Parloa's Verpflichtungen unter DORA (EU) 2022/2554

Parloa ist bewusst, dass Unternehmen der Finanzbranche verpflichtet sind, spezifische Vorgaben der DORA-Verordnung auf IKT-Drittdienstleister in angemessenem Umfang zu übertragen. Wir haben uns aus diesem Grund dafür entschieden, einen umfassenden Maßnahmenkatalog auszuarbeiten, um es unseren Kunden zu erleichtern, den Vorgaben der Verordnung gerecht zu werden. Wir beobachten die weitere Entwicklung und zukünftige Konkretisierungen, die sich aus weiteren Vorgaben seitens der europäischen Aufsichtsbehörden ergeben werden, aufmerksam und werden unsere Standards entsprechend anpassen.

Jährliche Berichterstattung

Parloa verpflichtet sich dem Auftraggeber regelmäßig nachfolgend genannten Prüf- und Kontrollberichte kostenneutral zur Verfügung zu stellen:

Jährliche Berichterstattung	Prüfberichte (Jährlich)
	Ergebnis der Jahresabschlussprüfung (Finanzen)
	Aktuelles Zertifikat ISO27001:2022
	Aktueller Bericht: SOCII Type 2
	ISM-Jahresbericht
	ISM-Prozessbeschreibung
	Dokument zur Informationssicherheitsorganisation

Durchführung von Audits gemäß DORA-Verordnung

Parloa verpflichtet sich, Audits in enger Abstimmung mit unseren Kunden durchzuführen. Wir stellen so die Qualität unserer Dienstleistungen sicher, halten überdies aber auch die regulatorischen Anforderungen ein.
Zusätzlich führt Parloa regelmäßig interne Audits im Zusammenhang mit unseren Zertifizierungen wie ISO27001, SOC II, etc. durch.

Leitlinien und organisatorischen Eckpunkte für Audits

Allgemeine Regelungen	• **Transparenz** Parloa stellt die für ein Audit relevanten Unterlagen und Berichte bereit. • **Zusammenarbeit** Parloa stellt sicher, dass die Prüfungs- und Kontrollrechte unserer Kunden und deren Aufsichtsbehörden gewahrt bleiben, indem wir transparente Audit-Prozesse, standardisierte Compliance-Nachweise und individuelle Prüfungsmechanismen bereitstellen. • **Zugang** Parloa gewährt Kunden einen angemessenen Zugang zu relevanten Informationen, Systemen und Prozessen, im Rahmen der regulatorischen Anforderungen und sofern keine Sicherheitsrisiken enthalten sind.

Vor Ort Audits	• **Planung und Anmeldung** Audits erfordern eine Abstimmung 30 Werktage im Voraus, um eine angemessene Ressourcen-einteilung zu gewährleisten. • **Kommunikation der Inhalte** Bitte teilen Sie uns die spezifischen Bereiche und Themen der Prüfung im Vorfeld schriftlich mit. Es ist unabdingbar, die Zielsetzung und den Fokus der Auditmaßnahmen gemeinsam zu definieren. • **Teilnehmer und Lokalitäten** Eine frühzeitige Abstimmung über die Teilnehmer (Kunden- und Parloa-Seite) sowie die Lokalität des Audits (Vor Ort, Remote oder Hybrid) ist erforderlich.
Hybride Audits	• **Ressourcenschonende Umsetzung** Parloa setzt auf effiziente Prüfungsprozesse. Wir bieten unseren Kunden vor Ort, Remote und hybride Audit-Ansätze an. So können wir sowohl den Prüfungsanforderungen als auch den internen Ressourcen unserer Kunden gerecht werden. • **Planung und Anmeldung** Audits erfordern eine Abstimmung 30 Werktage im Voraus, um eine angemessene Ressourcen-einteilung zu gewährleisten. • **Kommunikation der Prüfungsinhalte** Bitte teilen Sie uns die Prüfungsschwerpunkte im Vorfeld schriftlich mit. Es ist unabdingbar, vorab

	ein gemeinsames Verständnis der Zielsetzung und der Audit-Durchführung zu schaffen. ● **Teilnehmer und Lokalitäten** Eine frühzeitige Abstimmung über die Teilnehmer (Kunden- und Parloa-Seite) sowie die Lokalität der Prüfung (Vor Ort, Hybrid, Remote) ist erforderlich.

IKT-Vorfall Meldeprozess

Parloa hat verlässliche Prozesse und Verfahren für das Vorfallmanagement etabliert, die im Einklang mit den Anforderungen der DORA-Verordnung stehen. Unsere Prozesse zielen darauf ab, die Kontinuität der Dienstleistungen zu gewährleisten und die Auswirkungen potenzieller Vorfälle auf die Stabilität und Sicherheit der Finanzdienstleistungsbranche zu minimieren.
Sollte es zu einem schwerwiegenden IKT-Vorfall kommen, werden die internen Notfall-pläne aktiviert und folgender Meldeprozess greift:

Kriterien für Aktivierung des Meldeprozesses	● Es wurde eine Störung erkannt, die eine erhebliche Beeinträchtigung für den Kunden als Auftraggeber zur Folge hat oder erwarten lässt (z.B. “Prio1-Störung”). ● Es gibt Anzeichen für einen Datenabfluss, eine Kompromittierung oder Sabotage der Systeme des Auftragnehmers oder eines Unterauftragnehmers. ● Ein Notfallplan oder der Krisenstab wurden aktiviert. ● Es bestehen schwerwiegende Schwachstellen (bspw. auf Basis des CVE-Scores), die nicht zeitnah behoben oder angemessen mitigiert werden können.

Erstmeldung	Die Erstmeldung eines schwerwiegenden IKT-Vorfalls wird unverzüglich nach Kenntnisnahme erfolgen. Dabei werden mindestens folgende Informationen übermittelt: ● Datum und Uhrzeit der Feststellung und Einstufung des Vorfalls ● Beschreibung des Vorfalls und der betroffene Infrastrukturkomponenten ● Angaben zu den Einstufungskriterien, die die Meldung des Vorfalls ausgelöst haben ● Informationen darüber, wie der Vorfall entdeckt wurde ● Angabe, ob ein Plan zur Aufrechterhaltung des Geschäftsbetriebs (Notfallplan, Krisenstab) aktiviert wurde
Folgemeldung	Spätestens 72 Stunden (3 Werktage) nach Erstmeldung oder einer Zwischenmeldung erfolgt eine (weitere) Zwischenmeldung. Dabei werden mindestens folgende Informationen übermittelt: ● Beschreibung der aktuellen Lagebewertung ● (Noch) betroffene Infrastrukturkomponenten ● Gegenmaßnahmen, die ergriffen wurden oder geplant sind ● Erkenntnisse zu Ursachen oder Bedrohungen und Techniken, die eingesetzt wurden ● Informationen über Indikatoren für eine Kompromittierung ● Auswirkungen auf den Kunden oder der Kunden des Kunden

	• Informationen über ggf. erfolgte Meldungen an andere Behörden
Abschlussmeldung	Die Bereitstellung eines Abschlussberichts erfolgt spätestens einen Monat nach dem letzten Zwischenbericht. Dabei werden mindestens folgende Informationen übermittelt: • Informationen über die Behebung des Vorfalls • Beschreibung der Ursachen (Root-Cause-Analyse) und der umgesetzten oder noch umzusetzenden Maßnahmen zur Verhinderung einer Wiederholung • Informationen über wiederkehrende ähnliche Vorfälle (falls zutreffend)

Migrationsprozess

We hate to let you go. Nichtsdestotrotz bietet Parloa klare Migrationsprozesse, welche eine reibungslose Datenübergabe gewährleisten, falls ein Wechsel zwingend erforderlich wird. Wie von DORA gefordert, sind Migrationen zu einem alternativen Anbieter in der Regel mit zeitlich überschaubarem Aufwand möglich.
Parloa hat folgende Maßnahmen etabliert, um eine technisch zeitnahe Migration der Daten sicherzustellen:

Datenspeicherung	• **Datenhaltung** Geringe Datenmengen reduzieren den Migrationsaufwand und erfüllen die Anforderungen der DSGVO. Parloa speichert Daten maximal 30 Tage, sofern vertraglich nicht anders festgelegt. Die finale Löschung der Backups erfolgt binnen 28 Tagen.

	• **Datenformat** Parloa unterstützt eine zügige Datenmigration durch die Bereitstellung der Daten in Standard Datenformaten. • **Risiken bei der Migration** Die Hauptherausforderungen einer Migration liegen in der Neukonfiguration der Systeme mit einem neuen Anbieter und den möglichen Abweichungen in spezifischen Funktionen und Arbeitsabläufen.
Proaktive Unterstützung	• **Technische Dokumentation** Wir stellen ausführliche Informationen zur Verfügung. • **Kundenorientierung** Parloa berücksichtigt individuelle Kundenanforderungen, um die Umstellung möglichst reibungslos zu gestalten.

Flexibilität

Parloa versteht die Wichtigkeit der Prozesskontinuität unserer Kunden, weshalb wir umfassende Maßnahmen definiert haben, welche die Risiken eines Anbieterwechsel reduzieren. Der Markt für B2B Kundenservice ist ein hoch kompetitives Segment und geprägt von technischen Alternativen für Kundenkommunikation - so stehen zur Kundenbetreuung neben AI-Agenten auch weiterhin zahlreiche andere Kanäle zur Verfügung wie bspw. Online Help Center, Chatbots, FAQs oder telefonischer Kundenservice durch Mitarbeitende.

Schulungen

Parloa schult Mitarbeitende regelmäßig und wiederholt durch Trainings und jährliche Bestätigung der Richtlinien:

Trainings	• Datenschutz • Training Informationssicherheit • Zulässige und unzulässige Nutzung des Firmen-netzwerks, der firmeneigenen Endgeräte oder anderer Ressourcen • Sicherheit mobiler Endgeräte • Phishing und Social Engineering • Sichere Remote Arbeit
Richtlinien	• Passwort Richtlinie • Informationssicherheitsrichtlinie • IT-Vorfallmanagement Richtlinie • Sicherheitsrichtlinie für Remote Arbeit • Richtlinie für saubere und ordentliche Arbeitsplätze • Disziplinar Richtlinie • Parloa-Verhaltenskodex • Vereinbarung mit Geschäftspartnern • Sensibilisierung für Bankgeheimnis • Sensibilisierung für Gesundheitsdaten