proLogistik
GROUP

Auftragsverarbeitungsvertrag

proLogistik Group | Fallgatter 1 | 44369 Dortmund | Deutschland | +49 231 5194 0 | www.proLogistik.com
Geschäftsführer: Jörg Sänger, Katharina Grasser, Thulackshan Mohan
Sparkasse Dortmund, IBAN DE90 4405 0199 0001 1366 07, BIC DORTDE33XXX
Deutsche Bank AG, IBAN DE51 4407 0050 0150 4729 00, BIC DEUTDEDE440
Handelsregister: Amtsgericht Dortmund, Handelsregister-Nr.: HRB 34342, Umsatzsteuer-ID: DE187969600
Einige Abbildungen in diesem Dokument wurden mithilfe Künstlicher Intelligenz (KI) erstellt.

F4_32_intern_V1
Stand 10.04.2026

Technische und organisatorische Maßnahmen

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

Zutrittskontrolle
Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

☒ Alarmanlage
☒ Schließsystem mit Codesperre
☒ Schlüsselregelung (Schlüsselausgabe etc.)
☒ Besucherempfang
☒ Sorgfältige Auswahl von Personal (Reinigung, Pförtner, etc.)
☒ Bauliche Maßnahmen (einbruchshemmende Fenster, etc.)
☒ Dokumentiere Regelungen für die Zutrittskontrolle
☒ Aufteilung der Gebäude in Sicherheitszonen
☒ Absicherung von Gebäudeschächten
☒ Chipkarten- / Transponder-Schließsystem
☒ Manuelles Schließsystem
☒ Sicherheitsschlösser
☒ Personenkontrolle beim Pförtner / Empfang
☒ Etablierte Kontrollmechanismen (Stichprobenkontrolle der Schlüsselverwaltung, etc.)

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

☒ Zuordnung von Benutzerrechten
☒ Passwortrichtlinie (komplexe Passwörter)
☒ Authentifikation mit Benutzername / Passwort
☒ Gehäuseverriegelung
☒ Sperrung von externen Schnittstellen
☒ Einsatz von Intrusion-Detection-Systemen
☒ Einsatz von Intrusion-Prevention-Systemen
☒ Verschlüsselung von Smartphone-Inhalten
☒ Einsatz von Anti-Viren-Software
☒ Segmentierung von Netzwerken
☒ Protokollierung der Zugänge
☒ Auswertung von Log-Dateien

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

☒ Anzahl der Administratoren auf das Notwendigste beschränkt
☒ Protokollierung von Zugriffen
☒ Einsatz von externen Dienstleistern zur Vernichtung von Datenträgern
☒ Sichere Aufbewahrung von Datenträgern
☒ Verwaltung der Rechte durch Systemadministrator
☒ Ordnungsgemäße Vernichtung von Datenträgern (ISO/IEC 21964)
☒ Protokollierung von Vernichtungen
☒ Dokumentation der Berechtigungsvergabe

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

☒ Logische Mandantentrennung
☒ Datentrennung durch Netzsegmentierung
☒ Trennung von Entwicklungs-, Test- und Produktivsystemen
☒ Physikalische Trennung von Daten

Pseudonymisierung
Maßnahmen, die geeignet sind, eine Identifikation des Betroffenen zu erschweren oder zu verhindern.

☒ Verwaltung durch die datenverantwortliche Stelle

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

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

☒ Kontrollierte Vernichtung von Datenträgern durch zertifizierten Entsorger
☒ Weitergabe an Dritte nur nach Prüfung der Rechtsgrundlage
☒ Schriftliche Festlegung der Weitergabe in Drittländer
☒ Sichere Übertragung von Datenlieferungen (SFTP, VPN)
☒ Beschränkung des zur Übermittlung befugten Personenkreises
☒ Protokollierung von Datenabruf oder –übermittlung
☒ Sicherer Transport von Datenträgern (z.B. Backup, Tapes)

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

☒ Vergabe von Schreibrechten nach Usern
☒ Zuordnung der Logins zu datenverarbeitenden Mitarbeitern
☒ Protokollierung der Eingabe, Änderung und Löschung personenbezogener Daten

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

Verfügbarkeitskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

☒ Datensicherungskonzept mit regelmäßigem Backup
☒ Regelmäßige Kontrolle des Zustands und der Beschriftung von Datenträgern und Datensicherungen
☒ Betrieb und regelmäßige Prüfung von USV, Notstrom, Überspannungsschutz
☒ Sicherheitsvorkehrungen für Serverräume
☒ Feuer- / Rauchmeldeanlage
☒ Überwachung der Betriebsparameter in Serverräumen
☒ Redundante Speicherung personenbezogener Daten
☒ Auslagerung von Datenträgern zur Datensicherung
☒ Alarmanlage für Serverräume
☒ Klimaanlage in Serverräumen
☒ Feuerlöschgeräte für Serverräume
☒ Dokumentierter Notfall-Plan

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

Datenschutz-Management
Maßnahmen, die die Zulässigkeit, Angemessenheit und Wirksamkeit des Datenschutzes sicherstellen sollen.

☒ Einrichtung einer Datenschutzorganisation
☒ Datenschutzbeauftragter bestellt
☒ Verzeichnis von Verarbeitungstätigkeiten
☒ Datenschutzfreundliche Voreinstellungen
☒ Datenschutzschulung / -trainings
☒ Interne Überwachung der Ordnungsmäßigkeit
☒ Meldewege für Sicherheitsvorfälle

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

☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
☒ schriftliche Weisungen an den Auftragnehmer (z. B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. Art. 28 DSGVO
☒ Auftragnehmer hat Datenschutzbeauftragten bestellt
☒ Kontrollrechte gegenüber dem Auftragnehmer vereinbart
☒ vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Vertraulichkeit / Geheimhaltung
☒ laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

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

Zutrittskontrolle
Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

☒ Alarmanlage
☒ Automatische Zugangskontrolle
☒ Schließsystem mit Codesperre
☒ Lichtschranken / Bewegungsmelder
☒ Schlüsselregelung (Schlüsselausgabe etc.)
☒ Protokollierung der Besucher
☒ Sorgfältige Auswahl von Personal (Reinigung, Pförtner, etc.)
☒ Bauliche Maßnahmen (einbruchshemmende Fenster, etc.)
☒ Aufteilung der Gebäude in Sicherheitszonen
☒ Chipkarten- / Transponder-Schließsystem
☒ Videoüberwachung der Zugänge
☒ Personenkontrolle beim Pförtner / Empfang
☒ Dokumentiere Regelungen für die Zutrittskontrolle
☒ Etablierte Kontrollmechanismen (Stichprobenkontrolle der Schlüsselverwaltung, etc.)

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

☒ Zuordnung von Benutzerrechten
☒ Passwortrichtlinie (komplexe Passwörter)
☒ Authentifikation mit Benutzername / Passwort
☒ Sperrung von externen Schnittstellen
☒ Protokollierung der Besucher
☒ Einsatz von Intrusion-Detection-Systemen
☒ Einsatz von Anti-Viren-Software
☒ Einsatz einer Hardware-Firewall
☒ Segmentierung von Netzwerken
☒ Protokollierung der Zugänge
☒ 4-Augen-Prinzip bei der Vergabe von Berechtigungen
☒ Auswertung von Log-Dateien
☒ Einsatz von Penetrationstests
☒ Erstellen von Benutzerprofilen
☒ Zuordnung von Benutzerprofilen zu IT-Systemen
☒ Einsatz von VPN-Technologie
☒ Verschlüsselung von mobilen Datenträgern
☒ Verschlüsselung von Datenträgern in mobilen Endgeräten
☒ Einsatz von MDM-Software
☒ Einsatz einer Software-Firewall
☒ Regelmäßiger Passwortwechsel
☒ Kontosperrung bei fehlerhaften Zugangsversuchen
☒ Automatische Bildschirmsperre nach definiertem Zeit-intervall

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

☒ Erstellen eines Berechtigungskonzepts
☒ Anzahl der Administratoren auf das Notwendigste beschränkt
☒ Protokollierung von Zugriffen
☒ Physische Löschung von Datenträgern vor Wiederverwendung
☒ Einsatz von externen Dienstleistern zur Vernichtung von Datenträgern
☒ Verschlüsselung von Datenträgern

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

☒ Logische Mandantentrennung
☒ Erstellung Berechtigungskonzept und Vergabe nach Rollen
☒ Datentrennung durch Netzsegmentierung
☒ Physikalische Trennung von Daten
☒ Trennung von Entwicklungs-, Test- und Produktivsystemen

Pseudonymisierung
Maßnahmen, die geeignet sind, eine Identifikation des Betroffenen zu erschweren oder zu verhindern.

☒ Pseudonymisierung im Produkt active avis auf Anfrage

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

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

☒ Kontrollierte Vernichtung von Datenträgern durch zertifizierten Entsorger
☒ Weitergabe an Dritte nur nach Prüfung der Rechtsgrundlage
☒ Schriftliche Festlegung der Weitergabe in Drittländer
☒ Sichere Übertragung von Datenlieferungen (SFTP, VPN)
☒ Nutzung gemeinsamer Netzwerke
☒ Weitergabe in anonymisierter oder pseudonymisierter Form
☒ Verschlüsselung von Datenlieferungen (mobile Datenträger)
☒ Beschränkung des zur Übermittlung befugten Personenkreises
☒ Dokumentation von Abruf- und Übermittlungsprogrammen
☒ Protokollierung von Datenabruf oder –übermittlung
☒ Sicherer Transport von Datenträgern (z.B. Backup, Tapes)
☒ Erstellung von Begleitpapieren bei Transport

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

☒ Vergabe von Schreibrechten nach Rollen / Organisationseinheiten
☒ Zuordnung der Logins zu datenverarbeitenden Mitarbeitern
☒ Protokollierung der Eingabe, Änderung und Löschung personenbezogener Daten
☒ Regelmäßige Kontrolle von Protokolldaten

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

Verfügbarkeitskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

☒ Datensicherungskonzept mit regelmäßigem Backup
☒ Regelmäßige Kontrolle des Zustands und der Beschriftung von Datenträgern und Datensicherungen
☒ Betrieb und regelmäßige Prüfung von USV, Notstrom, Überspannungsschutz
☒ Sicherheitskonzept für Serverräume
☒ Betrieb und Test von Notfallplänen
☒ Feuer- / Rauchmeldeanlage
☒ Business Continuity Planung
☒ Dokumentierter Desaster Recovery Plan
☒ Überwachung der Betriebsparameter in Serverräumen
☒ Redundante Speicherung personenbezogener Daten
☒ Regelmäßiger Test der Rücksicherungsfähigkeit
☒ Auslagerung von Datenträgern zur Datensicherung
☒ Alarmanlage für Serverräume
☒ Klimaanlage in Serverräumen
☒ Feuerlöschgeräte für Serverräume

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

Datenschutz-Management
Maßnahmen, die die Zulässigkeit, Angemessenheit und Wirksamkeit des Datenschutzes sicherstellen sollen.

☒ Einrichtung einer Datenschutzorganisation
☒ Datenschutzbeauftragter bestellt
☒ Sicherheitskonzepte
☒ Datenschutzfreundliche Voreinstellungen
☒ Meldewege für Sicherheitsvorfälle
☒ Datenschutzschulung / -trainings
☒ Interne Überwachung der Ordnungsmäßigkeit
☒ Externe Überwachung der Ordnungsmäßigkeit

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

☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
☒ schriftliche Weisungen an den Auftragnehmer (z. B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. Art. 28 DS GVO
☒ Auftragnehmer hat Datenschutzbeauftragten bestellt
☒ vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis /-geheimhaltung
☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☒ laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
☒ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
☒ Teilweise Vertragsstrafen bei Verstößen