Testlizenzvertrag über die Nutzung des Softwaretools Universal Data Orchestration

1 Zustandekommen des Testlizenzvertrages sowie dessen Anlage

Mit ordnungsgemäßer Registrierung durch den Kunden über https://udo.schober.de/testphase („Registrierung“) schließt der Kunde mit der Schober Information Group Deutschland GmbH, Meisenweg 65, 70771 Leinfelden-Echterdingen den vorliegenden Testlizenzvertrag einschließlich dessen Anlage über die Nutzung der Plattform Universal Data Orchestration (“UDO”).

2 Testlizenz

Nach der Registrierung räumt Schober für den Kunden an UDO einen auf die Laufzeit dieses Testlizenzvertrages beschränkten, nicht übertragbaren, nicht ausschließlichen und kostenlosen Kundenzugang („Testlizenz“) ein. Schober erbringt die Testlizenz als sog. Application Service Provider. Die Testlizenz setzt das Uploaden der durch Schober zu verarbeitenden Kundendaten in UDO auf der Rechtsgrundlage eines Vertrages über Datenauftragsverarbeitung gemäß beigefügter Anlage voraus.

3 Pflichten von SCHOBER

SCHOBER verpflichtet sich, für die Laufzeit der Testlizenz dem Kunden UDO mittels Benutzername und Passwort zugänglich zu machen. Im Übrigen sichert Schober keine Funktionalitäten, Verfügbarkeiten und sonstige Beschaffenheiten von UDO gegenüber dem Kunden zu.

4 Pflichten und Obliegenheiten des Kunden

Der Kunde stimmt mit der Registrierung, dem hier in der Anlage zu diesem Testlizenzvertrag beigefügten Vertrag über Datenauftragsverarbeitung im Sinne des Art. 28 DSGVO („AV“) zu und verpflichtet sich, die durch UDO zu verarbeitende Kundendaten innerhalb von 7 Kalendertagen in UDO nach den Vorgaben von Schober hochzuladen.

Der Kunde verpflichtet sich, die durch Schober zugeteilten Kunden-Zugangsdaten ausschließlich durch den berechtigten Mitarbeiter des Kunden zu verwenden und diese weder an Dritte weiterzugeben noch in sonstiger Weise für andere Zwecke als den Zugang zu UDO durch den berechtigten Mitarbeiter zu nutzen.

5 Lizenzdauer, Beendigung

Die Testlizenz beginnt mit Registrierung und beträgt 4 Wochen („Testlizenzphase“). Die Testlizenz endet automatisch nach Ablauf der Testlizenzphase ohne gesonderte Kündigung.

Nach Beendigung der Testlizenz ist Schober verpflichtet, die in UDO hochgeladenen Daten des Kunden nach Maßgabe des als Anlage hier beigefügten Vertrages über Datenauftragsverarbeitung vollständig zu löschen oder nach Wahl des Kunden diese an den Kunden herauszugeben.

6 Datenschutz

Schober verarbeitet die in UDO hochgeladenen Kundendaten ausschließlich als Auftragsverarbeiter des Kunden auf der Grundlage der AV.

Kunde sichert gegenüber SCHOBER zu, zum Upload der Kundendaten in UDO gemäß Bestimmungen der AV berechtigt zu sein und ausschließlich solche Kundendaten in UDO hochzuladen, deren rechtmäßige Verarbeitung der Kunde auf eine der Rechtsgrundlagen des Art. 6 (1) (a) – (f) DS-GVO stützen kann.

7 Haftung

SCHOBER haftet im Rahmen dieses Testlizenzvertrages für die Zusendung der Zugangsdaten an den Kunden. Die Haftung von Schober, seiner gesetzlichen Vertreter oder eines Erfüllungsgehilfen ist im Übrigen mit Ausnahme der Haftung für Vorsatz und grobe Fahrlässigkeit sowie der Haftung für Leben und körperliche Unversehrtheit und der Haftung nach dem Produkthaftungsgesetz ausgeschlossen. Die Haftung von Schober als Auftragsverarbeiter wird ausschließlich durch die Bestimmungen der AV geregelt.

8 Schlussbestimmungen

Auf diesen Testlizenzvertrag findet ausschließlich das Recht der Bundesrepublik Deutschland Anwendung unter Ausschluss des internationalen Privatrechts und des UN- Kaufrechts. Sollte eine Bestimmung dieses Testlizenzvertrages ganz oder teilweise unwirksam sein oder werden, so berührt dies die Wirksamkeit der restlichen Bestimmungen nicht. Vielmehr verpflichten sich Schober und Kunde, anstelle der unwirksamen Bestimmung eine Regelung zu treffen, die dem Gewollten am nächsten kommt. Ergänzungen dieses Testlizenzvertrages bedürfen der Schriftform. Gleiches gilt für die Aufhebung dieser Schriftformklausel. Ausschließlicher Gerichtsstand für alle Ansprüche aus und aufgrund dieses Testlizenzvertrages sowie sämtliche zwischen den Vertragsparteien sich ergebende Streitigkeiten über das Zustandekommen, die Abwicklung oder die Beendigung des Vertrages ist Stuttgart; dies gilt auch für den Urkunden- und Wechselprozess.

Testlizenzvertrag über die Nutzung des Softwaretools Universal Data Orchestration

ANLAGE

Vertrag über die Datenauftragsverarbeitung durch die Schober Information Group Deutschland GmbH

Im Rahmen der Testlizenz verarbeitet Schober Kundendaten des Kunden („Auftraggeber") als sog. Auftragsverarbeiter („Auftragnehmer"). Diese Datenverarbeitung erfolgt auf der Grundlage der hier vorliegenden Vereinbarung über Auftragsverarbeitung (im Folgenden Vereinbarung genannt) nach Art. 28 DSGVO.

1. Gegenstand des Auftrages

1.1 Umfang der vorhergesehenen Erhebung, Verarbeitung oder Nutzung

Der Gegenstand des Auftrages ist die analytische Datenverarbeitung durch Schober in und mittels UDO. Der Auftragnehmer nutzt oder verarbeitet die personenbezogenen Daten des Auftraggebers ausschließlich im Rahmen des Auftrages und der speziellen schriftlichen Einzelweisungen des Auftraggebers. In Eilfällen können durch bevollmächtigte Mitarbeiter des Auftraggebers Weisungen auch mündlich erteilt werden. Diese bedürfen der unverzüglich schriftlichen Bestätigung. Im Rahmen der spezifizierten Auftragserbringung ist der Auftragnehmer zur Durchführung aller erforderlichen Verarbeitungen und Nutzungen der Daten, soweit die Verarbeitung nicht zu einer inhaltlichen Umgestaltung führt, berechtigt.

1.2 Art der Verarbeitung

Die Art des Auftrages ist die testweise analytische Datenverarbeitung in und mittels UDO.

1.3 Zweck der Verarbeitung

Der Zweck der Auftragsverarbeitung ist die testweise Nutzung von UDO durch den Kunden.

1.4 Art der Daten

Die Art der von der Auftragsverarbeitung betroffenen personenbezogenen Daten sind Kundendaten: Name, Vorname, postalische Adresse, E-Mail-Adresse, Telefonnummer, sonstige kundenbezogene Verhaltensinformationen.

1.5 Kreis der Betroffenen

Der Kreis der Betroffenen umfasst Kunden oder Interessenten des Auftraggebers.

2. Weisungsbefugnis des Auftraggebers

2.1 Der Auftragnehmer darf die Daten nur im Rahmen des Auftrages und sonstiger Weisungen des Auftraggebers verarbeiten.

2.2 Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Mündliche Weisungen oder Weisungen in Textform (z.B. E-Mail) sind unverzüglich vom Auftraggeber schriftlich zu bestätigen.

2.3 Die Parteien vereinbaren als Weisungsberechtigte für die laufende datenschutzrechtliche Abwicklung auf Seiten des Auftraggebers die in der Registrierung hinterlegte Person.

2.4 Bei einem Wechsel oder einer dauerhaften Verhinderung des verantwortlichen Ansprechpartners ist dies durch den Auftraggeber unverzüglich schriftlich unter Benennung eines Vertreters mitzuteilen.

3. Pflichten des Auftragnehmers

3.1 Verpflichtung auf Vertraulichkeit

Der Auftragnehmer ist verpflichtet, den bei der Auftragsverarbeitung mitwirkenden Mitarbeiter des Auftragnehmers auf Vertraulichkeit zu verpflichten. Er hat insbesondere mit der gebotenen Sorgfalt darauf hinzuwirken, dass alle Personen, die mit der Bearbeitung oder Erfüllung dieser Vereinbarung betraut sind, sorgfältig ausgewählt wurden, die gesetzlichen Bestimmungen über die Vertraulichkeit von personenbezogenen Informationen beachten und insbesondere solche Informationen nicht an Dritte weitergeben oder sonst verwerten.

3.2 Kontrollrechte

Der Auftraggeber ist gesetzlich verpflichtet, sich von der Einhaltung der in dieser Vereinbarung niederlegten Verpflichtungen des Auftragnehmers, insbesondere von der Wirksamkeit der Datensicherheitseinrichtungen beim Auftragnehmer, zu überzeugen.

Der Auftragnehmer duldet daher, dass der Auftraggeber die Verarbeitung der von ihm überlassenen Daten durch Einsichtnahme und Prüfung der mit dieser Vereinbarung in Zusammenhang stehenden Datenverarbeitungseinrichtungen, der gespeicherten Daten, der Datenverarbeitungsprogramme vor Ort und der Dokumentation der Datenschutzorganisation, einschließlich Arbeitsanweisungen, in der Regel einmal jährlich kontrolliert.

Der Auftragnehmer hat die mit dieser Vereinbarung in Zusammenhang stehenden Dokumente zur Einsicht bereitzuhalten und Antworten auf Fragen in angemessener Frist zu geben.

Die Einsicht ist dem Datenschutzbeauftragten des Auftraggebers und von ihm beauftragten zur gesetzlichen Berufsverschwiegenheit verpflichteten Personen zu gewähren.

3.3 Erfüllung der Betroffenenrechte durch den Auftraggeber

Soweit aus der Sphäre des Auftragnehmers eine Mitwirkung für die Wahrung von Betroffenenrechten – insbesondere auf Auskunft und Löschung – durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen.

3.4 Subunternehmer

Der Auftragnehmer ist ausschließlich dann berechtigt bei der Ausführung der Datenverarbeitung Unterauftragnehmer zu beauftragen, wenn zuvor der Auftraggeber zur Beauftragung des Unterauftragnehmers seine vorherige schriftliche Zustimmung erteilt hat.
Es dürfen nur solche Unterauftragnehmer vom Auftragnehmer beauftragt werden, die sich gegenüber dem Auftragnehmer zur Einhaltung der Bestimmungen des Datenschutzes schriftlich verpflichtet haben.

3.5 Mitteilungspflicht bei Datenschutzverstößen

Bei Störungen, Verdacht auf Datenschutzverletzungen und anderen Unregelmäßigkeiten bei der Datenverarbeitung ist der Auftragnehmer verpflichtet, den Auftraggeber unverzüglich zu informieren.
In gleichem Maße ist der Auftragnehmer zur unverzüglichen Information des Auftraggebers verpflichtet, sofern der Auftragnehmer der Auffassung ist, eine Weisung des Auftraggebers über die Datenverarbeitung verstoße gegen die Regelungen der EU-DS-GVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

3.6 Rückgabe- und Löschpflichten

In jedem Fall der Beendigung dieser Vereinbarung, gleich aus welchem Rechtsgrund, hat der Auftragnehmer die durch den Auftraggeber übermittelten Daten und übergebenen Datenträger nach Wahl des Auftraggebers vollständig an den Auftraggeber zu übergeben oder nach DSGVO datenschutzkonform zu löschen bzw. zu vernichten, sowie im Falle der Löschung den Nachweis der Löschung bzw. Vernichtung zu führen.
Der Auftragnehmer wird dem Auftraggeber auf dessen Wunsch die Löschung oder Vernichtung in Textform innerhalb von fünf Werktagen bestätigen. Auf Wunsch stellt der Auftragnehmer dem Auftraggeber ein Löschprotokoll bzw. einen Vernichtungsbeleg zur Verfügung.
Die Verpflichtung zur Herausgabe oder zur Löschung gilt nicht, wenn der Auftragnehmer gesetzlich zu einer Aufbewahrung oder in sonstiger Weise zur Speicherung der konkreten Daten verpflichtet ist.

3.7 Sonstige Mitwirkungs- und Unterstützungspflichten

Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Evaluierung der Wirksamkeit der Datenschutzsicherheitsmaßnahmen des Auftragnehmers sowie bei dessen sonstigen in der DSGVO niedergelegten datenschutzrechtlichen Verpflichtungen in angemessenem Rahmen zu unterstützen und mitzuwirken.

4. Technisch-organisatorische Maßnahmen

4.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Datenverarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber, insbesondere soweit der Auftraggeber vor Beginn der Datenverarbeitung keine Einwände erhebt, wird das Sicherheitskonzept Grundlage des Auftrags.
4.2 Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c DSGVO und Art. 32 DSGVO, insbesondere in Verbindung mit Art. 5 Abs. 1 und 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 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.
4.3 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.

5. Dauer der Datenverarbeitung

5.1 Die Vereinbarung beginnt mit Erteilung des Auftrages (Testlizenz) und endet automatisch mit Beendigung des Auftrages (Beendigung der Testlizenz), gleich aus welchem Rechtsgrund.

Technische und organisatorische Maßnahmen des Auftragnehmers nach Art. 32 DSGVO

Übersicht Versionsnummer – Revision

*VNr.: Versionierung - *Änd.: Änderungsdatum - *Zust.: Zuständigkeit - *Rev.: Revisionsdatum

*VNr.	*Änd.	*Zust.	Bemerkung	*Rev.	*Zust.
1.0	26.08.14	AE BF WD	Aktualisierung Änderung der Zeichnungsvollmacht durch GF-Wechsel		
1.1	12.11.14	AE	Ergänzung um Seite 1 und 2 Versionierung Ergänzung Fußzeile		
1.2	09.12.14	AE PA WD BF	Ergänzung Protokollierung Zutritt Punkt 1,4 Aufbewahrung von Sicherungskopien Punkt 3.2 Regelung für Abwicklung, Änderung der Begrifflichkeiten Punkt 7.2		
1.3	22.04.15	AE PA WD BF	1.2 detailliertere Beschreibung der Sicherheitszonen (Anforderung aus ISO-Zertifizierung)		
1.4	18.06.15	AE	Einarbeitung der erforderlichen Änderungen Punkte 1, 1.1, 1.2, 1,3, und redaktionelle / textliche Überarbeitung		
1.5	18.05.16 30.05.16	AE ST WD	Änderungen / Aktualisierungen Ergänzung neue Seite 3 1. Zutrittskontrolle 1.1 Objektsicherung 1.2 Sicherheitszonen 1.3 Art der Zutrittskontrolle 1.4 Regelung der Zutrittsberechtigungen 3.1 Personenkontrolle 3.2 Aufbewahrung 7.3 Überwachung und Einhaltung von Regelungen		
1.6	05.08.16	AE	Aktualisierung Unterschrift CEO		
1.7	01.04.17	AE	Aktualisierung aufgrund der Kündigung des WSD und personeller Änderung beim DSB		
1.8	13.04.18	PA GD GS	Änderung in Folge Auslauf der Zertifizierung ISO/IEC 27001: 2013		
1.9	20.05.18	PA	Neu Gestaltung Auftragsverarbeitung und T&O-Maßnahmen nach DS-GVO-Vorgaben	25.05.18	PA
2.0	15.11.18	PA GD GS	Anpassung T&O-Maßnahmen unter Berücksichtigung neuer Firmengebäude • Zutrittskontrolle • Objektsicherung • Sicherheitszonen • Art der Zutrittskontrolle • Regelung der Zutrittsberechtigungen	10.12.18 29.03.19 28.06.19 30.09.19 20.12.19 29.03.20	PA- GD PA- GD PA- GD PA- GD PA- GD PA- GD

Testlizenzvertrag über die Nutzung des Softwaretools Universal Data Orchestration

Bei Schober gelten von jeher die allerhöchsten Sicherheitsstandards bei der täglichen Arbeit mit Daten.

Schober ließ sich durch ein Zertifizierungsverfahren seines Dachverbandes, der Deutschen Dialogmarketing Verband e.V. (DDV) in Frankfurt, auf die Einhaltung der durch die DDV festgelegten Qualitäts- und Leistungsstandards (QuLS) prüfen und erhielt nach Bestehen folgendes Gütesiegel.

Schober führte für das Management der Informationssicherheit innerhalb der unternehmerischen Tätigkeiten ein Informationssicherheitsmanagementsystem (ISMS) gemäß ISO/IEC 27001: 2013 ein und ließ diese durch die TÜV SÜD Management Service GmbH auditieren (Audit, Bericht-Nr. 707035948). Seit der Einführung des ISMS werden die Forderungen entsprechend der Vorgaben der ISO/IEC 27001: 2013 intern umgesetzt.

A. Technische und organisatorische Sicherheitsmaßnahmen

Gemäß Art. 28 Abs. 3 lit. c DSGVO in Verbindung mit Art. 32 DSGVO sind Auftragnehmer und Auftraggeber verpflichtet, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Sicherheitsmaßnahmen zu treffen.

Der Auftragnehmer wird dabei seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen festzulegen, die je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien für ein angemessenes Schutzniveau geeignet sind.

B. Konkretisierung der Einzelmaßnahmen

In Umsetzung der datenschutzrechtlichen Anforderungen werden die bei der Schober Information Group Deutschland GmbH getroffenen technischen und organisatorischen Maßnahmen wie folgt beschrieben:

Nr.	Maßnahmen	Beschreibung
1.	Organisation	Innerbetriebliche Gestaltung, um den Stellenwert des Datenschutzes zu verdeutlichen – Datenschutzbeauftragter, Datenschutz-Awareness, Verarbeitungsdokumentation.
1.1.	Datenschutzbeauftragter	Ein interner Datenschutzbeauftragter ist zur Wahrnehmung der Beratungs- und Kontrollfunktion entsprechend der Vorgaben der DSGVO bestimmt.
1.2	Name & Kontaktdaten des Datenschutzbeauftragten	Rechtsanwalt Peter Ambrus +49-7156-304-548 ambrus@schober-holding.com
1.3	Datenschutzschulung	Schobers Datenschutzkonzept ist es, die Mitarbeiter bereits bei Eintritt und Beginn ihrer Aufgaben mit dem Datenschutz vertraut zu machen. Die ständige Awareness und die konstante Wissensentwicklung bzw. Stabilisierung wird durch laufende Schulungsmaßnahmen (mind. 2x jährlich) und besondere Einzelfall-Schulungen gewährleistet.
1.4	Auftragsverarbeiter-Verfahrensverzeichnis	Alle Datenverarbeitungsvorgänge werden entsprechend der Vorgaben der Art. 30 Abs. 2 DSGVO schriftlich geführt.
1.5	Datenschutz-Folgeabschätzung	In Fällen des Art. 35 DSGVO unterstützt der Auftragnehmer in angemessener Weise bei der Erstellung einer Datenschutz-Folgeabschätzung durch den Verantwortlichen.
1.6	Informationssicherheitsmanagementsystem	In 2015 wurde ein Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001: 2013 eingeführt. Das ISMS wird seit 2015 entsprechend den Vorgaben der ISO/IEC 27001: 2013

		angewendet.
1.7	IT-Sicherheitskonzept	Festlegung eines IT-Sicherheitskonzepts
1.8	IT-Sicherheitsbeauftragter	Ernennung eines IT-Sicherheitsbeauftragten
1.9	Unterauftragnehmer	Eine Beauftragung von Unterauftragnehmern erfolgt nur nach Zustimmung des Auftraggebers - Unterauftragnehmer haben mit dem Auftragnehmer vor der Ausführung von entsprechenden Datenverarbeitungsleistungen eine Auftragsverarbeitungs-vereinbarung zu schließen
2.	Objektsicherung	Vorbeugende Sicherungsmaßnahmen; Einrichtung von Sicherheitszonen.
2.1	Vorbeugende Sicherungsmaß-nahmen	- Datenverarbeitungsanlagen im Firmengebäude des Auftragneh-mers - Rechnerraum mit Brandschutz- und Einbruchschutzmaßnahmen (RC3), unabhängige Stromversorgung, Klima- und Belüftungssysteme, ohne Außenfron-ten, abgetrennten Brandabschnitten mit F90-Anforderungen
2.2	Sicherheitszonen	Sicherheitszone 1: Bürogebäude / Haupteingang - automatische Schließzeiten 19.30Uhr – 7.30 Uhr - Schließanlagen Schlüssel Sicherheitszone 2: Zugang zum Büro / Zutrittssystem - Transponder Chip Sicherheitszone 3: besondere Zutrittsbeschränkungen innerhalb Büro - Transponder Chip IT / Campaign Operations Sicherheitszone 4: besondere Zutrittsbeschränkungen innerhalb Büro - Transponder Chip A. Rechnerraum mit zentralem Serversystem, Speichersystem,primäre Backup-System, Local und Wide Area Network - zusätzlicher Schließanlagen Schlüssel notwendig B. Backup-Raum und Datensicherungsräume
3.	Vertraulichkeit	Der Auftragnehmer gewährleistet eine angemessene Sicherheit der personenbe-zogenen, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.
3.1	Zutrittskontrolle	Sicherung des Büro, Datenverarbeitungsräume und -anlagen vor unbefugtem Zutritt.
3.1.1	Bürogebäude	Der Zugang zum Bürogebäude verfügt über: - Schließanlagensystem - automatisches Schließkonzept
3.1.2	Büro	Das Büro verfügt über: - Personalisierter Smart-Card-Zutrittskontrollanlage mit zentralem Zeit- und Raumzonenkonzept
3.1.3	Besucherregelung	Einlass und Betreuung von Besuchern erfolgt nach Verfahrensanweisungen in der Besucherregelung; Zutritt und Aufenthalt und Verlassen des Büro ausschließlich mit protokolliertem Besucherausweis unter Beaufsichtigung des besuchsverant-wortlichen Mitarbeiters.
3.1.4	Rechenzentrum	Das Rechenzentrum verfügt über - personalisierte Smart-Card-Zutrittskontrollanlage - Zutrittsdokumentation - Alarmfunktion - Videoüberwachung mit Aufzeichnungsarchivierung

3.1.5	BackUp-Raum / Datensicherungsräume	- personalisierte Smart-Card-Zutrittskontrollanlage - Zutrittsprotokoll
3.2	Zugangskontrolle	Zugangsbeschränkungen zu Datenverarbeitungsanlagen
3.2.1	Benutzerzugang	- Benutzerzugänge werden nur sehr selektiv und nur nach Genehmigung durch die IT-Abteilung vergeben - Rechtevergabe und Änderungen sind dokumentiert - Zugriff auf Dokumente und Kommunikationsinformationen Passwörter geschützt
3.2.2	Benutzerzugangsrevision	Regelmäßige Revision der vergebenen Rechte durch die IT-Abteilung und internen Audits im Rahmen des Informationsmanagementsystems sollen Gültigkeit und Aktualität der Berechtigungen prüfen.
3.2.3	Dokumentation	Benutzerzugänge werden durch das Dokument „Anforderung technische Infrastruktur“ dokumentiert
3.2.4	Rechtevergabe	Die Rechtevergabe erfolgt selektiv entsprechend den Vorgaben der Datenvermeidung und Datensparsamkeit und nur nach Genehmigung durch die IT-Abteilung.
3.2.5	Systemsicherheit	Zugriff auf die IT-Systeme wird gesichert durch: - BSI-zertifizierte, mehrstufige Firewall - regelmäßige Sicherheits-Audits durch externe Sicherheitsberater - Antiviren-Software auf allen sicherheitsrelevanten Systemen und Clients - Benutzerkennung / Passwortschutz auf Datenbank-Ebene - Protokoll über die Benutzung der IT-Systeme - Sicherheitssystem zur Frontend-Identifikation mit Zugriffsrechten und Benutzergruppen
3.2.6	Externer Zugang	Zugänge von außen sind nur mit firmeneigener Hardware, die den Sicherheitsbestimmungen gemäß IT-Sicherheitskonzept entspricht, erlaubt. Verbindungen zum Unternehmensnetzwerk ausschließlich über verschlüsselte VPN-Verbindung möglich.
3.3.	Zugriffskontrolle	Es wird Sorge getragen, dass Datenträger mit personenbezogenen Daten weder unbefugt gelesen, noch kopiert, verändert oder entfernt werden können.
3.3.1	Zugriffsberechtigung	- Zugriff auf Benutzergruppen beschränkt - Login mittels Username und Passwort - Erstvergabe Username und Passwort über die IT-Abteilung
3.3.2	Passwortvergabe / -komplexität	- Passwörter sind vom User zu vergeben - Länge mindestens 10 Stellen - Keine Speicherung von Passwörtern - Systemeinstellung - Passwortweitergabe verboten - Regelmäßige Schulungen / Einweisung für Awarness
3.3.3	Passwortfrequenz	- Änderungsfrequenz monatlich - Nach Ablauf ist Systemnutzung nicht möglich - Vergabe eines neuen Passwortes nach Systemblock durch die IT-Abteilung - Systemeinstellung
3.3.4	Überwachung	Vergabe, Prüfung, Einschränkungen ausschließlich über die IT-Abteilung; Benutzerstruktur und -rechte unterliegen regelmäßiger Überprüfung der IT-Abteilung; Missbrauchsvermeidung durch regelmäßige Auswertung und Kontrolle der Zugriffsprotokolle
3.4.	Trennungskontrolle	Physikalische Trennung unterschiedlicher Kunden, Trennung von Echt- und Testdaten sowie –systemen
3.4.1	Kundentrennung	Durch einzeln zugeordnete Auftragsverarbeitungsvorgänge und entsprechende serverseitige Umsetzungen werden Daten unterschiedlicher Auftraggeber voneinander getrennt gehalten und verarbeitet
3.4.2	Test- und Echtdaten / -systeme	Eine Trennung von Entwicklungs-, Test- und Produktivsystemen ist gegeben.
3.4.3	Überwachung	Die strikte Einhaltung der Datentrennung wird durch regelmäßige Sicherheitskontrollen der IT-Sicherheitsbeauftragten im Rahmen des ISMS geprüft.
3.5	Pseudonymisierung	- Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können - Gesonderte Aufbewahrung der zusätzlichen Informationen

		- Technische und organisatorische Maßnahmen zur Vermeidung der Zusammenführung
3.5.1	Organisatorische Maßnahmen	- Datenschutzkonzept zur getrennten Datenhaltung identifizierender und sonstiger Merkmale - Aufsetzen und Überwachung eines entsprechenden Zugriffskonzepts durch die IT-Abteilung; Kontrolle durch den IT-Sicherheitsbeauftragten - Entsprechende Verpflichtung der datenverarbeitenden Mitarbeiter auf den Datenschutz - Datenschutzschulung
4.	Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit	Systeme und Dienste im Zusammenhang mit der Datenverarbeitung haben dauerhaft Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sicherzustellen
4.1	Weitergabekontrolle	Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten durch: - Datenübertragung ausschließlich verschlüsselt; Filetransfer über sFTP-Server (eigener User mit Passwort) oder mittels Kunden-Transferserver - Ergänzend wird durch die IT-Abteilung im Rahmen der zentralen Prozessverantwortung sichergestellt und überprüft, an welchen Stellen, personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können. - Dokumentation der Transferserver-Benutzer durch die IT-Abteilung - Eingeschränkte, verschlüsselte Datenfernübertragungsmöglichkeiten durch mehrstufige Passwortverfahren und Abschottung der Hardware - Datenfernübertragung verschlüsselt mit individuellen Passwörtern und getrennter Bekanntgabe des Passworts - Strikte Rechtevergabe sichert unberechtigten Zugriff auf Datenübertragungssysteme - Schutz der Datenübertragungssysteme durch Firewalls - VPN-Verbindung bei Zugriff von außerhalb des Firmennetzwerks - Überprüfung von Berechtigungen und Incidents im Rahmen des internen ISMS-Audits
4.2	Eingabekontrolle	- Die unbefugte Eingabe sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten wird durch die IT-Abteilung verhindert. - Zur Einräumung von Befugnissen und deren Überwachung wurden Maßnahmenkataloge und Regelungen durch die IT-Abteilung beschlossen. - Nutzung des Datenverarbeitungssystems ausschließlich durch berechtigte Personen mit Zugriffsberechtigungskonzept. - Dokumentation über Zugriffsberechtigungen für Personen, Programme und Daten. - Sicherheitsmaßnahmen zur Identifizierung der Front-Ends, Zuweisung der Benutzergruppen, individuelle Zugriffsrechte, Maßnahmen bei wiederholtem Fehlversuch. - Nachweis des Zugriffs durch Vorgangsprotokolle über Änderungen und Löschungen in Bezug auf Daten, Zeitpunkte der Verarbeitung und Benutzer - Software zur Regelung und Steuerung der Zugriffsberechtigungen - Protokolle der Online- und Batch-Eingaben - Überprüfung Datenverarbeitung auf Zeitpunkt und Zugriff. Protokollierung mit laufender Nummerierung
4.3	Verfügbarkeit	Schutz der personenbezogenen Daten bei der Datenverarbeitung vor elementaren Einflüssen (Feuer, Wasser, elektromagentische Abstrahlung etc.)
4.3.1	Schutz vor Naturgewalten	- Server wurden in verschiedene Brandabschnitte mit F90-Anforderungen untergebracht - Konstante Stromversorgung durch USV-System - Klima- und Belüftungssysteme ohne Außenfronten
4.3.2	Schutz vor Schadprogrammen	- alle Recheneinheiten mit marktführender Antivirensoftware - von Antivirenmanagementsoftware überwacht und aktualisiert - Einsatz von verschiedenen Firewallsystemen - Protokollierung des Firewallsystems - Überwachung / interne Auditierung im Rahmen des ISMS

4.3.3	Entsorgung von Datenträgern	- Regelung zur Vernichtung von Datenträgern in Abhängigkeit von der Art der Datenträger - Vernichtung von Datenträger durch zertifizierte Fremdfirma - magnetisches Löschgerät im Bereich der IT-Abteilung
5.	Wiederherstellbarkeit	Die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen wird bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt.
5.1	Sicherheitsmaßnahmen	- 4 Generationen von Online-Sicherungskopien jeweils für: - Tagessicherung - Wochensicherung - Monatssicherung - Quartalssicherung - Lagerung an zwei Orten (primäres und sekundäres Backup-System) - Lagerorte feuerschutz- und diebstahlgesichert, in unterschiedlichen Brandschutzzonen - Überprüfung und interne Auditierung im Rahmen des ISMS
6.	Überprüfung, Bewertung und Evaluierung der T&O-Maßnahmen und Sicherheit der Datenverarbeitung	Entsprechende Verfahren sind organisatorisch eingerichtet, um die getroffenen T&O-Maßnahmen an der stetigen technischen Entwicklung und entsprechenden Sicherheitsanforderungen zu messen und zu entwickeln.
6.1	Informationssicherheitsmana-gementsystem	- Im Rahmen des ISMS werden die T&O-Maßnahmen insbesondere durch regelmäßige Überprüfung, Bewertung, durch Feststellung der Nichtkonformität und entsprechender Korrektur, Wertemanagement und interne Audits kontrolliert, bewertet und evaluiert - Entsprechende Reports werden im Rahmen des ISMS erstellt - Benennung eines IT-Sicherheitsbeauftragten - Benennung eines ISMS-Beauftragten - Interne ISMS-Audits
6.2	Überwachung	- Problem-Ticketing-System mit Logbuch über Störmeldungen - Kontrolle durch Vorgesetzten - Überprüfung durch den ISMS- und IT-Sicherheitsbeauftragten, den betrieblichen Datenschutzbeauftragten - Jährlich durch den Deutschen Dialogmarketing Verband e.V. (DDV)
6.3	Auftragskontrolle	- Dokumentation der Auftragsvergaberichtlinien im ISMS - Prüfung aller Auftragsverarbeitungsverhältnisse durch den Datenschutzbeauftragten - Aufträge nur schriftlich abgeschlossen - Auftragsverarbeitungsvereinbarung entsprechend den Vorgaben des DDV