Anlage A

Fragenkatalog zur Dokumentation von Prüfungen im Zusammenhang mit Auftragsverarbeitung nach Art. 32 DSGVO

Auftraggeber	Auftragnehmer	Daten zur (Rahmen-)ADV	Datum
	Porsche Informatik GmbH		*2025-09-17*

Nr.	Prüfungspunkt			Beurteilung der TOM (wird vom Auftraggeber ausgefüllt)
0.	**Organisationskontrolle**			
0.1	**Ist die Umsetzung des Datenschutzes organisiert?**	☒ Ja	☐ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):			
	• Verantwortungsstrukturen für Datenschutz innerhalb des Unternehmens bis zur Leitungsebene		☒	
	• Einbindung von Mitarbeitern in den Fachabteilungen (z.B. als „Datenschutzkoordinatoren“ für den jeweiligen Fachbereich)		☒	
	• Benennung eines Datenschutzbeauftragten?	☐ Extern	☒ Intern	
	○ bei intern: herausgehobene Stellung		☒	
	○ bei intern: eigene Mitarbeiter		☒	
	○ bei extern: hohes Renommee		☐	
	• formalisierter Austausch zwischen Datenschutzbeauftragtem, den für den Datenschutz Verantwortlichen und den Fachbereichen (z.B. „Datenschutzkreis Konzern“, „Jour Fix Datenschutz“)		☒	
	• Einbindung von Datenschutzanforderungen in relevante Prozesse		☒	
	• Zertifizierung des Datenschutzmanagements/ Orientierung an DIN/ISO-Standards: ggf. welche: _____		☐	
	• Sonstiges: ISAE3402		☒	
0.2	**Wurden organisatorische Maßnahmen zur gesetzeskonformen Verarbeitung personenbezogener Daten getroffen?**	☒ Ja	☐ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):			
	• Implementierung von unternehmensinternen Gremien unter Mitarbeit des Datenschutzbeauftragten		☒	
	• Implementierung von Prozessen zur Sicherstellung der Mitarbeit des Datenschutzbeauftragten		☒	
	• klare interne Regeln zum Datenschutz (z.B. Datenschutz-Policy)		☒	
	• Verpflichtung der Mitarbeiter auf das Datengeheimnis		☒	
	• Sonstiges: _____		☐	
0.3	**Wird sichergestellt, dass die internen Prozesse/Arbeitsabläufe gemäß den jeweils gültigen Datenschutzbestimmungen und nur auf Anweisung des Auftraggebers ablaufen?**	☒ Ja	☐ Nein	
	Wenn ja, erfolgt insoweit eine regelmäßige Qualitätsprüfung?	☒ Ja	☐ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):			
	• Auditierung der Prozesse durch renommierte externe Stellen		☒	

Anlage A

Fragenkatalog zur Dokumentation von Prüfungen im Zusammenhang mit Auftragsverarbeitung nach Art. 32 DSGVO

Nr.	Prüfungspunkt				Beurteilung der TOM (wird vom Auftraggeber ausgefüllt)
	• Verfahren zur Beobachtung der Entwicklung der rechtlichen und technischen Datenschutzanforderungen			☒	
	• Einbindung neuer Erkenntnisse in die Produktivprozesse			☒	
	• Zertifizierung der Prozesse nach DIN/ISO-Standards: _____			☒	
	• Sonstiges: Internes Kontrollsystem, Dokumentation der Audits und Arbeitsabläufe			☒	
0.4	**Werden die Mitarbeiter in Bezug auf die Umsetzung der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO geschult?**	☒ Ja	☐ Nein		
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):				
	• für jeden Mitarbeiter verfügbares, umfangreiches Handbuch			☒	
	• unternehmensinternes Wiki zum Datenschutz			☒	
	• datenschutzrechtliche Schulungen von Mitarbeitern				
	○ bei Einstellung neuer Mitarbeiter			☒	
	○ in regelmäßigen Abständen verpflichtend für alle Mitarbeiter			☒	
	○ freiwillige Auffrischungsschulungen (z.B. web-based) für alle Mitarbeiter verfügbar			☐	
	○ sonstiges (z.B. Einweisung): Einweisung Datenschutzerklärung_____			☒	
	• strukturiertes Verfahren zur Ermittlung und Umsetzung der Schulungsnotwendigkeit hinsichtlich aktueller Entwicklungen			☒	
	• Umsetzung neuer Erkenntnisse bei den Schulungsmaßnahmen			☒	
	• sonstige Awarenessmaßnahmen			☒	
	○ regelmäßige Information über aktuelle datenschutzrechtliche Themen innerhalb des Unternehmens			☒	
	○ sonstiges (z.B. „Privacy day“): Termin der DSB mit den Datenschutzkoordinatoren,+ Veranstaltungen			☒	
	• Einbeziehung von Fremdkräften insb. Leiharbeitnehmer, Mitarbeiter von Dienstleistern in die o.g. Maßnahmen			☒	
	• Sonstiges: _____			☐	
0.5	**Werden die einschlägigen Datenverarbeitungen hinsichtlich ihrer datenschutzrechtlichen Zulässigkeit dokumentiert?**	☒ Ja	☐ Nein		
	Wenn ja, wird insoweit ein Verfahrensverzeichnis für den Auftragsverarbeiter erstellt?	☒ Ja	☐ Nein		
0.6	**Werden die Privacy-/Data Protection-by-Design- und –by-Default-Prinzipien unternehmensintern umgesetzt?**	☒ Ja	Nein ☐		
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):				
	• Aufnahme der Privacy-/Data Protection-by-Design- und –by-Default-Anforderungen in Einkaufsrichtlinien			☒	
	• Aufnahme der Privacy-/Data Protection-by-Design- und –by-Default-Anforderungen in Entwicklungsrichtlinien			☒	

Anlage A

Fragenkatalog zur Dokumentation von Prüfungen im Zusammenhang mit Auftragsverarbeitung nach Art. 32 DSGVO

Nr.	Prüfungspunkt			Beurteilung der TOM (wird vom Auftraggeber ausgefüllt)
	• testgetriebene Entwicklung auch mit dem Ziel der Einhaltung von Privacy-by-Design		☐	
	• Verwendung von nicht-personenbezogenen Testdaten bei der Entwicklung		☐	
	• umfassende Verwendung von Verschlüsselungstechnologie		☒	
	• Sonstiges: _____		☐	
1.	**Maßnahmen zur Zutrittskontrolle**			
1.1	**Werden die Gebäude, in denen die Datenverarbeitung stattfindet, vor unbefugtem Zutritt gesichert?**	☒ Ja	☐ Nein	
	Ergriffene Maßnahmen zur Gebäudesicherung (Mehrfachauswahl möglich):			
	• detailliertes Zutrittsberechtigungsmanagement		☒	
	• Verbindung der HR-Software mit der Zutrittsverwaltung (z.B. automatische Erfassung Austritte, Freistellungen usw)		☒	
	• organisatorische Anweisung zur Meldung von Austritten, Freistellungen etc. an die Zutrittsverwaltung		☒	
	• besondere Schließverfahren, elektronische Zutrittskontrolle (z.B. Keycard o.ä.)		☒	
	• Zugangskontrolle am Empfang		☒	
	• Videoüberwachung		☒	
	• Wachpersonal		☐	
	• besondere technische Maßnahmen gegen unbefugtes Betreten			
	○ einbruchsichere Fenster		☒	
	○ einbruchsichere Türen		☒	
	○ Alarmanlage		☒	
	○ Bewegungsmelder		☒	
	○ Rollläden mit Hochschiebesicherung		☐	
	• Einhaltung einschlägiger Standards (VdS, DIN)		☐	
	• Sonstiges: _____		☐	
1.2	**Werden die Räume/Büros, in denen die Datenverarbeitung stattfindet, vor unbefugtem Zutritt gesichert?**	☒ Ja	☐ Nein	
	Ergriffene Maßnahmen zur Sicherung der Gebäude bzw. Räume/Büros (Mehrfachauswahl möglich):			
	• Büros mit separaten Schlössern für ausschließlichen Zugang durch Zutrittsberechtigte		☐	
	• detailliertes Zutrittsberechtigungsmanagement für die Räume		☒	
	• Verbindung der HR-Software mit der Zutrittsverwaltung (z.B. automatische Erfassung Austritte, Freistellungen usw.)		☒	
	• risikoorientiertes Schutzzonenkonzept für Zutrittsberechtigungen		☒	
	• Beschränkung des Kreises der Zutrittsberechtigten über das Need-to-know-Prinzip		☒	
	• besondere Schließverfahren, elektronische Zutrittskontrolle (z.B. Keycard o.ä.)		☒	
	• Videoüberwachung		☒	
	• Wachpersonal		☐	
	• besondere technische Maßnahmen gegen unbefugtes Betreten			

Anlage A

Fragenkatalog zur Dokumentation von Prüfungen im Zusammenhang mit Auftragsverarbeitung nach Art. 32 DSGVO

Nr.	Prüfungspunkt		Beurteilung der TOM (wird vom Auftraggeber ausgefüllt)
	○ einbruchsichere Fenster	☒	
	○ einbruchsichere Türen	☒	
	○ Alarmanlage	☒	
	○ Bewegungsmelder	☐	
	○ Rollläden mit Hochschiebesicherung	☐	
	• Anordnung zur Einhaltung einschlägiger Standards (VdS, DIN)	☐	
	• Sonstiges: _____	☐	
1.3	**Werden die Hardwarekomponenten / physische Datenspeicher vor Missbrauch geschützt?**	☒ Ja ☐ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):		
	• speziell gesicherter Server-Schrank	☒	
	• Alarm bei Öffnung der Tür des Serverschrankes	☒	
	• Notebookschloss	☐	
	• Anweisung zum sorgfältigen Umgang mit mobilen Endgeräten	☒	
	• Verbot der Weitergabe mobiler Endgeräte	☒	
	• lückenlose Verschlüsselung nach BSI State-of-the-Art	☒	
	• Anweisung zum Wegschließen von Notebooks und anderer mobiler Endgeräte	☐	
	• Anweisung zum Wegschließen von vertraulichen Papierdokumenten	☒	
	• Sonstiges: _____	☐	
1.4	**Werden die oben genannten Zutrittskontrollmaßnahmen auf Tauglichkeit überprüft?**	☒ Ja ☐ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):		
	• regelmäßige, dokumentierte Testverfahren	☒	
	• regelmäßige Überprüfung (mindestens einmal jährlich) der Zutrittsberechtigungen	☒	
	• regelmäßige Untersuchung und Bestätigung des Standards durch Dritte	☒	
	• regelmäßige Untersuchung und Bestätigung des Standards durch den Datenschutzbeauftragten	☐	
	• Sonstiges: Regelmäßige Kontrolle, ob bei allen Notebooks die Festplatte verschlüsselt ist, Überpüfung der Wirksamkeit der Sicherheitsmaßnahme	☒	
2.	**Maßnahmen zur Zugangskontrolle**		
2.1	**Benutzerverwaltung**		
2.1.1	**Erfolgt eine kontrollierte Vergabe von Benutzerzugängen (-accounts)?**	☒ Ja ☐ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):		
	• Errichtung einer zentralen Stelle für die Benutzerverwaltung	☒	
	• klares Vergabekonzept (standardisierter Prozess zur Antragstellung, Genehmigung, Einrichtung, Änderung, Löschung etc.)	☒	
	• restriktive Vergabe von Benutzerkennungen (Need-to-Know-Prinzip)	☒	

Anlage A

Fragenkatalog zur Dokumentation von Prüfungen im Zusammenhang mit Auftragsverarbeitung nach Art. 32 DSGVO

Nr.	Prüfungspunkt					Beurteilung der TOM (wird vom Auftraggeber ausgefüllt)
	• restriktive Vergabe / Differenzierung von Rechten für die jeweiligen Benutzer (z.B. Administratorrechten)				☒	
	• Sonstiges: zeitliche Befristung von Accounts gem. ISO 27001				☒	
2.1.2	**Wird die Gültigkeit von Benutzerzugängen (-accounts) überprüft?**	☒	Ja	☐	Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):					
	• regelmäßige, stichprobenartige Überprüfung der Zugänge				☒	
	• automatische Deaktivierung / Löschung inaktiver Zugänge				☒	
	• Abbildung von Standardänderungen (z.B. Versetzung, Austritt, Elternzeit etc.) im Nutzerkonzept				☒	
	• Sonstiges:				☐	
2.1.3	**Werden die Benutzerzugänge (-accounts) dokumentiert?**	☒	Ja	☐	Nein	
	Wird das Antrags- und Genehmigungsverfahren sowie das Änderungsverfahren dokumentiert?	☒	Ja	☐	Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):					
	• Dokumentation wird vom System automatisch erstellt (z.B. Systemprotokollierung, Workflow-Management etc.)				☒	
	• Benutzerverwaltung durch zentrale, hierfür verantwortliche Stelle				☒	
	• Sonstiges: _____				☐	
2.1.4	**Wird sichergestellt, dass die Vergabe von Administrationszugängen auf die notwendige Anzahl beschränkt ist?**	☒	Ja	☐	Nein	
	Wird sichergestellt, dass die Administratoren fachlich und persönlich geeignet sind?	☒	Ja	☐	Nein	
	Wird sichergestellt, dass externe Administratoren, Service oder Wartungstechniker persönlich geeignet sind?	☐	Ja	☒	Nein	
2.2	**Passwortsicherheit**					
2.2.1	**Wird durch Maßnahmen sichergestellt, dass Passwörter nur dem jeweiligen Benutzer und keinem Unbefugten bekannt sind?**	☒	Ja	☐	Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):					
	• technisch zwingende Änderung des Initialpassworts				☒	
	• Verbot der Weitergabe von Passwörtern				☒	
	• Anweisung zur Geheimhaltung von Passwörtern				☒	
	• Anweisung zur sicheren Übermittlung von Passwörtern				☒	
	• Verbot jeglicher Dokumentation von Passwörtern				☒	
	• Benutzerverwaltung durch zentrale, hierfür verantwortliche Stelle				☒	
	• Sonstiges: _____				☐	
2.2.2	**Werden erhöhte Anforderungen an die Komplexität von Passwörtern gestellt?**	☒	Ja	☐	Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):					

Anlage A

Fragenkatalog zur Dokumentation von Prüfungen im Zusammenhang mit Auftragsverarbeitung nach Art. 32 DSGVO

Nr.	Prüfungspunkt				Beurteilung der TOM (wird vom Auftraggeber ausgefüllt)
	• interne Kennwortrichtlinie mit konkreten Vorgaben			☒	
	• technische Voreinstellung, die nur die der Richtlinie entsprechende Kennwörter zulässt			☒	
	• Sonstiges: _____			☐	
2.2.3	**Wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändern kann bzw. muss?**	☒ Ja	☐ Nein		
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):				
	• technisch zwingende Erneuerung des Passworts in bestimmten zeitlichen Abständen (z.B. monatlich)			☒	
	• Verpflichtung zur Erneuerung des Passworts			☒	
	• Verpflichtung zur sofortigen Änderung voreingestellter Passwörter			☒	
	• Speicherung einer Kennworthistorie zur Vermeidung identischer Kennwörter innerhalb bestimmter Zeiträume			☒	
	• Sonstiges: _____			☐	
2.2.4	**Werden Passwörter durch eine zentrale Einheit verwaltet?**	☒ Ja	☐ Nein		
	Wenn ja, ist innerhalb dieser zentralen Einheit ein Rollen- und Rechtekonzept festgelegt?	☒ Ja	☐ Nein		
2.2.5	**Werden bei gescheitertem Anmeldeversuchen Maßnahmen ergriffen?**	☒ Ja	☐ Nein		
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):				
	• Benutzerkonto wird automatisch gesperrt			☒	
	• Verantwortlicher (Administrator / zentrale Einheit) wird automatisch über den gescheiterten Anmeldeversuch informiert			☒	
	• Mitteilung an Mitarbeiter, Passwort unverzüglich zu ändern			☐	
	• automatische Freigabe nach bestimmtem Zeitablauf			☒	
	• Freigabe durch Administrator			☒	
	• Sonstiges: _____			☐	
2.2.6	**Wurden organisatorische Vorkehrungen zur Verhinderung unberechtigter Zugriffe auf personenbezogene Daten am Arbeitsplatz getroffen?**	☒ Ja	☐ Nein		
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):				
	• regelmäßige Unterweisungen zum Umgang mit diverser Hardware			☒	
	• regelmäßige Unterweisung zum Umgang mit Dokumenten			☒	
	• Zwei-Faktor-Authentifizierung (Beispiel: Neben Benutzername und Passwort ist z.B. eine Smartcard / ein Hardware-Token erforderlich)			☒	
	• Vorkehrungen, dass nur unternehmenseigene und verschlüsselte USB-Sticks eingesetzt werden können			☐	
	• Einsatz spezieller Data-Loss-Software			☐	
	• Einsatz spezieller Data-Leakage-Prevention-Software			☐	
	• Einführung eines Data-breach-Prozesses			☒	
	• Einführung eines Incident-response-Systems			☒	
	• Sonstiges: _____			☐	
3.	**Maßnahmen zur Zugriffkontrolle**				

Anlage A

Fragenkatalog zur Dokumentation von Prüfungen im Zusammenhang mit Auftragsverarbeitung nach Art. 32 DSGVO

Nr.	Prüfungspunkt			Beurteilung der TOM (wird vom Auftraggeber ausgefüllt)
3.1	**Ist sichergestellt, dass Rollen / Zugriffsberechtigungen anforderungsgerecht und zeitlich beschränkt vergeben werden?**	☐ Ja	☒ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):			
	• Identitätsmanagementsystem (IDMS) zur Festlegung von Rollen / Berechtigungen		☐	
	• regelmäßige Auditierung bestehender Rollen / Berechtigungen		☐	
	• Beantragung von Rechten über IDMS und Genehmigung durch Vorgesetzten		☒	
	• Sonstiges: _____		☐	
3.2	**Werden die Zugriffsberechtigungen dokumentiert?**	☒ Ja	☐ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):			
	• Es besteht ein verpflichtendes Berechtigungskonzept (Differenzierung bspw. lokaler Admin / Group Admin / Standard-Benutzer).		☒	
	• Benutzer, Rollen und Anträge werden im IDMS dokumentiert		☒	
	• Sonstiges: _____		☐	
3.3	**Ist sichergestellt, dass Benutzer ihre Zugriffsberechtigung nicht missbräuchlich verwenden?**	☒ Ja	☐ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):			
	• Monitoring durch IDMS		☐	
	• Nutzung von Protokollierungs- und Protokollauswertungssystemen		☒	
	• Nutzung eines Systems zur Feststellung von auffälligen bzw. verdächtigen Aktivitäten		☒	
	• Sonstiges: _____		☐	
4.	**Maßnahme zur Weitergabekontrolle**			
4.1	**Wird die Integrität und Vertraulichkeit bei der Weitergabe personenbezogener Daten gewährleistet?**	☒ Ja	☐ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):			
	• Klassifizierung von Daten nach Grad der Vertraulichkeit		☒	
	• Pseudonymisierung / Anonymisierung der Daten vor Weitergabe		☐	
	• vertragliche Geheimhaltungsabreden mit Dienstleistern / Subunternehmern		☒	
	• Verschlüsselung von Mails und sonstiger elektronischer Kommunikation		☒	
	• elektronische Signaturen für Mails		☐	
	• Passwortsicherung / Verschlüsselung von mobilen Geräten		☒	
	• organisatorische Vorgaben / Unternehmensrichtlinie zur Beschränkung der Verwendung mobiler Geräte / Datenträger (z.B. Verbot von USB-Sticks, Verbot der Nutzung privater mobiler Geräte)		☒	
	• technische Trennung von dienstlicher und privater Kommunikation		☐	
	• sorgfältige Auswahl der Transportmittel und Boten beim Transport von Datenträgern		☒	
	• Unternehmensrichtlinie mit entsprechenden organisatorischen Maßnahmen		☒	
	• Data-breach-Prozess		☒	

Nr.	Prüfungspunkt	Beurteilung der TOM (wird vom Auftraggeber ausgefüllt)
	• Incident-response-System ☒ • Sonstiges: Überwachung/Auditierung der Dienstleistern ☐	

4.2	**Werden bei der Weitergabe von personenbezogenen Daten Verschlüsselungssysteme eingesetzt?** ☒ Ja ☐ Nein
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):
	• Ipsec-Verfahren ☐
	• SSH-Verfahren ☐
	• Verwahrung von Schlüsselmaterial über Hardware Security Module ☒
	• Bitlocker zur Verschlüsslung von Laptops ☒
	• TLS-Verschlüsselung ☒
	• verschlüsselte Plattformen zum Datenaustausch ☒
	• E-Mail-Verschlüsselung
	  ○ Ende-zu-Ende-Verschlüsselung ☐
	  ○ Transportverschlüsselung ☒
	• Sonstiges: _____ ☐	

Anlage A

Fragenkatalog zur Dokumentation von Prüfungen im Zusammenhang mit Auftragsverarbeitung nach Art. 32 DSGVO

Nr.	Prüfungspunkt				Beurteilung der TOM (wird vom Auftraggeber ausgefüllt)
4.3	**Wird die Weitergabe personenbezogener Daten dokumentiert?**	☒	Ja	☐ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):				
	• Erstellung eines Konzepts zur Weitergabe von Daten			☐	
	• Protokollierung von Datenabrufen			☒	
	• Erstellung einer Empfängerliste			☐	
	• Auswahl von Dienstleistern nach risikobasiertem Ansatz			☒	
	• Sonstiges: Weitergabe nur nach Weisung des Auftraggebers			☒	
4.4	**Wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt?**	☒	Ja	☐ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):				
	• Verpflichtung zum Schutz von Datenträgern gegen Verlust, Beschädigung etc.			☒	
	• Berechtigungen für Download			☐	
	• Beschränkung des Ausdrucks			☐	
	• Beschränkung der Speicherung / automatische Löschung bei bestimmten Ereignis bzw. Zeitablauf			☐	
	• System zur sicheren Vernichtung von Datenträgern			☒	
	• Sonstiges: Dokumente werden mit dem follow-me prinzip gedruckt			☒	
4.5	**Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von personenbezogenen Daten aufdecken kann?**	☒	Ja	☐ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):				
	• systemseitige Protokollierung			☒	
	• regelmäßiger Auswertungsprozess			☐	
	• Nutzung eines Systems zur Feststellung von auffälligen bzw. verdächtigen Aktivitäten			☐	
	• Sonstiges: _____			☐	
5.	**Maßnahme zur Eingabekontrolle**				
5.1	**Werden Maßnahmen ergriffen, um Einzelheiten (Zeitpunkt, Dauer) eines Zugriffs auf die Daten nachvollziehen zu können?**	☒	Ja	☐ Nein	
	Werden die Login-, Logout-Daten protokolliert?	☒	Ja	☐ Nein	
5.2	**Werden Maßnahmen getroffen, die es nachvollziehbar machen, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden?**	☒	Ja	☐ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):				
	• Protokollierung von Eingabe, Änderungs- bzw. Löschzugriffen			☒	
	• Starten von Reports			☐	
	• Nutzung eines Systems zur Feststellung von auffälligen bzw. verdächtigen Aktivitäten			☒	

Anlage A

Fragenkatalog zur Dokumentation von Prüfungen im Zusammenhang mit Auftragsverarbeitung nach Art. 32 DSGVO

Nr.	Prüfungspunkt			Beurteilung der TOM (wird vom Auftraggeber ausgefüllt)
	• Sonstiges: _____		☐	
6.	**Maßnahmen zur Auftragskontrolle**			
6.1	**Werden Maßnahmen ergriffen, damit die Verarbeitung der personenbezogenen Daten durch die damit betrauten Mitarbeiter nur gemäß den Weisungen des Auftraggebers erfolgen kann?**	☒ Ja	☐ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):			
	• Richtlinien, Arbeitsanweisungen zum Datenschutz / Datensicherheit		☒	
	• Einweisung der mit dem Auftrag betrauten Mitarbeiter		☐	
	• Dokumentation aller Weisungen des Auftraggebers		☒	
	• Zugriffssteuerung (insbes. Differenzierung externe / interne Mitarbeiter)		☒	
	• Verpflichtung der Mitarbeiter auf Datengeheimnis / Datenschutz		☒	
	• Verpflichtung auf besondere Geheimhaltungspflichten (z.B. strafrechtlich geschützte Informationen)		☐	
	• Sonstiges: _____		☐	
6.2	**Werden Maßnahmen getroffen, damit auch ein Unterauftragnehmer keine unbefugten Aktivitäten mit den zur Verfügung gestellten Daten durchführt?**	☒ Ja	☐ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):			
	• Anweisung zur sorgfältigen Auswahl der Unterauftragnehmer		☒	
	• Verbot der Einbindung von Unterauftragnehmern in (unsicheren) Drittstaaten		☒	
	• entsprechende vertragliche Verpflichtung der Unterauftragnehmer		☒	
	• regelmäßige Auditierung der Unterauftragnehmer auf ISO- bzw. TISAX-Grundlage und Dokumentation der Audits		☐	
	• Sonstiges: _____		☐	
6.3	**Werden Maßnahmen getroffen, die am Ende des Aufbewahrungszwecks der personenbezogenen Daten deren Löschung / Sperrung sicherstellen?**	☒ Ja	☐ Nein	
	Sind diese technisch implementiert?	☒ Ja	☐ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):			
	• Arbeitsanweisungen / Unternehmensrichtlinien zu Löschung / Sperrung / Speicherbegrenzung		☒	
	• Technische / automatisierte Löschkonzepte		☒	
	• entsprechende vertragliche Verpflichtung der Unterauftragnehmer		☒	
	• Sonstiges: _____		☐	

Anlage A

Fragenkatalog zur Dokumentation von Prüfungen im Zusammenhang mit Auftragsverarbeitung nach Art. 32 DSGVO

Nr.	Prüfungspunkt			Beurteilung der TOM (wird vom Auftraggeber ausgefüllt)
7.	**Maßnahmen zur Verfügbarkeitskontrolle**			
7.1	**Werden organisatorische und technische Maßnahmen getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten?**	☒ Ja	☐ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):			
	• Backup und Disaster-Recovery mit Notfallplänen		☒	
	• Unternehmensrichtlinien zu Backup-Prozessen		☒	
	• Synchron und/oder asynchrones physikalisches Spiegeln von Festplatten an getrennten Data-Center-Lokationen mit adäquaten Betriebsszenarien (unabhängige Stromversorgung)		☒	
	• Zertifizierung des Major Incident Prozesses durch den TÜV (ISO9k)		☐	
	• Data-breach-Prozess		☒	
	• Incident-response-System		☒	
	• Sonstiges: _____		☐	
7.2	**Wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetische Abstrahlungen etc.) geschützt sind?**	☒ Ja	☐ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):			
	• Rauch- und Brandmelder		☒	
	• Sprinkleranlage		☒	
	• Brandschutztüren		☒	
	• Wasserschutzeinrichtungen		☒	
	• Schirmdämpfung		☒	
	• Notstromversorgung		☒	
	• Standardisiertes Verfahren zur regelmäßigen Überprüfung der Angemessenheit der ergriffenen Schutzmaßnahmen		☒	
	• Hausordnung, die Zutritt nur nach Schulung/Unterweisung oder in Begleitung erlaubt		☒	
	• Sonstiges: _____		☐	
7.3	**Werden Schutzmaßnahmen zur Bekämpfung von Schadprogrammen eingesetzt?**	☒ Ja	☐ Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):			
	• Anti-Malware Software		☒	
	• Virenscanner		☒	
	• Anti-Spy-Programme		☒	
	• Regelmäßige „Full-Scan“ und „Quick-Scans“ der gesamten Rechnerbestände		☒	
	• Firewalls		☒	

Anlage A

Fragenkatalog zur Dokumentation von Prüfungen im Zusammenhang mit Auftragsverarbeitung nach Art. 32 DSGVO

Nr.	Prüfungspunkt					Beurteilung der TOM (wird vom Auftraggeber ausgefüllt)
	• Spam-Filter				☒	
	• IDS-/IPS-Systeme				☐	
	• Sonstiges: Advanced Threat Protection				☒	
	Wird deren Aktualität gewährleistet?	☒	Ja	☐	Nein	
	Bestehen Unternehmensrichtlinien zur Aktualisierung der Programme?	☒	Ja	☐	Nein	
7.4	**Wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden?**	☒	Ja	☐	Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):					
	• Beauftragung von speziellen Entsorgungsunternehmen und deren Überprüfung				☒	
	• ausschließliche Beauftragung von Unternehmen, die den Standard DIN 66399 erfüllen				☐	
	• Sicherstellung durch Arbeitsanweisungen, Richtlinien				☒	
	• Entsorgung nach DIN 66399				☐	
	• Server-Festplatten/SSDs nur mit „No-Return"-Policy (verlassen in keinem Fall mehr eigene Räumlichkeiten)				☐	
	• Sonstiges: _____				☐	
8.	**Maßnahme zur Trennungskontrolle**					
8.1	**Werden Maßnahmen getroffen, um das Trennungsgebot, insbesondere in Bezug auf die Zweckgebundenheit der personenbezogenen Daten, zu gewährleisten?**	☒	Ja	☐	Nein	
	Ergriffene Maßnahmen (Mehrfachauswahl möglich):					
	• Nutzung von differenzierten, kundenspezifischen bzw. mandantenfähigen Systemen				☒	
	• gesonderte Speicherung bei Pseudonymisierung von personenbezogenen Daten				☐	
	• Trennung von Test- und Produktivdaten				☒	
	• detaillierte Zugriffskonzepte				☒	
	• technische Beschränkung des Zugriffs				☒	
	• Verschlüsselung der Datensätze				☒	
	• Arbeitsanweisungen / Unternehmensrichtlinien zur Zweckbindung				☒	
	• Sonstiges: _____				☐	