Auftragsverarbeitung gemäß Art. 28 Abs. 3 DSGVO

Vereinbarung zwischen

_____

(Eigentümer/Vermieter)

- Verantwortlicher gem. Art. 24 DSGVO –

(nachstehend **Auftraggeber**)

und

Home HT GmbH

Mulackstr. 19

10119 Berlin

- Auftragsverarbeiter -

(nachstehend **Auftragnehmer**)

1. Gegenstand und Dauer des Auftrags

1.1. Der Gegenstand des Auftrags

Der Auftragnehmer erhebt und/oder verarbeitet und/oder nutzt Auftraggeber-Daten im Auftrag und nach Weisung des Auftraggebers i. S. v. Art. 28 Abs. 3 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt im datenschutzrechtlichen Sinn Verantwortlicher („Herr der Daten“). Gegenstand des Auftrages ist die Abwicklung der Betriebskostenabrechnung bei Mietern der Wohnobjekte des Auftraggebers, bei denen ein Mietverhältnis besteht.

1.2. Die Dauer des Auftrags

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrages. Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen. Der Auftragnehmer darf die Auftraggeber-Daten im Rahmen des datenschutzrechtlich Zulässigen für eigene Zwecke auf eigene Verantwortung verarbeiten und nutzen, wenn eine gesetzliche Erlaubnisvorschrift oder eine Einwilligungserklärung des Betroffenen das gestattet. Auf solche Datenverarbeitungen findet dieser Vertrag keine Anwendung. In jedem Fall darf der Auftragnehmer die Auftraggeber-Daten anonymisieren und in anonymisierter Form für eigene Zwecke verarbeiten und nutzen.

2. Konkretisierung des Auftragsinhalts

2.1. Art und Zweck der vorgesehenen Verarbeitung von Daten sind konkret beschrieben in den Allgemeinen Geschäftsbedingungen die bei der Anmeldung Bestandteil des Hauptvertrages werden.

Die Erhebung und/oder Verarbeitung und/oder Nutzung der Auftraggeber-Daten dient der Erfüllung der Leistungen des Auftragnehmers im Sinne des Hauptvertrages.

2.2. Die Art der verwendeten personenbezogenen Daten

Nachfolgende Datenkategorien und Betroffene Personengruppen sind Gegenstand der Erhebung und/oder Verarbeitung und/oder Nutzung:

Betroffenen Personengruppen:
- Mieter

Datenkategorien:
- Vorname
- Name
- Anschrift
- Geburtsdatum
- Familienstatus
- Titel
- E-Mail-Adresse
- Mobilnummer
- Festnetznummer
- Kontodaten

2.3. Angemessenheit des Schutzniveaus personenbezogener Daten

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

Das angemessene Schutzniveau wird in diesem Fall durch das Vorliegen mindestens einer der folgenden Voraussetzungen erfüllt:

- einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3) oder
- verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b) i. V. m. Art. 47 DSGVO) oder
- Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. C) und d) DSGVO) oder
- genehmigte Verhaltensregeln (Art 46 Abs. 2 lit. e) i. V. m. Art. 40 DSGVO) oder
- einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f) i. V. m. Art. 42 DSGVO).

3. Technische und organisatorische Maßnahmen

3.1. 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.

3.2. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c), 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 DSGVO zu berücksichtigen (Einzelheiten in Anlage 1).

3.3. 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 und dem Auftraggeber schriftlich mitzuteilen.

4. Berichtigung, Einschränkung und Löschung von Daten

4.1. 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.

4.2. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Löschung, 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 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Soweit eine gesetzliche Verpflichtung besteht, die Benennung eines Datenschutzbeauftragten gem. Art. 37 bis 39 DSGVO. Die Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Bei einem Wechsel des Datenschutzbeauftragten wird der Auftraggeber unverzüglich informiert. Der Datenschutzbeauftragte des Auftragnehmers ist:

   WS Datenschutz GmbH
   Christian Scholtz , LL. M.
   Meinekestraße 13
   10719 Berlin
   kontakt@ws-datenschutz.de
   +49 30 / 88 72 07 88

b) Soweit der Auftragnehmer nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet ist, wird stattdessen ein Ansprechpartner beim Auftragnehmer benannt.

c) Soweit der Auftragnehmer seinen Sitz außerhalb der Union hat, wird ein Ansprechpartner beim Vertreter nach Art. 27 Abs. 1 DSGVO in der Union benannt.

d) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b), 29, 32 Abs. 4 DSGVO. 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. 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.

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

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

g) 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.

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

6. Unterauftragsverhältnisse

6.1. Als Unterauftragsverhältnisse 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.

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

Der Auftraggeber stimmt der Beauftragung der im Folgenden aufgeführten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu.

Unterauftragnehmer	Sitz	Tätigkeit	Auftrags-verarbeitungs-vertrag	Garantien im Fall von Drittländern
n/a	**n/a**	**n/a**	**n/a**	**n/a**

Die Auslagerung auf Unterauftragnehmer oder der Wechsel eines bestehenden Unterauftragnehmers sind dabei zulässig, soweit:

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

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

c) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten.

6.3. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

6.4. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende

Maßnahmen nach 2.4 sicher. Gleiches gilt, wenn Dienstleister im Sinne von 6.1 Satz 2 eingesetzt werden sollen.

6.5. Eine weitere Auslagerung durch den Unterauftragnehmer an weitere Unterauftragnehmer bedarf der ausdrücklichen Zustimmung (min. Textform) des Hauptauftraggebers. Dabei sind sämtliche vertraglichen Regelungen in der Vertragskette auch den weiteren Unterauftragnehmern aufzuerlegen.

7. Kontrollrechte des Auftraggebers

7.1. 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 rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Mehrfache Überprüfungen innerhalb eines Kalenderjahres sind nur mit Zustimmung des Auftragnehmers zulässig.

7.2. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO 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.

7.3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann durch mindestens einer der folgenden Nachweise erfüllt werden:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO oder
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO oder
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, Informationssicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder
- eine geeignete Zertifizierung durch Informationssicherheits- oder Datenschutzaudit (z. B. nach ISO 27001, PCI DSS, BSI IT-Grundschutz, European Privacy Seal).

7.4. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen, sofern die Kontrolle des Auftraggebers über das übliche Ausmaß hinausgeht.

8. Mitteilung bei Verstößen des Auftragnehmers

8.1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO 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.

8.2. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

9.1. Mündliche Weisungen bestätigt der Auftraggeber zu Zwecken der Dokumentation unverzüglich (mind. Textform).

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

10. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

11. Löschung und Rückgabe von personenbezogenen Daten

11.1. 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.

11.2. 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.

11.3. 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.

12. Vertraulichkeitsvereinbarung

Beide Parteien verpflichten sich, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

13. Salvatorische Klausel

Sollten eine oder mehrere Klauseln dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sein, so soll dies die Gültigkeit der Vereinbarung im Übrigen nicht berühren. Die Parteien werden die unwirksame bzw. undurchführbare Klausel durch eine Bestimmung ersetzen, die dem Sinn und Zweck der unwirksamen Klausel zulässigerweise wirtschaftlich und rechtlich möglichst nahekommt. Das Gleiche gilt für Lücken in dieser Vereinbarung.

Ort, Datum

Auftraggeber (Eigentümer/Vermieter)

Ort, Datum

Auftragnehmer (Home HT GmbH)

Anlage 1
Übersicht: technisch-organisatorische Maßnahmen zur Datensicherheit gem. Art. 32 DSGVO

Firma: Home HT
Verantwortlicher: Thilo Konzok
Anschrift: Mulackstraße 19, 10119 Berlin
Telefon: 030 88789123
E-Mail: info@home.ht
Internet: home.ht

Datenschutzbeauftragter:

Christian Scholtz, LL.M.
WS Datenschutz GmbH
Meinekestraße 13
10719 Berlin

F: 030 / 88 72 07 88
kontakt@ws-datenschutz.de

1. Organisationskontrolle

Zweck: Die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Gemeint ist damit, dass sich der Datenschutz nicht an die Organisation, sondern die Organisation an den Datenschutz anpassen sollte.

Maßnahmen:

☑ Mitarbeiter werden regelmäßig (mindestens alle zwei Jahre) auf das Datengeheimnis verpflichtet
☑ Mitarbeiter werden regelmäßig (mindestens einmal jährlich) auf den Datenschutz am Arbeitsplatz sensibilisiert
☐ Es wird regelmäßig eine Auditierung durch den Datenschutzbeauftragten vorgenommen
☐ Ein Datensicherheitskonzept/Informationssicherheitsmanagement ist vorhanden
☐ Anmerkungen: Klicken oder tippen Sie hier, um Text einzugeben.

2. Pseudonymisierung gem. Art. 32 Abs. 1 lit. a DSGVO

Maßnahmen:

☐ Personenbezogenen Daten mit normalem Schutzbedarf werden in zwei Teile aufgebrochen und damit pseudonymisiert
☐ Personenbezogenen Daten mit erhöhtem Schutzbedarf werden in zwei Teile aufgebrochen und damit pseudonymisiert
☑ Es werden, soweit möglich, pseudonymisierte und anonymisierte Daten verwendet
☐ Anmerkungen: Klicken oder tippen Sie hier, um Text einzugeben.

3. Verschlüsselung gem. Art. 32 Abs. 1 lit. a DSGVO

Maßnahmen:

☐ Verschlüsselung von Festplatten mit personenbezogenen Daten
☐ Verschlüsselung von Smartphone-Inhalten
☐ Verschlüsselung von mobilen Datenträgern
☐ Verschlüsselung von E-Mails (z. B. PGP)
☐ Anmerkungen: Klicken oder tippen Sie hier, um Text einzugeben.

4. Vertraulichkeit gem. Art. 32 Abs.1 lit. b DSGVO

Zutrittskontrolle

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

Maßnahmen:

☐ Schriftliche Zutrittsregelungen zum Betreten des Rechenzentrums/der Räume mit DV-Anlagen sind vorhanden
☐ Alarmanlage
☐ Automatisches Zutrittskontrollsystem, Ausweisleser
☑ Schlüsselregelung (Schlüsselverwaltung: Schlüsselausgabe etc.)
☐ Sicherheitsschlösser
☐ Chipkarten-/Transponder-Schließsystem
☐ Biometrie (Fingerabdrücke o. ä.)
☑ Manuelles Schließsystem
☐ Schranken/Vereinzelungsanlagen (Drehkreuze o. ä.)
☐ Werkschutz/Pförtner
☐ Empfang mit Anmeldung
☐ Sorgfältige Auswahl von Wachpersonal
☑ Sorgfältige Auswahl von Reinigungspersonal
☐ Lichtschranke/Bewegungsmelder
☐ Feuerfeste Türen
☐ Fenstervergitterung
☑ Videoüberwachung der Zugänge
☐ Anmerkungen: Klicken oder tippen Sie hier, um Text einzugeben.

Zugangskontrolle

Zweck: Verhinderung, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Maßnahmen:

☑ Authentifikation mit Benutzer und Passwort
☑ Verwaltung von Benutzerberechtigungen
☑ Erstellen von Benutzerprofilen
☐ Einsatz von Anti-Viren-Software
☑ Passwortvergabe/Passwortregeln
☐ Einsatz von Firewalls
☐ Einsatz von VPN-Technologie
☑ Umgehende Sperrung von Berechtigungen beim Ausscheiden von Mitarbeitern
☐ Blickschutzfolien für mobile Rechner
☐ Anmerkungen: Klicken oder tippen Sie hier, um Text einzugeben.

Zugriffskontrolle

Zweck: 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.

Maßnahmen:

☐ Schriftliches Berechtigungskonzept vorhanden
☑ Zuordnung von Benutzerrechten/Erstellen von Benutzerprofilen
☑ Verwaltung der Rechte durch System-Administrator
☑ Anzahl der Administratoren auf das "Notwendigste" reduziert
☐ Gesicherte Nutzung von USB-Schnittstellen
☐ Automatische Sperrung des Arbeitsplatzes
☑ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
☑ Einsatz von Akten-/Datenträgervernichtern
☑ Verschlüsselung von Datenträgern
☑ Sichere Aufbewahrung von Datenträgern
☑ Ordnungsgemäße Vernichtung von Datenträgern
☐ Löschungskonzept für Daten
☐ Protokollierung der Vernichtung
☐ Anmerkungen: Klicken oder tippen Sie hier, um Text einzugeben.

Trennungskontrolle

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

Maßnahmen:

☐ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
☐ Logische Mandantentrennung (softwareseitig)
☑ Trennung von Produktiv- und Testsystem
☑ Technologie zur Festlegung von Datenbankrechten
☑ Trennung von Daten verschiedener Auftraggeber
☐ Anmerkungen: Klicken oder tippen Sie hier, um Text einzugeben.

Weitergabekontrolle

Zweck: Gewährleistung, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Maßnahmen:

☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln
☐ Firewall: Die nach dem Stand der Technik erforderlichen Firewall-Technologien sind implementiert und werden auf dem aktuellen Stand gehalten
☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form bzw. Verschlüsselung
☑ E-Mail-Verschlüsselung
☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
☐ Protokollierung von Übermittlungen
☐ Anmerkungen: Klicken oder tippen Sie hier, um Text einzugeben.

5. Integrität gem. Art. 32 Abs. 1 lit. b DSGVO

a) Eingabekontrolle

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

Maßnahmen:

☑ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
☑ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
☐ Zentraler Protokoll-/Log-Server
☐ Hash-Werte werden erzeugt und zur Überprüfung benutzt
☐ Protokollauswertungsroutinen/-systeme vorhanden
☐ Aufbewahrungs-/Löschungsfrist für Protokolle vorhanden
☐ Anmerkungen: Klicken oder tippen Sie hier, um Text einzugeben.

b) Dokumentationskontrolle

Zweck: Gewährleistung, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

☐ Führung eines Verarbeitungsverzeichnisses
☐ Dokumentation der eingesetzten IT-Systeme und deren Systemkonfiguration
☐ Anmerkungen: Klicken oder tippen Sie hier, um Text einzugeben.

Auftragskontrolle

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

Maßnahmen:

☑ Vorhandene Vereinbarungen zur Auftragsverarbeitung
☐ Kontrolle der Vertragsausführung
☑ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☐ Regelung zu Wartungen (speziell Fernwartung)
☑ Zugriffsberechtigte Mitarbeiter sind auf das Datengeheimnis verpflichtet
☑ Mitarbeiter haben Arbeitsanweisungen/Richtlinien oder Merkblätter erhalten, die über Maßnahmen zur Einhaltung des Datenschutzes sowie der IT-Sicherheit informieren
☑ Bei Fehlern hinsichtlich der Datenverarbeitung oder Verstoß gegen den Datenschutz erfolgt unverzügliche Information an den Auftraggeber
☐ Anmerkungen: Klicken oder tippen Sie hier, um Text einzugeben.

6. Verfügbarkeitskontrolle gem. Art. 32 Abs. 1 lit. b DSGVO

Zweck: Gewährleistung, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahmen:

☐ Unterbrechungsfreie Stromversorgung (USV)
☐ Überspannungsschutz
☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
☐ Feuer- und Rauchmeldeanlagen
☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
☐ Klimaanlage in Serverräumen
☐ Redundante Netzwerktechnik
☐ Schutzsteckdosenleisten in Serverräumen
☐ Feuerlöschgeräte in Serverräumen
☐ Virenschutzsystem
☐ Spiegelung von Festplatten (z. B. RAID-Verfahren)
☐ Festplatten, Cluster Storage (z. B. Cluster, Ceph, S2D)
☐ Intrusion-Detection-System (z. B. Snort)
☐ Automatisierte Standardroutinen für regelmäßige Aktualisierung von Schutzsoftware (z. B. Virenscanner, Malware-Protection und Firewallsysteme)
☐ Anmerkungen: Klicken oder tippen Sie hier, um Text einzugeben.

7. Belastbarkeit gem. Art. 32 Abs. 1 lit. b DSGVO

Zweck: Gewährleistung, dass die Systeme auch unter unvorhergesehener Last noch arbeiten.

Maßnahmen:

☐ Memory-Over-Commitment disabled
☐ Disk-Over-Commitment disabled
☐ High-Avail-Cluster
☑ Virtuelle Serverumgebung
☐ Mixed Cloud-Anwendung
☐ Festgelegte/Nachvollziehbare Belastungsgrenzwerte
☐ Überwachungssoftware im Einsatz (z. B. Nagios)
☐ Automatische Server-Alarmmeldungen an verantwortliche Personen
☐ Anmerkungen: Klicken oder tippen Sie hier, um Text einzugeben.

8. Wiederherstellung gem. Art. 32 Abs. 1 lit. c DSGVO

Zweck: Gewährleistung, dass nach einer Störung eine Wiederherstellung personenbezogener Daten erfolgen kann.

Maßnahmen:

☐ Backup-Konzept
☑ Backups (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und -ort)
☑ Existierende Vollsicherungen der Server
☐ Desaster-Recovery-Konzept
☐ Testen von Datenwiederherstellungen
☐ Testen von Serverwiederherstellungen
☐ Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
☐ Anmerkungen: Klicken oder tippen Sie hier, um Text einzugeben.

9. Regelmäßige Überprüfung gem. Art. 32 Abs. 1 lit. d DSGVO

Zweck: Gewährleistung, dass Verfahren aktuell bleiben und eingesetzte Techniken dem „Stand der Technik“ entsprechen.

Maßnahmen:

☑ Regelmäßige Bewertung eingesetzter Verfahren
☐ Meldepflicht an den Datenschutzbeauftragten von neu eingesetzten Verfahren
☐ Regelmäßige Software-Security-Updates
☐ Penetrationstests werden durchgeführt und dokumentiert
☐ Regeln zur Hardwarebeschaffung
☐ Anmerkungen: Klicken oder tippen Sie hier, um Text einzugeben.