Vertrag gemäß Art. 28 DSGVO

zwischen dem/der

_____

_____

_____

- nachstehend **Auftraggeber** genannt -

und dem/der

SHEROES GmbH
Spitaler Straße 16
20095 Hamburg
Deutschland

- nachstehend **Auftragnehmer** genannt -

1. Gegenstand und Dauer des Vertrags

(1) Dieser Vertrag zur Auftragsverarbeitung ist Bestandteil eines Hauptauftragsverhältnisses auf welches ausdrücklich verwiesen wird (im Folgenden Leistungsvereinbarung).

(2) Gegenstand des Vertrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:
• Bereitstellung einer Online-Software "Priware" als Software-as-a-Service Tool
• Beratungs- und Schulungsleistungen im Bereich Datenschutz

(3) Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung. Eine Kündigung oder anderweitige Beendigung des Hauptauftragsverhältnisses beendet gleichzeitig diese Vereinbarung zur Auftragsverarbeitung.

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

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

2. Konkretisierung des Vertragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten
Nähere Beschreibung des Vertragsgegenstandes im Hinblick auf Art und Zweck der Aufgabe des Auftragnehmers:
• Bereitstellung einer Online-Software "Priware" zur unternehmensinternen Datenschutzverwaltung durch den Auftraggeber
• Datenschutzschulung und -sensibilisierung des Auftragsgebers und seiner Mitarbeiter
• Beratung hinsichtlich konkreter Datenschutzanfragen des Auftragsgebers
• Verarbeitung der vom Auftraggeber bereitgestellten personen- und nicht-personenbezogen Daten zur Erbringung vorgenannter Leistungen
• Statistische Auswertung verarbeiteter Kundendaten in anonymisierter Form zur Produktverbesserung

(2) Art der Daten
Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:
- Datenschutzdokumentation
- Kommunikationsdaten
- Personenstammdaten
- Vertragsstammdaten

(3) Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
- Beschäftigte
- Interessenten
- Kunden
- Lieferanten

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorischen Maßnahmen gem. Art. 32 DSGVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung. Die entsprechend getroffenen technisch-organisatorischen Maßnahmen sind in Anlage I spezifiziert. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags.

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

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

4. Rechte von betroffenen Personen

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

wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

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

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(a) 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 berechtigterweise Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

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

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

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

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

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

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

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

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

(2) Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DSGVO.

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 in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
Der Auftraggeber stimmt der Beauftragung der in Anlage II bezeichneten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO mit dem Unterauftragnehmer zu. Die vertragliche Vereinbarung wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.
Die Auslagerung auf weitere Unterauftragnehmer oder der Wechsel der gemäß Anlage II bestehenden Unterauftragnehmer ist zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, vorab schriftlich oder in Textform anzeigt und
- 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 DSGVO 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. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

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

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform).
Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Internationale Datentransfers

(1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DSGVO. Der Auftraggeber gestattet eine Datenübermittlung in ein Drittland. In der Anlage II werden die Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus aus Art. 44 ff. DSGVO im Rahmen der Unterbeauftragung spezifiziert.

(2) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DSGVO verantwortlich.

8. 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 während der üblichen Geschäftszeiten zu überzeugen.

(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.

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

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, ITSicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

9. Weisungsbefugnis des Auftraggebers

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

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

11. Vergütungsanspruch

(1) Soweit der Auftraggeber Unterstützung bei der Wahrung der Rechte von betroffenen Personen nach Ziffer 4 dieses Vertrags benötigt, hat er die hierdurch entstehenden Kosten zu erstatten.
(2) Soweit der Auftraggeber Kontrollrechte nach Ziffer 8 dieses Vertrags ausübt, sind die Aufwände des Auftragnehmers zu erstatten. Insofern in der Leistungsvereinbarung über die Höhe des Entgelts keine Regelung getroffen wurde, orientiert sich das Entgelt an einem vorab festzulegenden Stundensatz für das durch den Auftragnehmer zur Betreuung bereitgestellte Personal.
(3) Erteilt der Auftraggeber dem Auftragnehmer Weisungen nach Ziffer 9, so hat er die durch diese Weisung entstehenden Kosten zu erstatten.

12. Schlussbestimmungen

(1) Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form.
(2) Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.
(3) Es gilt das Recht der Bundesrepublik Deutschland.
(4) Die Parteien vereinbaren als Gerichtsstand das für den Sitz des Auftragnehmers zuständige Gericht.

Ort, Datum	Ort, Datum
Auftraggeber	Auftragnehmer

Anlage I
Technisch-organisatorische Maßnahmen

Beschreibung der technischen undorganisatorischen Maßnahmen des Auftragnehmers unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten betroffener Personen.

Datenintegrität (organisatorisch)

1. Datenübertragungskontrolle
   Verarbeitungsvorgänge (z.B. Abruf- und Übermittlungsvorgänge) werden in regelmäßigen Abständen bzgl. Sicherheit und Konformität geprüft
2. Datenübertragungskonzept
   Es existiert ein Konzept, welches den sicheren Datenaustausch regelt (z.B. für die Kommunikation mit der betroffenen Person, Server-Server-Kommunikation oder Datenübertragung an Auftragnehmer)
3. Dokumentation der Datenempfänger
   Ausführliche Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung
4. Nachvollziehbarkeit der Eingabe
   Verwendung eindeutiger Benutzernamen um nachvollziehen zu können, wer Daten eingegeben, geändert oder gelöscht hat

Datenintegrität (technisch)

1. Datenänderungsprotokoll
   Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
2. E-Mail-Transportverschlüsselung
   Einsatz einer verschlüsselten Verbindung zum Schutz vor dem Zugriff durch unberechtigte Dritte beim Transport von E-Mails zwischen beteiligten Servern
3. SSL-Webseitenverschlüsselung
   Einsatz einer verschlüsselten Verbindung (HTTPS) für die Übertragung der Webseiteninhalte und das Übermitteln von Formularinhalten
4. Verschlüsselte Verbindungen
   Nutzung verschlüsselter Verbindungen für den Datenverkehr (z.B. SFTP oder HTTPS) zum Schutz vor unberechtigtem Zugriff durch Dritte
5. VPN-Verbindungen
   Einsatz einer verschlüsselten Verbindung mittels VPN (Virtual Private Network) für den Zugriff auf entfernte Arbeitsplatzrechner oder Server

Datenschutzmaßnahmen

1. Bearbeitung von Auskunftsanfragen
   Einhaltung der Auskunftspflichten nach DSGVO gegenüber Betroffenen
2. Datenminimierung
   Es werden nur so wenig wie möglich Daten verarbeitet, wie zur Erreichung des Zwecks der Verarbeitung benötigt werden
3. Datenschutz-Folgenabschätzung
   Es existiert eine Datenschutz-Folgenabschätzung zur Bewertung von Risiken für persönliche Rechte und Freiheiten der Betroffenen
4. Datenschutzbeauftragter (intern)

Einsatz eines firmeninternen Datenschutzbeauftragten

5. Datenschutzmanagement-System
   Nutzung eines Organisationstools zur Planung, Steuerung und Kontrolle der gesetzlichen Anforderungen des Datenschutzes
6. Dokumentation von Datenpannen
   Einhaltung der nach DSGVO vorgeschriebenen Dokumentations- und Meldepflichten bei Datenpannen
7. Dokumentation von Sicherheitsvorfällen
   Dokumentierung von IT-Sicherheitsvorfällen unter Beachtung etwaiger Meldepflichten (z.B. bei DSGVO-Verstößen oder vertraglicher Verpflichtung)
8. Home-Office-Regelung
   Es existieren feste Regeln für den Umgang mit personenbezogenen Daten am Telearbeitsplatz
9. Incident-Response-Management
   Es existieren feste Regeln für das Vorgehen und für erforderliche Maßnahmen bei IT-Sicherheitsvorfällen und Datenpannen
10. Informationspflichten nach DSGVO
    Einhaltung der Informationspflichten nach DSGVO (Aufklärung der Betroffenen über Datenverarbeitungen und Betroffenenrechte)
11. ISO/IEC 27001 zertifizierte Rechenzentren
    Die eingesetzten Rechenzentren sind hinsichtlich Informationssicherheits-Managementsystems nach ISO/IEC 27001 zertifiziert
12. Kontrolle von Auftragnehmern
    Sorgfältige Auswahl von Auftragnehmern (Prüfung von Sicherheitsmaßnahmen und Sorgfaltspflicht, sowie Vereinbarung wirksamer Kontrollrechte)
13. Mitarbeiterverpflichtung
    Mitarbeiter sind auf die Vertraulichkeit bzw. auf das Datengeheimnis verpflichtet
14. Sensibilisierung der Mitarbeiter
    Mitarbeiter sind in den Grundlagen des Datenschutzes sensibilisiert und geschult
15. Trennungskontrolle
    Personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden auch getrennt voneinander verarbeitet
16. Umsetzung Widerrufsrecht
    Es existiert ein Prozess, um das Widerrufsrecht des Betroffenen nach DSGVO umzusetzen
17. Vereinbarung zur Auftragsverarbeitung
    Abschluss einer Vereinbarung zur Auftragsverarbeitung zur Sicherstellung einer datenschutzkonformen Verarbeitung personenbezogener Daten
18. Weisungen an Auftragnehmer
    Der Auftragnehmer und jede ihm unterstellte Person ist verpflichtet, Daten ausschließlich auf dokumentierte Weisung zu verarbeiten

Verfügbarkeit (organisatorisch)

1. Backup- und Recoverykonzept
   Es existiert ein Konzept zur Durchführung von Datensicherung und -wiederherstellung
2. Backupprotokollierung
   Protokollierung der regelmäßigen Datensicherung
3. Dezentrale Aufbewahrung der Sicherungsmedien
   Sicherungsmedien werden an mindestens einem weiteren Ort aufbewahrt (z.B. Nebengebäude oder andere Betriebsstätte)
4. Disaster-Recovery-Plan
   Es existiert ein Notfallplan zur Datenwiederherstellung bei einem Ausfall von Komponenten oder Systemen
5. Tests zur Datenwiederherstellung

Durchführung regelmäßiger Tests zur Datenwiederherstellung

Verfügbarkeit (technisch)

1. Infrastruktur- und Applikations-Monitoring
   Einsatz geeigneter Überwachungssoftware zur automatisierten Benachrichtigung bei Ausfällen und Problemen mit Hard- oder Software
2. Regelmäßige Backups
   Es werden regelmäßige Backups wichtiger Daten erstellt
3. Regelmäßige Updates
   Systeme werden regelmäßig aktualisiert (z.B. durch Firmware-, Betriebssystem- und Software-Updates)

Zugangskontrolle (organisatorisch)

1. Clean-Desk-Richtlinie
   Es existieren feste Regeln, wie ein Mitarbeiter seinen Arbeitsplatz zu hinterlassen hat, damit sensible Daten jederzeit vor anderen Personen geschützt sind
2. Manuelle Zugangssperre
   Es ist festgelegt, dass Endgeräte beim (vorübergehenden) Verlassen des Arbeitsplatzes gegen unbefugte Nutzung zu sichern sind (z.B. manuelles Aktivieren der Bildschirmsperre, Abmeldung vom System)
3. Regelungen zur Sperrung ehemaliger Mitarbeiter
   Es existiert ein Prozess, welcher die Sperrung von Zugängen von Mitarbeitern regelt, deren Arbeitsverhältnis endet oder beendet ist
4. Richtlinie für mobile Geräte
   Es existieren feste Regeln für den Einsatz oder bei Verlust mobiler Endgeräte durch Mitarbeiter
5. Richtlinie für sichere Passwörter
   Es existieren feste Regeln, die für die Erstellung von sicheren Passwörtern eingehalten werden müssen (z.B. Passwortlänge und -komplexität)
6. Zentrale Benutzerverwaltung
   Die Benutzerprofile und -berechtigungen der einzelnen Mitarbeiter werden zentral verwaltet
7. Zugangskonzept
   Es existiert ein Konzept, welches den Zugang von Mitarbeitern zu datenverarbeitenden Systemen regelt (z.B. durch Benutzerlogins für Betriebssysteme und Anwendungen)

Zugangskontrolle (technisch)

1. Anti-Viren-Software (Client)
   Auf Arbeitsplatzrechnern und Notebooks wird eine Antivirensoftware eingesetzt und regelmäßig aktualisiert
2. Automatische Bildschirmsperre
   Das System wird nach einer festgelegten Zeit der Inaktivität automatisch gegen unbefugte Nutzung gesperrt (z.B. durch Bildschirmpasswort)
3. Benutzerlogin (Anwendung)
   Verwendung von geschützten Logins für die zur Verarbeitung genutzte Anwendungssoftware (z.B. durch Benutzername und Passwort)
4. Benutzerlogin (Betriebssystem)
   Verwendung von geschützten Logins zur Anmeldung am Betriebssystem (bspw. durch Benutzername und Passwort)
5. Dateiverschlüsselung
   Dateien, welche personenbezogene Daten enthalten, werden durch Verschlüsselung vor dem unberechtigten Zugriff durch Dritte geschützt
6. Datenträgerverschlüsselung
   Vollständige Verschlüsselung von Datenträgern in Arbeitsplatzrechnern und Notebooks

7. E-Mail-Inhaltsverschlüssung
   Die Kommunikationsinhalte von E-Mails werden zum Schutz vor unberechtigtem Auslesen oder Verändern durch Dritte mittels Verschlüsselung geschützt (z.B. durch PGP, S/MIME)
8. Firewall (Client)
   Einsatz einer geeigneten Firewall mit regelmäßiger Aktualisierung auf Endgeräten (z.B. Arbeitsplatzrechner, Notebooks)
9. Firewall (Server)
   Einsatz einer geeigneten Firewall oder Sicherheits-Gateways mit regelmäßiger Aktualisierung auf Servern
10. Spamfilter
    Beim Empfang von E-Mails werden Spamfilter eingesetzt und regelmäßig aktualisiert
11. Verschlüsselung mobiler Datenträger
    Mobile Datenträger (z.B. USB-Sticks, externe Festplatten) sind zum Schutz vor Datenverlust vollständig verschlüsselt
12. Verschlüsselung von Mobilgeräten
    Verschlüsselung von betrieblich genutzten, mobilen Endgeräten (z.B. Smartphones, Tablets, Notebooks)
13. Zertifikatbasierte Authentifizierung
    Verwendung eines digitalen Zertifikats, um einen Benutzer, einen Computer oder ein Gerät zu identifizieren
14. Zugangsprotokoll
    Der Zugang zu Datenverarbeitungssystemen wird protokolliert (z.B. Benutzerkennung und Zeitpunkt der Anmeldung an Betriebssystem oder Anwendung)

Zugriffskontrolle (organisatorisch)

1. Einsatz von Administratoren
   Einsatz einer minimalen Anzahl von Administratoren, welche über besondere Zugriffsberechtigungen verfügen
2. Löschkonzept
   Es existiert ein Konzept, welches regelt, wann und wie personenbezogene Daten gelöscht werden müssen
3. Richtlinie Löschen und Vernichten
   Es existieren feste Regeln für das sichere Löschen und Vernichten von Datenträgern
4. Systemtrennung
   Es wird eine Funktionstrennung zwischen Entwicklungs-, Test- und Produktionsumgebung gewährleistet
5. Zugriffskonzept (Berechtigungskonzept)
   Es existiert ein Konzept, welches die Zugriffsberechtigungen der Mitarbeiter zum Lesen, Ändern und Löschen personenbezogener Daten im für die Aufgabenerfüllung erforderlichen Umfang regelt

Zugriffskontrolle (technisch)

1. Anonymisierung
   Personenbezogene Daten werden so verarbeitet, dass mit ihnen eine Identifizierung einer Person nicht mehr möglich ist
2. Automatisierte Datenlöschung
   Die regelmäßige Löschung nicht mehr benötigter Daten erfolgt automatisiert nach Vorgabe des Löschkonzepts
3. Datenträgerlöschung
   Digitale Speichermedien werden durch das Überschreiben von Daten mittels geeigneter Algorithmen sicher gelöscht, um eine Rekonstruktion zu verhindern
4. Datenträgervernichtung
   Physische Datenträger werden durch Zerstörung unbrauchbar gemacht (z.B. durch direkte

Gewalteinwirkung, Hitze oder Schreddern)

5. Einsatz von Aktenschreddern
   Papierdokumente werden durch Aktenschredder mit genormter Zerkleinerungsstufe vernichtet
6. Externe Aktenvernichtung
   Für die Vernichtung von Akten wird ein externer professioneller Dienstleister beauftragt
7. Logische Mandantentrennung
   Die Kundendaten verschiedener Mandanten werden logisch getrennt voneinander verarbeitet
8. Manuelle Datenlöschung
   Die regelmäßige Löschung nicht mehr benötigter Daten erfolgt manuell nach Vorgabe des Löschkonzepts
9. Nutzung von Blickschutzfiltern
   Einsatz von Blickschutzfiltern für Monitore und mobile Geräte bei Nutzung im öffentlichen Bereich
10. Pseudonymisierung
    Personenbezogene Daten werden so verarbeitet, dass sie ohne gesondert aufbewahrte Informationen keiner bestimmten Person zugeordnet werden können
11. Zugriffsberechtigungen
    Einsatz von Nutzer- oder Rollen-Berechtigungen zum Schutz vor unbefugtem Zugriff (z.B. Unix-Dateirechte für Nutzer und Gruppen, Datenbankrechte, Rollen in der Anwendung)

Zutrittskontrolle (organisatorisch)

1. Besucherprotokoll
   Der Zutritt von Besuchern und Fremdpersonal zum Firmengelände/zu Firmengebäuden wird protokolliert
2. Festlegung von Sicherheitsbereichen
   Der Schutzbedarf von Gebäuden und Räumen wurde auf Grundlage der darin stattfindenden Datenverarbeitungen/-verarbeitungsanlagen festgestellt
3. Regelung der Schlüsselvergabe
   Schlüssel für den Zutritt werden nur an berechtigte Personen herausgegeben, die Herausgabe wird dabei protokolliert
4. Zutrittskonzept
   Es existiert ein Konzept zur Regelung von Zutrittsberechtigungen und -kontrollen zu Firmengebäuden/-räumen

Zutrittskontrolle (technisch)

1. Manuelles Schließsystem/Schlüssel
   Es wird eine mechanische Schließanlage mit handelsüblichen Schlüsseln verwendet
2. Sicherheitsschlösser
   Türen und Tore sind mit Sicherheitsschlössern ausgestattet

Anlage II
Genehmigte Unterauftragsverhältnisse

Firma/Unterauftragnehmer	Anschrift/Land	Leistung	Garantien bei Datenübermittlungen
Hetzner Online GmbH	Industriestraße 25 91710 Gunzenhausen	Hostingdienstleister und E-Mail-Serviceprovider	Es erfolgt kein Drittlandtransfer
Mailgun Technologies, Inc.	112 E Pecan St #1135 San Antonio, TX 78205, USA	E-Mail-Kampagnen/Transaktionale E-Mails	Drittlandtransfer: USA Geeignete Garantien i.S.v. Art. 46 DSGVO: *AV-Vertrag unter Einbeziehung der EU-Standardvertragsklauseln*
Typeform S.L.	Carrer Bac de Roda, 163 (Local) 08018 Barcelona, Spanien	Online-Fragebögen	Drittlandtransfer: USA Geeignete Garantien i.S.v. Art. 46 DSGVO: *AV-Vertrag unter Einbeziehung der EU-Standardvertragsklauseln*