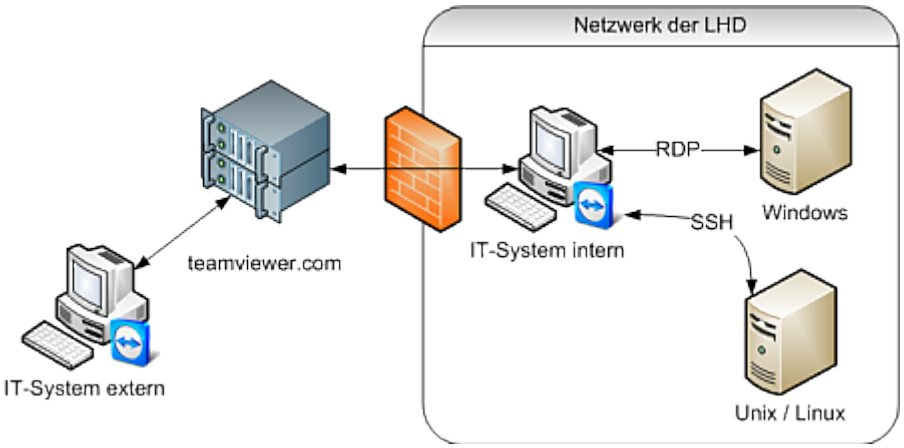
zur Erbringung der im Vertrag angegebenen Vertragsinhalte

Systemvoraussetzungen

Der externe Dienstleister muss die TeamViewer-Software für sich selbst beschaffen, diese wird nicht durch den EB IT bereitgestellt (IT-System extern). Der externe Dienstleister muss somit eine gültige TeamViewer-Lizenz besitzen, als auch eine aktuelle, zu der vom EB IT bereitgestellten kompatible Version verwenden.

Funktionsweise

Die Fernwartung mit TeamViewer setzt auf einem 4-Augen-Prinzip auf, d.h. der externe Dienstleister kann sich erst nach Bestätigung des internen Mitarbeiters mittels TeamViewer auf dessen Rechner aufschalten. Entweder kann der externe Dienstleister nun direkt diesen Mitarbeiter auf dessen Rechner unterstützen oder sich zu anderen internen IT-Systemen (z.B. Servern) weiterverbinden. Der interne Mitarbeiter muss die Fernwartung beobachten und kann im Notfall die Sitzung unterbrechen. Dateiübertragungen in bzw. aus dem Netzwerk der LHD sind nach Bestätigung durch den internen Mitarbeiter ebenfalls möglich. Der Verbindungsaufbau / -abbau und die Übertragung von Dateien wird auf dem IT-System des internen Mitarbeiters protokolliert.



Zusätzliche Sicherheitsmaßnahmen

Wie oben schon erwähnt wird mit dem Software-Paket eine geprüfte und freigegebene TeamViewer-Konfiguration ausgerollt. Die von EB IT bereitgestellte TeamViewer-Konfiguration enthält folgende weitere Maßnahmen:

- der Externe kann die interne TeamViewer-Installation nicht steuern
- der Externe kann die Tastatur und Maus am internen IT-System nicht sperren
- der Externe kann Dateien nur nach Bestätigung durch den internen Mitarbeiter übertragen
- die Protokollierung der Verbindungen und der Dateiübertragung ist auf dem internen IT-System immer aktiviert
- diese Konfiguration kann nicht durch den Externen verändert werden
- eine Veränderung dieser Konfiguration durch den internen Mitarbeiter ist aufgrund dieser Betriebsanweisung nicht zulässig und kann nicht ohne administrative Benutzerrechte durchgeführt werden

Weiterhin verweisen wir neben der zugehörigen Anlage „Allgemeine technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO“ auf die ebenfalls zum Vertrag zugehörigen aktuellen "Sicherheitsinformationen" der TeamViewer GmbH, welche unter folgenden Quellen einzusehen sind:

- https://dl.teamviewer.com/docs/de/TeamViewer-Security-Statement-de.pdf
- https://www.teamviewer.com/de/eula/#dpa
- https://www.teamviewer.com/de/trust-center/sicherheit/
- https://www.teamviewer.com/de/dpa-annex/
    - speziell: https://static.teamviewer.com/resources/2020/12/ANNEX-2_TV-Technical-and-Organizational-Measures_DE.pdf und nachfolgende Versionen aktuellen Standes

Anlage X zum Vertrag Nr. xxx

Subunternehmer

zur Erbringung der im Vertrag angegebenen Vertragsinhalte

1.

Firma

Straße

PLZ Ort

Kontaktdaten: (Telefon/Mail)

2.

Firma

Straße

PLZ Ort

Kontaktdaten: (Telefon/Mail)