



Vereinbarung über eine Auftragsverarbeitung nach Art.28 EU-DSGVO

Vereinbarung

Zwischen

_____ Firma
_____ Gesetzlicher Vertreter
_____ Straße, Hausnummer
_____ PLZ, Ort

- im Folgenden Auftraggeber genannt –

Und

Quest Consulting AG
Kunstmühlstraße 12a

83026 Rosenheim

– im Folgenden Auftragnehmer genannt –

Quest Consulting AG
Sitz der Gesellschaft
Kunstmühlstr. 12a
D-83026 Rosenheim
Telefon +49 (0)8031 408 66-10
Telefax +49 (0)8031 408 66-11
BDU-Unternehmensberater

Vorstand
Rosenheim
Registergericht
Traunstein
HRB 15916
www.questconsulting.de

Bankverbindung
Albert Hager, Helmut Haberl,
Attila Lottner, Tobias Riegger
Aufsichtsratsvorsitzender
Prof. Dr. Claus Breit

Sparkasse Rosenheim
IBAN: DE5471150000000057141
BIC: BYLADEM1ROS
UST-ID DE 218203634



§01 Gegenstand

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des oben bezeichneten Auftraggebers.

Der Auftrag umfasst eine oder mehrere der folgenden Arbeiten:

- Interne Analyse des Unternehmens
- Erarbeitung einer integrierten Geschäftsplanung mit Umsatz-, Rohertrags-, Personal-, Kosten- und Ergebnisplanung sowie einer Planbilanz
- Ableitung einer Liquiditätsplanung
- Verarbeitung der Daten in der Planungssoftware der LucaNet AG

Die Zulässigkeit dieser Auftragsverarbeitung wurde vom Auftraggeber geprüft.

Folgende Daten werden dabei erhoben/übermittelt/verarbeitet:

Definition der personenbezogenen Daten, die im Auftrag verarbeitet werden, z.B.:

- Organigramme
- Personallisten / Lohnjournale und die in dem Zusammenhang personenbezogenen Daten
- Vertragslisten
- OPOS Kreditoren- und Debitorenlisten
- Aktuelle Auftragslisten
- Alle Informationen in Bezug auf eine betroffene Person, die dem Schutz des Datenschutzrechts unterliegen und die im Rahmen der Nutzung der Software der LucaNet AG in die Software übertragen werden
- Protokolle über Systemzugriffe autorisierter Benutzer der Software der LucaNet AG
- In Finanz- Buchhaltungs- und Controllingdaten üblicherweise enthaltene personenbezogene Daten

Betroffene Personen können in jedem Fall sein:

- Mitarbeitende des Auftraggebers
- Kunden, Lieferanten oder Dienstleister des Auftraggebers

§02 Pflichten des Auftraggebers

- (1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 EU-DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Art. 6 Nr. 4 EU-DSGVO das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.
- (2) Der Auftraggeber versichert, die Eignung des Auftragnehmers hinsichtlich der Einhaltung der Vorschriften nach den geltenden Datenschutzgesetzen, u.a. EU-



Datenschutzgrundverordnung und Bundesdatenschutzgesetz vor der Auftragsvergabe überprüft zu haben (Art.28 Abs.1 EU-DSGVO).

- (3) Der Auftraggeber erteilt alle Aufträge oder Teilaufträge ausschließlich in schriftlicher Form.
- (4) Der Auftraggeber ist für die Meldung des Verfahrens an das interne Verzeichnis eigenverantwortlich, wobei ihn der Auftragnehmer bei der Erstellung der Unterlagen hinsichtlich der verfahrenstechnischen Angaben unterstützt.
- (5) Der Auftraggeber nimmt alle sich aus den geltenden Datenschutzgesetzen ergebenden Rechte gegenüber dem Betroffenen wahr. Dazu zählen die Berichtigung, Einschränkung der Verarbeitung und Löschung von personenbezogenen Daten sowie die Erledigung der Auskunftspflicht an den Betroffenen.
- (6) Der Auftraggeber legt keine weiteren technischen und organisatorischen Maßnahmen, die über den Art. 28 Abs. 3 Nr. c) EU-DSGVO hinausgehen, die bei Verarbeitung einzuhalten sind, fest.
- (7) Der Auftraggeber ist für die Sicherheit aller Unterlagen auf dem Transportweg zum Auftragnehmer verantwortlich, wobei er die Art der Sicherheitsmaßnahmen bestimmt.
- (8) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Arbeitsergebnisse festgestellt hat.
- (9) Etwaige Unterauftragsverhältnisse (des Auftragnehmers) sind durch den Auftraggeber schriftlich zu genehmigen (Art.28 Abs.2 EU-DSGVO). Hiervon unberührt ist die Verarbeitung der Daten im Softwaresystem der LucaNet AG (siehe §03 Pflichten des Auftragnehmers Absatz (7))
- (10) Der Auftraggeber bleibt hinsichtlich der Verarbeitung der Daten weisungsbefugt.

§03 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer sichert zu, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten alle in der Anlage dieses Vertrages vereinbarten technischen und organisatorischen Sicherheitsmaßnahmen ordnungsgemäß zu erfüllen.
- (2) Der Auftragnehmer berechtigt den Auftraggeber, die Einhaltung der Vorschriften über den Datenschutz und die von ihm getroffenen Weisungen jederzeit zu überprüfen. Die Überprüfung findet nach Absprache statt (Art.28 Abs.3 Nr. h) EU-DSGVO).
- (3) Der Auftragnehmer setzt für die Verarbeitung personenbezogener Daten nur Personal ein, das auf den sonstigen einzuhaltenden Geheimhaltungsregelungen verpflichtet wurde. Außerdem versichert er, dass das Personal über genügend Sachkunde für eine ordnungsgemäße Abwicklung der auszuführenden Aufgaben verfügt. Der Auftragnehmer versichert ferner, einen Beauftragten für den Datenschutz bestellt zu haben, der die ordnungsgemäße Verarbeitung der Daten regelmäßig überprüft und die Kontrollergebnisse dokumentiert.
- (4) Der Auftragnehmer verarbeitet die personenbezogenen Daten ausschließlich nach den Weisungen des Auftraggebers. Er verwendet die zur Datenverarbeitung



überlassenen Daten nicht für andere Zwecke und bewahrt sie nicht länger auf, als es der Auftraggeber bestimmt hat.

- (5) Der Auftragnehmer versichert, die personenbezogenen Daten nach Weisung durch den Auftraggeber unverzüglich zu berichtigen oder zu löschen.
- (6) Anfallendes Test- und Ausschussmaterial wird vom Auftragnehmer unter Verschluss gehalten, bis es entweder vom Auftragnehmer datenschutzgerecht vernichtet oder an den Auftraggeber zurückgegeben wird. Dasselbe gilt für nicht mehr benötigte Unterlagen mit personenbezogenen Daten aus dieser Auftragsdatenverarbeitung (Art.28 Abs.3 Nr. g) EU-DSGVO).
- (7) Aufträge an Unterauftragnehmer werden nur nach schriftlicher Zustimmung durch den Auftraggeber vergeben. Hierunter fallen auch Wartungsarbeiten durch Dritte an den DV-Systemen des Auftragnehmers. Anlass und Art der Arbeiten sind zu protokollieren. Der Auftragnehmer setzt zur Steuerung und Visualisierung von Unternehmensdaten das Softwareprodukt LucaNet der LucaNet AG, als Unterauftragnehmer ein. Hier besteht seitens des Auftragnehmers eine gesonderte Vereinbarung zur Auftragsverarbeitung nach Art. 28 EU DSGVO. Der Auftraggeber erteilt hiermit seine Zustimmung zur Verarbeitung seiner Daten im Softwaresystem der LucaNet AG. Die Vereinbarung kann jederzeit beim Auftragnehmer angefordert werden, bzw. wird bei Vertragsabschluss dem Auftraggeber zur Verfügung gestellt.
- (8) Der Auftragnehmer unterrichtet den Auftraggeber umgehend bei schwerwiegenden Störungen im Betriebsablauf, bei Verdacht auf Verletzungen gegen Datenschutzbestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers, insbesondere bei Ausfall der Sicherheitsmaßnahmen sowie wenn er der Auffassung ist, dass eine Weisung rechtswidrig ist. Bei Störungen im Betriebsablauf, etwa bei Hard- und Softwareaustausch, sorgt der Auftragnehmer dafür, dass keine Kundendaten an Dritte weitergegeben werden bzw. dass die Kundendaten vor der Weitergabe zuverlässig gelöscht wurden.
- (9) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann. Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:
 - eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten



und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

§04 Mitwirkungspflichten des Auftragnehmers

- (1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.
- (2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.
- (3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

§05 Kontrolle der Auftragsdatenverarbeitung

- (1) Der Auftragnehmer erklärt sich damit einverstanden, dass die Aufsichtsbehörde, die für die Kontrolle des Datenschutzes beim Auftraggeber zuständig ist, auch bei ihm im begründeten Einzelfall kontrollieren kann. Die Kontrolle wird rechtzeitig angekündigt und findet im Beisein des Auftraggebers statt. In den Fällen, in denen der Auftraggeber mehreren Aufsichtsbehörden zugeordnet ist, muss man sich auf eine bestimmte Aufsichtsbehörde einigen.
- (2) Bei Auftreten von Unregelmäßigkeiten in der Auftragsverarbeitung oder von Verstößen gegen den Datenschutz kann die Überprüfung vor Ort auch unangekündigt erfolgen.
- (3) Der Auftragnehmer sorgt dafür, dass geeignete Unterlagen zur Verfügung stehen, die eine Kontrolle der ordnungsgemäßen Durchführung des Auftrags durch einen sachkundigen Dritten ermöglichen.

§05 Vertragsdauer

- (1) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung. Die Regelungen zur Kündigung der Leistungsvereinbarung gelten auch für diesen Vertrag. Eine Beendigung der Leistungsvereinbarung berechtigt beide Parteien zur Kündigung dieses Vertrages.
- (2) Der Auftraggeber ist zu einer außerordentlichen Kündigung des Vertrags berechtigt. Wenn der Auftragnehmer trotz schriftlicher Aufforderung, die nach §1 des Vertrages



vereinbarte Leistung nicht ordnungsgemäß erbringt oder seine Pflichten nach §3 dieses Vertrages verletzt.

- (3) Nach der Beendigung des Auftrags gibt der Auftragnehmer alle überlassenen Datenträger an den Auftraggeber zurück und löscht unverzüglich alle bei ihm gespeicherten personenbezogenen Daten aus diesem Auftrag, sofern nicht etwas anderes mit dem Auftraggeber vereinbart wurde.

§06 Vergütung

Die Regelungen zur Vergütung der beauftragten Arbeiten findet in gesonderten Vereinbarungen statt.

§07 Nichterfüllung der Leistung

- (1) Bei Nichterfüllung der Auftragsleistung durch den Auftragnehmer ist der Auftraggeber berechtigt, soweit er nicht von seinem Kündigungsrecht nach §5 dieses Vertrages Gebrauch macht, im Benehmen mit dem Auftragnehmer ein anderes Dienstleistungsunternehmen zu beauftragen. Die dabei entstehenden Mehrkosten gehen zu Lasten des Auftragnehmers.
- (2) Kann der Auftragnehmer die vereinbarte Leistung wegen höherer Gewalt (wie Zerstörung der IT-Technik durch Brand oder eine andere Naturkatastrophe) nicht rechtzeitig erfüllen, so ist er von der Leistung frei. Die Beweislast hierfür obliegt jedoch dem Auftragnehmer. Der Auftraggeber hat in diesem Falle keinen Anspruch auf Schadensersatz. Er hat jedoch das Recht, ein anderes Dienstleistungsunternehmen mit der Auftragsausführung zu beauftragen.

§08 Sonstiges

- (1) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, etwa durch Pfändung, durch ein Konkurs- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich und vor Eintritt dieser Maßnahmen zu verständigen, damit die Auftraggeberdaten rechtzeitig von den DV-Komponenten des Auftragnehmers genommen werden können.
- (2) Es besteht bei den Vertragsparteien Einigkeit darüber, dass die „Allgemeinen Geschäftsbedingungen“ des Auftragnehmers auf diesen Vertrag keine Anwendung finden.
- (3) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag



erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

- (4) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.
- (5) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

Quest Consulting AG
Sitz der Gesellschaft
Kunstmühlstr. 12a
D-83026 Rosenheim
Telefon +49 (0)8031 408 66-10
Telefax +49 (0)8031 408 66-11
BDU-Unternehmensberater

Vorstand
Rosenheim
Registergericht
Traunstein
HRB 15916
www.questconsulting.de

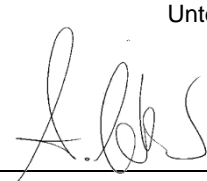
Bankverbindung
Albert Hager, Helmut Haberl,
Attila Lottner, Tobias Riegger
Aufsichtsratsvorsitzender
Prof. Dr. Claus Breit

Sparkasse Rosenheim
IBAN: DE5471150000000057141
BIC: BYLADEM1ROS
UST-ID DE 218203634



§09 Gerichtsstand und Schlussbestimmungen

(1) Gerichtsstand ist das jeweils zuständige Amts- bzw. Landgericht.

Ort, Datum	Unterschrift Auftraggeber
Rosenheim, 18.12.2020	 Quest Consulting AG Kunstmühlstraße 12 a 83026 Rosenheim Telefon 08031 / 408 66-10
	Unterschrift Auftragnehmer

Anmerkung:

Der Vertrag ist bereits von uns unterzeichnet und in dieser Form gültig. Bitte unterzeichnen Sie als „Auftraggeber“ und senden Sie diesen uns als digital unterzeichnetes PDF oder Scan / hochauflösendes Photo per Mail zurück an:

datenschutz@questconsulting.de

Erst dann gilt der Vertrag als abgeschlossen.

Kontakt des Datenschutzbeauftragten der Quest Consulting AG:

Datenschutzbeauftragter	Frau Dr. Jeannette Sieber
Externes Unternehmen:	Elektro Kreuzpointner GmbH Burgkirchener Straße 3 84489 Burghausen
Kontaktmöglichkeiten	Telephon: +49 8677 8703 233 eMail: datenschutz@questconsulting.de

[Version: Stand 18.12.2020]

Anlagen:

(1) TOM - Technisch- und Organisatorische Maßnahmen

Quest Consulting AG
Sitz der Gesellschaft
Kunstmühlstr. 12a
D-83026 Rosenheim
Telefon +49 (0)8031 408 66-10
Telefax +49 (0)8031 408 66-11
BDU-Unternehmensberater

Vorstand
Rosenheim
Registergericht
Traunstein
HRB 15916
www.questconsulting.de

Bankverbindung
Albert Hager, Helmut Haberl,
Attila Lottner, Tobias Riegger
Aufsichtsratsvorsitzender
Prof. Dr. Claus Breit

Sparkasse Rosenheim
IBAN: DE5471150000000057141
BIC: BYLADEM1ROS
UST-ID DE 218203634

ANLAGE 1

DSGVO: Checkliste technischer und organisatorischer Maßnahmen

Die Datenschutzgrundverordnung verpflichtet insbesondere dazu, die Sicherheit der Datenverarbeitung zu gewährleisten. Das Schutzniveau soll dabei dem Stand der Technik und dem Risiko für die von der Datenverarbeitung betroffenen Personen angemessen sein. Es gibt dazu keine letztverbindliche Empfehlung einzelner Maßnahmen, aber zu ergreifenden technischen und organisatorischen Maßnahmen (TOM) müssen die „prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken, aber auch Implementierungskosten“ berücksichtigen (Plath/Drages, DSGVO, 2. Auflage, Art. 32 Rn.3). Daher muss das Vorliegen oder der Verzicht auf einzelne der hier aufgeführten Maßnahmen immer individuell auf die konkrete Bedrohungssituation gesehen werden: Je sensibler die Daten und je höher das Risiko eines Datenverlustes, desto höher die Vorsorgemaßnahmen.

1. Zutrittskontrolle

...hat das Ziel, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Maßnahmen	Nein	Ja	Anmerkungen
Abschließbare Schränke		X	
Alarmanlage	X		
Abschließbare Serverschränke		X	
Absicherung von Gebäudeschächten			
Automatische Zugangskontrolle	X		Keine Datenverarbeitung mehr im Haus
Biometrische Zugangskontrolle	X		
Chipkarten-Schließsystem	X		
Eingangskontrolle Empfang	X		
Gästeausweise	X		
Lichtschanke oder Bewegungsmelder	X		
Manuelles Schließsystem			
Regelungen Schlüsselvergabe/-rückgabe/-verlust		X	

Schließsystem mit Passwort oder Code	X		
Sichtschutzfolien für Laptops, Smartphones	X		
Sonstige Schließanlagen	X		
Sorgfältige Auswahl von Reinigungspersonal		X	
Videoüberwachung der Zugänge (inkl. Warnhinweise)	X		

2. Zugangskontrolle

...verhindert, dass Unbefugte keine Möglichkeit zur Nutzung der Datenverarbeitungssysteme haben

Maßnahmen	Nein	Ja	Anmerkungen
Anti-Viren-Software (keine Freeware)		X	
Benutzerberechtigungen erstellen/verwalten		X	Sharepoint / Cloud
Firewall		X	Je Rechner
Gehäuseverriegelungen			
Löschen von Daten auf gewarteten Geräten (z.B. Kopierern)		X	
Mobile Device Management		X	Via Apple
Passwortgeschützte Mitarbeiter-Accounts		X	
Personenkontrolle beim Pförtner / Empfang	X		
Protokollierung der Besucher/ Besucherbuch (ohne dass der Besucher den Vorbesucher erkennen kann)	X		
Schlüsselregelung / Schlüsselbuch		X	
Sichere Passwortregeln		X	Individuell

Sicherung externer Schnittstellen (z.B. USB-Anschlüsse)	X		
Sorgfältige Auswahl von Reinigungspersonal		X	
Sorgfältige Auswahl von Sicherheitspersonal		X	
Vermeidung unbekannter Software und Hardware (z.B. fremde USB-Sticks)		X	
Verschlüsselung von Datenträgern	X		
VPN-Technologie	X		Nicht mehr, Cloudlösung
Zugriffssperre bei Smartphones, auch bei deren Verlust		X	PIN, IT- Vereinbarung

3. Zugriffskontrolle

Gewährleistet, dass nur berechtigte Personen im vorgesehenen Umfang auf die verwendeten Daten und DV-Anlagen zugreifen können.

Maßnahmen	Nein	Ja	Anmerkungen
Aktenvernichtung/Schreddern		X	
Berechtigungskonzept		X	
Möglichst geringe Zahl an Administratoren		X	
Passwortrichtlinie inkl. Länge und Wechsel, Rhythmus	X		RiLi ja, Rhythmus nein
Physische Löschung von Datenträgern vor deren Wiederverwendung oder Abgabe (insbes. Festplatten)		X	
Protokollierung der Vernichtung von Daten	X		Kann eingeführt werden
Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten			Sharepoint ja
Regelung Benutzerrechte durch Systemadministratoren		X	

Sichere Aufbewahrung von Datenträgern			Individuell
Vernichtung von Datenträgern, ggf. durch professionelle Dienstleister			Löschung durch IT-Dienstleister software- und hardwaretechnisch
Verschlüsselung von Datenträgern	X		
Zugriffssperre bei Smartphones, auch bei deren Verlust		X	PIN, IT- Vereinbarung

4. Weitergabekontrolle

...soll eine sichere Übermittlung von personenbezogenen Daten gewährleisten.

Maßnahmen	Nein	Ja	Anmerkungen
E-Mail-Verschlüsselung		X	
System, das es erlaubt, erfolgte Übermittlungsvorgänge zu überprüfen		X	Ausgang wird protokolliert
System, das sicherstellt, dass nur befugte Personen Datenübermittlungen vornehmen dürfen	X		Individuell
VPN-Technologie	X		Nicht mehr, Cloud
Weitergabe von Daten in anonymisierter oder pseudonymisierter Form		X	individuell

5. Eingabekontrolle

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

Maßnahmen	Nein	Ja	Anmerkungen
Protokollierung der Eingabe, Änderung und Löschung von Daten		X	Sharepoint ja

6. Auftragskontrolle

Quest Consulting AG
 Sitz der Gesellschaft
 Kunstmühlstr. 12a
 D-83026 Rosenheim
 Telefon +49 (0)8031 408 66-10
 Telefax +49 (0)8031 408 66-11
 BDU-Unternehmensberater

Vorstand
 Rosenheim
Registergericht
 Traunstein
 HRB 15916
 www.questconsulting.de

Bankverbindung
 Albert Hager, Helmut Haberl,
 Attila Lottner, Tobias Riegger
 Aufsichtsratsvorsitzender
 Prof. Dr. Claus Breit

Sparkasse Rosenheim
 IBAN: DE5471150000000057141
 BIC: BYLADEM1ROS
 USt-ID DE 218203634

...soll sicher stellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

Maßnahmen	Nein	Ja	Anmerkungen
Kontrollrechte gegenüber dem Auftragverarbeiter		X	
Regelmäßige Überprüfung des Auftragverarbeiters		X	Individuell
Sorgfältige Auswahl des Auftragnehmers inkl. Prüfung der beim Auftragverarbeiter getroffenen Sicherheitsmaßnahmen und entsprechende Dokumentation		X	
Überspannungsschutz			Abhängig vom Verarbeiter
Weisungen an den Auftragverarbeiter durch Auftragsdatenverarbeitungsvertrag in Schriftform, eMail oder online		X	Vertragsbasis

7. Verfügbarkeitskontrolle

...gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden.

Maßnahmen	Nein	Ja	Anmerkungen
Backup-& Recoverykonzept		X	Cloud
Datensicherung (sicherer, ausgelagerter Ort)		X	
Feuerlöschgeräte, insbesondere in Serverräumen		X	
Feuer- und Rauchmeldeanlage		X	
Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen	X		keine Server mehr im Haus
Klimaanlage in Serverräumen	X		
Notfallplan	X		

Schutzsteckdosenleisten in Serverräumen		X	
Sicherung gegen Stromausfälle	X		Keine Server mehr im Haus
Testen Datenwiederherstellung		X	Rhythmus soll festgelegt werden
Wasserschutz (Serverräume nicht unter sanitären Anlagen; in Hochwassergebieten: Serverräume über der Wassergrenze)		X	6. Stock

8. Trennungsgebot

...gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

Maßnahmen	Nein	Ja	Anmerkungen
Festlegung von Datenbankrechten		X	
Prozessuale Trennung der Datenverwendung z.B. durch Verarbeitung in unterschiedlichen Arbeitsschritten oder Zuständigkeiten		X	
Sicherstellung, dass nur solche Daten gemeinsam verarbeitet werden, die auch zum gleichen Zweck erhoben wurden.		X	
Versehen der Datensätze mit Zweckattributen/Datenfeldern			LucaNet

[Version: Stand 01.10.2020]