



DAS DACH- MARKTEINTRITTS- PLAYBOOK

Von Aegiron Capital Group

Leseprobe · Ausgabe September 2026

Inhaltsübersicht, ein Kapitel und eine Checkliste aus dem Paket

LESEPROBE

Diese Leseprobe darf frei weitergegeben werden. Sie dient der allgemeinen Information und ist keine Rechts-, Steuer- oder Finanzberatung. Die Unterlagen sind aus kaufmännischer Sicht geschrieben; eine anwaltliche Prüfung hat nicht stattgefunden.

INHALTSVERZEICHNIS

Über diese Leseprobe	3
Inhalt des vollständigen Pakets	4
Das Playbook	4
Die 16 Checklisten und Vorlagen	4
Die fünf Praxis-Kits	5
Kapitel 8: Enterprise-Readiness – was DACH-Kunden von Anbietern verlangen	6
8.1 Sicherheitsnachweise: ISO 27001, BSI C5, TISAX und SOC 2	6
8.2 Datenschutz: Auftragsverarbeitung und Datenübermittlung	7
8.3 DORA: die Anforderungen Ihrer Finanzkunden	8
8.4 NIS2 und Cyber Resilience Act aus Anbietersicht	8
8.5 Der Betriebsrat entscheidet mit	9
8.6 Barrierefreiheit bei Verbraucherprodukten	10
8.7 Das Vertrauenspaket: was Sie vor dem ersten Termin fertig haben sollten	10
Checkliste 11: Enterprise-Readiness-Checkliste für SaaS- und Technologieanbieter	12
A. Sicherheitsnachweise	12
B. Datenschutz	12
C. Regulierte Kunden: DORA, NIS2, Cyber Resilience Act	13
D. Betriebsrat und Mitbestimmung	14
E. Verbraucherprodukte: Barrierefreiheit	14
Das vollständige Paket	16

Über diese Leseprobe

Das DACH-Markteintritts-Playbook ist ein Paket aus drei Teilen: dem Playbook mit elf Kapiteln, dem Begleitdokument mit 16 Checklisten und Vorlagen sowie fünf Praxis-Kits. Alle Dokumente gibt es auf Deutsch und Englisch als PDF, Playbook und Checklisten zusätzlich als bearbeitbare Word-Datei.

Diese Leseprobe zeigt, was Sie erwartet: die vollständige Inhaltsübersicht, Kapitel 8 des Playbooks und die dazugehörige Checkliste 11 in voller Länge. Beide behandeln, was Banken, Versicherer und Konzerne im deutschsprachigen Raum von Software- und Technologieanbietern verlangen, bevor sie kaufen.

Inhalt des vollständigen Pakets

Das Playbook

- Management Summary
- Kapitel 0: Einführung
- Kapitel 1: Die Regulierungslandschaft im DACH-Raum
- Kapitel 2: Lizenzantrags-Roadmaps
- Kapitel 3: Aufbau Ihres AML/KYC-Rahmenwerks
- Kapitel 4: Markteintrittsstrategie
- Kapitel 5: Kultureller Navigationsleitfaden
- Kapitel 6: Compliance-Zeitplanvorlagen
- Kapitel 7: Regulatorischer Ausblick 2026-2028
- Kapitel 8: Enterprise-Readiness – was DACH-Kunden von Anbietern verlangen (in dieser Leseprobe)
- Kapitel 9: Eintrittswege ohne eigene Lizenz und die Wahl des Herkunftsstaats
- Kapitel 10: Illustrative Fallstudien
- Anhang A: Offizielle Anlaufstellen und Register
- Anhang B: Änderungshistorie
- Schlusswort

Die 16 Checklisten und Vorlagen

- 1. BaFin-Lizenzantrags-Checkliste
- 2. AML/KYC-Implementierungs-Checkliste
- 3. Bereitschaftsbewertung für den Markteintritt
- 4. ZAG-Lizenzzeitplan-Vorlage
- 5. MiCA-CASP-Zulassungszeitplan-Vorlage
- 6. Vorlagen für behördliche Korrespondenz
- 7. DACH-Regulatorisches Glossar (DE / EN)
- 8. AMLA/AMLR-Readiness-Checkliste
- 9. PSD3/PSR-Übergangs-Checkliste
- 10. DORA-Readiness-Checkliste für Technologie-Dienstleister
- 11. Enterprise-Readiness-Checkliste für SaaS- und Technologieanbieter (in dieser Leseprobe)
- 12. Checkliste Rechtsform, erste Mitarbeiter und Betriebsstätte
- 13. Partner-Due-Diligence für Lizenz-light-Modelle und Banking-as-a-Service
- 14. Schweiz-Check: grenzüberschreitende Dienstleistungen aus der EU
- 15. Regulatorischer Fristenkalender 2026-2028

- 16. Budget- und Business-Case-Vorlage für den Markteintritt

Die fünf Praxis-Kits

- DORA Vendor Kit: Vertragsklauseln und Nachweise für IKT-Dienstleister von Finanzunternehmen
- ZAG-Roadmap: der Weg zur Erlaubnis als Zahlungs- oder E-Geld-Institut
- MiCA-CASP-Roadmap: der Weg zur Zulassung als Kryptowerte-Dienstleister
- AMLR-Umstellungsguide 2027: Umstellung auf die EU-Geldwäscheverordnung
- CCD2-Umstellungsguide 2026: das neue Verbraucherkreditrecht für Ratenkauf, Ratenkauf und BNPL

Kapitel 8: Enterprise-Readiness – was DACH-Kunden von Anbietern verlangen

Für Fintech- und SaaS-Unternehmen, die an Banken, Versicherer, Konzerne oder den Mittelstand verkaufen, entscheidet sich der Markteintritt oft nicht im Lizenzverfahren, sondern im Einkauf. Deutsche Einkaufsabteilungen arbeiten mit standardisierten Fragebögen, Datenschutzbeauftragte verhandeln Auftragsverarbeitungsverträge Wort für Wort, regulierte Kunden geben ihre DORA- und NIS2-Pflichten vertraglich an ihre Anbieter weiter – und nach der Vertragsunterschrift entscheidet der Betriebsrat mit, ob und wie die Software eingeführt wird. Dieses Kapitel beschreibt, welche Nachweise und Dokumente erwartet werden und in welcher Reihenfolge sich der Aufbau lohnt. Checkliste 11 im Begleitdokument übersetzt es in eine Arbeitsliste.

8.1 Sicherheitsnachweise: ISO 27001, BSI C5, TISAX und SOC 2

Im deutschen Enterprise-Vertrieb kommt der Sicherheitsfragebogen vor dem Vertragsentwurf. Einkäufer wollen Nachweise, die sie kennen und ablegen können, statt Erklärungen, die sie bewerten müssen.

Nachweis	Was er ist	Wer ihn erwartet	Hinweise
ISO/IEC 27001:2022	Zertifikat für das Managementsystem der Informationssicherheit	Praktisch alle Enterprise-Einkäufer	Die Übergangsfrist von der Ausgabe 2013 endete im Oktober 2025; Einkäufer erwarten die aktuelle Ausgabe. Geltungsbereich und Erklärung zur Anwendbarkeit werden gelesen.
BSI C5 (Typ 1 / Typ 2)	Testat eines Prüfers über Cloud-Kontrollen nach dem Kriterienkatalog des BSI	Öffentliche Auftraggeber, Banken und Versicherer (DORA-Prüfung), Gesundheitswesen	Der überarbeitete C5:2026 (ausgerichtet an ISO 27001:2022 und NIS2) ist im April 2026 erschienen. Anzuwenden ist er für Typ-1-Berichte mit Stichtag ab dem 1. Juni 2027 und für Typ-2-Berichte, deren Prüfungszeitraum ab dem 1. Juni 2027 beginnt; bis dahin sind Testate nach C5:2020 weiter üblich, eine frühere Anwendung ist zulässig. Verlangt Transparenz zu Datenstandort, Gerichtsstand und Behördenzugriffen.

Nachweis	Was er ist	Wer ihn erwartet	Hinweise
TISAX	Informationssicherheits-Assessment der Automobilindustrie (ENX, VDA-ISA)	Automobilhersteller und Zulieferer	Außerhalb der Automobilbranche ohne Bedeutung – nur bei passendem Zielsegment investieren.
SOC 2 Type II	US-Prüfbericht über Kontrollen	Viele Einkäufer als Ergänzung	Selten Ersatz für ISO 27001 oder C5.

Die Reihenfolge, die sich auszahlt: mit ISO 27001:2022 beginnen, und zwar mit einem Geltungsbereich, der das in Deutschland verkaufte Produkt tatsächlich abdeckt; ein C5-Testat (zuerst Typ 1, dann Typ 2) ergänzen, wenn öffentliche Auftraggeber, Finanzdienstleister oder das Gesundheitswesen Zielkunden sind; TISAX nur für die Automobilbranche. Ergänzend gehören Zusammenfassungen von Penetrationstests, Ergebnisse von Notfalltests und eine aktuelle Liste der Unterauftragsverarbeiter in jedes Nachweispaket.

8.2 Datenschutz: Auftragsverarbeitung und Datenübermittlung

In DACH-Enterprise-Deals ist der Auftragsverarbeitungsvertrag (AVV) keine Anlage, die im Vorbeigehen unterschrieben wird. Er wird verhandelt – oft vom Datenschutzbeauftragten des Kunden, oft auf dessen eigener Vorlage. Das rechtliche Minimum setzt Artikel 28 DSGVO. Verhandelt wird vor allem über:

- **Technische und organisatorische Maßnahmen:** Eine konkrete Anlage wird erwartet, kein Verweis auf eine Webseite – und sie wird mit Ihren Zertifizierungen abgeglichen.
- **Unterauftragsverarbeiter:** aktuelle Liste, Vorabinformation über Änderungen (Fristen um 30 Tage sind üblich) und ein echtes Widerspruchsrecht.
- **Kontrollrechte:** Anbieter bevorzugen Zertifikate und Prüfberichte, Kunden Vor-Ort-Kontrollen. Üblicher Kompromiss: zuerst Berichte, Vor-Ort-Prüfungen bei Anlass.
- **Meldung von Datenpannen:** Die DSGVO verlangt eine Meldung „unverzüglich“; Kunden fordern oft feste Stundenfristen, weil ihre eigene 72-Stunden-Frist von Ihrer abhängt.
- **Haftung:** Einkäufer drängen auf unbegrenzte oder gesondert begrenzte Datenschutzhaftung – der umstrittenste kommerzielle Punkt.
- **Datenstandort:** Verarbeitung in der EU oder im EWR ist zunehmend Voraussetzung, insbesondere bei Banken, Versicherern und öffentlichen Auftraggebern.

Übermittlungen in die USA. Für Übermittlungen an zertifizierte US-Unternehmen besteht seit Juli 2023 mit dem EU-US Data Privacy Framework ein Angemessenheitsbeschluss. Im September 2025 hat das Gericht der Europäischen Union die Klage gegen diesen Beschluss abgewiesen; ein Rechtsmittel ist beim Gerichtshof anhängig. Weil der Gerichtshof beide Vorgänger – Safe Harbor und Privacy Shield – für ungültig erklärt hat, fragen DACH-Kunden, was geschieht, wenn auch dieses Framework fällt. Die belastbare Antwort: DPF-Zertifizierung plus EU-Standardvertragsklauseln als Auffangmechanismus im AVV, eine dokumentierte

Transfer-Folgenabschätzung (einschließlich Support-Zugriffen von außerhalb des EWR), EU-Hosting für Kunden mit strengen Anforderungen und eine transparente Beschreibung des Umgangs mit Behördenanfragen.

Schweiz. Das revidierte Datenschutzgesetz gilt seit September 2023. EU und Schweiz erkennen ihr Schutzniveau gegenseitig an; für die USA ist seit September 2024 das Swiss-US Data Privacy Framework anerkannt. Schweizer Kunden erwarten dennoch dieselbe vertragliche Absicherung wie EU-Kunden.

8.3 DORA: die Anforderungen Ihrer Finanzkunden

DORA reguliert nicht den Technologieanbieter, sondern seine Kunden – und diese geben die Anforderungen weiter. Wer an Banken, Zahlungsinstitute, Versicherer, Wertpapierinstitute oder Krypto-Dienstleister verkauft, muss mit folgenden Punkten rechnen:

- **Vertragsinhalte nach Artikel 30 DORA:** vollständige Leistungsbeschreibung, Datenstandorte, Sicherheitsstandards, Unterstützung bei IKT-Vorfällen, Zugangs-, Prüf- und Inspektionsrechte für Kunde und Aufsicht, Kündigungsrechte, Exit-Unterstützung und – bei kritischen oder wichtigen Funktionen – erweiterte Pflichten wie Mitwirkung an Resilienztests.
- **Informationsregister:** Ihre Kunden müssen alle IKT-Verträge in einem standardisierten Register führen und jährlich melden. Ein Datenblatt mit allen registerrelevanten Angaben (LEI, Dienstkategorie, Datenstandorte, Unterauftragnehmerkette) verkürzt jedes Onboarding.
- **Vorfälle:** Ihre Kunden haben enge Meldefristen gegenüber der Aufsicht – und erwarten, von Ihnen mindestens ebenso schnell informiert zu werden.
- **Kritische IKT-Drittdienstleister:** Die ersten 19 Benennungen vom November 2025 betreffen große Cloud- und Infrastrukturanbieter. Für ein typisches SaaS-Unternehmen ist eine Benennung kein kurzfristiges Szenario; die Konzentration Ihrer Kundschaft im Finanzsektor bleibt dennoch ein Beobachtungspunkt.

Der Klauselbaukasten, ein Registerdatenblatt, ein Incident-Playbook und ein Antwortkatalog für Due-Diligence-Fragebögen finden sich im DORA Vendor Kit aus dem Playbook-Paket; Checkliste 10 fasst die Anforderungen zusammen.

8.4 NIS2 und Cyber Resilience Act aus Anbietersicht

Ein SaaS-Anbieter unterhalb der NIS2-Schwellen begegnet NIS2 trotzdem – über die Lieferketten-Sicherheitspflichten seiner Enterprise-Kunden. Oberhalb der Schwellen (in der Regel ab 50 Beschäftigten oder mehr als 10 Millionen EUR Jahresumsatz und Jahresbilanzsumme in einem erfassten Sektor, für bestimmte digitale Dienste auch darunter) kann er selbst erfasst sein, mit Registrierung, Risikomanagementmaßnahmen und Meldepflichten (Kapitel 7.7).

Der Cyber Resilience Act erfasst die Teile Ihres Angebots, die beim Kunden installiert werden: mobile Apps, Desktop-Clients, On-Premise-Agenten, Browser-Erweiterungen und SDKs. Seit dem 11. September 2026 laufen die Meldefristen für aktiv ausgenutzte Schwachstellen.

Voraussetzungen sind eine Richtlinie zur koordinierten Offenlegung von Schwachstellen, ein überwachter Eingangskanal, eine Triage-Rolle in Rufbereitschaft mit Eskalationsbefugnis und Software-Stücklisten (SBOMs), mit denen sich ausgenutzte Drittkomponenten binnen Stunden den betroffenen Produkten zuordnen lassen.

Praxistipp: Bauen Sie einen einzigen Vorfallprozess mit mehreren Ausgängen – CRA-Meldung an die ENISA, NIS2-Meldung an BSI oder österreichische Behörde, vertragliche Kundeninformation nach DORA, Datenpanne nach DSGVO. Parallele Prozesse versagen genau in der Nacht, in der es darauf ankommt.

8.5 Der Betriebsrat entscheidet mit

Viele SaaS-Anbieter erleben im ersten deutschen Enterprise-Deal dieselbe Überraschung: Der Vertrag ist unterschrieben, das Budget freigegeben – und dann steht die Einführung monatelang still. Grund ist § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz: Der Betriebsrat bestimmt bei der Einführung und Anwendung technischer Einrichtungen mit, die geeignet sind, Verhalten oder Leistung der Beschäftigten zu überwachen. Nach der Rechtsprechung des Bundesarbeitsgerichts genügt die objektive Eignung – auf die Absicht kommt es nicht an. Praktisch betrifft das fast jede Business-Software, die Nutzeraktivität protokolliert.

- **Ohne Einigung keine Einführung.** Der Betriebsrat kann verlangen, dass die Nutzung unterbleibt; einigen sich die Parteien nicht, entscheidet die Einigungsstelle.
- **Frühe Unterrichtung.** Der Arbeitgeber muss den Betriebsrat bei der Planung neuer technischer Anlagen – einschließlich KI-Anwendungen – unterrichten, bevor Entscheidungen feststehen. Geht es um KI, gilt die Hinzuziehung eines Sachverständigen auf Arbeitgeberkosten kraft Gesetzes als erforderlich.
- **Datenschutzebene.** Betriebsvereinbarungen dienen oft als Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten. Der Gerichtshof der Europäischen Union hat klargestellt, dass sie die Anforderungen der DSGVO vollständig erfüllen müssen.
- **Österreich** hat ein vergleichbares, teils strengeres Regime (Zustimmungspflicht bei Kontrollmaßnahmen, die die Menschenwürde berühren; Betriebsvereinbarung für Personaldatenysteme). **Die Schweiz** kennt kein vergleichbares Mitbestimmungsrecht, verbietet aber Systeme, die das Verhalten der Beschäftigten überwachen sollen.

Was Anbieter vorbereiten: ein Betriebsrats-Paket auf Deutsch (Systembeschreibung, Datenflüsse, protokollierte Nutzerdaten), ein Rollen- und Berechtigungskonzept mit abschaltbaren Leistungsauswertungen, ein Lösch- und Aufbewahrungskonzept je Datenkategorie, Musterklauseln für eine Betriebsvereinbarung, die bestehende Kunden bereits akzeptiert haben, und für KI-Funktionen eine Dokumentation von Zweck, Eingaben, menschlicher Aufsicht und dem Ausschluss automatisierter Personalentscheidungen. Planen Sie die Mitbestimmung als Projektphase von Wochen bis Monaten in den Einführungsplan des Kunden ein.

8.6 Barrierefreiheit bei Verbraucherprodukten

Seit dem 28. Juni 2025 verlangt der European Accessibility Act, dass Bank- und Zahlungsdienste für Verbraucher barrierefrei sind – vom Onboarding über Identifizierung und starke Kundenauthentifizierung bis zur Zahlung. Umgesetzt ist er in Deutschland durch das Barrierefreiheitsstärkungsgesetz (BFSG), in Österreich durch das Barrierefreiheitsgesetz (BaFG). Maßstab in der Praxis ist die Norm EN 301 549 auf Basis der WCAG 2.1 (Stufe AA); Informationen zur Dienstleistung sollen ein Sprachniveau von B2 nicht übersteigen. Nicht erfasst sind Dienstleistungen ausschließlich für Unternehmen; Kleinunternehmen (weniger als zehn Beschäftigte und höchstens 2 Millionen EUR Jahresumsatz oder Bilanzsumme) sind bei Dienstleistungen ausgenommen. In Deutschland setzt die gemeinsame Marktüberwachungsstelle der Länder (MLBF) in Magdeburg die Anforderungen durch. Die Schweiz ist an die Richtlinie nicht gebunden.

8.7 Das Vertrauenspaket: was Sie vor dem ersten Termin fertig haben sollten

Dokument	Zweck	Sprache
Sicherheitsüberblick mit Zertifikaten (ISO 27001, ggf. C5)	Erste Hürde im Einkauf nehmen	DE und EN
Antwortbibliothek für Sicherheitsfragebögen	Fragebögen in Tagen statt Wochen beantworten	DE und EN
Auftragsverarbeitungsvertrag mit TOM-Anlage und Unterauftragsverarbeiter-Liste	Datenschutzverhandlung verkürzen	DE
Transfer-Folgenabschätzung und Beschreibung des Umgangs mit Behördenanfragen	Fragen zu US-Bezügen beantworten	DE und EN
DORA-Vertragsanhang und Registerdatenblatt	Onboarding bei Finanzkunden	DE und EN
Incident- und Schwachstellenprozess (CRA/NIS2/DORA)	Nachweis operativer Reife	DE und EN
Betriebsrats-Paket mit Muster-Betriebsvereinbarung	Einführung nach Vertragsschluss beschleunigen	DE
Exit- und Datenportabilitätskonzept (Data Act)	Wechselrechte und DORA-Exit bedienen	DE und EN
Bei Verbraucherprodukten: Barrierefreiheitsinformationen	BFSG/BaFG-Pflichten erfüllen	DE

Ein Trust Center, in dem Kunden diese Unterlagen unter Vertraulichkeitsvereinbarung abrufen können, verkürzt jede künftige Prüfung. Die Investition amortisiert sich typischerweise mit dem ersten Enterprise-Vertrag, dessen Einkaufsprozess nicht drei Monate länger dauert.

Wichtigste Erkenntnisse – Kapitel 8

- *Im DACH-Enterprise-Vertrieb verkaufen Sie Nachweise: ISO 27001:2022 als Basis, BSI C5 für öffentliche Auftraggeber, Finanz- und Gesundheitssektor, TISAX nur für die Automobilbranche.*
- *Der Auftragsverarbeitungsvertrag ist Verhandlungsgegenstand. Ein vollständiger deutscher AVV mit TOM-Anlage und belastbarem Transfer-Setup spart Wochen.*
- *DORA erreicht Anbieter über die Verträge ihrer Finanzkunden: Artikel-30-Klauseln, Registerdaten, Vorfallunterstützung, Exit.*
- *Seit dem 11. September 2026 laufen die CRA-Meldefristen für installierbare Produktteile; NIS2 wirkt über die Lieferkette auch unterhalb der Schwellen.*
- *Der Betriebsrat entscheidet über die Einführung fast jeder Business-Software mit. Ein Betriebsrats-Paket macht aus Stillstand eine planbare Projektphase.*
- *Verbraucherprodukte müssen seit Juni 2025 barrierefrei sein; reine B2B-Dienste und Kleinstunternehmen sind ausgenommen.*

Checkliste 11: Enterprise-Readiness-Checkliste für SaaS- und Technologieanbieter

Kontext: Deutsche Unternehmens- und Finanzkunden kaufen Nachweise. Diese Checkliste bündelt, was Einkauf, Informationssicherheit, Datenschutzbeauftragte und Betriebsrat typischerweise verlangen (Playbook Kapitel 8). Sie gilt unabhängig davon, ob Ihr Unternehmen selbst eine Lizenz benötigt.

A. Sicherheitsnachweise

Status	Punkt	Beschreibung / Hinweise
[]	ISO/IEC 27001:2022	Zertifikat nach der aktuellen Ausgabe; Geltungsbereich deckt das in Deutschland verkaufte Produkt und die betreibenden Teams ab. Erklärung zur Anwendbarkeit bereithalten.
[]	BSI C5 (falls Zielsegment)	Bei öffentlichen Auftraggebern, Banken, Versicherern oder im Gesundheitswesen: C5-Testat, zuerst Typ 1, dann Typ 2, auf Basis des C5:2026 (anzuwenden für Stichtage und Prüfungszeiträume ab 1. Juni 2027; bis dahin ist C5:2020 weiter zulässig). Prüfer frühzeitig einbinden.
[]	TISAX (nur Automobilbranche)	Nur verfolgen, wenn Automobilhersteller oder Zulieferer Zielkunden sind; erforderliches Prüfniveau vorab klären.
[]	Ergänzende Berichte	SOC 2 Type II (falls vorhanden), Zusammenfassung des letzten Penetrationstests, Ergebnisse der Notfalltests.
[]	Antwortbibliothek	Standardantworten für Sicherheitsfragebögen auf Deutsch und Englisch, versioniert und mit Verantwortlichem.
[]	Trust Center	Nachweise unter Vertraulichkeitsvereinbarung abrufbar; Aktualität mindestens quartalsweise geprüft.

B. Datenschutz

Status	Punkt	Beschreibung / Hinweise
[]	Auftragsverarbeitungsvertrag (Art. 28 DSGVO)	Deutsche Fassung, verhandlungsfähig, mit konkreter TOM-Anlage.
[]	Unterauftragsverarbeiter	Aktuelle Liste mit Sitz, Funktion und Datenstandort; Änderungsinformation mit Vorlauf (üblich: rund 30 Tage) und Widerspruchsrecht.

Status	Punkt	Beschreibung / Hinweise
[]	Kontroll- und Auditrechte	Abgestuftes Modell: zuerst Zertifikate und Prüfberichte, Vor-Ort-Prüfungen bei Anlass.
[]	Meldung von Datenpannen	Feste interne Frist (in Stunden) für die Information des Kunden, abgestimmt auf dessen 72-Stunden-Frist.
[]	Datenstandort	EU/EWR-Verarbeitung für Kunden mit entsprechenden Anforderungen; Support- und Administrationszugriffe dokumentiert.
[]	Drittlandübermittlung	Bei US-Bezug: Zertifizierung nach dem Data Privacy Framework plus Standardvertragsklauseln als Auffangmechanismus; Transfer-Folgenabschätzung dokumentiert.
[]	Behördenzugriffe	Beschreibung des Umgangs mit Zugriffersuchen (Prüfung, Anfechtung, Information des Kunden, Transparenzbericht).
[]	Unterstützung der Datenschutz-Folgenabschätzung	Informationspaket für die DSFA des Kunden: Datenkategorien, Zwecke, Löschfristen, Risiken, Maßnahmen.

C. Regulierte Kunden: DORA, NIS2, Cyber Resilience Act

Status	Punkt	Beschreibung / Hinweise
[]	DORA-Vertragsanhang	Klauseln nach Art. 30 DORA (Leistungsbeschreibung, Datenstandorte, Sicherheitsstandards, Vorfallunterstützung, Audit- und Zugangsrechte, Kündigung, Exit); Erweiterungen für kritische oder wichtige Funktionen.
[]	Registerdatenblatt	Alle Angaben, die Finanzkunden für ihr Informationsregister brauchen (LEI, Dienstkategorie, Datenstandorte, Unterauftragnehmerkette).
[]	Incident-Playbook	Eskalationsmatrix, Vorlage für die Erstinformation, Fristen passend zu den Meldepflichten der Kunden.
[]	NIS2-Betroffenheit	Eigene Einordnung geprüft (Sektor, Größe, Dienst); bei Betroffenheit Registrierung: in Deutschland beim BSI binnen drei Monaten ab Betroffenheit (für Einrichtungen, die seit dem 6. Dezember 2025 erfasst sind, lief die Frist am 6. März 2026 ab – falls noch offen, umgehend nachholen); in Österreich beim Bundesamt für Cybersicherheit bis 1. Jänner 2027 (nach Angabe der Behörde; wegen Feiertag und Wochenende spätestens 4. Jänner 2027).

Status	Punkt	Beschreibung / Hinweise
[]	CRA-Betroffenheit	Installierbare Komponenten (Apps, Clients, Agenten, SDKs) erfasst; Herstellerrolle bestimmt.
[]	Schwachstellenprozess	Richtlinie zur koordinierten Offenlegung, überwachter Eingangskanal, Triage in Rufbereitschaft, 24-Stunden-Frühwarnung über die ENISA-Plattform vorbereitet, SBOMs gepflegt.
[]	Ein Vorfallprozess	Gemeinsamer Prozess für CRA-, NIS2-, DORA- und DSGVO-Meldungen mit klaren Ausgängen.
[]	Exit und Portabilität	Exportformate, Übergangsunterstützung und Fristen dokumentiert; deckungsgleich mit den Wechselflichten des Data Act.

D. Betriebsrat und Mitbestimmung

Status	Punkt	Beschreibung / Hinweise
[]	Betriebsrats-Paket	Deutschsprachige Systembeschreibung, Datenflüsse, protokollierte Nutzerdaten, Zweck jeder Auswertung.
[]	Rollen- und Berechtigungskonzept	Wer sieht welche nutzerbezogenen Daten; Leistungsauswertungen konfigurierbar bzw. abschaltbar.
[]	Lösch- und Aufbewahrungskonzept	Je Datenkategorie, abgestimmt auf die Datenschutz-Folgenabschätzung des Kunden.
[]	Muster-Betriebsvereinbarung	Klauseln, die bestehende Kunden bereits akzeptiert haben; für Österreich angepasst.
[]	KI-Funktionen	Zweck, Eingaben, menschliche Aufsicht und Ausschluss automatisierter Personalentscheidungen dokumentiert.
[]	Zeitplanung	Mitbestimmungsphase (Wochen bis Monate) im Einführungsplan des Kunden berücksichtigt.

E. Verbraucherprodukte: Barrierefreiheit

Status	Punkt	Beschreibung / Hinweise
[]	Anwendungsbereich geklärt	Richtet sich die Dienstleistung an Verbraucher? Greift die Ausnahme für Kleinunternehmen?
[]	Prüfung nach EN 301 549 / WCAG 2.1 AA	Kritische Nutzerwege zuerst: Onboarding, Identifizierung, Authentifizierung, Zahlung, Kontoschließung.

Status	Punkt	Beschreibung / Hinweise
[]	Komponenten Dritter	KYC-, Authentifizierungs- und Karten-SDKs barrierefrei; vertraglich gefordert.
[]	Informationen zur Barrierefreiheit	Veröffentlicht; zentrale Kundeninformationen auf Sprachniveau B2.

Das vollständige Paket

Das vollständige Paket erhalten Sie auf aegironcapitalgroup.com/playbook: Playbook, 16 Checklisten und Vorlagen sowie fünf Praxis-Kits, auf Deutsch und Englisch, mit Aktualisierungen bei wesentlichen regulatorischen Änderungen für 24 Monate ab Kaufdatum.

Der Verkauf richtet sich ausschließlich an Unternehmen. Für Fragen, die über das Paket hinausgehen, erreichen Sie uns über aegironcapitalgroup.com/contact.