Auftragsverarbeitung gemäß Art. 28 DSGVO

Vereinbarung

zwischen

_____

_____

_____

_____

- Verantwortlicher, nachstehend Auftraggeber genannt –

und

M•SOFT Organisationsberatung GmbH, Große Straße 10, 49201 Dissen

- Auftragsverarbeiter, nachstehend Auftragnehmer genannt -

§ 1 Gegenstand und Dauer des Auftrags

(1) Diese Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien aus dem Vertragsverhältnis, sie endet mit der Beendigung des letzten Hauptvertrages gem. Anlage B.

(2) Der Auftragnehmer erklärt, dass er in der Lage ist, die aufgetragenen Arbeiten nach Maßgabe des Art. 28 DSGVO ordnungsgemäß und gewissenhaft durchzuführen.

(3) Der Gegenstand des Auftrags ergibt sich aus der/den vertraglichen Vereinbarungen der Hauptverträge, auf die hier verwiesen wird (nachfolgend „Leistungsvereinbarung(en)“ genannt). In diesem Zusammenhang kann der Auftragnehmer oder von diesem beauftragte Dritte mit personenbezogenen Daten in Berührung kommen insbesondere durch den Remote-Zugriff per Fernwartung auf das IT-System des Auftraggebers (DSK Kurzpapier Nr. 13).

§ 2 Konkretisierung des Auftragsinhalts

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

(2) 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. DSGVO erfüllt sind.

☒ Eine Verlagerung personenbezogener Daten in ein Drittland findet nicht statt.

(3) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

1. Personenstammdaten (Vorname, Name, Firma, Straße, PLZ, Ort, u.a.)
2. Kommunikationsdaten (Telefon, E-Mail, u.a.)
3. Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
4. Kundenhistorie
5. Vertragsabrechnungs- und Zahlungsdaten
6. Planungs- und Steuerungsdaten
7. Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
8. _____
9. _____

(4) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

a. Kunden
b. Interessenten
c. Abonnenten
d. Beschäftigte
e. Lieferanten
f. Handelsvertreter
g. Mitglieder
h. _____

§ 3 Technisch-organisatorische Maßnahmen

(1) **Der Auftragnehmer hat die Umsetzung der technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Diese Dokumentation hat sich an den Kriterien der in der Anlage A beschriebenen Anforderungen der DSGVO zu orientieren. 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 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.

(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 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☒ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.

☒ Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

☒ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer bestellt:
Herr Detlef Breuker, c/o C&S Consulting, Telefon: 05226 8873801, E-Mail: info@datenschutz-os.de

☒ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) Für die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO setzt der Auftragnehmer 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 DSGVO.

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

Firma Unterauftragnehmer	Ort/Land	Leistung
Heiko Bick Aktenvernichtung GmbH & Co KG	Osnabrück	Akten- und Datenträgervernichtung nach DIN 66399
M-SOFT Hamburg GmbH	Hamburg	EDV-Dienstleistungen
M-SOFT Koblenz GmbH	Kaisersesch	EDV-Dienstleistungen
M-SOFT Südwest GmbH	Güglingen	EDV-Dienstleistungen

c) ☒ Die Auslagerung auf Unterauftragnehmer oder

d) ☒ 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) 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

☐ ist nicht gestattet;
☒ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
☐ bedarf der Zustimmung des Hauptauftragnehmers (mind. Textform);

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 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 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, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren); eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

§ 8 Mitteilung bei Verstößen des Auftragnehmers

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 im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

§ 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 Abstimmung 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.

§ 11 Gefährdung personenbezogener Daten

(1) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten im Rahmen dieser Auftragsverarbeitung schuldhaft verursachen. Für den Ersatz von Schäden, die ein Betroffener wegen einer nach der Datenschutzgrundverordnung oder anderen Vorschriften über den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen des Auftragsverhältnisses erleidet, ist die verantwortliche Stelle gegenüber dem Betroffenen verantwortlich. Soweit die verantwortliche Stelle zum Schadenersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihr der Rückgriff beim Auftragnehmer vorbehalten.

(2) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber liegen.

§ 12 Aufhebung bisheriger Vereinbarungen

Die Parteien vereinbaren, dass zeitgleich mit Beginn dieser Vereinbarung (frühestens zum 25.05.2018) zur Auftragsverarbeitung die zwischen den Parteien bestehende Vereinbarung zur Auftragsdatenverarbeitung gemäß § 11 Bundesdatenschutzgesetz sowie etwaige weitere Vereinbarungen zur Auftragsdatenverarbeitung einvernehmlich aufgehoben und durch diese neue Vereinbarung zur Auftragsverarbeitung ersetzt werden.

§ 13 Sonstige Bestimmungen

Mündliche Nebenabreden bestehen nicht. Änderungen oder Ergänzungen bedürfen der Schriftform; das gilt auch für die Abbedingung der Schriftform.

Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein, berührt dies nicht die Wirksamkeit der übrigen Bestimmungen. Eine unwirksame Bestimmung ist durch eine solche zu ersetzen, die dem beabsichtigten Zweck am nächsten kommt.

....., den	Dissen, den
_____	_____
Auftraggeber	Auftragnehmer

Anlage A	Dokumentation der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO
Anlage B	Hauptverträge, Betroffene Datenkategorien und Personen, Unterauftragnehmer

Anlage A

Dokumentation

der technischen und organisatorischen Maßnahmen gemäß Art. 32 (1) DSGVO für Auftragsverarbeiter (Art. 30 (2) lit. d DSGVO)

Stand 01.05.2018

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

1.1 Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen durch:

Alarmanlage mit Aufschaltung Wachschutz
Besucherregelung (Abholung am Empfang)
Zutrittskontrollsystem
Serverraum ist separat gesichert und kann nur von einem eingeschränkten Personenkreis geöffnet werden
Schließanlage
Schlüsselverwaltung/ Dokumentation der Schlüsselvergabe
RFID-Chips im Einsatz

1.2 Zugangskontrolle

Keine unbefugte Systembenutzung durch:

Authentifikation mit Benutzer und Passwort
Verwaltung der Zugriffsberechtigungen
weitere Benutzerauthentifizierungen für bestimmte Softwareanwendungen
Anti-Viren-Software
Einsatz von Firewalls
Einsatz von VPN-Technologie
Erstellen von Benutzerprofilen
Kennwortrichtlinien komplex, automatischer Kennwortwechsel

1.3 Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:

Anzahl der Administratoren auf das Mindeste begrenzt
Einsatz von Aktenvernichtern
Einsatz von Dienstleister zur Aktenvernichtung
Vernichtung von Datenträgern nach DIN 66399
Kennwortrichtlinie (Mindestlänge, Komplexitätsanforderungen)
Sichere Aufbewahrung von Datenträgern
Autorisierungsprozess für Berechtigungen
Verwaltung der Benutzerrechte durch Systemadministratoren

1.4 Trennungskontrolle

Getrennte Verarbeitung von Daten:

:

Festlegung von Datenbankrechten
Logische Mandantentrennung (softwareseitig)
Daten und Dokumentationen unterschiedlicher Auftraggeber sind an getrennten Speicherorten hinterlegt.

1.5 Pseudonymisierung

Als Auftragsverarbeiter werden im Hause zusätzliche Maßnahmen getroffen, die sich aus den jeweiligen Leistungsbeschreibungen der Produkte / Dienstleistungen ergeben oder durch den Verantwortlichen im Rahmen der Beauftragung vorgenommen werden.

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

2.1 Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport:

Die Verbindung der Außendienstmitarbeiter mit dem Firmennetzwerk erfolgt über eine VPN-Verbindung. Beim Transport der Daten auf externen Datenträgern sowie innerhalb des Netzwerkes greifen verschiedene Sicherheitsmaßnahmen, wie z. B. Firewall und Virenschutzprogramme, die zentral verwaltet werden.

2.2 Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten
Protokollierung der Eingabe, Änderung und Löschung von Daten
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)

3.1 Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:

Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
Brandmeldeanlage
Sicherheitskonzept für Software,- und IT-Anwendungen
Datensicherungskonzept
Weiterer Serverraum in einem zweiten Brandabschnitt
Gewährleistung der Datenspeicherung im gesicherten Netzwerk
Bedarfsgerechtes Einspielen von Sicherheits-Updates
Spiegeln von Festplatten
Unterbrechungsfreie Stromversorgung (USV)
Geeignete Archivierungsräumlichkeiten für Papierdokumente
Klimatisierte Serverräume
Virenschutzprogramme
Firewall
Feuerlöschgeräte in Serverräumen
Schutzsteckdosenleisten in Serverräumen
Serverräume nicht unter sanitären Anlagen
Testen von Datenwiederherstellung

3.2 Belastbarkeit der Systeme

Notfallplan für bestimmte Szenarien
Redundante Stromversorgung
Ausreichende Kapazität von IT-Systeme und Anlagen
Redundante Systeme/ Anlage
Einsatz von Disaster-Recovery-Lösung

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

4.1 Datenschutz-Management

Dokumentation nach Art. 24 Abs. 1 und Art.5 Abs. 2 DSGVO

Einheitliche Regelungen für die Umsetzung der DSGVO, in dieser Dokumentation werden nach derzeitigem Wissensstand die rechtlichen Bestimmungen interpretiert und Handlungsempfehlungen gegeben. Diese Dokumentation ist in Bezug auf die Verarbeitung personenbezogener Daten verbindlich. Diese Dokumentation ist ein lebendes Element, sie wird entsprechend den weiteren offiziellen Erklärungen und Interpretationen fortlaufend aktualisiert.

Verarbeitungsübersichten nach Art. 30

Datenschutzschulungen Mitarbeiter

4.2 Incident-Response-Management

Bestandteil der Dokumentation nach Art. 24 Abs. 1 und Art.5 Abs.2 DSGVO

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Regelmäßige Überprüfung im Rahmen der Vorgaben und Möglichkeiten.

4.4 Auftragskontrolle

Es gibt eine klare Vertragsgestaltung mit Auftragsverarbeitern im Sinne des Art. 28 DSGVO zum Thema Auftragsverarbeitung:

Die Auswahl der Auftragnehmer findet unter größter Sorgfalt statt und richtet sich nach den Sicherheitsrichtlinien im Hause.

In den AV-Vereinbarungen werden Weisungsbefugnisse und Sicherheitsmaßnahmen festgelegt.

Die Überprüfung der TOM´s bei den Auftragnehmern erfolgt durch Selbstkontrolle, Beibringung von Checklisten oder Testaten Dritter betreffend Datenschutz und Datensicherheit.

Anlage B

Hauptverträge, Betroffene Datenkategorien und Personen, Unterauftragnehmer

Stand 01.01.2019

Bitte gültige Hauptverträge markieren

	Hauptvertrag	Datenkategorien Personengruppen	Unterauftragnehmer	Leistung
☐	Hardwarewartung		PDV-System GmbH, Goslar	Hardwarewartung
☐	IT-Monitoring			
☐	ELO Dokumentenmanagement	1,2,3,4,5,a,d,e,f	ELO Digital Office GmbH, Stuttgart ELO Digital Office AT GmbH, Linz (AT)	Softwarewartung
☐	Dokumentenmanagement	1,2,3,4,5,a,d,e,f		Softwarewartung
☐	Zeiterfassung	1,2,5,a,d,g	VegaSystems GmbH & Co KG, Paderborn Telekom Deutschland GmbH, Bonn	Hosting Hosting
☐	Warenwirtschaft	1,2,3,4,5,7,a,b,d,e,f,		
☐	Finanzbuchhaltung	1,2,5,a,e,f,	syska GmbH, Karlsruhe	Softwarewartung
☐	Lohnbuchhaltung	1,2,3,5,a,d,g	VegaSystems GmbH & Co KG, Paderborn Telekom Deutschland GmbH, Bonn UBM Drecker GmbH, Fockbek	Hosting Hosting Übermittlung Lohnmeldungen

Durch den modularen Aufbau einzelner Produkte ist es möglich, dass nicht alle Datenkategorien oder Personengruppen betroffen sind. Die Programmnutzung kann individuell angepasst werden. Für die Art und Weise der Programmnutzung ist der Auftraggeber bzw. der User verantwortlich. Im Rahmen von (Fern-)Wartungen kann daher für den Auftragnehmer oder Unterauftragnehmer ein Zugriff auf andere als die hier erwarteten personenbezogenen Daten nicht ausgeschlossen werden.