Technische und organisatorische Maßnahmen der QUADRESS GmbH nach Art. 28 DS-GVO

Allgemeine Angaben:

Firma: QUADRESS GmbH

Anschrift: Josef-Haumann-Str. 7a, 44866 Bochum

Ansprechpartner: Name: Daniel Simon **Funktion: Geschäftsführer**

Tel.-Nr.: +46 2327 3038- 10 **E-Mail: simon@quadress.de**

QUADRESS®
Der Zielgruppenspezialist

Nach den Vorschriften der EU-Datenschutzgrundverordnung (Art. 28 DSGVO) muss der Auftraggeber vor Beginn der Datenverarbeitung prüfen, ob beim Auftragnehmer geeignete technische und organisatorische Maßnahmen zum Datenschutz eingerichtet sind und eingehalten werden. Das Ergebnis dieser Prüfung ist zu dokumentieren.

Der Text von Art. 28 und Art. 32 DSGVO über die Sicherheit der Verarbeitung sind zu Ihrer Information beigefügt.

Im Nachfolgenden finden Sie die technischen und organisatorischen Maßnahmen der QUADRESS GmbH.

Anforderung	Erfüllt		Bemerkung/Erläuterung
	Ja	Nein	
1. Allgemeine Maßnahmen			
Wie viele Beschäftigte umfasst das Unternehmen?			Anzugeben sind nur diejenigen Beschäftigten, die mit der Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten befasst sind. Anzahl Beschäftigte: **13**
Ist ein Datenschutzbeauftragter bestellt?	☒	☐	Bitte Name und Kontaktdaten angeben: Ulrich Braunbach, zb Datenschutz GmbH & Co. KG, ubraunbach@zb-datenschutz.de
Unterzieht sich der Datenschutzbeauftragte einer regelmäßigen Fortbildung, wenn ja, bei welchen Einrichtungen?	☒	☐	Bitte Einrichtungen angeben: Externer DSB
Welche Position/en bekleidet der Datenschutzbeauftragte neben dieser Aufgabe noch?	☐	☐	⇨ nur externer DSB
Sind die Mitarbeiter auf das Datengeheimnis verpflichtet?	☒	☐	Bitte Verpflichtungsmuster beilegen
Ist die Verpflichtung nachweisbar dokumentiert?	☒	☐	Wo und in welcher Form? ⇨ Personalakte
Werden die Mitarbeiter laufend in die Anforderungen des Datenschutzes eingewiesen?	☒	☐	Nachweise liegen vor? ☒ Ja ☐ Nein
Besteht ein Testat über eine gesetzeskonforme Umsetzung des Datenschutzes im Unternehmen?	☐	☒	Welche Stelle hat das Testat ausgestellt? Auf welcher Normengrundlage wurde das Testat ausgestellt? Beruht das Testat auf einem externen Audit? ☐ Ja ☐ Nein Wie lange ist das Zertifikat noch gültig?
Welche Unternehmensbereiche			

umfasst das Zertifikat?			Bitte Kopie beifügen.
Gibt es ein Datenschutzkonzept bzw. ein Datenschutzhandbuch zur Regelung und Umsetzung des Datenschutzes im Unternehmen?	☒	☐	Ist der Datenschutz ggf. durch andere Verfahrensanweisungen geregelt? ☒ Ja ☐ Nein Welche? ☐ Liegt bei ☒ Steht zur Einsichtnahme zur Verfügung
Gibt es ein IT-Sicherheitshandbuch oder bestehen sonstige Regelungen für die technischen und organisatorischen Maßnahmen zum Datenschutz?	☒	☐	☐ Liegt bei ☒ Steht zur Einsichtnahme zur Verfügung
Werden Unterauftragnehmer eingesetzt?	☒	☐	
Werden ggf. Unterauftragnehmern dieselben Verpflichtungen auferlegt, die zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind?	☒	☐	
Bestehen auch mit Wartungs- und Pflegedienstleistungsunternehmen die erforderlichen datenschutzrechtlichen Vereinbarungen bzw. Verpflichtungen, ggf. in welcher Art?	☒	☐	Vertrag zur ADV
Wird die Datenverarbeitung auf dem Gebiet der Bundesrepublik Deutschland bzw. innerhalb der Europäischen Union oder der Staaten des Europäischen Wirtschaftsraums durchgeführt?	☒	☐	Ggf. in welchem Staat außerhalb dieses Gebiets?

Erfüllungsgrad der Maßnahmen:

Anmerkungen:

Anforderung	Erfüllt		Bemerkung/Erläuterung
	Ja	Nein	
2. Technische und organisatorische Maßnahmen			
2.1 Zutrittskontrolle			
Sind Gelände und Gebäude außerhalb der Betriebszeit gesichert?	☒	☐	☐ Wachpersonal ☒ Bewegungsmelder/Alarmanlage ☒ Videoüberwachung ☐ Sonstiges:
Sind die Zu- und Ausgänge gesichert?	☒	☐	Gebäudeeingangstüren ☒ Ja ☐ Nein Fluchttüren/Notausgänge ☒ Ja ☐ Nein ☐ Entfällt Lüftungsöffnungen ☐ Ja ☐ Nein ☒ Entfällt Feuerleitern und -treppen ☐ Ja ☐ Nein ☒ Entfällt
Besteht eine Regelung/Verfahren zur Besucherführung?	☒	☐	☒ Empfang ☐ Besucherbuch ☐ Besucherausweis ☒ Persönliche Besucherführung ☐ Sonstiges:
Wird Fremdpersonal, z. B. Wartungs- und Servicepersonal, beaufsichtigt?	☒	☐	
Sind Zutrittssicherungen eingerichtet?	☒	☐	☒ Zutrittskontrollsystem ☒ mit ☐ ohne Sicherheitszonen ☒ Zentrales Schließsystem ☒ Sicherheitsschlösser ☐ Sonstiges:
Sind Sicherheitsbereiche definiert, z.B. Serverraum, TK-Anlage, Archive, Netzwerkverteiler?	☒	☐	Welche? ⇨ Serverraum
Sind diese Sicherheitsbereiche gegen unbefugten Zutritt besonders	☒	☐	Art des Schutzes?

geschützt, ggf. wie?			⇨ Verstärkter Raum + Sicherheitstür
Sind die Zutrittsberechtigungen zu diesen Sicherheitsbereichen geregelt und dokumentiert?	☒	☐	
Werden zu diesen Sicherheits-bereichen Anwesenheits-aufzeichnungen geführt?	☐	☒	In welcher Form? Zugang nur für Geschäftsleitung durch Rechte im Schließsystem
Sind sonstige Schutzmaßnahmen eingerichtet?	☒	☐	☐ Pförtner ☐ Wachdienst ☐ Alarmanlage ☐ Sonstiges:

Erfüllungsgrad der Maßnahmen:

Anmerkungen:

Anforderung	Erfüllt		Bemerkung/Erläuterung
	Ja	Nein	
2.2 Zugangskontrolle			
Sind Maßnahmen zur Zugangskontrolle zum Desktop und zu den vernetzten Systemen eingerichtet?	☒	☐	☒ Userkennung ☒ Sicheres Passwort ☒ Passwortwiederholungssperre nach Fehlversuchen ☐ Andere Verfahren:
Bestehen für alle Zugriffsebenen (Netz, Server, Anwendungen) Passwortregeln zur Gewährleistung eines sicheren und vertraulichen Passworts?	☒	☐	
Wird die Einhaltung dieser Regeln auf allen Ebenen bei der Eingabe automatisiert kontrolliert?	☐	☒	
Ist eine zeitgesteuerte passwortgeschützte Pausenschaltung (Bildschirmschoner) eingerichtet?	☒	☐	
Sind die Systeme gegen unbefugtes Eindringen geschützt?	☒	☐	☒ Firewall ☒ Virenscanner ☐ Schnittstellenschutz (Netzwerkschaltschränke, Schutz nicht benötigter Netzwerksteckdosen etc.) In welcher Form?
Sind Protokollierungen/ Überwachungsmaßnahmen eingerichtet, ggf. welche?	☒	☐	☒ Testung, Freigabe und Einrichtung von Verfahren ☒ Einrichtung Benutzer und Rechte ☒ Systemänderungen ☒ Zugriffe und Zugriffsversuche ☒ Systemüberwachung ☒ Protokollierung der Administratortätigkeiten ☒ An- und Abmeldung an Datenverarbeitungsverfahren

Werden die Protokolldaten revisionssicher und zugriffsgeschützt gespeichert?	☐	☒	
Werden die Protokolldaten zeitnah und regelmäßig auf sicherheitsrelevante Aktionen und Vorgänge überprüft?	☒	☐	☐ Automatisiert ☒ Manuell Durch wen? ➔ Netzwerkadmin
Ist ein zuverlässiger und aktueller Internetschutz eingerichtet?	☒	☐	☒ Firewall ☒ Virenscanner
Bestehen Regelungen zur sicheren E-Mail- und Internetnutzung?	☒	☐	Art und Inhalt der Regelungen? ⇨ in der Betriebsvereinbarung

Erfüllungsgrad der Maßnahmen:

Anmerkungen:

Anforderung	Erfüllt		Bemerkung/Erläuterung
	Ja	Nein	
2.3 Zugriffskontrolle			
Besteht ein dokumentiertes Berechtigungsprofil, das sicherstellt, dass jeder Mitarbeiter nur über die Zugriffsbefugnisse verfügt, die er zur Aufgabenerledigung benötigt?	☒	☐	In welcher Form? ⇨ Servergesteuert Soweit erforderlich auch differenziert nach: ☒ Leseberechtigung ☒ Schreibberechtigung ☐ Sonstigen Berechtigungen, ggf. welche
Ist die Urlaubsvertretung mit entsprechender Rechtegestaltung geregelt?	☒	☐	
Sind die festgelegten Berechtigungen und deren Veränderungen nachvollziehbar dokumentiert?	☒	☐	In welcher Form? ⇨ in Server-Software
Ist eine Rechteverwaltung eingerichtet, die bei einer Veränderung des Aufgabengebiets eine zeitnahe Aufhebung nicht mehr benötigter Rechte sicherstellt?	☒	☐	In welcher Form? ⇨ Richtlinie / Arbeitsanweisung

Erfüllungsgrad der Maßnahmen:

Anmerkungen:

Anforderung	Erfüllt		Bemerkung/Erläuterung
	Ja	Nein	
2.4 Weitergabekontrolle			
Werden die Daten bei ihrer Übertragung vor unbefugter Kenntnisnahme geschützt?	☒	☐	☒ Verschlüsselung ☒ Sichere Verbindungen, z. B. VPN ☐ Sonstige Maßnahmen:
Werden Datenübermittlungen nachvollziehbar protokolliert und kontrolliert?	☒	☐	Wie und in welcher Form? ⇨ 4-Augen-Prinzip, Dokumentation zentral auf dem Server gespeichert
Werden bei Datenträgertransporten die erforderlichen Sicherheits-vorkehrungen beachtet?	☒	☐	☒ Verschlüsselung der Daten ☐ Sicherheitsbehälter ☐ Übergabeprotokolle, Lieferscheine ☒ Sicherer Versand, nur eigene oder geprüfte Kuriere ☒ Vollständigkeitskontrollen ☐ Ein- und Ausgangsbücher ☐ Sonstiges:
Werden Schnittstellen von PCs und externe Laufwerke (mobile Fest-platten, USB-Sticks etc.) gegen Missbrauch geschützt?	☒	☐	☒ Sperrung unbefugter Geräte ☒ Protokollierung der Nutzung der Geräte ☐ Verschlüsselung der mobilen Datenträger ☒ Überwachung/Protokollierung des Datenstroms an USB-Schnittstellen ☒ Sicherheitsrichtlinien ☐ Sonstiges:
Ist die sichere Nutzung mobiler Datenträger geregelt?	☒	☐	Wie und in welcher Form? ⇨ Verschlüsselung aller Dateien
Ist eine sichere Löschung, Vernichtung und Entsorgung von Datenträgern gewährleistet?	☒	☐	Wie sind die Löschung, Vernichtung und Entsorgung geregelt? ⇨ Schredder im Hause
Ist die Löschung/Vernichtung von Datenträgern an ein Dienstleistungs-unternehmen vergeben?	☒	☐	Teilweise: Rückläufer und alte Rechnungen

Besteht hierzu ein Vertrag/Auftrag nach den Vorgaben des Art. 28 DSGVO?	☒	☐	
Ist die sichere und vertrauliche Außerbetriebnahme von Geräten mit Datenträgern (z.B. Server, Multifunktionsgeräte etc.) geregelt?	☒	☐	Art und Inhalt der Regelungen: ⇨ Fachgerechte Entsorgung durch IT-Firma
Erfolgt bei Fernwartung der Zugriff auf die Kundendaten und Kundensysteme nur über sichere Leitungen?	☒	☐	Wie sind die Leitungen gesichert? ☒ VPN ☐ Verschlüsselung ☐ Sonstiges: Ist dies auch bei einem Zugriff von anderen Stellen aus der Fall, z. B. im Home-Office-Betrieb? ☒ Ja ☐ Nein
Ist bei Fernwartung eine sichere Identifizierung/Authentifizierung gewährleistet?	☒	☐	Bitte das Verfahren kurz beschreiben: ⇨ Siehe Verarbeitungsverzeichnis
Werden bei Fernwartung die Leitungen durch geeignete Sicherheitseinrichtungen, z. B. Protokollierung und Protokollauswertung, überwacht?	☒	☐	Art der Maßnahmen: ⇨ Protokoll in der Firewall

Erfüllungsgrad der Maßnahmen:

Anmerkungen:

Anforderung	Erfüllt		Bemerkung/Erläuterung
	Ja	Nein	
2.5 Eingabekontrolle			
Werden die Einwahlvorgänge in Kundensysteme nachvollziehbar protokolliert und überwacht?	☒	☐	In welcher Form? ⇨ Zugang nur über VPN, Logs in beispielsweise CRM-System
Werden die Benutzung von Datenverarbeitungssystemen und die Eingabe von Daten protokolliert?	☒	☐	Protokollierung der Dateibenutzung: ☐ Ja ☐ Nein Protokollierung von Eingaben und Veränderungen: ☐ Datenfeldbezogen ☒ Datensatzbezogen ☐ Dateibezogen ☐ Keine Protokollierung

Erfüllungsgrad der Maßnahmen:

Anmerkungen:

Anforderung	Erfüllt		Bemerkung/Erläuterung
	Ja	Nein	
2.6 Auftragskontrolle			
Wird die Durchführung des Kundenauftrags/der Serviceaktion nachvollziehbar überwacht, um eine auftragskonforme Erledigung zu gewährleisten?	☒	☐	In welcher Form? ⇨ 4-Augen-Prinzip
Sind geeignete Protokollierungs- und Auswertungsmechanismen eingerichtet, um unzulässige Zugriffe auf Kundensysteme und Kundendaten zu überwachen?	☒	☐	In welcher Form? ⇨ Händische Protokolle der Mitarbeiter
Werden bei einer Vergabe von Serviceaufträgen (z. B. IT-Service) die Vorgaben des Art. 28 DSGVO beachtet?	☒	☐	☒ Auswahl des Auftragnehmers ☒ Überprüfung der technischen und organisatorischen Maßnahmen beim Auftragnehmer ☒ Abschluss eines Vertrags gemäß Art. 28 DSGVO ☒ Regelmäßige Überprüfung des Auftragnehmers

Erfüllungsgrad der Maßnahmen:

Anmerkungen:

Anforderung	Erfüllt		Bemerkung/Erläuterung
	Ja	Nein	
2.7 Verfügbarkeitskontrolle			
Sind die Kundendaten durch geeignete Sicherungsverfahren vor Zerstörung und Verlust geschützt?	☒	☐	z. B. ☒ Gespiegelter Datenbestand ☒ Regelmäßige Sicherungskopien/ Back-up-Lösung ☐ Sonstiges Gibt es ein Sicherungskonzept, in dem die Art und Weise einer regelmäßigen Sicherung und die Rekonstruktion der Daten festgelegt ist? ☒ Ja ☐ Nein
Werden die Sicherungsbestände sicher verwahrt?	☒	☐	In welcher Weise (z. B. Tresor der Güteklasse S120P für Papierdokumente oder S120D bzw. S120DIS für Datenträger nach Brandprüfung gemäß ECB:S/EN 1047-1)? ⇨ Gesicherter Serverraum
Besteht ein geregeltes Verfahren zur Datenträgerverwaltung mit einer Nachweisführung über Eingang, Ausgang, Versand und Bestand von Datenträgern?	☒	☐	
Sind Maßnahmen zur Sicherung des Serverraums und der IT-Infrastruktur eingerichtet?	☒	☐	☒ Unterbrechungsfreie Stromversorgung mit Überspannungsschutz ☒ Klimaanlage mit Überwachung der Funktionen ☒ Branderkennung ☐ Brandschutz, Feuerlöscheinrichtungen ☐ Automatischer Shutdown (Notabschaltung) der Systeme ☐ Automatische Stromabschaltung Sonstiges:

Gibt es ein Notfallhandbuch mit Alarmierungs- und Wiederanlaufplan?	☐	☒	⇨ Im Notfall Weiterarbeiten bei Partnerunternehmen mit konsistentem Datenbestand möglich durch externe Datensicherung aller relevanten Daten
Ist das Notfallhandbuch transportabel und schnell erreichbar, z. B. auf einem mobilen Datenträger, oder sicher ausgelagert?	☐	☒	⇨ nicht zutreffend!

Erfüllungsgrad der Maßnahmen:

Anmerkungen:

Anforderung	**Erfüllt**		**Bemerkung/Erläuterung**
	Ja	**Nein**	
2.8 Datentrennung			
Sind die Daten der verschiedenen Kunden in geeigneter Weise voneinander getrennt, um eine getrennte Verarbeitung zu gewährleisten?	☒	☐	Art der Trennung: Logische Trennung auf ☒ Betriebssystemebene ☒ Anwendungsebene ☐ Mandantentrennung ☐ Physikalische Trennung

Anmerkungen:

Anlagen:

Ort, Datum Unterschrift

Erfüllungsgrad der Maßnahmen:

Anmerkungen:

Art. 28 DSGVO – Auftragsverarbeitung

1. Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.
2. Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.
3. Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter
    a. die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;
    b. gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
    c. alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;
    d. die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;
    e. angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;
    f. unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;
    g. nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;
    h. dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

    Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

4. Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind, wobei insbesondere hinreichende Garantie dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.
5. Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.
6. Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vorliegenden Artikels genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 und 43 erteilten Zertifizierung sind.
7. Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 93 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.
8. Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.
9. Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.
10. Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

Art. 32 DSGVO – Sicherheit der Verarbeitung

1. 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 treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:
    a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
    b. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
    c. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
    d. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
2. Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.
3. Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.
4. Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.