Part of collana IT

Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

Zwischen

App-Nutzer

- Verantwortlicher, nachfolgend „**Auftraggeber**" genannt -

und

MAC IT-Solutions GmbH, 24941 Flensburg, vertreten durch den Geschäftsführer Aida Dia und Jörn Fischer

- Auftragsverarbeiter, nachfolgend „**Auftragnehmer**" genannt

§ 1
Gegenstand und Dauer des Auftrags

(1) Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung vom 17.10.2023 auf die hier verwiesen wird (nachfolgend „**Leistungsvereinbarung**").

(2) Die Laufzeit dieses Auftrags zur Datenverarbeitung entspricht der Laufzeit der Leistungsvereinbarung.

(3) Das Recht zur außerordentlichen fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

(4) Die Vertragspartner schließen diesen Auftrag in Ansehung der ab dem 25.05.2018 geltenden EU-Datenschutzgrundverordnung (DSGVO) in dem Bestreben, bereits jetzt den sich aus der DSGVO ergebenden künftigen Anforderungen einer Auftragsverarbeitung vollumfänglich gerecht zu werden. Diese Regelung zur Auftragsverarbeitung stellt daher auf die Normen und Anforderungen der DSGVO ab, gilt dessen ungeachtet jedoch bis zur Gültigkeit der DSGVO entsprechend auch in Ansehung der derzeit noch geltenden Normen und Anforderungen des BDSG, insbesondere im Hinblick auf § 11 BDSG als zum Zeitpunkt des Abschlusses dieser Vereinbarung noch geltende Rechtsgrundlage einer Auftragsdatenverarbeitung.

§ 2
Auftragsinhalt

(1) Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in der Leistungsvereinbarung konkret beschrieben.

(2) Die Erbringung der vertragsgegenständlichen 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 Artt. 44 ff. DSGVO erfüllt sind.

(3) Der Gegenstand der Verarbeitung personenbezogener Daten ist in der Leistungsvereinbarung konkret beschrieben; hierzu zählen insbesondere folgende Datenarten/-kategorien: Kundendaten, Abrechnungsdaten, Userzugänge und Passwörter.

(4) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen Kunden des Auftraggebers.

§ 3
Technische/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 zu übergeben.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 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. Die Einzelheiten hierzu haben die Vertragspartner in **Anlage 1** zu dieser Regelung zur Auftragsverarbeitung vereinbart.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist der Auftragnehmer berechtigt, 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 des Auftragnehmers umfasst, sind das Recht auf Vergessenwerden, die erforderliche Berichtigung fehlerhafter Daten, die Datenportabilität und

Auskunftsansprüche nach dokumentierter Weisung des Auftraggebers durch den Auftragnehmer umzusetzen.

§ 5
Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DSGVO zu erfüllen; insofern setzt er folgende Vorgaben um:

a) Benennung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DSGVO ausübt. Der Auftragnehmer wird die Kontaktdaten des Datenschutzbeauftragten dem Auftraggeber auf Anfrage mitteilen. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen. Die jeweils aktuellen Kontaktdaten des Datenschutzbeauftragten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) Der Auftragnehmer wahrt die Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Er 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) Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß 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 insoweit zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig seine internen Prozesse sowie die Maßnahmen gem. Anlage 1.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 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) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Unterauftragnehmer	Anschrift	Leistung
Microsoft Ireland Operations Limited	Atrium Building Block A Carmen Hall Road Sandyford Industrial Park Dublin, 18, Ireland	Cloud-Services
Hetzner Online GmbH	Industriestrasse 25, 91710 Gunzenhausen, Deutschland	Hosting-Services
Also Deutschland GmbH	Lange Wende 43, 59494 Soest, Deutschland	Zwischenhändler Cloud Dienste
Pipedrive OÜ	Mustamae tee 3a Tallin 10615 Estonia	CRM System für Vertriebsdaten
Stadtwerke Flensburg	Batteriestrasse 48, 24937 Flensburg, Deutschland	Hosting-Services

b) Die Auslagerung auf weitere 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 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.

§ 7
Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem 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.

(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 solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann insbesondere erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO; Vorlage aktueller Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. interne Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren); eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit.

(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 im Rahmen der vom Auftragnehmer nach der Leistungsvereinbarung geschuldeten Leistungen bei der Einhaltung der in den Art. 32 bis 36 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 schnellstmögliche Feststellung von relevanten Verletzungsereignissen ermöglichen;

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich nach Kenntnisnahme 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) soweit vom Auftraggeber gewünscht die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung gegen gesondertes Entgelt;

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde gegen gesondertes Entgelt.

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

§ 9
Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in 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 so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Dies begründet keine Prüfpflicht des Auftragnehmers bzgl. erhaltener Weisungen des Auftraggebers.

§ 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.

Anlage 1: Technische/organisatorische Maßnahmen Art. 32 Abs. 1 DSGVO

1. Vertraulichkeit (Art. 32 Abs. 1 lit. a, b DSGVO)

- **Zutrittskontrolle**
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;

  - Ein räumlich unbefugter Zutritt zu unseren Räumlichkeiten wird mittels folgendem Kontrollsystem verhindert:
    - Gebäudezugang über PIN und persönlichen Token
    - Abteilungszugang über PIN und persönlichen Token
  - EDV Räume über persönlichen Token
    Schlüssel
    - keine allgemeine Schlüsselvergabe

- Archiv / Tresor nur mit Schlüssel zugänglich, Archivschlüssel ist personengebunden
- Notfallschlüssel bei Feuerwehr hinterlegt

- Überwachungseinrichtungen
  - Sicherung der Abteilungen über Zutrittskontrolle mit Echtzeitüberwachung
  - Temperaturüberwachung der Serverräume mit ext. Meldung an das IT-Personal

Die Daten der Auftraggeber werden ggf. auch im Rechenzentrum der Microsoft Ireland Operations Limited (nachfolgend „Microsoft") verarbeitet, in dem eine Zutrittskontrolle auf höchstem Niveau gegeben ist.

- **Zugangskontrolle**
  Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
  - Es sind die Standard-Richtlinien von Windows 10 für Passwörter umgesetzt. Die Passwörter sind 90 Tage gültig.
  - Root- und Administrator-Accounts sind nur den Administratoren bekannt
  - Ein externer Zugang der Mitarbeiter in das Firmennetz erfolgen ausschließlich über ein verschlüsseltes VPN (3DES/MD5 mit 1536 Bitverschlüsselung).
  - Darüber hinaus gibt es einen Zugang für die Niederlassung Hamburg, der über ein mit verschlüsseltes VPN realisiert ist.
  - Der Zugriff auf das Rechenzentrum von Microsoft erfolgt über https. Auf dem Server ist ein von einer öffentlichen zertifizierungsstelle signiertes Zertifikat mit einer Schlüssellänge von 2048 Bit installiert. Für externe Zugriffe ist eine 2-Faktor-Authentifizierung erforderlich.
  - Für den Malware-Schutz kommt ein System von Securepoint zum Einsatz.

- **Zugriffskontrolle**
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

  - Unerlaubte Tätigkeiten in unseren DV-Systemen sowie den Systemen bei Microsoft außerhalb eingeräumter Berechtigungen werden mittels Berechtigungskonzept verhindert, und zwar per
    - Autorisierung über Gruppenzuordnung in Netzwerk
    - Autorisierung im ERP System über Rollenzuweisung
    - Autorisierung über Benutzername, Passwort und Multifaktor Authentifizierung

- **Trennungskontrolle**

  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

  - Um Daten, die zu unterschiedlichen Zwecken erhoben werden auch getrennt zu verarbeiten, wird folgende Funktionstrennung vorgenommen:
    - Es stehen unterschiedliche Ablageorte zur Verfügung für
      - Produktion
      - Test

        - Datenablage
        - Mail
    - Strikte Trennung der Daten in unterschiedlichen Datenbanken
    - Strikte Trennung der Daten nach Mandanten

- **Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)**
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

    - Stellt der Auftraggeber Testdaten zur Verfügung, die personenbezogene Daten enthalten und auf Systemen des Auftragnehmers zu Testzwecken genutzt werden sollen, so sind diese in anonymisierter Form zur Verfügung zu stellen.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- **Weitergabekontrolle**
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

    - Die Weitergabe von personenbezogenen Daten erfolgt im Einzelfall nur nach schriftlicher Aufforderung durch den Auftraggeber über ein sicherheitsoptimiertes Verfahren (Verschlüsselung, VPN, Anonymisierungstools).
    - Der Zugriff des Auftraggebers auf seine bei Microsoft gehaltenen Daten erfolgt über eine verschlüsselte HTTPS-Verbindung.

- **Eingabekontrolle**
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

    - Soweit wir - mittels gesicherter Zugänge - direkt auf personenbezogene Daten unserer Auftraggeber auf deren Systemen zugreifen, obliegt es den Auftraggebern, die ggf. erforderlichen Protokollierungen in den Systemen einzurichten, die eine Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und-pflege gewährleistet.
    - Der Zugriff von MAC-Mitarbeitern auf die Kundensysteme erfolgt ausschließlich über MARS. MARS baut zu den Kundensystemen eine verschlüsselte Verbindung (HTTPS bzw. VPN) inkl. Anmeldung auf. Kennworte der Kundensysteme sind in MARS verschlüsselt hinterlegt und die für die Nutzer nicht sichtbar. Die Anmeldung der MAC-Mitarbeiter wird protokolliert und ist nur durch die Administratoren einsehbar. In Verbindungen mit den Log-Dateien auf den Kundensystemen ist eine eindeutige Zuordnung der Aktivitäten zu einem Nutzer möglich. Der Kunde ist für die Vorhaltedauer der Log-Dateien auf seinen Systemen verantwortlich.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- **Verfügbarkeitskontrolle**
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

  - Unsere Daten werden gegen zufällige Zerstörung oder Verlust wie folgt geschützt:
    - Server / Blades / SAN
    - Energieabsicherung durch USV Anlage
    - Datensicherheit auf Festplatten über RAID5 bzw. Spiegelung
    - tägliche Datensicherung auf Magnetbänder mit einem Bandroboter
    - Aufbewahrung der Bänder in einem feuersicheren Datentresor außerhalb der Serverräume
    - Verwahrung einer wöchentlichen Datensicherung in einem Bankschließfach
    - Bei Microsoft vorgehaltene Daten sind 3-fach redundant gegen Verlust abgesichert.
  - Allgemein:
    - Server und Clients sind mit Antivirus Software versehen
    - Antivirensoftware wird mindestens alle 24 Stunden aktualisiert
    - Die Aktualisierung der Clients wird überwacht.
    - Internetzugang über Firewall abgesichert
    - Webzugriff nur über Proxy Server
    - Der Anschluss an das externe Netz erfolgt standardmäßig über je eine Glasfaser bei den Anbietern
      - Stadtwerke Flensburg
      - QSC

      die wechselseitig als Backup dienen.

    - Für den Fall eines Komplettausfalles des Objektes von MAC können Räume der Nachbarfirma als Ausweichobjekt genutzt werden.

- **Rasche Wiederherstellbarkeit** (Art. 32 Abs. 1 lit. c DSGVO);
  Es erfolgt eine tägliche Komplettsicherung aller Daten und Lizenzen. Dabei wird ein 5-Tage-Generationen-Prinzip verwirklicht.

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

- Datenschutz-Management;
  Es besteht ein Datenschutz- und Sicherheitskonzept, welches jährlich überprüft und ggfs. an sich ändernde Bedingungen angepasst wird.

- Incident-Response-Management;
  Datenschutzvorfälle werden unverzüglich von der Geschäftsleitung mit dem Datenschutzbeauftragten aufgearbeitet und alle notwendigen Maßnahmen ergriffen bzw. eingeleitet

- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Die Voreinstellungen der Systeme werden in Workshops mit den Kunden durchgeführt. Hierbei erfolgt eine gemeinsame Einrichtung der aus Auftraggebersicht erforderlichen Grundeinstellungen.

- Auftragskontrolle.
  Der Auftragsdatenverarbeitung durch MAC liegt eine Leistungsvereinbarung (in der Regel ein Projektvertrag mit anschließender Pflegevereinbarung) als Hauptvertrag nebst einer Vereinbarung für die Auftragsverarbeitung vor, die die Auswahl der eingeschalteten Unterauftragnehmer und durchzuführende Kontrollen etc. vorgibt. Grundsätzlich erfolgt eine Zusammenarbeit nur, soweit durch geeignete und aktuelle Nachweise die Sicherheit der Datenverarbeitung gewährleistet ist.