Datenschutz-Konzept
Technische und organisatorische Maßnahmen im Sinne des Art. 32 Abs. 1 DSGVO

Datum: Juli 2023
Autor: Maximilian Musch – Deutsche Datenschutzkanzlei
Version: 4.3
Klassifikation: öffentlich

1 Dokumenteninfomation

Die EU-Datenschutzgrundverordnung (DSGVO) sowie das Bundesdatenschutzgesetz neuer Fassung (BDSG-neu) enthalten Vorgaben darüber, wie in technischer und organisatorischer Hinsicht mit personenbezogenen Daten umgegangen werden soll. Dies dient dem Ziel der Datensicherheit. Die Datensicherheit stellt damit einen weiteren und ergänzenden Aspekt des Datenschutzes dar.

Gesetzlich geregelt ist die Datensicherheit in Art. 32 Abs. 1 DSGVO. Die Vorschriften fordern, dass solche technischen und organisatorischen Maßnahmen zu treffen sind, die erforderlich sind, um den Schutz personenbezogener Daten zu gewährleisten.

Die DSGVO nennt verschiedene Kontrollbereiche, die jeweils noch verschiedene Unterpunkte beinhalten:

1. Vertraulichkeit
2. Integrität
3. Verfügbarkeit und Belastbarkeit
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
5. Pseudonymisierung und Verschlüsselung

2 Versionshistorie

Version	Status	Datum	Verantwortlich	Änderung
3.4	Änderungen	12.08.2019	DKO/DSB	Anpassung/Ergänzung Weitergabekontrolle und Eingabekontrolle
3.5	Anpassungen / Aktualisierungen	18.12.2020	IT	Anpassung/Ergänzung
3.6	Überarbeitungen	29.12.2020	DKO	Anpassungen/Ergänzungen
3.7	Überprüfung und Ergänzung	10.02.2021	DSB	Ergänzung/Anpassung
4.0	Freigabe		DKO	Prüfung und Freigabe
4.1	Aktualisierung und Freigabe	20.07.2022	DKO	Ergänzung Integrität Weitergabekontrolle
4.2	Anpassungen / Aktualisierungen	24.07.2023	DSB / IT	Verweis auf Zertifizierung 27001 Anpassung Auftragskontrolle Ergänzungen Zugangskontrolle, Weitergabekontrolle und Verfügbarkeit
4.3	Aktuelles CI	25.07.2023	DKO	Formatanpassungen

3 Organisatorisches

Die KUMAVISION AG hat gemäß Art. 37 DSGVO bzw. § 38 Abs. 1 BDSG-neu einen externen Datenschutzbeauftragten, in Person von Maximilian Musch – Deutsche Datenschutzkanzlei bestellt. Die bei der Datenverarbeitung eingesetzten Mitarbeiter sind schriftlich auf das Datengeheimnis sowie auf die Vertraulichkeit verpflichtet. Der Datenschutzbeauftragte und die Datenschutzkoordination führen regelmäßig Überwachungsaudits, sowie fachspezifische Schulungen durch.

Die KUMAVISION AG gewährleistet die schriftliche Dokumentation des aktuellen Datenschutzniveaus, sowie der schriftlichen Arbeitsanweisungen, Richtlinien und Merkblätter für Mitarbeiter. Ein Datenschutzbereich im Intranet sowie allgemeine und fachspezifische Handlungshilfen, Richtlinien, Factsheets etc. werden zur Schulung und Sensibilisierung sowie Aufrechterhaltung des Sicherheitsniveaus genutzt. Zudem sind Verfahren/Prozesse im Bereich Benachrichtigung, Meldung von Vorfällen, Auskunftsersuchen, sowie Anliegen zur Berichtigung, Löschung und Sperrung implementiert (siehe Ziffer 4.4 ergänzend).

4 Sicherungsmaßnahmen

Die folgenden Punkte beschreiben die technischen und organisatorischen Maßnahmen, die von der KUMAVISION AG zum Datenschutz gemäß Art. 32 Abs. 1 DSGVO betrieben werden.

Die Server, Datenbanken sowie die Datensicherung (Backup) werden bei der KUMAVISION AG oder beauftragten Dritten in professionellen Rechenzentren betrieben und gewartet. Die Unterbeauftragten werden sorgfältig ausgewählt und hinsichtlich ihres Sicherheitsbewusstseins und ihrer Fachkompetenz überprüft.

Einige diesen Bereich betreffenden Sicherungsmaßnahmen der folgenden Prüfliste sind nicht gesondert ausgewiesen, da sie in die Verantwortung der Unterbeauftragten fallen oder aus Gründen der Aufrechterhaltung der Sicherheit durch Vertraulichkeit nicht detailliert veröffentlicht werden. Nähere Informationen zu den Datenschutz-/Datensicherheitsprozessen sowie der Überprüfung und Kontrolle der eingesetzten Maßnahmen finden sich in Ziffer 4.4 („Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung“).

4.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

4.1.1 Zutrittskontrolle

Die Zutrittskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, zu verwehren.

#	Maßnahmen
1	Die Zutrittskontrolle zu den Serverräumen wird durch die räumliche Struktur des jeweiligen Rechenzentrums und die dort eingesetzten Kontrollsysteme gewährleistet (restriktives, dokumentiertes, doppeltes Zutrittsberechtigungsverfahren: Karte und Schlüssel; verschlossene Türen; Einbruchmeldeanlage: zusätzliche Karte, um Anlage zu entschärfen; ausschließlich IT-Administration hat Zutritt).
2	Es wird dem Schutzbedarf der Daten angemessenes Schließsystem verwendet (Schlüssel; Chipkarten-/Transponder-Schließsystem; Codesperre).
3	Besucher: Anmeldung über Gegensprechanlage, um Gebäude zu betreten bzw. Abholung/Empfang/ Eintritt durch Standortassistenz.
4	Es ist eine verantwortliche Person für die Verwaltung der Zutrittsmittel bestimmt.
5	Eine Dokumentation der Zutrittsmittel wird geführt und laufend aktualisiert (Register).
6	Zutrittsmittel werden bei Verlust umgehend gesperrt (Sperrung Chipkarten/Transponder).
7	Abschließbare Einzelbüros in den meisten Fällen.
8	Gebäude bzw. Räumlichkeiten sind verschlossen und können nur manuell durch die Mitarbeiter geöffnet werden.
9	Es gibt einen zentralen Besucherempfang. Die Büros sind nur darüber zu erreichen.
10	Eine Alarmanlage sichert das Rechenzentrum auch außerhalb der Geschäftszeiten vor unberechtigtem Zutritt.
11	Wach- und Schließdienst: Aufschaltung Einbruchmeldeanlage (Rechenzentrum).
12	Das Archiv ist ebenfalls verschlossen und darf nur von berechtigten Mitarbeitern (Geschäftsführung, Buchhaltung) betreten werden.
13	Besucher halten sich ausschließlich in Begleitung eines Mitarbeiters in den Geschäftsräumen auf. Wartungsdienste und Besucher des Rechenzentrums werden ständig überwacht/begleitet.
14	Videoüberwachung (Standorte: Dortmund, Markdorf, Nürnberg, Stuttgart)
15	Protokollierung der Zutrittskontrollsysteme zur Nachverfolgung des Betretens/Verlassens bestimmter Räumlichkeiten, Bereiche und Schutzzonen. Regelmäßige Auswertung bei Auffälligkeiten sowie nach (potenziellen) Sicherheitsverletzungen.

4.1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

#	Maßnahmen
1	Reduktion der zugriffsberechtigten Personen auf ein Minimum.
2	Clientsysteme sind erst nach passwortgestützter Authentifizierung nutzbar
3	Ein verbindliches Verfahren zur Vergabe von Berechtigungen ist implementiert.
4	Unbefugten wird der Zugang auf das Unternehmensnetzwerk sowie den IT-Diensten verwehrt. Eine Anmeldung ist ausschließlich über registrierte Benutzerkontos und Passwort möglich. Bei externem Zugriff wird für die Anmeldung zudem ein zweiter Faktor gefordert.
5	Das Gäste-WLAN ist von eigentlichem System getrennt (Gast-WLAN-Vereinbarung mit Passwort).
6	Eine Policy mit Vorgaben für den Passwort-Standard liegt vor.
7	Eine eindeutige Zuordnung von Benutzerkonten zu Benutzern ist möglich.
8	Admin und User werden namentlich, eindeutig zugeordnet.
9	Einsatz von Firewalls und Intrusion-Detection-Systemen zur Verhinderung und Erkennung von Angriffen.
10	Firewalls nach aktuellem Stand der Technik (restriktiv von außen nach innen; Ports sind verschlossen).
11	Eine Passwortrichtlinie mit ausreichendem Schutzstandard ist implementiert (12 Zeichen Minimum mit Großschreibung, Kleinschreibung, Zahlen, Sonderzeichen (3 Kriterien sind zu erfüllen)). Zusätzliche Vorgaben für Aufbau des Passworts (u.a. Kontoname oder mehr als zwei Zeichen aus dem vollständigen Namen des Benutzers dürfen nicht verwendet werden); Änderung (einmal jährlich); Meldewege bei Verdacht auf Bekanntwerden Passwort durch Dritte; Ersetzen Initial-/Einmalpasswörter nach Erstnutzung; Deaktivierung Funktion „Passwort merken/speichern.“
12	Spamfilter und Virenschutzprogramme (Client und Server) sind vorhanden und werden immer auf dem aktuellsten Stand gehalten (alle Clients und Server). Bedrohungsschutz ist für die gesamte M365-Umgebung mit MS-Tools gewährleistet.
13	Einsatz eines zentralen Spamfilters (zentraler Eingang-E-Mail). E-Mails werden gekennzeichnet und eine Weiterleitung ggf. verhindert. Einsatz automatischer Updates und Signaturerkennung.
14	Automatische Bildschirmsperren bei Verlassen des Arbeitsplatzes (passwortgeschützt) werden über eine interne Policy geregelt.
15	Funktionelle Beschränkung der Nutzung von Arbeitsplätzen (restriktive Rechtevergabe nach Funktion/Tätigkeit).
16	Einsatz von Firewall- und Network-Policy (u.a. Nutzung von WLAN im Firmennetz).
17	Festplattenverschlüsselung kommt zum Einsatz (Bitlocker).
18	Patchmanagement Automatisierte Verteilung von Updates und Patches von Software innerhalb des Unternehmens. Updates/Patches können nicht umgangen werden bzw. werden automatisiert durchgeführt. Nur freigegebene Patches/Updates können installiert werden.
19	Durchführung von Penetrationstests zur Überprüfung der Sicherheitsarchitektur und den eingesetzten Maßnahmen.
20	Automatische Abmeldung aus Systemen bei längerer Inaktivität.

4.1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

#	Maßnahmen
1	Unbefugtes Lesen, Kopieren, Verändern oder Löschen von Datenträgern wird verhindert durch: ▪ Datenträgerverwaltung-/Management. ▪ Verwendung externer Datenträger (Kunden) nur in Ausnahmefällen in separater Entwicklungsumgebung. ▪ Softwareseitigen Ausschluss (Berechtigungskonzept). ▪ Gesicherte Schnittstellen.
2	Die Einschränkung der Zugriffsmöglichkeiten des zur Benutzung eines DV-Systems Berechtigten ausschließlich auf die seiner Zugriffsberechtigung unterliegenden Daten wird gewährleistet durch: ▪ Automatische Prüfung der Zugriffsberechtigung mittels Credentials des Benutzers und bei M365-Applikationen durch Zwei-Faktor-Authentifizierung. ▪ Benutzerprofile nach Aufgabenbereich (need-to-know-Prinzip). ▪ Ausschließliche Menüsteuerung je nach Berechtigung. ▪ Die Vergabe, der Entzug und die Änderung von Berechtigungen (Benutzerverwaltung) ist nachvollziehbar. ▪ Differenzierte Zugriffsberechtigung auf Anwendungsprogramme. ▪ Differenzierte Verarbeitungsmöglichkeiten (Lesen/Ändern/Löschen). ▪ Eingeschränkte Domänenfunktionen. ▪ Freigabeverfahren für neue Nutzer und für Nutzer bei Änderung von Rollen/Aufgabengebieten (Ablauf).
3	Führung eines Administrationskonzeptes (ohne Abstufungen).
4	Ein Konzept zur Laufwerksnutzung und -zuordnung liegt vor (AD-technischer-Zugang auf freigegebene Verzeichnisse).

4.1.4 Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

#	Maßnahmen
1	Personenbezogene Daten dürfen nur für den Zweck genutzt werden, für den sie ursprünglich erhoben wurden Die unterschiedliche und getrennte Verarbeitung wird gewährleistet durch: ▪ Softwareseitiger Ausschluss (Mandantentrennung). ▪ Datenbankprinzip, Trennung über Zugriffsregelung (Berechtigungskonzept). ▪ Trennung von Test- und Produktivdaten (zwei unterschiedliche Systeme). ▪ Funktionstrennung. ▪ Trennung von Entwicklungs- und Produktionsprogrammen (zwei unterschiedliche Active Directories).

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

4.2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

#	Maßnahmen
1	Ein Versand von Datenträgern erfolgt nur in Ausnahmefällen. Versendete Datenträger werden mit Passwörtern geschützt. Ggf. Migration für Kunden (Festplatte kommt von Kunden).
2	Nicht mehr benötigte magnetische Datenträger werden durch mehrfaches Überschreiben zerstört (Ausmusterung/Löschung nach Firmenvorgabe).
3	Eine dem Schutzbedarf entsprechende Entsorgung und Vernichtung von Dokumenten und Datenträgern wird eingesetzt. Server werden nach Spezifikation zerstört bzw. gelöscht (Zertifizierung durch externen Dienstleister).
4	Notebooks und Datenträger werden bei Aussortierung fachgerecht gelöscht.
5	Verbot Einsatz privater Datenträger.
6	Das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten bei der Übertragung wird verhindert durch: ▪ OneDrive: Zugangsfreischaltung durch Link an den Empfänger per E-Mail. ▪ Zugangsdaten an Kunden für Zugriff; Verschlüsselung der Daten. ▪ Vollständigkeitsüberprüfung soweit relevant. ▪ Aufbau einer verschlüsselten Transportverbindung.
7	Die Weitergabe personenbezogener Daten erfolgt durch Nutzung folgender Dienste: ▪ Regelmäßig WWW (https, VPN). ▪ Andere Dienste und Transportverfahren, die dem gewünschten Zweck und dem aktuellen Stand der Sicherheitstechnik äquivalent oder besser entsprechen (FTP-Server in Verbindung mit Passwort-geschützten ZIP-Dateien).
8	Kontrollierte Vernichtung von Datenträgern und Papierdokumenten nach DIN-Norm 66399 mit Sicherheitsstufe 4.
9	Gesicherter Eingang für An- und Ablieferung.
10	Festplattenverschlüsselung: Clientsysteme.

11	Zur besseren Unterstützung bei Analyse-, Installations-, Konfigurations- und Support-Dienstleistungen auf IT-Systemen des Auftraggebers nutzt KUMAVISION die Fernwartungslösung TeamViewer. Über die Fernwartungslösung können die o.a. Dienstleistungen erbracht werden, ohne sich zum Aufstellungsort der jeweiligen IT-Systeme begeben zu müssen. Für die Auswahl und Bereitstellung einer Fernwartungslösung ist der Auftraggeber verantwortlich. Der Auftraggeber kann anstelle von TeamViewer daher jederzeit auch eine andere Fernwartungslösung einsetzen. Der Auftraggeber kann hierzu Vorschläge machen und seinen Sicherheitsanspruch an Fernwartungszugriffe - z.B. in Form eines Sicherheitskonzepts- erläutern. Der Aufbau der Datenfernverbindung wird grundsätzlich für die jeweilige Session durch den Auftraggeber freigeschaltet. Die Verantwortung für die IT-Sicherheit der IT-Systeme des Auftraggebers verbleibt vollumfänglich beim Auftraggeber. Soll die Fernwartung im Wissen des Auftraggebers ohne Beteiligung von KUMAVISION direkt durch einen genehmigten Unterauftragnehmer von KUMAVISION oder durch einen Dritten erfolgen, so entsteht zwischen Auftraggeber und Unterauftragnehmer bzw. Drittem ein unmittelbares, eigenständiges Auftragsverarbeitungsverhältnis außerhalb der tatsächlichen oder rechtlichen Verantwortlichkeit von KUMAVISION. Der Auftraggeber einerseits und der Unterauftragnehmer bzw. Dritte andererseits müssen in diesem Falle eine Vereinbarung über die Auftragsverarbeitung in eigener Verantwortlichkeit für die datenschutzrechtliche Zulässigkeit, die vertraglichen Rahmenbedingungen sowie die zum Einsatz kommenden technischen und organisatorischen Maßnahmen treffen. Informationen zur Verbindungs- und Datensicherheit sowie Anleitungen zur Installation und Parametrisierung von TeamViewer sind unter https://www.teamviewer.com/de/dokumente zu finden. KUMAVISION setzt für die Anmeldung an ihren TeamViewer Konten eine Zwei-Faktor-Authentifizierung ein und nutzt die Möglichkeit, in TeamViewer vertrauenswürdige Geräte zu bestimmen.
12	Zugriff von Externen nur über gesicherte Verbindungen/Systeme. VPN-Zugänge für mobile Arbeitsplätze/Heimarbeitsplätze.

4.2.2 Eingabekontrolle

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

#	Maßnahmen
1	Ob und von wem Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind, kann nachträglich überprüft und festgestellt werden durch: ▪ Benutzerprofile. ▪ Benutzeridentifikation. ▪ Protokollierung über Active Directory. ▪ Firewall-Protokollierung (TCP/IP). ▪ Protokollierung eingegebener Daten (Verarbeitungsprotokoll). ▪ NAVISION und weitere Applikationen (CRM, SharePoint): Ersteller und letzte Änderung. ▪ Protokollierung gescheiterter Anmeldeversuche. ▪ Protokollierung administrative Tätigkeiten über Ticketsystem.
2	Die KUMAVISION AG erhebt, verändert oder löscht personenbezogene Daten primär im Rahmen der eigenen Kundenverwaltungssysteme (Bestands- und Nutzungsdaten). Eine weiterführende Verarbeitung (Zweckänderung) der durch den Kunden bei der KUMAVISION AG im Rahmen der bereitgestellten Dienstleistung gespeicherten Daten (Inhaltsdaten) erfolgt nicht.

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

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung, Verlust oder zu hohe Beanspruchung geschützt sind.

#	Maßnahmen
1	Dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind, wird gewährleistet durch: ▪ Einsatz von RAID-Festplattensystemen sowie Cloudsysteme mit entsprechender Verfügbarkeit mit komplettem Backup-System. ▪ Nächtliche Sicherung des Gesamtsystems. ▪ Einsatz von USV: Abschaltung Systeme: Cache speichert Daten. ▪ Feuer- und Rauchmeldeanlagen. ▪ Betrieb einer Alarmanlage. ▪ Einsatz einer Klimaanlage mit Raumtemperaturüberwachung. ▪ Softwareseitigen Ausschluss: Aufteilung der Server zur unabhängigen und eigenständigen Erfüllung der Aufgaben (Shared-Nothing-Architektur). ▪ Für jede Aufgabe eigener Server. ▪ Mehrfache inkrementelle Datenbank- und Systembackups (nächtliche Gesamtsicherung). ▪ Backups nach einem Zeitplan, der die Veränderungen der Daten durch Nutzung angemessen reflektiert. ▪ Rekonstruktion von Datenbeständen (Datensicherungskonzept) wird sichergestellt. ▪ Trennung der Backupdaten von Produktivumgebung durch Cloudbackup-Provider. ▪ Tägliche Sicherung mit 33 Tagen Vorhaltung. ▪ Monatliche Sicherung mit 12 Monaten Vorhaltung.

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

4.4.1 Datenschutz-Management

Die KUMAVISION AG wird von der Deutschen Datenschutzkanzlei (externer Datenschutzbeauftragter: Maximilian Musch) betreut. Die Deutsche Datenschutzkanzlei nutzt ein eigens erstelltes Datenschutzmanagementsystem (DSMS), in dem alle Maßnahmen, Verfahren, Tätigkeiten etc. im Bereich Datenschutz abgebildet werden. Das DSMS beinhaltet die wichtigsten datenschutzrechtlichen Vorgaben und eine umfassende Struktur zur Abbildung der Datenschutzmaßnahmen und beinhaltet darüber hinaus einen Maßnahmenplan zur rechtskonformen Umsetzung der EU-Datenschutzgrundverordnung (Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO).

Das DSMS fungiert, neben der Erfüllung der Rechenschaftspflicht auch als Maßnahmenplan zur Umsetzung und Überprüfung der notwendigen Datenschutzmaßnahmen. Es werden hieraus regelmäßige Kontrollmaßnahmen abgeleitet und sowohl über das DSMS als auch die internen Arbeits-/Statusprotokolle sowie Auditberichte nachgehalten. Das DSMS ist an die DIN-Norm 27001 der Informationssicherheit angelehnt und ermöglicht die regelmäßige Prüfung, Bewertung, Evaluierung sowie Dokumentation der Maßnahmen.

4.4.2 Incident-Response-Management / Prozesse

Ein Helpdesk System (Ticketsystem) zur unverzüglichen Meldung aller Arten von Incidents an die IT ist implementiert. In der Anwenderrichtlinie sind Prozesse und Meldewege mit Vorgehen und Verantwortlichen dokumentiert. Zudem kommen Intrusion-Detection-Systeme zur Anwendung.

Zudem sind interne Prozesse zum Umgang mit Datenschutz-/Datensicherheitsvorfällen, Betroffenenanfragen, Einführung von (neuen) Datenverarbeitungssystemen, ein Dienstleister-/Lieferantenmanagementsystem usw. implementiert. Entsprechende Vorlagen, Dokumente zum besseren Verständnis sowie zur Dokumentation werden ebenfalls vorgehalten.

4.4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Grundsätzlich werden nur Daten erhoben und verarbeitet, die für die Geschäftszwecke zweckmäßig und erforderlich sind. Verfahren der automatisierten Datenerfassung- und -verarbeitung sind so gestaltet, dass nur die erforderlichen Daten erhoben werden. Die KUMAVISION AG ist bspw. Dienstleister im Microsoft Dynamics Umfeld und nicht für die Konzeption des Produktes verantwortlich. Bei Gestaltung, Umsetzung, Implementierung und Support des Systems handelt die KUMAVISION AG nach Kundenvorgabe.

Zur möglichst datenschutzkonformen Nutzung und Gestaltung der Systeme liegen jedoch unterschiedliche Hilfsmittel, Prozesse und Dokumente bereit, die es den, an der Datenverarbeitung beteiligten Personen erleichtern sollen, die Systeme und Datenverarbeitungsprozesse möglichst datenschutzgerecht zu nutzen. Der externe Datenschutzbeauftragte wird bei der Systemimplementierung und neuen Datenverarbeitungs-prozessen bei Bedarf hinzugezogen.

4.4.4 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

#	Maßnahmen
1	Alle Mitarbeiter sind hinsichtlich des Datenschutzes belehrt, auf das Datengeheimnis verpflichtet und haben als Bestandteil ihres Arbeitsvertrags entsprechende Verschwiegenheits- und Geheimhaltungsvereinbarungen akzeptiert.
2	Es bestehen detaillierte Angaben über Zweck, Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers nach Vorgabe des Art. 28 DSGVO. Die entsprechenden Angaben sind vertraglich fixiert.
3	Der Dienstleister hat, sofern erforderlich einen betrieblichen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse.
4	Eine regelmäßige Prüfung der beauftragten Dienstleister wird durch den eigenen Datenschutzbeauftragten, den IT-Sicherheitsbeauftragten bzw. die interne IT-Administration vorgenommen und dokumentiert. Diese Prüfungen finden ggf. auch vor Ort statt.
5	Mündliche Aufträge müssen schriftlich bestätigt und dokumentiert werden.
6	Eine Vergabe von Einzelaufträgen erfolgt nur über namentlich benannte Ansprechpartner.
7	Auf die betreffenden technischen Umgebungen werden nur restriktive Zugriffsberechtigungen vergeben. Bei externem Zugriff auf das System wird der Zugang nach Beendigung der Zusammenarbeit deaktiviert oder gesperrt.

4.5 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

Entsprechende Verschlüsselungssysteme für Datenträger und mobile Endgeräte sind implementiert (Bitlocker-Verschlüsselung). Verschlüsselungstechnologien bei der Übermittlung von Daten kommen ebenfalls zum Einsatz. Eine Richtlinie zum Umgang mit (mobilen) Datenträgern kommt zur Anwendung. Auch restriktive Zugriffsrechte beim Zugriff auf Server/Testdatenbanken/ Entwicklungssystem etc. werden angewandt.

Pseudonymisierungsverfahren sind grundsätzlich möglich, liegen bei der Datenverarbeitung jedoch im Verantwortungsbereich des Auftraggebers und sind nicht Bestandteil der originären Dienstleistung der KUMAVISION AG.

4.6 Zertifizierung ISO/IEC 27001:2013

Die KUMAVISION AG ist im Bereich „Entwicklung, Implementierung und Betreuung kundenindividueller branchenspezifischer Business-Software-Lösungen, kombiniert mit der Beratung zur Digitalisierung von Unternehmensprozessen“ nach der Norm ISO/IEC 27001 zertifiziert und führt ein Informationssicherheitsmanagementsystem.

Das aktuelle Zertifikat kann hier abgerufen werden: https://kumavision.com/zertifizierungen

4.7 Externer Datenschutzbeauftragter

Externer Datenschutzbeauftragter der KUMAVISION AG gemäß Art. 37 Datenschutzgrundverordnung (DSGVO) bzw. § 38 Abs. 1 BDSG-neu.

Maximilian Musch
Magister Artium (TU Darmstadt), geprüfter fachkundiger Datenschutzbeauftragter

Deutsche Datenschutzkanzlei
Büro Bodensee
Richard-Wagner-Str. 2, 88094 Oberteuringen
www.deutsche-datenschutzkanzlei.de

Kontakt Datenschutzbeauftragter
E-Mail: datenschutz@kumavision.com
Tel. +49 7542 / 94921-02