DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

Brands Consulting
DATENSCHUTZ&BERATUNG

Informationsblatt: „Technische und organisatorische Maßnahmen (TOM) nach Art. 32 Abs. 1 DS-GVO“

Geltungsbereich / Unternehmen:	atrify GmbH
Datenschutzbeauftragter (DSB):	Dr. Herwig Pant

Änderungshistorie			
Ver.	**Datum**	**Geändert von**	**Änderung**
0.1	29.06.2021	Director Internal IT/ CISO	Erstellung der TOM
0.2	13.07.2021	DSB	Prüfung und Kommentierung der Angaben
0.3	19.01.2022	Director Internal IT/ CISO und Legal Counsel	Finalisierung der TOM
0.4	08.08.2022	Legal Counsel	Aktualisierung der Unterschrift wegen Ausscheiden eines Geschäftsführers
0.5	01.09.2022	Director Internal IT/ CISO	Aktualisierung der TOM

Inhaltsverzeichnis

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

1 Vorbemerkung

Gemäß Art. 31 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) sind alle Stellen, die personenbezogene Daten verarbeiten, dazu verpflichtet, technische und organisatorische Maßnahmen (kurz TOM) zu treffen, um die Anforderungen der DS-GVO (vormals des BDSG) zu erfüllen. Der Anwendungsbereich des vorliegenden Informationsblattes „Technische und organisatorische Maßnahmen (TOM) nach Art. 32 Abs. 1 DS-GVO“ ist nicht nur auf den Schutz der sogenannten personenbezogenen Daten ausgerichtet, sondern findet vielmehr freiwillig auch analoge Anwendung auf den Schutz von sonstigen schützenswerten Daten / (Betriebs-)Geheimnissen.

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

2 Ergriffene Maßnahmen

2.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

2.1.1 Zutrittskontrolle

Unter Zutrittskontrolle ist die Verwehrung der räumlichen Annäherung an Datenverarbeitungssysteme durch Unbefugte zu verstehen.

2.1.1.1 Bauliche und technische Maßnahmen (Bürogebäude)

	Ja	Nein
• Einsatz einer Einbruchmeldeanlage:	☒	☐
o Schließkontaktmelder für Türen und Fenster	☐	☒
o Glasbruchsensoren	☐	☒
o Bewegungsmelder / Lichtschranken	☐	☒
o Sonstige Sensorik	☐	☒
• Einsatz sicherer Türen und Fenster (Verbund-Sicherheitsglas)	☒	☐
• Fenster (insbesondere im Erdgeschoss) und Türen sind in Betriebszeiten geschlossen	☒	☐
• Räume werden bei Nichtanwesenheit generell verschlossen	☐	☒
• Mit PC ausgestatteten Räume werden bei Nichtanwesenheit verschlossen	☐	☒
• Fahrzeuge, in denen sich mobile Endgeräte befinden, werden verschlossen	☒	☐
• Sensibler Bereiche des Gebäudes werden videoüberwacht	☒	☐
• Einfriedung des Grundstücks	☐	☒
• Absicherung von Gebäudeschächten	☐	☒
• Einschränkung des ungehinderten Zutritts	☒	☐
• Einsatz von Vereinzelungsmechanismen	☐	☒
• Gegensprechanlage vorhanden	☒	☐
• Sichtkontrolle (Sichtkontakt durch Fenster innerhalb von Türen) vorhanden	☒	☐
• Einsatz eines Chipkarten- / Transponderschließsystems und/oder eines Schließsystems mit Codesperre	☒	☐
• Einsatz biometrischer Zutrittssperren	☐	☒

2.1.1.2 Organisatorische Maßnahmen (Bürogebäude)

	Ja	Nein
• Pförtnerdienst / Empfang / Information als Gebäudezutrittskontrolle ist vorhanden:	☐	☒

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

o Besucher können das atrify Büro nicht unbemerkt betreten	☒	☐
o Besucher können ihr Anliegen diskret schildern (Diskretionszone)	☐	☒
o Mitarbeiter am Empfang können vertrauliche Gespräche führen, ohne dass Unbefugte zuhören	☐	☒
o Unterlagen sind vor dem Zugriff und der Einsicht von Unbefugten geschützt	☒	☐
o Faxgeräte, Drucker und Monitore sind vor der Einsichtnahme durch Dritte geschützt	☒	☐
o Empfang ist deutlich vom Wartebereich getrennt	☐	☒
• Zutritte und Abgänge werden protokolliert	☐	☒
• Zutritts- / Abgangsprotokolle werden regelmäßig ausgewertet	☐	☒
• Für jeden Besucher wird ein eigener Besucherzettel verwendet	☐	☒
• Besucher werden abgeholt und stets begleitet	☒	☐
• Tragepflicht von Berechtigungsausweisen (für Mitarbeiter)	☒	☐
• Tragepflicht von Berechtigungsausweisen (für Besucher)	☒	☐
• Kontrollgängen werden durchgeführt	☒	☐
• Zentrale Schlüsselverwaltung und -vergabe ist vorhanden	☒	☐
• Nicht ausgegebenen Zutrittsmittel werden revisionssicher dokumentiert	☐	☒
• Zutrittsberechtigungen werden klar und eindeutig zugewiesen, einschließlich zu Räumen mit Verteilerkästen	☒	☐
• Zutrittsberechtigungen werden in einem Berechtigungskonzept revisionssicher geregelt und regelmäßig überprüft	☒	☐
• Verlorene Zutrittsmittel (Transponder, Chipkarten) werden unmittelbar gesperrt	☒	☐
• Zutrittsrechte werden zeitlich beschränkt	☒	☐
• Wachpersonal / Gebäudeschutz wird sorgfältig ausgewählt	☒	☐
• Einsatz von Wachpersonal / Gebäudeschutz auch an Wochenenden und nachts	☒	☐
• Reinigungspersonal wird sorgfältig ausgewählt	☒	☐
• Serverräume werden nur unter Aufsicht der berechtigten Mitarbeiter gereinigt	☒	☐
• Kriminalpolizeiliche Beratungsstellen werden zur Gebäudesicherheit konsultiert	☐	☒

2.1.1.3 Bauliche und technische Maßnahmen (Rechenzentrum)

	Ja	***Nein***
• Einsatz einer Einbruchmeldeanlage:	☒	☐
o Schließkontaktmelder für Türen und Fenster	☒	☐
o Glasbruchsensoren	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

o Bewegungsmelder / Lichtschranken	☒	☐
o Sonstige Sensorik	☒	☐
• Einsatz sicherer Türen	☒	☐
• Alle Bereiche des Gebäudes werden videoüberwacht	☒	☐
• Einfriedung des Grundstücks	☒	☐
• Absicherung von Gebäudeschächten	☒	☐
• Einschränkung des ungehinderten Zutritts	☒	☐
• Einsatz von Vereinzelungsmechanismen	☒	☐
• Gegensprechanlage vorhanden	☒	☐
• Sichtkontrolle (Sichtkontakt durch Fenster innerhalb von Türen) vorhanden	☒	☐
• Einsatz eines Chipkarten- / Transponderschließsystems und/oder eines Schließsystems mit Codesperre	☒	☐
• Zugang nur für operative Mitarbeitende, die zuvor über eine Identitätsprüfung autorisiert wurden.	☒	☐

2.1.1.4 Organisatorische Maßnahmen (Rechenzentrum)

	Ja	***Nein***
• Pförtnerdienst / Empfang / Information als Gebäudezutrittskontrolle ist vorhanden:	☒	☐
o Besucher können das Gebäude nicht unbemerkt betreten	☒	☐
• Zutritte und Abgänge werden protokolliert	☒	☐
• Zutritts- / Abgangsprotokolle werden regelmäßig ausgewertet	☒	☐
• Mitarbeitende werden abgeholt und stets durch Sicherheitspersonal begleitet	☒	☐
• Tragepflicht von Berechtigungsausweisen (für Mitarbeiter)	☒	☐
• Kontrollgängen werden durchgeführt	☒	☐
• Zentrale Schlüsselverwaltung und -vergabe ist vorhanden	☒	☐
• Nicht ausgegebenen Zutrittsmittel werden revisionssicher dokumentiert	☒	☐
• Zutrittsberechtigungen werden klar und eindeutig zugewiesen, einschließlich zu Räumen mit Verteilerkästen	☒	☐
• Zutrittsberechtigungen werden in einem Berechtigungskonzept revisionssicher geregelt und regelmäßig überprüft	☒	☐
• Verlorene Zutrittsmittel (Transponder, Chipkarten) werden unmittelbar gesperrt	☒	☐
• Zutrittsrechte werden zeitlich beschränkt	☒	☐
• Wachpersonal / Gebäudeschutz wird sorgfältig ausgewählt	☒	☐
• Einsatz von Wachpersonal / Gebäudeschutz 24/7	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

• Kriminalpolizeilicher Beratungsstellen werden zur Gebäudesicherheit konsultiert	☒	☐

2.1.2 Zugangskontrolle

Unter Zugangskontrolle ist die Verhinderung des Eindringens Unbefugter in Datenverarbeitungssysteme, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verstehen.

2.1.2.1 Technische Maßnahmen

	Ja	***Nein***
• Sicherheitsanforderungen an Informationssysteme / IT-Systeme (inkl. mobiler Endgeräte) werden genau bestimmt und die Systeme entsprechend konfiguriert	☒	☐
• Anmeldung an IT-Systeme erfolgt mit Benutzername und Passwort:	☒	☐
o Verhinderung der Auswahl sehr schwacher Passwörter	☒	☐
o Starke Passwörter auch auf internen Systemen	☒	☐
o 2-Faktor Authentifizierung	☒	☐
• Anmeldung an IT-Systeme erfolgt mit Chipkarten	☐	☒
• Anmeldung an IT-Systeme erfolgt mit biometrischen Merkmalen	☐	☒
• Passwortqualität wird technisch geprüft	☒	☐
• Einsatz von Passwortmanagement	☒	☐
• gescheiterte Anmeldeversuche aktivieren einen Sperrmechanismus	☒	☐
• Gültigkeitsdauer von Zugangsberechtigungen ist begrenzt	☒	☐
• Verschlüsselung von IT-Systeme (inkl. mobile Endgeräte)	☒	☐
• Verschlüsselung von Datenträgern (z. B. USB-Sticks, externe Festplatten)	☒	☐
• Mitnahme dienstlicher Geräte und Datenträger wird geregelt	☒	☐
• Einsatz eines Intrusion Detection Systems	☒	☐
• Passwortgesicherte Bildschirmsperrung	☒	☐
• Zugangsdaten werden bei Fernzugriffen sicher übertragen	☒	☐
• Verlorene Zugangsmittel (Transponder, Chipkarten) werden unmittelbar gesperrt	☒	☐
• Firewall:	☒	☐
o Zentraler / serverseitiger Einsatz einer Hardware- und Software-Firewall, um alle internetfähigen Geräte vom Internet abzuschotten	☒	☐
o Lokaler Einsatz von Software-Firewalls	☒	☐
o Einsatz von Firewalls auch auf Anwendungsebene	☒	☐
o Ordnungsgemäße Konfiguration der Firewall werden regelmäßig geprüft	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

o Monitoring der Firewall, um Zugriffsversuche zu erkennen	☒	☐
• Zentraler / serverseitiger Einsatz von Virenschutzsoftware	☒	☐
• Lokaler Einsatz von Virenschutzsoftware	☒	☐
• Virenschutzsoftware für mobile Endgeräte	☒	☐
• Keine Remotedesktop-Zugänge (RDP-TCP-Ports) offen	☒	☐
• Remotedesktop-Zugänge (RDP-TCP-Ports) über das Internet werden auf ein Mindestmaß beschränkt und bei Fernzugriff auf PCs und laufende Anwendungen abgesichert	☒	☐
• Keine Verwendung von WLAN	☐	☒
• WLAN wird abgesichert durch Verschlüsselung inkl. 802.1X Authentifizierung	☒	☐
• Einsatz von Zwei- oder Mehr-Faktor-Authentisierung:	☒	☐
o Verschlüsselte VPN-Verbindungen werden mit Zwei-Faktor-Authentifizierung abgesichert	☒	☐
o Zwei-Faktor-Absicherung für Administratorzugänge - zumindest für Internetdienste	☒	☐
o Tokens / Chipkarten werden standardmäßig zur Anmeldung an IT-Systemen verwendet	☒	☐
• Einsatz eines Mobile Device Managements (MDM) / Enterprise Mobility Managements (EMM)	☒	☐
• Möglichkeit der Fernlöschung von Smartphones / mobilen Endgeräten	☒	☐
• Anmeldungen an IT-Systemen werden protokolliert	☒	☐
• PC-Gehäuse werden verriegelt	☐	☒
• Drucker und Faxgeräte werden vor unbefugtem Zugang geschützt	☒	☐

2.1.2.2 Organisatorische Maßnahmen

	Ja	***Nein***
• Informationssysteme / IT-Systeme (inkl. mobiler Endgeräte) werden regelmäßig auf die Einhaltung von Sicherheitsanforderungen geprüft	☒	☐
• Einsatz eines Identity- und Access Management (IAM)	☒	☐
• Passwort-Schutz:	☒	☐
o Passwortrichtlinie ist wirksam vorhanden	☒	☐
o Mitarbeiter sind sich bewusst, was starke Passwörter sind und wie mit diesen umzugehen ist. Anforderungen der ISO 27001 werden erfüllt.	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

o Sperrung und Neuvergabe von Passwörtern nach einem Vorfall wird geregelt	☒	☐
• IT-Sicherheitsrichtlinie wird wirksam umgesetzt	☒	☐
• Telearbeit / Mobile Office / Home Office wird geregelt	☒	☐
• Zugangsberechtigungen werden klar und eindeutig zugewiesen	☒	☐
• Zugangsberechtigungen und ihre Gültigkeitsdauer werden in einem Berechtigungskonzept revisionssicher geregelt und regelmäßig überprüft	☒	☐
• Log-Dateien werden regelmäßig ausgewertet, um Missbrauch von Zugangsberechtigungen zu identifizieren	☒	☐
• Elektronische Zugangsmittel (Transponder / Chipkarte) werden zentrale verwaltet und vergeben	☒	☐
• Mitarbeiter sind angewiesen bei PC-Abwesenheit Bildschirme zu sperren	☒	☐
• Bildschirme sind für Dritte nicht einsehbar	☒	☐
• Richtlinie für die Nutzung betrieblicher DV-Geräte / IT-Systeme ist wirksam vorhanden	☒	☐
• Drucker, Kopierern und Faxgeräte werden an geeigneter Stelle aufgestellt	☒	☐
• Mobiler Endgeräte werden auf geeignete Weise aufbewahrt	☒	☐
• Firewall:	☒	☐
o Einsatz von qualifiziertem Personal / Dienstleister zur Konfiguration der Firewall	☒	☐

2.1.3 Zugriffskontrolle

Die Zugriffskontrolle stellt sicher, dass ausschließlich berichtigte Benutzer von Datenverarbeitungssystemen die Daten einsehen, benutzen oder verarbeiten können, die für Ihre spezifische Aufgabenerfüllung erforderlich sind und für die Ihnen eine Berechtigung erteilt wurde.

2.1.3.1 Technische Maßnahmen

	Ja	***Nein***
• Einsatz eines zentralen Verzeichnisdienstes	☒	☐
• Einsatz von Virenschutzsoftware	☒	☐
• Verschlüsselung von Dateien und Ordnern	☐	☒
• Verschlüsselung von Servern und Datenbanken	☐	☒
• Dateien und Ordnern sind passwortgeschützt	☒	☐
• Zugriffsereignissen werden protokolliert, einschließlich gescheiterter Zugriffsversuche	☒	☐
• Abfragemöglichkeiten von Datenbanken werden beschränkt	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

• Zugriffsberechtigte auf notwendigen Ressourcen und Peripheriegeräte im Netzwerk werden beschränkt	☒	☐
• Nicht autorisierte Computer und Endgeräte im Netzwerk werden abgewiesen	☒	☐
• Nicht autorisierte (mobile) Speichermedien werden abgewiesen	☒	☐
• Kundenprofile werden softwareseitig parallel und getrennt voneinander geführt	☒	☐
• Nicht benötigte sicherheitsrelevante Programme und Funktionen (z. B. Apps) werden deinstalliert / deaktiviert	☒	☐
• Home Office:		
o Verschlüsselte VPN-Verbindung i.V.m. einer Zwei-Faktor-Authentisierung	☒	☐
• Fernwartung:		
o Fernwartungszugänge werden nur auf die konkret zu wartenden Systeme begrenzt statt auf komplette Netzwerksegmente, ggf. zusätzlich abgesichert durch sog. "Jumpserver"	☒	☐
o Fernwartungszugriffe werden nur für konkrete Zwecke und zeitlich begrenzt freigeschaltet	☒	☐
o Übertragung von Dateien wird deaktiviert, wenn sie nicht für die Fernwartung erforderlich sind	☒	☐
o Fernwartungszugriffe werden vollständig protokolliert	☒	☐
o Protokolle zur Fernwartung werden regelmäßig ausgewertet	☒	☐
o Verschlüsselung des Transportweges bei Fernzugriffen (VPN / TLS)	☒	☐
o Fernwartungszugriffen werden nach Beendigung eines Dienstleistungsvertrags gesperrt / unterbunden	☒	☐
• Verwaltung:		
o Abschließbare Aktenschränke sind vorhanden und werden bei Dienstschluss verschlossen	☒	☐
o "Alte Akten" werden für Unbefugte unzugreifbar aufbewahrt	☒	☐
o Reinigungspersonal kann nicht auf sensible Daten zugreifen	☒	☐
o Daten werden ausschließlich auf autorisierter Hard- und Software verarbeitet	☒	☐

2.1.3.2 Organisatorische Maßnahmen

	Ja	***Nein***
• Einsatz eines Identity- und Access Management (IAM)	☒	☐
• Berechtigungen für Anwender und Administratoren werden differenziert vergeben	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

• Zugriffsberechtigungen und ihre Gültigkeitsdauer werden in einem Berechtigungskonzept (Profile / Rollen) revisionssicher geregelt, dokumentiert und regelmäßig durch einen unabhängigen Revisor überprüft	☒	☐
• Differenziertes Ordnerkonzept vorhanden zur einheitlichen und nachvollziehbaren Benennung und Abspeicherung	☒	☐
• Speichermedien werden eindeutig gekennzeichnet und sicher aufbewahrt	☒	☐
• Sichere Datenträgeraufbewahrung, -verwaltung und -entsorgung	☒	☐
• Speichermedien und Laufwerke werden nicht wiederverwendet, sondern physisch zerstört	☒	☐
• Speichermedien und Laufwerke werden sicher und vollständig gelöscht	☒	☐
• Vernichtungen von Datenträgern werden mit Vernichtungsbelege dokumentiert	☒	☐
• Aktivitäten des Systemadministrators werden protokolliert	☒	☐
• Clear Desk / Clean Screen / Ordnung am Arbeitsplatz wird wirksam umgesetzt	☒	☐
• Home Office:	☒	☐
o Überblick über Mitarbeiter, denen die Arbeit im Home Office grundsätzlich möglich ist	☒	☐
o Überblick über Mitarbeiter, die aktuell im Home Office arbeiten	☒	☐
o Überblick über datenverarbeitende Geräte der Mitarbeiter im Home Office	☒	☐
o Mitarbeiter im Home Office sind über verschiedene Kommunikationskanäle im Falle eines Vorfalls erreichbar	☒	☐
o Nutzung von privaten Endgeräten in Ausnahmefällen wird geregelt	☒	☐
o Mitarbeiter werden zum Umgang mit Videokonferenz-Tools sensibilisiert	☒	☐
o Mitnahme und Entsorgung sensibler Papierdokumente wird geregelt	☒	☐

2.1.4 Getrennte Verarbeitung (Trennungskontrolle)

Das Ziel der getrennten Verarbeitung ist die Sicherstellung der Zweckbindung der personenbezogenen Daten und die Prävention der Zweckentfremdung.

2.1.4.1 Technische Maßnahmen

	Ja	***Nein***
• Einsatz eines zentralen Verzeichnisdienstes	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

• Datenbankabfragen / freier Abfragesprachen (insbesondere SQL) werden eingeschränkt	☒	☐
• Entwicklungs- und Produktivsystem werden getrennt	☒	☐
• Kundenprofile werden softwareseitig parallel und getrennt voneinander geführt	☒	☐
• Verschlüsselung wird kundenspezifisch durchgeführt	☒	☐
• Kryptografische Schlüssel dienen nur einem Einsatzzweck	☒	☐
• Daten werden logisch oder physikalisch getrennt gespeichert	☐	☒
• Systemumgebungen, auf denen Dienste für Kunden angeboten werden, werden virtuell oder physikalisch getrennt	☐	☒
• Zuordnungstabellen für pseudonymisierte Daten werden von diesen getrennt und auf einem getrennten, abgesicherten System aufbewahrt	☒	☐
• Partitionen für Betriebssysteme und Daten werden getrennt	☐	☒
• Netzwerke werden getrennt (Netzwerksegmentierung):	☒	☐
o Internetserver werden in einer sog. "demilitarisierten Zone" (DMZ) betrieben	☒	☐
o Protokollierung auf Firewall-Ebene, um auch unbefugte Zugriffe zwischen den Netzen festzustellen und zu analysieren	☒	☐
o IT-Administratoren werden bei Verdacht auf unbefugte Verarbeitungen automatisch benachrichtigt	☒	☐

2.1.4.2 Organisatorische Maßnahmen

	Ja	***Nein***
• Datenbanken werden ausführlich dokumentiert	☒	☐
• Fachabteilungen und IT-Abteilung sind nach Funktion / Aufgaben voneinander getrennt	☒	☐
• Neue Datenverarbeitungsverfahren und wesentliche Änderungen von Altverfahren durchlaufen einen formalisierten Freigabeprozess	☒	☐
• Datenbankberechtigungen werden in einem Berechtigungskonzept revisionssicher geregelt und dokumentiert	☒	☐
• Datensätze werden mit Zweckattributen versehen	☒	☐
• Datensätze, die zum selben Zweck verarbeitet werden, werden verschlüsselt	☐	☒
• Netzwerke werden getrennt (Netzwerksegmentierung):	☒	☐
o Prozess zur ordnungsmäßigen Konfiguration der Firewalls und ihrer regelmäßigen Überprüfung wird geregelt	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

2.1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

2.1.5.1 Technische Maßnahmen

	Ja	*Nein*
● Pseudonyme werden in Sekundärsystemen verwendet, die der strategischen Datenanalyse und der Entscheidungshilfe dienen	☒	☐
● Pseudonyme werden bei der Erstellung von Testdaten verwendet	☒	☐
● Pseudonyme werden in Teilprozessen von Geschäftsprozessen verwendet, in denen die Originaldaten nicht erforderlich sind:	☒	☐
o Personenidentifizierenden Daten werden festgelegt, die durch Pseudonymisierung zu ersetzen sind	☐	☒
o Pseudonymisierungsregel werden definiert, ggf. anknüpfend an Personal- oder Kunden-Kennziffern	☐	☒
o Mitarbeiter werden festgelegt, die zur Verwaltung der Pseudonymisierungsverfahren, zur Durchführung der Pseudonymisierung und ggf. der Depseudonymisierung berechtigt sind	☒	☐
o Zulässigen Anlässe für Pseudonymisierungs- und Depseudonymisierungsvorgänge werden festgelegt	☒	☐
o Zuordnungstabellen oder die geheimen Parameter, die in eine algorithmische Pseudonymisierung eingehen, werden zufällig erzeugt	☒	☐
o Zuordnungstabellen bzw. geheimen Parameter werden in einem getrennten und abgesicherten System sowohl gegen unautorisierten Zugriff als auch gegen unautorisierte Nutzung geschützt / aufbewahrt	☒	☐
o Pseudonymisierenden Daten werden von den zu ersetzenden, personenidentifizierenden Daten getrennt	☒	☐

2.1.5.2 Organisatorische Maßnahmen

	Ja	*Nein*
● Personendaten werden im Falle einer Weitergabe anonymisiert / pseudonymisiert	☒	☐
● Personendaten werden nach Ablauf der Aufbewahrungsfrist anonymisiert / pseudonymisiert	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

2.2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.2.1 Weitergabekontrolle

Unter der Weitergabekontrolle ist die Kontrolle von Übermittlung und Transport personenbezogener Daten sowie die Kontrolle der Speicherung der Daten auf Datenträger zu verstehen.

2.2.1.1 Technische Maßnahmen

	Ja	*Nein*
• Verschlüsselung der VPN-Verbindung	☒	☐
• Daten werden per SFTP / HTTPS bereitgestellt	☒	☐
• Verschlüsselung von Datenträgern	☒	☐
• Verschlüsselung mobiler Endgeräte	☒	☐
• Verschlüsselung von Datenbanken	☒	☐
• Verschlüsselung von Daten	☒	☐
• Geeignete kryptografische Verfahren mit in der Fachwelt etablierten Algorithmen werden ausgewählt	☒	☐
• Einsatz von geeignetem Schlüsselmanagement für kryptografische Schlüssel mit geeigneten Schlüsselgeneratoren in einer sicheren Umgebung	☒	☐
• Einsatz von Passwortmanagement	☒	☐
• Authentizität der übermittelten Daten wird durch Signaturverfahren sichergestellt	☒	☐
• Personenbezogene Daten werden anonymisiert oder pseudonymisiert weitegegeben	☒	☐
• Veränderungen / Manipulationen übertragener Daten nachträglich feststellbar	☒	☐
• Datenträger werden auf Malware-Befall überprüft	☒	☐
• Speichermedien und Laufwerke werden vor der Wiederverwendung sicher und rückstandsfrei gelöscht bzw. physische zerstört (z. B. Shreddern):	☒	☐
o Löschverfahren werden festgelegt	☒	☐
• Einsatz eines Mobile Device Managements (MDM) / Enterprise Mobility Management (EMM)	☒	☐
• Zugriffe, Übermittlungen und Abrufe werden geloggt / protokolliert	☒	☐
• Druckerwarteschlange wird nur nach persönlicher Anmeldung am Drucker abgearbeitet	☒	☐
• Datenspeicher von Druckern / Kopierern / Multifunktionsgeräten werden vor der Entsorgung sicher und rückstandsfrei gelöscht oder physisch zerstört	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

● Einsatz von Aktenvernichtern (Sicherheitsstufe P-3 / P-4 / P-5, cross-cut)	☒	☐
● E-Mail-Sicherheit:	☒	☐
o Verschlüsselung des Transportweges von E-Mails (SSL / TLS)	☒	☐
o Ende-zu-Ende-Verschlüsselung von E-Mails (E2EE)	☐	☒
o E-Mails werden im "Nur-Text-Format" angezeigt	☐	☒
o Links in E-Mails werden vor Aufruf der E-Mails geprüft	☒	☐
o Eingehende E-Mails werden auf Malware geprüft	☒	☐
o Gefährliche Anhänge werden blockiert	☒	☐
o Pauschaler Weiterleitungsregelungen bei Cloud-Hosting wird deaktiviert	☒	☐

2.2.1.2 Organisatorische Maßnahmen

	Ja	***Nein***
● Protokollierte Übermittlungs-, Zugriffs- und Abrufdaten werden durch einen unabhängigen Revisor regelmäßige / anlassbezogene ausgewertet	☒	☐
● Maßnahmen sind festgelegt, wenn Schwächen in Schlüssellängen und Verschlüsselungsverfahren oder -produkten entdeckt werden	☒	☐
● Mit Sicherheitskopien / Backups wird sorgfältig und reguliert umgegangen	☒	☐
● Datenträgerverzeichnis wird geführt	☐	☒
● E-Mails werden nicht an private E-Mail-Accounts von Mitarbeitern weitergeleitet	☒	☐
● Daten werden ausschließlich auf autorisierter Hard- und Software verarbeitet	☒	☐
● Einsatz von mobilen Datenträgern wird geregelt	☒	☐
● E-Mail-Sicherheit:	☒	☐
o Mitarbeiter werden über die Gefahren verschlüsselter E-Mail-Anhänge sensibilisiert	☒	☐
o Mitarbeiter werden mind. jährlich über aktuelle Angriffsvarianten informiert	☒	☐
o Mitarbeiter werden sensibilisiert, gefälschte E-Mails zu erkennen	☒	☐
● Beauftragung zuverlässiger Transportunternehmen:	☒	☐
o Externe Dienstleister mit möglichem Zugriff auf Daten werden auf die Wahrung des Datenschutzes verpflichtet	☒	☐
o Transportwege werden dokumentiert	☒	☐
o Speicherort und Datenträger werden dokumentiert	☒	☐
o Dauer der Überlassung wird dokumentiert	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

	o Persönliche Informationen werden aus den Metadaten von Dateien entfernt	☒	☐
	o Mitnahme von Behältnissen aus geschützten Bereichen wird protokolliert	☒	☐
	o Taschen werden stichprobenartig kontrolliert	☐	☒
	o Geeignete Verpackung von Datenträgern, die eine Beschädigung möglichst ausschließt	☒	☐
	o Nachweisverfahren über den Versand und den Empfang datentragender Sendungen wird umgesetzt	☒	☐
	o Sicherungskopien von Datenträgern werden angelegt, die transportiert werden sollen	☒	☐
	o Berechtigungen für Versand, Weitergabe und Empfang von Datenträgern werden klar und eindeutig zugewiesen	☒	☐
	o Datenträgern werden bezüglich Absender und Empfänger eindeutig gekennzeichnet	☒	☐
	o Transportbehälter werden klar und eindeutig beschriftet, um Verwechslungen zu vermeiden	☒	☐
	o Versand wird durch sorgfältig ausgewähltes und vertrauenswürdiges Personal durchgeführt	☒	☐
	o Transportart und eingesetzter Transportdienst werden in Abhängigkeit von der Sensibilität der transportierten Daten bestimmt	☒	☐
	o Transportwege und Transportmittel werden vorgegeben	☒	☐
	o Einsatz verschließbarer / verplombter / versiegelter und stabiler Transportbehälter	☒	☐
	o Kenntnisnahme des Transporteurs über die transportierten Daten wird vermieden	☒	☐
	o Bei regelmäßigem Datenträgeraustausch mit einem Empfänger werden die gleichen Datenträger verwendet	☒	☐
	o Datenträger werden vor dem Transport bezüglich der Nicht-Rekonstruierbarkeit gelöschter Datenbestände geprüft, die nicht übermittelt werden sollen	☒	☐
	o Datenträgereingangs- bzw. -ausgangsbuch wird geführt	☒	☐

2.2.2 Eingabekontrolle

Unter der Eingabekontrolle ist die nachträgliche Überprüfung zu verstehen „wer – wann – welche Personendaten – in welcher Weise - eingesehen, eingegeben, verändert, übermittelt oder gelöscht hat“.

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

2.2.2.1 Technische Maßnahmen

	Ja	*Nein*
• Einsatz eines Log Management (Protokollierungs- und Protokollauswertungssystem)	☒	☐
• Eingaben, Änderungen und Löschungen von Daten durch individuelle Benutzernamen werden überwacht und protokolliert	☒	☐
• Änderungen an Anwendungen und IT-Systemen werden überwacht und protokolliert	☒	☐
• Eingabe in Logfiles oder Tabellen werden revisionssicher und automatisch protokolliert	☒	☐
• Aktivitäten der (System-)Administratoren werden protokolliert	☒	☐
• Veränderungen / Manipulationen gespeicherter Daten sind nachträglich feststellbar (z. B. Signaturverfahren, Prüfsummen-Verfahren)	☒	☐
• Log-Dateien / Protokolle werden systemseitig sicher abgelegt	☒	☐

2.2.2.2 Organisatorische Maßnahmen

	Ja	*Nein*
• Protokollierungskonzept wird wirksam umgesetzt	☒	☐
• Log-Dateien werden durch einen Systemadministrator / unabhängigen Revisor regelmäßige / anlassbezogene, manuelle / automatisierte ausgewertet	☒	☐
• Log-Dateien werden nach dem Vier-Augen-Prinzip ausgewertet	☐	☒
• Einsatz eines Identity- und Access Management (IAM)	☒	☐
• Berechtigungen für Anwender und Administratoren werden differenziert vergeben	☒	☐
• Zugriffsberechtigungen und ihre Gültigkeitsdauer werden in einem Berechtigungskonzept (Profile / Rollen) revisionssicher geregelt, dokumentiert und regelmäßig durch einen unabhängigen Revisor überprüft	☒	☐
• Übersicht der zu verarbeitenden personenbezogenen Daten ist vorhanden	☒	☐
• Übersicht der Software ist vorhanden, mittels derer Daten eingegeben, geändert und gelöscht werden	☒	☐
• Datenfelder werden bei Sinnhaftigkeit auf Plausibilität geprüft	☒	☐
• Log-Dateien / Protokolle werden fristgerecht gelöscht	☒	☐
• Löschkonzept wird wirksam umgesetzt	☒	☐
• Löschroutinen mit klaren Zuständigkeiten für manuelle und digitale Daten werden wirksam umgesetzt	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

2.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

2.3.1 Verfügbarkeitskontrolle und Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Unter der Verfügbarkeitskontrolle ist der Schutz vor Datenverlust und Zerstörung sowie die gleichzeitige Möglichkeit der Wiederherstellung bei Bedarf zu verstehen.

2.3.1.1 Technische Maßnahmen

	Ja	*Nein*
• Firewall:	☒	☐
o Zentraler / serverseitiger Einsatz einer Hardware- und Software-Firewall, um alle internetfähigen Geräte vom Internet abzuschotten	☒	☐
o Lokaler Einsatz von Software-Firewalls	☒	☐
o Einsatz von Firewalls auch auf Anwendungsebene	☒	☐
o Ordnungsgemäße Konfiguration der Firewall werden regelmäßig geprüft	☒	☐
o Monitoring der Firewall, um Zugriffsversuche zu erkennen	☒	☐
• Zentraler / serverseitiger Einsatz von Virenschutzsoftware	☒	☐
• Lokaler Einsatz von Virenschutzsoftware	☒	☐
• Virenschutzsoftware für mobile Endgeräte	☒	☐
• Keine Remotedesktop-Zugänge (RDP-TCP-Ports) offen	☒	☐
• Remotedesktop-Zugänge (RDP-TCP-Ports) über das Internet werden auf ein Mindestmaß beschränkt und bei Fernzugriff auf PCs und laufende Anwendungen abgesichert	☒	☐
• Einsatz von Web-Filtern	☒	☐
• Sicherheitsrelevanten Netzwerke, IT-Systeme, Anwendungen und anderer IT-Komponenten werden regelmäßig gewartet und aktualisiert	☒	☐
• Neue Software wird durch die IT-Abteilung kontrolliert installiert und konfiguriert	☒	☐
• Störungen können durch Fernanzeige identifiziert werden	☒	☐
• IT-Infrastruktur (Netzwerk, Speicher, Server, Clients) ist redundant vorhanden	☒	☐
• Festplattenspiegelung (RAID-System) wird umgesetzt	☒	☐
• Fernwartung wird abgesichert umgesetzt	☒	☐
• Feuer- und Rauchmeldeanlagen vorhanden	☒	☐
• Datenschutztresor vorhanden	☒	☐
• Partitionen für Betriebssysteme und Daten werden getrennt	☐	☒

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

• Ausreichende Schutzmaßnahmen im Serverraum:	☒	☐
o Lokale unterbrechungsfreie Stromversorgung (USV) und Notstromversorgung vorhanden	☒	☐
o Überspannungsschutz vorhanden	☒	☐
o Serverraum befindet sich über der Wassergrenze (relevant insbesondere für Hochwassergebiete)	☒	☐
o Keine sanitären Anschlüsse im oder oberhalb des Serverraums	☒	☐
o Videoüberwachung vorhanden	☒	☐
o Bei unautorisiertem Zutritt wird ein Alarm ausgelöst	☒	☐
o Klimaanlage vorhanden	☒	☐
o Temperatur und Feuchtigkeit wird überwacht	☒	☐
o Brandschutzmaßnahmen (u.a. Feuerlöscher) werden wirksam umgesetzt	☒	☐
o Schutz vor Wasser- und Feuchtigkeitsschäden vorhanden	☒	☐
• Patch-Management / Update-Management wird betrieben:	☒	☐
o Ausschließlicher Einsatz von Desktop-Betriebssystemen, für die weiterhin Sicherheitsupdates zur Verfügung gestellt werden	☒	☐
o Desktop-Betriebssysteme werden automatisch aktualisiert	☒	☐
• Malware-Schutz:	☒	☐
o Endpoint Data Protection / Endpoint Security wird umgesetzt	☒	☐
o Antivirensignaturen werden täglich automatisch aktualisiert	☒	☐
o Alarmmeldungen werden durch die IT-Abteilung zentral erfasst	☒	☐
o Einsatz von Antivirenlösung mit als "hoch" konfigurierter lokaler heuristisher Erkennung	☒	☐
o Einsatz von Sandboxing-Verfahren oder Advanced Endpoint Detection and Response (EDR) nur unter strenger Berücksichtigung datenschutzrechtlicher Vorschriften	☒	☐
• Ransomware-Schutz:	☒	☐
o Auf Makros in Office-Dokumenten wird im Betriebsalltag weitestgehend verzichtet	☒	☐
o Ausschließlich signierte Microsoft Office-Makros werden zugelassen	☒	☐
o Automatischen Ausführung von heruntergeladenen Programmen wird verhindert	☒	☐
o Windows Script Hosts (WSH) auf Clients wird deaktiviert	☒	☐
o Prüfung, ob die Einschränkung von Powershell-Skripten mit dem "ConstrainedLanguageMode" auf Windows-Clients sinnvoll durchführbar ist	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

o Einsatz eines Web-Proxy-Servers mit (tages-)aktuellen Sperrlisten von Schadcode-Download-Seite (IOCs)	☐	☒
• Backup:	☒	☐
o Backupmedien werden geeignet und physisch sicher aufbewahrt	☒	☐
o Sicherheitskopien / Backups von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien und nicht vernetzten Systemen werden regelmäßig angefertigt	☒	☐
o Sicherheitskopien / Backups werden verschlüsselt	☒	☐

2.3.1.2 Organisatorische Maßnahmen

	Ja	***Nein***
• Zentrale und einheitliche Beschaffungsstrategie für Hard- und Software wird umgesetzt	☒	☐
• Passwörter werden geeignet und sicher hinterlegt	☒	☐
• Fremdsoftware wird vor der Einführung geprüft	☒	☐
• Netzwerken, IT-Systemen, Anwendungen, andere IT-Komponenten und Verfahren zur Gewährleistung eines personenunabhängigen IT-Betriebs werden dokumentiert	☒	☐
• Dienstanweisungen und Sicherheitsrichtlinien für die Datensicherung werden wirksam umgesetzt	☒	☐
• Notfallkonzept:	☒	☐
o Notfallkonzept wird wirksam umgesetzt und ist für die relevante Personengruppen in Papierform greifbar	☒	☐
o Aktualität des Notfallkonzepts wird regelmäßig geprüft	☒	☐
o Wiederaufnahme des Betriebs wird durch verschiedene bereits im Voraus geplante und getestete Ablaufstufen im Notfallplan ermöglicht	☒	☐
o Wiederanlaufszenarien werden regelmäßig geprobt	☒	☐
o Zuständige Behörden und Meldeverpflichtungen werden im Notfallplan angegeben	☒	☐
o Notfall-Reserve-Hardware vorhanden, um Ausfälle zu kompensieren	☒	☐
o Ausweichräume und -infrastrukturen für den Katastrophenfall vorhanden	☒	☐
o Rascher Aufbau einer Ausweichinfrastruktur ist möglich	☒	☐
o Gut strukturierter und aktueller Netzplan vorhanden	☒	☐
o Prozess zur Erkennung und Meldung von Sicherheits- und Datenvorfällen vorhanden	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

o Mitarbeiter sind über Ansprechpartner bei Sicherheitsvorfällen informiert	☒	☐
o Erreichbarkeit der Ansprechpartner bei Sicherheitsvorfällen ist gewährleistet	☒	☐
o Zentrale Administrationszugangsdaten und Zugangsmöglichkeiten werden für den Notfall sicher aufbewahrt	☒	☐
● IT-Administratoren:	☒	☐
o Auch Administratoren verwenden nicht-privilegierte Standardkonten für die sonstige Arbeit außerhalb der administrativen Tätigkeit	☒	☐
o Regelung wird wirksam umgesetzt, dass Administratoren nicht mit Administrator-Rechten im Internet surfen oder E-Mails lesen / versenden	☒	☐
o Sehr starke Passwörter für lokale Admin-Konten vorhanden	☒	☐
o Konsequenter Einsatz von Verfahren zur Zwei-Faktor-Authentisierung bei Anwendungen, soweit möglich	☒	☐
o Gesamter Betrieb ist nicht von einzelnen Administratoren abhängig	☒	☐
o Ausreichende Personalressourcen in der IT-Abteilunge vorhanden	☒	☐
o Vertretungsregelungen für Administratoren vorhanden	☒	☐
o Beim Ausfall von mehreren Administratoren wird gewährleistet, dass die Arbeitsfähigkeit des Betriebs aufrechterhalten werden kann	☒	☐
o Schnelle und geregelte Erreichbarkeit der Administratoren wird gewährleistet	☒	☐
● Patch-Management / Update-Management wird betrieben:	☒	☐
o Patch-Management-Konzept mit Update-Plan wird wirksam umgesetzt	☒	☐
o Informationen zu Sicherheitslücken der eingesetzten Hard- und Software werden regelmäßig ausgewertet	☒	☐
o Einspielen von Sicherheitsupdates der Server wird zeitnah geregelt	☒	☐
o Geregelter / automatischer Prozess für Browser-Updates vorhanden	☒	☐
o Geregelter / automatischer Prozess für Updates von Basiskomponenten (z. B. Java, PDF-Reader) vorhanden	☒	☐
● Malware-Schutz:	☒	☐
o Interne Anweisung an Mitarbeiter zum Umgang mit Alarmmeldungen wird wirksam umgesetzt	☒	☐
o Ablaufplan bei Malware-Befall ist in der IT-Abteilung vorhanden	☒	☐
● Ransomware-Schutz:	☒	☐
o Mitarbeiter werden mind. jährlich über Risiken der Makro-Aktivierung informiert	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

o Notfallplan für den Umgang mit Verschlüsselungstrojanern ist auf Papier vorhanden	☒	☐
o Backup- und Recovery-Strategie stellt sicher, dass Backups durch Ransomware nicht verschlüsselt werden können	☒	☐
• Datensicherungskonzept wird wirksam umgesetzt	☒	☐
• Sicherheitskopien / Backups werden getrennt aufbewahrt	☒	☐
• Sicherheitskopien / Backups werden an einem sicheren Ort außerhalb des Serverraums aufbewahrt	☒	☐
• Backup:	☒	☐
o Sicherheitskopien / Backups werden nach der 3-2-1 Regel durchgeführt	☒	☐
o Backup- und Wiederanlaufkonzept vorhanden	☒	☐
o Regelmäßige Tests, ob alle relevanten Daten im Backup-Prozess enthalten sind, die Wiederherstellbarkeit funktioniert und die Ergebnisse protokolliert werden	☒	☐
o Mindestens ein Backup-System ist durch Ransomware nicht verschlüsselbar	☒	☐

2.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

2.4.1 Auftragskontrolle

Unter Auftragskontrolle ist die Verarbeitung personenbezogener Daten im Auftrag (sog. Auftragsverarbeitung kurz AV), durch einen Dritten und nach Weisung des Auftraggebers, zu verstehen (Art. 28 DSGVO). Die Verantwortlichkeit bleibt beim Auftraggeber. Im Falle eines Datentransfers in ein Drittland sind zusätzliche Bestimmungen zu erfüllen, um ein gleichbleibend angemessenes Schutzniveau zu gewährleisten (Art. 44-49 DSGVO).

	Ja	***Nein***
• Eindeutige Vertragsgestaltung nach Maßgabe des Art. 28 DSGVO vorhanden	☒	☐
• Aufträge werden formalisiert erteilt (Auftragsformular)	☒	☐
• Ort der Verarbeitung wird festgelegt	☒	☐
• Prüfung, ob eine Auftragsverarbeitung zulässig ist	☒	☐
• Verträge und Vereinbarungen werden schriftlich abgeschlossen	☒	☐
• TOM des Auftragnehmers werden vor Beginn der Verarbeitung geprüft	☒	☐
• Kompetenzen und Pflichten zwischen Auftraggeber und Auftragnehmer werden klar abgegrenzt	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

• Auftragnehmer und Unterauftragnehmer haben einen ordnungsgemäßen Datenschutzbeauftragten bestellt	☒	☐
• Auftragnehmer werden nach dem Niveau ihrer technischen und organisatorischen Maßnahmen sorgfältig ausgewählt	☒	☐
• Auftragnehmer werden fortlaufend geprüft	☒	☐
• Sicherheitsmaßnahmen werden festgelegt, die der Auftragnehmer umzusetzen hat	☒	☐
• Berichtspflichten werden festgelegt	☒	☐
• Verhaltensregeln bei Störungen werden festgelegt	☒	☐
• Verarbeitungen werden nur nach schriftlich dokumentierter Weisung durchgeführt	☒	☐
• Ordnungsgemäße Vertragserfüllung beim Auftragnehmer wird kontrolliert (Datenschutz-Audit)	☒	☐
• Auftragnehmer unterstützen bei der Beantwortung der Anträge von Betroffenen	☒	☐
• Auftragnehmer unterstützen bei mitzuteilenden Verstößen	☒	☐
• Die vollständige Löschung / Rückgabe der Daten nach Beendigung des Auftrags wird sichergestellt	☒	☐
• Standardisierter AV-Prüfungsprozess für externe Datenverarbeitung wird umgesetzt	☒	☐
• Auftragnehmer unterstützen hinsichtlich der Sicherheit der Verarbeitung	☒	☐
• Auftragnehmer unterstützen bei Datenschutz-Folgenabschätzung und vorheriger Konsultation der Aufsichtsbehörde	☒	☐
• Mitteilungspflichten der Auftragnehmer bei Maßnahmen der Aufsichtsbehörde oder bei Ermittlungen werden festgelegt	☒	☐
• Wirksame Möglichkeiten zur Kontrolle werden im Rahmen des Vertrages eingeräumt, ebenso Duldungs- und Mitwirkungspflichten des Auftragnehmers	☒	☐
• Sanktionen bei Vertragsverletzung werden festgelegt	☐	☒
• Modalitäten von Übergabe und Transport der Daten werden festgelegt	☐	☒
• Sicherheitsklasse der im Auftrag zu verarbeitenden Daten wird definiert	☐	☒
• Unterauftragsverhältnisse werden definiert	☒	☐
• Unterauftragnehmer werden verpflichtet, die Datenschutzpflichten des Auftragnehmers einzuhalten	☒	☐
• Haftung des Auftragnehmers für die Einhaltung der Datenschutzpflichten des Unterauftragnehmers wird geregelt	☒	☐
• Mitteilungspflichten der Auftragnehmer hinsichtlich beabsichtigter Änderungen werden festgelegt, wenn Änderungen allgemein genehmigt sind	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

• Einspruchsrecht des Auftraggebers für geplante Unterauftragnehmer wird festgelegt, wenn diese allgemeine genehmigt sind	☒	☐
• Mitarbeiter von Auftragnehmern sind auf die Vertraulichkeit und verpflichtet	☒	☐
• Standardvertragsklauseln mit Empfängern außerhalb der EU/EWR werden abgeschlossen	☒	☐

2.4.2 Datenschutz-Management

Unter Datenschutz-Management (DSM) ist ein kontrollierter und gesteuerter Prozess über den Lebenszyklus von Verarbeitungstätigkeiten zu verstehen. Es zielt darauf gesetzlichen und betrieblichen Anforderungen des Datenschutzes umzusetzen.

2.4.2.1 Technische Maßnahmen

	Ja	***Nein***
• Einsatz von Software-Lösungen zum Datenschutz-Management	☒	☐

2.4.2.2 Organisatorische Maßnahmen

	Ja	***Nein***
• Verbindliches Sicherheitsleitlinien vorhanden	☒	☐
• (IT-)Sicherheitskonzept wird wirksam umgesetzt und regelmäßig geprüft	☒	☐
• Schwachstellenanalysen in der IT werden regelmäßig durchgeführt	☒	☐
• Richtlinie zur Nutzung von E-Mail und Internet wird wirksam umgesetzt	☒	☐
• Social Media Richtlinie wird wirksam umgesetzt	☒	☐
• Richtlinie zur Videoüberwachung wird wirksam umgesetzt	☒	☐
• Richtlinie zur Zeiterfassung wird wirksam umgesetzt	☐	☒
• Richtlinie über Ortungssysteme in Flottenfahrzeugen wird wirksam umgesetzt	☒	☐
• Datenschutz-Richtlinie / Datenschutzkonzept wird wirksam umgesetzt	☒	☐
• Verantwortlichkeiten für das Informationssicherheitsmanagement werden definiert	☒	☐
• Sicherheitsfaktor Mensch:	☒	☐
o Mitarbeiter werde mindestens jährlich geschult und sensibilisiert	☒	☐
o Mitarbeiter werden bezüglich aktueller und häufiger Cyberangriffe sensibilisiert	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

o Neuer Mitarbeiter werden konsequent zum fachgerechten Umgang mit den IT-Komponenten und zum Verhalten bei Social-Engineering-Angriffen eingewiesen	☒	☐
o Neuer Mitarbeiter werden bezüglich IT-Risiken vor der Aufnahme der Datenverarbeitung sensibilisiert (auch bei Aushilfskräften)	☒	☐
o Abläufe von Social-Engineering-Angriffen werden Mitarbeitern zur Sensibilisierung dargestellt	☒	☐
o Mitarbeiter sind über Meldewege und Zuständigkeiten informiert	☒	☐
• Verfahren zum Ein- / Austritt wird vorhanden	☒	☐
• Datenträgerverzeichnis wird geführt	☒	☐
• Mitarbeiter werden auf die Vertraulichkeit verpflichtet	☒	☐
• Clear Desk und Clear Screen Richtlinie werden wirksam umgesetzt	☒	☐
• Informationspflichten werden umgesetzt	☒	☐
• Formaler Prozess zur Bearbeitung von Betroffenenanfragen vorhanden	☒	☐
• Besucherrichtlinie wird wirksam umgesetzt	☒	☐
• Whistleblowing-Richtlinie / Hinweisgebersystem wird wirksam umgesetzt	☐	☒
• Verzeichnis von Verarbeitungstätigkeiten für Verantwortliche vorhanden und mind. jährlich geprüft	☒	☐
• Verzeichnis von Verarbeitungstätigkeiten für Auftragsverarbeiter vorhanden und mind. jährlich geprüft	☒	☐
• Richtlinie zur Fernwartung durch eigene Mitarbeiter wird wirksam umgesetzt	☒	☐
• Richtlinie zur Telearbeit / Mobile Office / Home Office wird wirksam umgesetzt	☒	☐
• Richtlinie zur Überlassung und Nutzung mobiler Endgeräte wird wirksam umgesetzt	☒	☐
• Risikoanalysen werden durchgeführt und ein Schutzstufenkonzept wirksam umgesetzt	☒	☐
• Protokollierungskonzept wird wirksam umgesetzt	☒	☐
• Meldeprozess für neu auftretende Schwachstellen und andere Risikofaktoren ist vorhanden und Risikoanalysen und -bewertungen werden ggf. überarbeitet	☒	☐
• Festgelegten Prozesse und Vorgaben zur Konfiguration und Bedienung der IT-Systeme werden eingehalten und die Einhaltung durch den DSB (und der IT-Revision) geprüft	☒	☐
• Externer Prüfungen (Audits) werden durchgeführt	☒	☐
• Zertifizierungen vorhanden (ISO 27001)	☒	☐
• IT-Sicherheitsbeauftragter / Informationssicherheitsbeauftragter (ISB) oder eines Verantwortlichen für die Informationssicherheit mit klar geregelter Kompetenzzuweisung wurde bestellt	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

• Datenschutzbeauftragten wurde bestellt	☒	☐
o DSB wird bei Sicherheitsfragen konsequent eingebunden	☒	☐
o Audits werden nach Art. 32 DSGVO zur Sicherheit der Verarbeitung regelmäßig durch den DSB durchgeführt	☒	☐
o Die Zusammenarbeit des DSB mit dem ISB wird durch die Unternehmensleitung unterstützt	☒	☐
• Datenschutz-Folgenabschätzung werden vom Verantwortlichen durchgeführt und der Rat des DSB eingeholt	☒	☐
• Technischen und organisatorischen Maßnahmen werden regelmäßig und bei wesentlichen Änderungen geprüft	☒	☐
• Geeigneter Garantien bei Drittlandübermittlung werden dokumentiert	☒	☐

2.4.3 Incident-Response-Management (Vorfallreaktionspläne)

Unter Incident-Response-Management ist die Dokumentation aller schriftlichen Anweisungen im Zusammenhang mit Sicherheitsvorfällen zu verstehen. Mit dessen Hilfe sollen Sicherheitsvorfälle entdeckt sowie auf angemessene und vordefinierte Weise auf sie reagiert werden, um Schäden einzugrenzen.

2.4.3.1 Technische Maßnahmen

	Ja	***Nein***
• Einsatz von Firewalls	☒	☐
• Einsatz von Virenschutzsoftware	☒	☐
• Einsatz von Spamfiltern	☒	☐
• Einsatz eines Online-Ticket-Systems	☒	☐
• Einsatz eines Intrusion Detection System (IDS)	☒	☐
• Einsatz eines Intrusion Prevention System (IPS)	☒	☐
• Einsatz einer Service Hotline / Helpdesk	☒	☐
• Sperrung und Neuvergabe von Passwörtern nach einem Vorfall wird geregelt	☒	☐

2.4.3.2 Organisatorische Maßnahmen

	Ja	***Nein***
• Prozess zur Erkennung und Meldung von Sicherheits- und Datenvorfällen vorhanden	☒	☐
• DSB und ISB werden in Sicherheits- und Datenvorfälle eingebunden	☒	☐
• Sicherheits- und Datenvorfällen werden dokumentiert	☒	☐
• Penetrationstests werden regelmäßig durchgeführt	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

• Betroffene können auf einfache Weise ihr Widerrufsrecht wahrnehmen	☒	☐
• Notfallkonzept wird wirksam umgesetzt	☒	☐
• Notfallübungen werden regelmäßig durchgeführt	☒	☐
• Notfallmanagement wird in Geschäftsprozesse integriert	☒	☐

2.4.4 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Unter datenschutzfreundliche Voreinstellungen sind technische und organisatorische Maßnahmen zu verstehen, die darauf ausgelegt sind, die Grundsätze des Datenschutzes wirksam umzusetzen und zu garantieren, dass die gesetzlichen Anforderungen eingehalten und die Betroffenenrechte geschützt werden.

	Ja	***Nein***
• Hard- und Software wird nach dem Privacy-by-Design-Ansatz entwickelt:	☒	☐
o Dokumentation der Entwicklung zur Ermöglichung von Audits	☒	☐
o Feinjustierung von Benutzerrechten wird ermöglicht	☒	☐
o Verschlüsselung wird ermöglicht	☒	☐
o Software unterstützt Kontrollmaßnahmen durch DSB / Auditor (Lesezugriff auf Daten und Protokolle)	☒	☐
o Datenlöschung / Profillöschungen werden ermöglicht und Löschroutinen unterstützt	☒	☐
o Datenübertragbarkeit wird ermöglicht	☒	☐
o Checkboxen sind standardmäßig deaktiviert	☒	☐
o Kontextbezogene Erläuterung von Formularfeldern, einschließlich Freitextfelder	☒	☐
o Verzicht auf Freitextfelder	☐	☒
• Einsatz von Hard- und Software nach dem Privacy-by-Default-Ansatz:	☒	☐
o Pflichtfeldern werden auf das erforderliche Maß begrenzt	☒	☐
o Bei Selbsteingaben in Formularen werden Felder kontextbezogen erläutert, einschließlich Freitextfelder	☒	☐
o Auf Freitextfelder wird verzichtet	☐	☒
o Benutzerrechte werden auf das erforderliche Maß begrenzt	☒	☐
o Kein automatisches Teilen von Inhalten bei Social-Media-fähigen Anwendungen	☒	☐
o Pflegbare Informationsseiten erlauben Transparenz	☒	☐

DocuSign Envelope ID: 595A505D-0FBA-4B17-95BB-E05D90F4A969

3 Sie haben eine Rückfrage zum Datenschutz?

3.1 Fragen Sie atrify

Im Hause atrify steht Ihnen Frau Rebecca Mannek, Legal Counsel, für Fragen zum Datenschutz wie folgt zur Verfügung:

rmannek@atrify.com

Für spezielle Fragen zu diesen TOM steht Ihnen im Hause, Herr Benjamin Herzog, Director Internal IT/ CISO, wie folgt zur Verfügung:

bherzog@atrify.com

3.2 Fragen Sie direkt den Datenschutzbeauftragten

atrify hat Herrn Dr. Herwig Pant zum externen Datenschutzbeauftragten bestellt. Der Datenschutzbeauftragte steht Auftraggebern, Kunden und Mitarbeitern der atrify für Fragen zum Datenschutz sehr gerne zur Verfügung.

Brands Consulting | Datenschutz & Beratung
Dr. Herwig Pant
Auf dem Hahn 11
D-56412 Niedererbach

E-Mail: atrify@brands-consulting.eu
Homepage: www.Brands-Consulting.eu

DocuSigned by:
Jochen Moll
BCB4B405D784B6...

Jochen Moll, Geschäftsführer