Vertrag zur Auftragsdatenverarbeitung gemäß Art. 28 ff. DS-GVO

[Stand: Januar 2019]

Vereinbarung

zwischen dem/der

[.....]

- **Verantwortlicher** - nachstehend Auftraggeber genannt -

und dem/der

Brunner & Schmidt Datentechnik GmbH
Lübener Straße 6

90471 Nürnberg

- **Auftragsverarbeiter** - nachstehend Auftragnehmer genannt

[ggf.: Vertreter gemäß Art. 27 DS-GVO:

1. Gegenstand und Dauer des Auftrags

(1) **Gegenstand**

☒ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Alle EDV Dienstleistungen, die für die Durchführung der Wartung, Instandhaltung und den sicheren Betrieb der EDV-Anlagen des Auftraggebers notwendig sind. Administration der Hardware und Software dieser Anlagen.

(2) **Dauer**

☒ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien ohne Frist gekündigt werden. Jedoch ist der Vertrag an das Auftragsverhältnis zur EDV-Dienstleistung gebunden.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

☒ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:
IT-Dienstleistungen vor Ort; Fernwartung; DATEV-Software Updates; Sonstige Software-Updates; Hotline; Rechenzentrumsdienstleistungen (PPU, PPU Basic), externe Datensicherung, Nutzung von Cloud-Diensten, z.B. Mailschutz, Monitoring, Virenschutz und Cloudspeicher und weitere (Definition der Aufgaben), etc.

☒ Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(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

☒ Kennwörter, Berechtigungen, …

☒ Planungs- und Steuerungsdaten

☒ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

(3) **Kategorien betroffener Personen**

☒ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
- ☒ Kunden
- ☒ Mandanten
- ☒ Mieter
- ☒ Interessenten
- ☒ Abonnenten
- ☒ Beschäftigte
- ☒ Lieferanten
- ☒ Handelsvertreter
- ☒ Ansprechpartner
- ☒ Kunden, Lieferanten und Beschäftigte der Kunden/Mandanten
- ☒ Mitglieder
- ☐...

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers 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.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 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 Datenschutzbeauftragte(r) ist beim Auftragnehmer Frau Mareike Rypalla (0911) 376525-0, datenschutz@brunner-schmidt.de bestellt. Ein Wechsel der(s) Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b) ☒ Die Wahrung der Vertraulichkeit gemäß Art. 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 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) ☒ Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

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

e) ☒ Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag 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.

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

g) ☒ Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(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 z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. 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 sowie Kontrollmaßnahmen zu ergreifen.

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

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☒ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Acmeo GmbH	Mailänder Straße 2 D-30539 Hannover	Cloud Distribution
Hornetsecurity GmbH	Am Listholze 78 D-30177 Hannover	Cloud Distribution
Kaspersky Labs GmbH	Despag-Str. 3 D-85055 Ingolstadt	Cloud Distribution
Bussymouse Business Systems GmbH	Am Mittelfelde 29 D-30519 Hannover	Cloud Distribution

c) ☒ Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

☒ der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

☒ der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

☒ eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(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.
(4) Eine weitere Auslagerung durch den Unterauftragnehmer

☒ ist nicht gestattet;

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

☒ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

☒ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

☒ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(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.

10. Löschung und Rückgabe von personenbezogenen Daten

(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.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens 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.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Nürnberg, den _____

Auftraggeber:

_____

Name, Vorname

_____

Unterschrift

Nürnberg, den

Auftragnehmer:
Brunner & Schmidt
Datentechnik GmbH
Lübener Straße 6
90471 Nürnberg

_____

Name, Vorname

_____

Unterschrift

Anlage – Technisch-organisatorische Maßnahmen – Brunner & Schmidt

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

a. Zutrittskontrolle

Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

	Technische Maßnahmen		Organisatorische Maßnahmen
☒	Festlegung der Sicherheitsbereiche	☒	Personenkontrolle beim Pförtner/Empfang
☒	Manuelles Schließsystem	☐	Protokollierung der Besucher / Besucherbuch
☒	Sicherheitsschlösser	☒	Schlüsselregelung / Schlüsselbuch
☒	Chipkarten / Transponder-Schließsystem	☐	Sorgfältige Auswahl von Sicherheitspersonal
☒	Lichtschranken / Bewegungsmelder	☐	Tragepflicht von Mitarbeiter- / Gästeausweis
☐	Schließsystem mit Codesperre	☒	Personelle und organisatorische Zutrittskontrollmaßnahmen:
☒	Automatisches Zugangskontrollsystem	☐	
☐	Alarmanlage	☐	
☒	Videoüberwachung der Zugänge	☐	
☐	Absicherung von Gebäudeschächten	☐	

b. Zugangskontrolle

Verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

	Technische Maßnahmen		Organisatorische Maßnahmen
☒	Authentifikation mit Benutzer + Passwort	☒	Benutzerberechtigungen verwalten
☒	Authentifikation mit biometrischen Daten	☒	Erstellen von Benutzerprofilen
☒	Einsatz von Anti-Viren-Software	☒	Passwortvergabe / Passwortregeln
☒	Einsatz von Firewalls	☒	Personenkontrolle beim Pförtner / Empfang
☒	Einsatz von Mobile Device Management	☐	Protokollierung der Besucher / Besucherbuch
☒	Einsatz von VPN-Technologie	☒	Schlüsselregelung / Schlüsselbuch
☐	Gehäuseverriegelungen	☒	Sorgfältige Auswahl von Reinigungspersonal
☐	Sperren von externen Schnittstellen (z.B. USB-Anschlüsse)	☐	Sorgfältige Auswahl von Sicherheitspersonal
☒	Verschlüsselung von Datenträgern	☐	
☒	Verschlüsselung von Smartphones	☐	

c. Zugriffskontrolle

Gewährleistung, 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.

	Technische Maßnahmen		Organisatorische Maßnahmen
☒	Einsatz von Aktenvernichtern	☒	Anzahl der Administratoren auf das „Notwendigste“ reduzieren
☒	Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)	☒	Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit Zertifikat)
☒	Physische Löschung von Datenträgern vor deren Wiederverwendung	☒	Erstellen eines Berechtigungskonzepts
☒	Protokollierung der Vernichtung von Daten	☒	Passwortrichtlinie inkl. Länge und Wechsel
☒	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	☒	Sichere Aufbewahrung von Datenträgern
☒	Verschlüsselung von Datenträgern	☒	Verwaltung der Benutzerrechte durch Systemadministratoren
☒	Verschlüsselung von Smartphones	☐	
☒	Einsatz von Anti-Viren-Software	☐	
☒	Einsatz von Firewalls	☐	
☒	Einsatz von Mailschutzsystemen	☐	
☐	Sandboxing		

d. Trennungskontrolle

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

	Technische Maßnahmen		Organisatorische Maßnahmen
☐	Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System	☒	Erstellung eines Berechtigungskonzepts
☒	Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern	☒	Festlegung von Datenbankrechten
☒	Trennung von Produktiv- und Testsystem	☒	Logische Mandantentrennung (softwareseitig)
☐	Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden	☐	Versehen der Datensätze mit Zweckattributen/Datenfeldern

e. Pseudonymisierung

Gewährleisten, dass die Pseudonymisierung, nach Art. 4 Nr. 5 DSGVO, die Identität der verarbeiteten Daten der Personen schützt, sodass keine Rückschlüsse auf eine konkrete Person möglich sind. Pseudonymisieren ist das Ersetzen des Namens und anderer

Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

	Technische Maßnahmen		Organisatorische Maßnahmen
☐		☐	Verwendung von Kennzeichen z.B. Kunden-/Mandantennummern anstelle von Namen (identifizierende Merkmale)
☐		☐	Trennung identifizierenden Daten und der personenbezogenen Daten, sowie räumlich getrennte Aufbewahrung
☐		☐	Prinzip der Datenminimierung wird ergriffen, d.h. Daten werden für die Zwecke der Verarbeitung notwendiger Maß beschränkt sein

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

a. Weitergabekontrolle

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.

	Technische Maßnahmen		Organisatorische Maßnahmen
☒	Einrichtungen von VPN-Technologie	☐	Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
☒	E-Mail-Verschlüsselung	☐	Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
☐	Sichere Transportbehälter/-verpackungen	☐	Sorgfältige Auswahl von Transportpersonal und –fahrzeugen
☒	Einsatz von Anti-Viren-Software	☐	Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
☒	Einsatz von Firewalls	☐	
☒	Einsatz von Mailschutzsystemen	☐	
☐	Sandboxing	☐	

b. Eingabekontrolle

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

	Technische Maßnahmen		Organisatorische Maßnahmen
☐	Protokollierung der Eingabe, Änderung und Löschung von Daten	☒	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
☒	Einsatz von revisionssicheren Archivsystemen, z.B. Mailarchivierung, DMS, DATEV-Belegarchiv	☐	Erstellen einer Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
☐		☒	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
☐		☒	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

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

a. Verfügbarkeitskontrolle

Gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

	Technische Maßnahmen		Organisatorische Maßnahmen
☒	Feuerlöschgeräte in Serverräumen	☐	Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
☐	Feuer- und Rauchmeldeanlagen	☒	Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
☐	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen	☒	Erstellen eines Backup- & Recoverykonzepts
☐	Klimaanlage in Serverräumen	☒	Erstellen eines Notfallplans
☒	Schutzsteckdosenleisten in Serverräumen	☒	Testen von Datenwiederherstellung
☒	Unterbrechungsfreie Stromversorgung (USV)	☒	Serverräume nicht unter sanitären Anlagen
☒	Redundante Daten / Datenträger / Datenverarbeitungssysteme	☐	In Hochwassergebieten: Serverräume über der Wassergrenze
☒	Monitoring	☐	
☒	Archivierungssysteme intern/extern	☐	
☒	Einsatz von Anti-Viren-Software	☐	
☒	Einsatz von Firewalls	☐	

b. Rasche Wiederherstellbarkeit

Gewährleistet, dass nach einem physischen oder technischen Zwischenfall die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen rasch wiederhergestellt werden kann. Sowie, dass die Wiederherstellbarkeit in regelmäßigen Abständen getestet wird.

Technische Maßnahmen	Organisatorische Maßnahmen

☐		☒	Aktuelle Datensicherung und Kontrolle
☐		☒	Errichtung eines Notfall-Management-Konzept
☐		☒	Erstellung von Notfallplänen, sowie Handlungsanweisungen (Leitfäden)
☐		☒	Regelmäßigen Termin der Datensicherung festlegen
☐		☒	Datenrücksicherung
☐		☒	Penetrationstests
☐		☒	Verfügbarkeit von Ersatzhardware

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

a. Datenschutz-Management

Gewährleistet, dass die Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und nach Außerbetriebnahme von Verfahren zur Informationsverarbeitung sicher zu stellen.

Technische Maßnahmen		Organisatorische Maßnahmen	
☐		☒	Nachweis, dass das Unternehmen angemessene und wirksame Maßnahmen ergreift, um datenschutzrechtliche Verpflichtungen und Grundsätze umzusetzen (Datenschutzkonzept)
☐		☒	Erstellung des Datenschutzkonzeptes Soll-Ist-Abgleich (Datenschutz-Check)
☐		☒	Verantwortliche der Bereiche festlegen
☐		☒	Mitarbeiterschulung zum Thema Datenschutz
☐		☒	Regelmäßige Überprüfung des Datenschutzes im laufenden Betrieb

b. Incident-Response-Management

Gewährleistet, dass Maßnahmen und Prozesse auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in IT-Bereichen ergriffen werden. Das IT-Störungsmanagement berücksichtigt dabei technische Probleme, sowie konkrete Angriffe auf die IT-Infrastruktur. Ziel ist die möglichst rasche Wiederherstellung des Systems.

	Technische Maßnahmen		Organisatorische Maßnahmen
☐		☒	Festlegung von Verantwortungsbereichen und Ansprechpartnern in allen Abteilungen/Bereichen des Unternehmens
☐		☒	Mechanismen zur frühzeitigen Erkennung und Meldung von Sicherheitsvorfällen
☐		☒	Vorliegen eines Notfall-Management-Konzepts (Geschäftsführer, Feuerwehr, IT-Firma, etc.)

c. Datenschutzfreundliche Voreinstellungen

Gewährleistet, dass Grundeinstellungen von Produkten und Diensten so gestaltet sind, dass möglichst wenig personenbezogene Daten erhoben oder verarbeitet werden. Sind Voreinstellungen schon vorhanden so ist zu gewährleisten, dass beim Zeitpunkt der Verarbeitung geeignete technische und organisatorische Maßnahmen ergriffen werden, z.B. Pseudonymisierung, Datenminimierung

	Technische Maßnahmen		Organisatorische Maßnahmen
☐		☐	Anwendung von Pseudonymisierung
☐		☐	

d. Auftragskontrolle

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

	Technische Maßnahmen		Organisatorische Maßnahmen
☐		☒	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
☐		☒	Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
☐		☒	Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG
☐		☒	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

☐		☒	Verpflichtung der Mitarbeiter des Auftrag-nehmers auf das Datengeheimnis (§ 53 BDSG)
☐		☐	Vertragsstrafen bei Verstößen
☐		☐	Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechender Dokumentation
☐		☒	Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbaren

Anlagen:

– Technisch-organisatorische Maßnahmen –
M-Net (für RZ-Kunden)

– Technisch-organisatorische Maßnahmen –
ACMEO

– Technisch-organisatorische Maßnahmen –
Hornet Security

– Technisch-organisatorische Maßnahmen –
Busymouse

Nürnberg, den

Ort/Datum

Unterschrift