GARRETT PARTRIDGE

OPERATIONS ARCHITECT

COMPLIANCE

Ein Faden, zwei Flaggen: Die auf US-Persons beschränkte Datengrenze für einen Verteidigungsbetrieb mit ausländischem Mutterkonzern

Wie die auf US-Persons beschränkte Datengrenze, die ITAR-Datengrenze und CMMC Level 2 in einem US-Betrieb in ausländischem Besitz zu einem einzigen prüfbaren digitalen Faden zusammengebaut werden.

Whitepaper · Garrett Partridge · 16. Juli 2026

garrettpartridge.com · Brookline, NH

DIE DIREKTE ANTWORT

Ja. Eine US-Tochtergesellschaft in ausländischem Besitz kann ITAR-kontrollierte technische Daten vorhalten und CMMC Level 2 erreichen. Keines der beiden Regelwerke fragt, wem Sie gehören. Beide fragen, wo die Daten liegen und wer sie erreichen kann. Nach ITAR ist Ihre US-Tochtergesellschaft eine US-Person, weil sie in den Vereinigten Staaten gegründet ist, und Ihr Mutterkonzern ist eine foreign person, weil er es nicht ist (22 CFR 120.62 und 120.63). Die Eigentumsverhältnisse ändern an keiner der beiden Antworten etwas. Die Weitergabe technischer Daten an eine foreign person innerhalb der Vereinigten Staaten ist eine Ausfuhr, ein deemed export (22 CFR 120.50(a)(2)). Die Ingenieure, IT-Administratoren und der Helpdesk Ihres Mutterkonzerns sind damit ausländische Empfänger der Daten Ihrer eigenen Tochtergesellschaft, sofern nicht eine Lizenz oder eine Ausnahmeregelung etwas anderes sagt. CMMC Level 2 verlangt sodann die Kontrollen nach NIST SP 800-171 auf den Systemen, die Controlled Unclassified Information vorhalten, und den Nachweis, dass diese Kontrollen tatsächlich laufen. In der Praxis ist das ein Aufbau und nicht drei: eine einzige auf US-Persons beschränkte Datengrenze um die kontrollierte Arbeit herum, mit dem Mutterkonzern außerhalb, durchgesetzt mit derselben Zugriffskontrolle, Segmentierung und Protokollierung, die ein Prüfer bewertet. Das Organigramm behält zwei Flaggen. Der digitale Faden bekommt eine.

Ihr Mutterkonzern ist eine foreign person

Der Satz, der dieses ganze Problem neu ordnet, ist kurz, und die meisten Mutterkonzerne hören ihn viel zu spät zum ersten Mal. Nach ITAR (der US-Rüstungsexportkontrolle) ist Ihr Mutterkonzern gegenüber den technischen Daten Ihrer US-Tochtergesellschaft eine foreign person, eine Person ohne US-Status im Sinne des Exportkontrollrechts. Kein Partner mit zusätzlichem Papierkram. Eine foreign person: dieselbe Kategorie wie jedes andere Unternehmen im Ausland, das keine Lizenz hält.

Die Vorschrift kommt über die Gründung dorthin, nicht über das Eigentum. Zu den US-Persons (Personen mit US-Status im Sinne des Exportkontrollrechts) zählt jede Einheit, die „incorporated to do business in the United States“ ist (22 CFR 120.62). Zu den foreign persons zählt jede Einheit, die „not incorporated or organized to do business in the United States“ ist (22 CFR 120.63). Ihre Gesellschaft in Delaware oder Massachusetts ist eine US-Person. Ihr Mutterkonzern in Ottawa, Brescia oder Stuttgart ist eine foreign person. Dass der Mutterkonzern 100 Prozent der Tochtergesellschaft hält, bewegt keine von beiden über die Linie. Der Text kennt keine Konzernausnahme, weil der Text nie nach dem Konzern fragt.

Führungskräfte hören darin eine Beleidigung einer Konzernbeziehung, die sie über Jahrzehnte aufgebaut haben. Das ist es nicht. Es ist eine Aussage über Daten, und nur über Daten. Der Mutterkonzern besitzt weiterhin das Unternehmen, besetzt den Aufsichtsrat, setzt die Strategie und nimmt den Gewinn. Was der Mutterkonzern nicht mehr automatisch bekommt, ist die Zeichnung.

Derselbe Reflex zeigt sich beim Status als Verbündeter, deshalb wird er hier gleich geschlossen.

Jedes Land, das ich bediene, ist ein nach DFARS (Ergänzung zur US-Bundesvergabeordnung für Verteidigungsbeschaffungen) qualifiziertes Land, im Rahmen eines gegenseitigen Verteidigungsbeschaffungsabkommens mit dem DoD (US-Verteidigungsministerium), siehe DFARS 225.003. Dieser Status ist eine Beschaffungspräferenz für Endprodukte und Komponenten. Er hebt ITAR nicht auf, er hebt CMMC nicht auf, und er räumt FOCI nicht aus. Der Status als Verbündeter bringt Ihre Teile durch die Buy-American-Prüfung. Er bringt Ihren Mutterkonzern nicht durch die Datengrenze.

ITAR definiert ausländisches Eigentum und ausländische Kontrolle sehr wohl, und zwar für seine eigenen Zwecke, in 22 CFR 120.65. Ausländisches Eigentum liegt bei mehr als 50 Prozent der ausstehenden stimmberechtigten Anteile vor. Ausländische Kontrolle ist die Befugnis oder die Fähigkeit, allgemeine Richtlinien oder das Tagesgeschäft festzulegen oder zu lenken, und sie wird vermutet, wenn foreign persons 25 Prozent oder mehr der ausstehenden stimmberechtigten Anteile halten, es sei denn, eine einzelne US-Person kontrolliert einen gleich großen oder größeren Anteil. Diese Definitionen sind maßgeblich für das, was Sie der Directorate of Defense Trade Controls mitteilen. Sie gehören ITAR selbst, und sie sind nicht das FOCI-Rahmenwerk der Defense Counterintelligence and Security Agency, das eigenen Regeln folgt. Halten Sie die beiden auseinander, und lassen Sie Ihren Rechtsbeistand für Exportkontrolle und einen auf die DCSA spezialisierten Fachmann ihre jeweilige Hälfte verantworten.

> **Der Test ist die Gründung, nicht das Eigentum. Ihre US-Tochtergesellschaft ist eine US-Person, weil sie hier gegründet ist. Ihr Mutterkonzern ist eine foreign person, weil er es nicht ist. 100 Prozent an der Tochtergesellschaft zu halten, ändert an keiner der beiden Antworten etwas.**

Was tatsächlich innerhalb der Grenze liegt

Bevor Sie eine Grenze ziehen können, müssen Sie wissen, was sie umschließt. Zwei Datenbestände sind im Spiel. Sie überschneiden sich stark, und die meisten Betriebe verschätzen sich bei beiden auf exakt dieselbe Weise: Sie warten auf eine Kennzeichnung.

Technische Daten im Sinne von ITAR sind Informationen, die für Entwurf, Entwicklung, Produktion, Herstellung, Montage, Betrieb, Reparatur, Prüfung, Wartung oder Änderung eines Rüstungsguts erforderlich sind, einschließlich Informationen in Form von Blaupausen, Zeichnungen, Fotografien, Plänen, Anweisungen oder Dokumentation (22 CFR 120.33(a)). Lesen Sie diese Definition noch einmal und achten Sie darauf, was in ihr fehlt. Eine Kennzeichnung kommt darin nicht vor. Technische Daten sind darüber definiert, was die Information jemanden tun lässt, und nicht darüber, ob ein Stempel in der Ecke der Seite gelandet ist. Eine CAM-Datei, die niemand beschriftet hat, gehört zu den technischen Daten, wenn sie zur Herstellung des Teils erforderlich ist.

Kontrollierte Verteidigungsinformationen folgen einer parallelen Logik. Nach DFARS 252.204-7012 sind das nicht klassifizierte kontrollierte technische Informationen oder andere Informationen des CUI-Registers (CUI, kontrollierte, nicht klassifizierte Informationen), die geschützt werden müssen und die entweder gekennzeichnet oder im Vertrag benannt sind, oder die „collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the

performance of the contract“ werden. Auch dieser zweite Zweig braucht keine Kennzeichnung.

Die Anweisung also, nach der Ihre Belegschaft bisher gelebt hat, schützt das gekennzeichnete Material, ist die falsche Anweisung. Zwei Regelwerke, zwei Definitionen, und keines von beiden wartet auf einen Aufkleber. Beide greifen über Funktion und Kontext, und genau deshalb lassen sie sich nicht an denjenigen delegieren, der den Stempel führt.

- Technische Daten sind funktional bestimmt. Wenn die Information erforderlich ist, um das Rüstungsgut zu entwerfen, herzustellen, zu prüfen, zu reparieren oder zu ändern, behandelt ITAR sie als technische Daten, gekennzeichnet oder nicht (22 CFR 120.33(a)).
- Kontrollierte Verteidigungsinformationen sind kontextbestimmt. Informationen, die zur Erfüllung des Vertrags genutzt oder gespeichert werden, sind kontrollierte Verteidigungsinformationen, ob sie nun gekennzeichnet ankamen oder nicht (DFARS 252.204-7012, Definitionen).
- Die Ausnahmen sind real, und sie sind nützlich. Zu den technischen Daten im Sinne von ITAR gehören nicht: allgemeine wissenschaftliche, mathematische oder ingenieurtechnische Grundlagen, wie sie üblicherweise an Hochschulen gelehrt werden, öffentlich zugängliche Informationen sowie grundlegende Marketinginformationen zu Funktion oder Zweck und allgemeine Systembeschreibungen von Rüstungsgütern (22 CFR 120.33(b)). Diese Ausnahme ist es, die Ihrem Mutterkonzern sein Berichtswesen erhält, und ich komme am Ende darauf zurück.
- Die abgeleiteten Dateien sind die, die Sie erwischen. Die Zeichnung ist offensichtlich, und man geht sorgfältig mit ihr um. Die CAM-Datei, die Vorrichtungszeichnung, das Prüfprogramm und der daraus abgeleitete Arbeitsplan sind die, die still auf einer Freigabe ohne Verantwortlichen landen.

> **Ihre Belegschaft ist darauf geschult, nach einer Kennzeichnung zu suchen. Technische Daten im Sinne von ITAR brauchen keine, und der zweite Zweig der kontrollierten Verteidigungsinformationen braucht ebenfalls keine. In dieser Lücke leckt ein Betrieb mit ausländischem Mutterkonzern zuerst.**

Die fünf Konzern-IT-Architekturen, die lecken

Das ist der Teil, der im Raum am härtesten einschlägt. Das größte einzelne Hindernis zwischen einem verbündeten Hersteller und einem DoD-Auftrag ist in der Regel nicht die Vorschrift. Es ist die Konzern-IT-Architektur, die der Mutterkonzern fünfzehn Jahre lang standardisiert hat und auf die er zu Recht stolz ist.

Nach 22 CFR 120.56(a)(3) werden technische Daten weitergegeben, indem access information (Zugangsinformationen) genutzt wird, um einer foreign person den Zugriff auf unverschlüsselte technische Daten zu verschaffen oder es ihr zu ermöglichen, sie einzusehen oder zu besitzen. Achten Sie auf das Verb. Ermöglichen. Die Klausel ist auf die Fähigkeit geschrieben, nicht auf die Absicht, und nicht darauf, ob überhaupt jemand die Datei geöffnet hat. Nach 22 CFR 120.56(b) ist bereits eine Genehmigung erforderlich, um einer foreign person diese access information überhaupt zu geben. Die Frage, die ein Exportrechtsanwalt und ein Prüfer gleichermaßen stellen, lautet also nicht, ob der Mutterkonzern hingeschaut hat. Sie lautet, ob dem Mutterkonzern der

Zugriff ermöglicht werden könnte.

Fünf Muster machen den Großteil dessen aus, was ich bei einem ersten Rundgang finde:

- Die gemeinsam genutzte ERP- oder PLM-Instanz. Ein Konzern-Mandant, ein Teilestamm, ein Dokumententresor und eine Konstruktionsabteilung auf Seiten des Mutterkonzerns mit Leserechten über das Ganze. Genau die Effizienz, die den Aufbau lohnend gemacht hat, ist das Problem. ERP steht für Enterprise Resource Planning, die Unternehmensressourcenplanung, PLM für Product Lifecycle Management, die Verwaltung des Produktlebenszyklus.
- Die Konzern-Dateifreigabe. Eine globale Freigabe oder ein globaler Mandant, in dem der US-Standort ein Ordner ist. Kontrollierte Zeichnungen landen dort, weil Zeichnungen immer schon dort gelandet sind, und jeder Konzernnutzer mit einem Pfad zu diesem Ordner ist eine Frage der Erreichbarkeit.
- Der Helpdesk im Ausland oder im Land des Mutterkonzerns. Der Service Desk, der jeden Standort betreut, auf jedem Endgerät Administratorrechte hält und eine Remote-Sitzung auf einem Arbeitsplatz übernehmen kann, auf dem eine Zeichnung geöffnet ist. Der Support ist wirklich gut. Genau deshalb wurde er zentralisiert.
- Identität und Netzwerk beim Mutterkonzern. Die Domäne des Mutterkonzerns, das VPN des Mutterkonzerns, die Domänenadministratoren des Mutterkonzerns. Ein Administrator, der jedes Passwort zurücksetzen kann, kann den Zugriff auf alles ermöglichen, was dieses Passwort schützt. Das ist 22 CFR 120.56(a)(3), geschrieben als Stellenbeschreibung.
- Backup und Disaster Recovery im Konzern. Replikation in das Rechenzentrum des Mutterkonzerns, während das Speicherteam des Mutterkonzerns die Wiederherstellungsschlüssel hält. Niemand denkt bei einem Backup an einen Datenpfad. Es ist der vollständigste Datenpfad im ganzen Gebäude.

> **Die Frage lautet nie, ob der Mutterkonzern die Zeichnung angesehen hat. Nach 22 CFR 120.56(a)(3) lautet die Frage, ob dem Mutterkonzern der Zugriff darauf ermöglicht werden könnte. Der Auslöser ist die Fähigkeit, und die Fähigkeit eines Domänenadministrators ist von Haus aus total.**

Verschlüsselung bewegt die Bits. Die Befugnis bewegt sie nicht.

Die erste Idee, die jeder fähige CTO zu diesem Problem mitbringt, ist Verschlüsselung, und der Instinkt ist richtig. ITAR gewährt der Verschlüsselung eine echte Ausnahme. Diese Ausnahme ist zugleich nützlicher und enger, als fast alle glauben, und in der Lücke zwischen diesen beiden Lesarten werden Programme teuer.

Das ist, was sie gewährt. Nach 22 CFR 120.54(a)(5) sind das Senden, Mitführen oder Speichern technischer Daten keine Ausfuhr, sofern mehrere Bedingungen zugleich erfüllt sind. Die Daten sind nicht klassifiziert. Sie sind mit einer Ende-zu-Ende-Verschlüsselung gesichert. Sie sind mit kryptografischen Modulen gesichert, die FIPS 140-2 oder dessen Nachfolgern entsprechen, oder mit anderen kryptografischen Mitteln, deren Sicherheitsstärke mindestens den 128 Bit von AES-128 vergleichbar ist. Und sie werden nicht absichtlich an eine Person in einem nach 22 CFR 126.1 gesperrten Land gesendet, nicht dort gespeichert und nicht von dort gesendet. Die Regel

räumt sogar die Sorge um die Routenführung unmittelbar aus: Daten, die über das Internet unterwegs sind, gelten nicht als in einem Land gespeichert, das sie nur durchqueren. Und 22 CFR 120.54(c) stellt klar, dass die Möglichkeit, technische Daten in verschlüsselter Form abzurufen, die diese Kriterien erfüllt, weder eine Weitergabe noch eine Ausfuhr darstellt.

Lesen Sie nun die Definition, auf der die Ausnahme beruht. Für diesen Zweck verlangt die Ende-zu-Ende-Verschlüsselung, dass die Daten zwischen dem Urheber und dem vorgesehenen Empfänger zu keinem Zeitpunkt unverschlüsselt vorliegen und dass „the means of decryption are not provided to any third party“ (22 CFR 120.54(b)(1)). Der vorgesehene Empfänger muss der Urheber sein, eine US-Person in den Vereinigten Staaten oder eine Person, die anderweitig zum Empfang der technischen Daten befugt ist (22 CFR 120.54(b)(2)).

Genau dort bricht sie für die meisten Konzernarchitekturen zusammen. Access information ist in 22 CFR 120.55 definiert als Information, die den Zugriff auf verschlüsselte technische Daten in unverschlüsselter Form erlaubt, und die Vorschrift nennt die Beispiele selbst: Entschlüsselungsschlüssel, Netzwerkzugangscodes und Passwörter. Geben Sie diese an eine foreign person, und 22 CFR 120.56(b) verlangt dafür eine Genehmigung. Nutzen Sie sie, um einer foreign person den Zugriff auf unverschlüsselte Daten zu ermöglichen, und Sie befinden sich in 22 CFR 120.56(a)(3), einer Weitergabe. Und 22 CFR 120.50(a)(6) macht die Weitergabe zuvor verschlüsselter technischer Daten zu einer Ausfuhr aus eigenem Recht.

Die Architektur fällt damit aus dem Text heraus, und sie ist die These dieses Papiers. Das Chiffrat darf die Infrastruktur des Konzerns durchqueren. Die Schlüssel dürfen nicht zum Mutterkonzern gelangen. Ihr Mutterkonzern darf den Speicher halten, den Verkehr tragen, die Leitung besitzen und die Replikation betreiben, solange das, was er hält, für ihn unlesbar bleibt und die Mittel zur Entschlüsselung innerhalb der auf US-Persons beschränkten Grenze bleiben. Diese eine Asymmetrie ist es, die einem Unternehmen erlaubt, eine IT-Beziehung und zwei Flaggen zu behalten.

Zwei Vorbehalte, und ich meine beide ernst. Die Bedingungen in 22 CFR 120.54(a)(5) und die Definition in (b) sind kumulativ: Sie müssen alle zugleich und auf Ihren tatsächlichen Sachverhalt zutreffen. Und ob Ihre konkrete Architektur die Ausnahme erfüllt, ist eine rechtliche Feststellung, die Ihr Rechtsbeistand für Exportkontrolle trifft, und keine, die ein Operations-Architekt für Sie trifft. Meine Aufgabe ist es, die Umgebung so zu bauen, dass diese Feststellung sauber, dokumentiert und leicht mit Ja zu beantworten ist. Die Feststellung selbst bleibt beim Rechtsbeistand, und ich sage das im ersten Gespräch und nicht im letzten.

> **Die Bits dürfen hinüber. Die Schlüssel nicht. Ein Mutterkonzern, der nur das Chiffrat hält und dem die Mittel zur Entschlüsselung nie gegeben wurden, hält Speicher. Ein Mutterkonzern, der den Schlüssel hält, hält technische Daten.**

CMMC zieht die Linie nicht. CMMC beweist, dass die Linie echt ist.

Die meisten Betriebe mit ausländischem Mutterkonzern führen ITAR und CMMC (den von der US-Verteidigung geforderten Cybersicherheits-Reifegrad) als zwei Projekte, mit zwei Anbietern und zwei Budgets, und oft einem dritten für den Netzwerkaufbau. Es ist ein Aufbau. Zu verstehen, warum, spart die sechs Monate, die diese Programme üblicherweise verlieren.

NIST SP 800-171 (der US-Standard zum Schutz kontrollierter, nicht klassifizierter Informationen) ist blind gegenüber der Staatsangehörigkeit. Seine Zugriffskontrollen fragen, ob ein Nutzer befugt ist. Sie fragen nicht, welchen Pass der Nutzer hält. Das ist keine Lücke im Standard, es ist eine Arbeitsteilung. ITAR ist das Regelwerk, das entscheidet, wer für exportkontrollierte technische Daten befugt werden kann. NIST SP 800-171 ist die Mechanik, die diese Entscheidung durchsetzt, protokolliert und die Nachweise erzeugt. CMMC Level 2 ist das US-Verteidigungsministerium, das prüft, ob die Mechanik echt ist.

Damit steht die Reihenfolge fest. ITAR zieht die Grenze. Die Kontrollen nach 800-171 halten sie. Der Prüfer bewertet sie. Bauen Sie sie in dieser Reihenfolge, und jede speist die nächste: Die Zugriffsmatrix, die Sie für die Exportfrage schreiben, wird zur Zugriffskontrolle, die der Prüfer testet. Bauen Sie sie als drei parallele Anbietergespräche, bekommen Sie drei Antworten, die sich am Tor widersprechen.

Eine einzige Definition in DFARS 252.204-7012 beendet den häufigsten Plan, den ich höre: dass die Konzern-IT den US-Standort einfach so führt, wie sie jeden anderen Standort führt. Ein covered contractor information system ist definiert als „an unclassified information system that is owned, or operated by or for, a contractor", das kontrollierte Verteidigungsinformationen verarbeitet, speichert oder überträgt. Operated by or for. Wenn die IT-Abteilung Ihres Mutterkonzerns Ihre US-Systeme betreibt, sind diese Systeme covered contractor information systems, und die Umgebung des Mutterkonzerns liegt nicht außerhalb Ihres Assessments. Sie liegt darin. Die Arbeit an den Konzern zu geben, verlagert die Pflicht nicht ins Ausland. Es zieht den Konzern in den Geltungsbereich hinein.

Die Klausel trägt den Rest der Form, für die Sie planen müssen:

- NIST SP 800-171 auf den covered contractor information systems umsetzen, in der Fassung, die zum Zeitpunkt der Ausschreibung gilt, oder wie vom Contracting Officer (dem Vergabebeamten) genehmigt (DFARS 252.204-7012(b)(2)(i)). Die Fassung ist an die Ausschreibung gebunden, also schneiden Sie den Kontrollumfang auf den Vertrag zu, der vor Ihnen liegt, und nicht auf die Folie eines Anbieters.
- Ein externer Cloud-Dienstleister, der kontrollierte Verteidigungsinformationen speichert, verarbeitet oder überträgt, muss Sicherheitsanforderungen erfüllen, die der FedRAMP-Moderate-Baseline gleichwertig sind, und die Absätze der Klausel zu Meldung von Cybervorfällen, Schadsoftware, Sicherung von Datenträgern, forensischem Zugriff und Schadensbewertung einhalten (DFARS 252.204-7012(b)(2)(ii)(D)). Wenn das Hosting des Konzerns dieser Dienstleister ist, verpflichtet sich der Konzern zu alldem.
- Einen Cybervorfall innerhalb von 72 Stunden nach Entdeckung melden. Die Klausel definiert „rapidly report" genau so. Ein vom Mutterkonzern geführter Helpdesk fünf Zeitzonen entfernt liegt damit innerhalb Ihrer 72-Stunden-Uhr, und das ist eine Personalfrage, bevor es eine Compliance-Frage ist.

- Die Klausel ist unverändert in Unterverträge zu übernehmen, außer zur Benennung der Parteien (DFARS 252.204-7012(m)). Konzerngesellschaften sind davon nicht befreit, weil sie Ihr Logo teilen.
- CMMC Level 2 bedeutet die 110 Sicherheitsanforderungen nach NIST SP 800-171, und mit Stand Juli 2026 wird es über eine Selbstbewertung alle drei Jahre mit einer jährlichen Bestätigung im SPRS (Supplier Performance Risk System, dem Lieferantenbewertungssystem des DoD) erreicht. Am 13. Juli 2026 hat das Ministerium die Zertifizierungspflicht durch einen Drittprüfer aus der Phase II ausgesetzt und eine Reformprüfung eingeleitet. Die Klausel oben hat sich nicht bewegt, und deshalb kann ein neuer US-Betrieb die Grenze weiterhin nicht als Projekt für das zweite Jahr behandeln. Geändert hat sich, wer erklärt, dass die Kontrollen laufen. Das sind jetzt Sie.

> **Operated by or for. Wenn die IT-Abteilung des Mutterkonzerns Ihre Systeme führt, liegen die Systeme des Mutterkonzerns innerhalb Ihres CMMC-Assessments. Die Zentralisierung beim Konzern verlagert die Pflicht nicht ins Ausland. Sie zieht den Konzern in die Grenze hinein.**

Die Grenze endet nicht am Büro

Alles bisher lässt sich leicht als Büroproblem vorstellen. Dateifreigaben, Postfächer, ein ERP, ein Helpdesk. Genau dieser Rahmen ist es, an dem Betriebe mit ausländischem Mutterkonzern scheitern, denn die kontrollierten Daten reisen dort am gefährlichsten, wo gefertigt wird.

In dem Moment, in dem eine Zeichnung das ERP verlässt und an der Maschine zur Arbeitsanweisung wird, sind technische Daten aus einem System, das Sie als geschützt behandeln, in ein System übergegangen, das Sie seit jeher als Maschine und nicht als Computer behandelt haben. Die CAM-Datei auf einem gemeinsam genutzten PC in der Fertigung. Das Programm, das auf der Steuerung liegt. Der Historian, der Prozessdaten zu einem kontrollierten Teil aufzeichnet und sie anschließend mit einem Server abgleicht, den das ganze Büro erreicht. Für einen inländischen Betrieb ist dieser Übergang bereits der am häufigsten übersehene Kontrollpunkt im Gebäude. Für einen Betrieb mit ausländischem Mutterkonzern trägt jeder dieser Übergänge eine zweite Frage auf der ersten: nicht nur, ob dies kontrolliert ist, sondern wer im Konzern das System erreichen kann, auf dem es gelandet ist.

Das Beispiel, das dies konkret macht, ist kein Bösewicht. Es ist Ihr bester Automatisierungsingenieur. Eine Linie in Nashua steht um 2 Uhr nachts still. Der Steuerungstechniker des Mutterkonzerns in Turin hat genau diese Fertigungszelle viermal in Betrieb genommen und bekommt sie über eine Remote-Sitzung in zwanzig Minuten wieder zum Laufen. Er ist eine foreign person. Die Steuerung hält ein Programm, das aus kontrollierten technischen Daten abgeleitet ist. Diese Remote-Sitzung ist die gesamte Vorschrift in einer einzigen Bildschirmfreigabe, und der Schichtleiter wird diese Entscheidung um 2 Uhr nachts treffen, sofern die Architektur sie nicht bereits für ihn getroffen hat.

Die Grenze wird deshalb in die Fertigung hineinkonstruiert und nicht um sie herum gezogen. Segmentieren Sie das OT-Netz so, dass ein erreichbares Büro-Endgerät kein Pfad zu einer Steuerung ist. Führen Sie die notwendigen Übergaben über einen kontrollierten, protokollierten Weg statt über einen USB-Stick. Entscheiden Sie im Voraus und schriftlich, welche

Fertigungszellen kontrollierte Programme halten und wer sie erreichen darf, damit die Entscheidung um 2 Uhr nachts ein Nachschlagen ist und keine Ermessensfrage. Und wo die Unterstützung durch die Konstruktion des Konzerns wirklich die richtige Antwort ist, holen Sie über Ihren Rechtsbeistand die ordnungsgemäße Genehmigung ein, solange die Linie noch läuft, statt die Frage während eines Vorfalls zu entdecken.

Deshalb behandle ich die Datengrenze und das Betriebsmodell als ein Entwurfsproblem und nicht als zwei. Derselbe zusammengeführte Faden, der einem Prüfer einen einzigen prüfbaren Weg vom Vertrag bis zum Schnitt gibt, ist der Faden, der der P&L (Gewinn- und Verlustrechnung) einen ehrlichen Blick darauf gibt, was die Fertigung tatsächlich tut. Einmal gebaut, ist er der Nachweis für den Prüfer und die Instrumententafel für den Inhaber. Zweimal gebaut, sind es zwei Systeme, die einander widersprechen.

> **Die Vorschrift interessiert nicht, dass es 2 Uhr nachts war und die Linie stand. Entscheiden Sie, wer eine Steuerung mit einem kontrollierten Programm erreichen darf, bevor die Nacht kommt, in der die Linie ausfällt, und es ist keine Entscheidung des Schichtleiters mehr.**

Das Organigramm behält zwei Flaggen

Jeder Mutterkonzern hört die auf US-Persons beschränkte Datengrenze als eine Mauer zwischen sich und dem Unternehmen, das ihm gehört. Diese Lesart bringt mehr dieser Projekte um als jede Kontrolle, und sie ist falsch. Richtig gebaut, verliert der Mutterkonzern fast nichts von dem, was er tatsächlich braucht.

Gehen Sie zurück zur Definition. Technische Daten im Sinne von ITAR sind Informationen, die erforderlich sind, um ein Rüstungsgut zu entwerfen, herzustellen, zu prüfen, zu reparieren oder zu ändern, und 22 CFR 120.33(b) nimmt grundlegende Marketinginformationen zu Funktion oder Zweck und allgemeine Systembeschreibungen ausdrücklich aus. Ein Konzernabschluss gehört nicht zu den technischen Daten. Auftragseingang, Auftragsbestand, Liefertreue, Ausschussquote, Durchsatz, Personalbestand, Investitionsausgaben, Qualitätskennzahlen und die SQDIP-Tafel gehören nicht zu den technischen Daten. Fast nichts, was der Aufsichtsrat eines Mutterkonzerns an einem Dienstag tatsächlich durchsieht, gehört zu den technischen Daten.

Die Entwurfsaufgabe ist damit präzise, und sie ist eine operative und keine rechtliche: Geben Sie dem Mutterkonzern jede Zahl, auf die er Anspruch hat, und keine der Zeichnungen, auf die er keinen hat. In der Praxis wird die Berichtsebene so gebaut, dass sie die Grenze überquert, und die Konstruktionsebene so, dass sie es nicht tut. Diese Unterscheidung ist die ganze Architektur, und deshalb wird sie zur Entwurfszeit entschieden, wo sie ein Gespräch kostet, statt zur Zeit des Assessments, wo sie eine neue Plattform kostet.

- Überquert die Grenze bewusst: Konzernabschluss, Auftragseingang und Auftragsbestand, Liefertreue, Ausschuss und Ausbeute, Durchsatz, Personalbestand, Investitionsausgaben und der SQDIP-Takt (Sicherheit, Qualität, Liefertreue, Bestände, Produktivität). Der Aufsichtsrat des Mutterkonzerns behält seine Dienstagsrunde.
- Bleibt innerhalb der Grenze: Zeichnungen, Spezifikationen, CAM- und Prüfprogramme, Arbeitspläne und jede abgeleitete Datei, die erforderlich ist, um das Rüstungsgut herzustellen,

zu prüfen oder zu reparieren (22 CFR 120.33(a)).

- Bleibt innerhalb der Grenze: die Schlüssel. Entschlüsselungsschlüssel, Netzwerkzugangscodes und Passwörter sind access information (22 CFR 120.55), und sie einer foreign person zu geben, erfordert eine Genehmigung (22 CFR 120.56(b)).
- Benannt und schriftlich festgehalten: ein Systemadministrator mit US-Person-Status für die Enklave, ein namentlich benannter Verantwortlicher mit US-Person-Status für die Zugriffsentscheidung und eine Zugriffsmatrix für technische Daten, die nach Rolle und Staatsangehörigkeit benennt, wer kontrollierte Daten erreichen darf und wer nicht. Der Auditor eines Hauptauftragnehmers und ein Prüfer der DDTC (US-Behörde für die Kontrolle des Verteidigungshandels) fragen beide nach dieser Matrix. Eine mündliche Verständigung ist kein Artefakt.
- Eigene Frage, eigener Zeitplan: FOCI. Die FOCI-Minderung (FOCI, ausländisches Eigentum, ausländische Kontrolle oder ausländischer Einfluss) ist das, was die DCSA (US-Behörde für Spionageabwehr und Sicherheit im Verteidigungsbereich) verlangt, wenn ein Unternehmen in ausländischem Besitz die Berechtigung zum Zugang zu klassifizierten Informationen braucht, ausgehandelt über Ihren auf sicherheitsermächtigte Betriebe spezialisierten Rechtsbeistand. Der Großteil der Zulieferfertigung im Verteidigungsbereich ist nicht klassifizierte Arbeit mit CUI und ITAR-Kontrolle, die niemals eine facility clearance (Sicherheitsermächtigung für den Standort) braucht. Diese Arbeit braucht diese Datengrenze dennoch vom ersten Tag an. FOCI hängt von der Auftragsklasse ab, die Sie anstreben. Die Datengrenze hängt von gar nichts ab.

> **Der Mutterkonzern behält das Unternehmen, die Unternehmensführung und jede Zahl, die sein Aufsichtsrat durchsieht. Die Tochtergesellschaft behält die Zeichnungen. Das ist keine Mauer zwischen einem Mutterkonzern und seiner Investition. Es ist die einzige Architektur, unter der diese Investition den Auftrag gewinnt.**

Was ich baue, und was beim Rechtsbeistand bleibt

Ich bin der operative Partner, und ich bin präzise, wo dessen Grenze verläuft. Ich baue den regelkonformen US-Betrieb auf und führe ihn: die Fertigung, das Betriebsmodell, den Aufbau der IT- und OT-Umgebung, die auf US-Persons beschränkte Datengrenze und die Bereitschaftsnachweise für das Tor, gegen das Sie laufen. Die Gründung der Gesellschaft, die Registrierung für ITAR und bei der DDTC, die FOCI-Minderung, die Feststellungen zu Lizenzen und Ausnahmeregelungen und Fragen des CFIUS (Committee on Foreign Investment in the United States, der US-Ausschuss für Auslandsinvestitionen) bleiben bei Ihrem Unternehmensrechtsbeistand und Ihrem Rechtsbeistand für Exportkontrolle. Ich stimme mich mit ihnen ab und verantworte das operative Ergebnis.

Diese Linie ist keine Bescheidenheit, sie ist der Grund, warum der Aufbau hält. Ob eine bestimmte Architektur die Ausnahme nach 22 CFR 120.54 erfüllt, ob eine bestimmte Übermittlung eine Lizenz braucht, ob Ihre Eigentümerstruktur eine Meldung an die DDTC auslöst: Das sind rechtliche Feststellungen mit rechtlichen Folgen. Ein Operations-Architekt, der sie für Sie beantwortet, verkauft Ihnen eine Haftung mit selbstsicherer Stimme. Was ich tue, ist den Betrieb so zu bauen, dass diese Feststellungen sauber, dokumentiert und leicht sind, und dass die Nachweise

vorliegen, bevor jemand danach fragt.

Dieser Aufbau ist weder theoretisch noch selten. Im April 2026 erreichte American Rheinmetall die Zertifizierung nach CMMC Level 2 an seinen US-Produktionsstandorten: ein US-Betrieb mit deutschem Mutterkonzern, der die Aufstellung hält, öffentlich belegt. Ich war selbst der Operator des ausländischen Mutterkonzerns in den USA und habe das Nordamerika-Geschäft eines italienischen Sensorkonzerns geleitet, und ich baue derzeit den US-Fertigungsbetrieb im Verteidigungsbereich für die Tochtergesellschaft eines kanadischen Mutterkonzerns auf. Der Weg existiert, und Menschen gehen ihn. Knapp ist der Operator, der ihn mit Ihnen geht. Sechs Ebenen von Firmen helfen einem ausländischen Hersteller in den US-Markt, vom FOCI-Rechtsbeistand über die Strukturierung durch die Big Four und die Standortwahl bis zu CMMC-IT-Anbietern, und jede einzelne von ihnen überreicht Ihnen ein Dokument, ein Gebäude oder ein Zertifikat. Der Standards Guide for Foreign Partners des Chief Information Officer des DoD ist das, was einer offiziellen Synthese am nächsten kommt, und er ist ein Kontroll-Overlay und keine Abfolge für einen Operator. Irgendjemand muss den Betrieb immer noch aufbauen und führen. Diese Ebene ist die eigentliche Arbeit, und sie ist die, die ich verantworte.

Das Fazit ist der Titel. Ihr Mutterkonzern ist gegenüber den technischen Daten Ihrer US-Tochtergesellschaft eine foreign person, und deshalb bleiben die Zeichnungen, die abgeleiteten Dateien und die Schlüssel innerhalb einer auf US-Persons beschränkten Grenze, während das Chiffrat, die Finanzzahlen und die Unternehmensführung sie frei überqueren. ITAR zieht diese Grenze, NIST SP 800-171 hält sie, und CMMC Level 2 beweist, dass sie hält. Bauen Sie die drei als einen Faden, und der Prüfer findet die Kontrollen bereits in Betrieb vor, weil sie die Art sind, wie die Arbeit getan wird. Bauen Sie sie als drei Anbietergespräche, und Sie erfahren am Tor, welches davon falsch lag, mit dem Vertrag auf dem Tisch. Ein Faden. Zwei Flaggen.

HÄUFIG GEFRAGT

Ist unser Mutterkonzern wirklich eine foreign person, wenn er uns zu 100 Prozent hält?

Ja. Nach ITAR ist der Test für eine Einheit die Gründung, nicht das Eigentum. Zu den US-Persons zählt jede Einheit, die in den Vereinigten Staaten zur Geschäftstätigkeit gegründet ist (22 CFR 120.62), und zu den foreign persons zählt jede Einheit, die nicht in den Vereinigten Staaten zur Geschäftstätigkeit gegründet oder errichtet ist (22 CFR 120.63). Ihre US-Tochtergesellschaft ist eine US-Person. Ihr im Ausland gegründeter Mutterkonzern ist eine foreign person. Die Tochtergesellschaft vollständig zu halten, bewegt keine von beiden über die Linie, weil die Definitionen nie nach dem Eigentum fragen. ITAR definiert ausländisches Eigentum und ausländische Kontrolle sehr wohl gesondert in 22 CFR 120.65, und diese Definitionen sind maßgeblich für das, was Sie der Directorate of Defense Trade Controls melden. Sie schaffen keine Konzernausnahme von den Datenregeln.

Kann unser US-Standort auf dem ERP des Mutterkonzerns laufen?

In der Regel nicht ohne eine Grenze. Wenn Ihr US-Betrieb kontrollierte technische Daten vorhält, bleiben diese Daten innerhalb einer auf US-Persons beschränkten Datengrenze. Eine gemeinsam genutzte Instanz, die Nutzern auf Seiten des Mutterkonzerns einen Pfad zu Zeichnungen oder Spezifikationen gibt, ist damit eine Frage der Weitergabe nach 22 CFR 120.56(a)(3), und die hängt daran, ob einer foreign person der Zugriff auf unverschlüsselte technische Daten ermöglicht werden kann. Manchmal ist die Antwort eine abgetrennte Instanz, manchmal ein separates

System, manchmal eine kontrollierte Schnittstelle, die Planungs- und Finanzdaten nach oben durchreicht, während der Konstruktionstresor innerhalb der Grenze bleibt. Die Architekturentscheidung ist Teil des Aufbaus, und sie wird an Ihren tatsächlichen Datenflüssen getroffen und nicht an einer Vorlage.

Löst es das Problem, wenn wir alles verschlüsseln?

Verschlüsselung löst das Transportproblem, nicht das Befugnisproblem. ITAR sieht in 22 CFR 120.54(a)(5) eine echte Ausnahme für das Senden, Mitführen oder Speichern nicht klassifizierter technischer Daten unter einer Ende-zu-Ende-Verschlüsselung vor, die FIPS 140-2 oder einer vergleichbaren Stärke entspricht, und 22 CFR 120.54(c) bestätigt, dass die Möglichkeit, ordnungsgemäß verschlüsselte Daten abzurufen, weder eine Weitergabe noch eine Ausfuhr ist. Die Ausnahme ist aber so definiert, dass die Mittel zur Entschlüsselung keinem Dritten gegeben werden dürfen (22 CFR 120.54(b)(1)), und Entschlüsselungsschlüssel, Netzwerkzugangscodes und Passwörter sind access information nach 22 CFR 120.55. Geben Sie diese an eine foreign person, und Sie sind in 22 CFR 120.56, einer Weitergabe, und in einer Ausfuhr nach 22 CFR 120.50(a)(6). Der Mutterkonzern darf also das Chiffrat halten. Den Schlüssel darf er nicht halten. Ob Ihre konkrete Konstellation jede Bedingung der Ausnahme erfüllt, ist eine Feststellung Ihres Rechtsbeistands für Exportkontrolle.

Darf die IT-Abteilung unseres Mutterkonzerns unsere US-Systeme administrieren?

Nicht, ohne den Mutterkonzern in Ihr Assessment zu ziehen, und nicht, ohne zuerst die ITAR-Frage zu beantworten. DFARS 252.204-7012 definiert ein covered contractor information system als eines, das einem Auftragnehmer gehört oder von ihm oder für ihn betrieben wird und das kontrollierte Verteidigungsinformationen verarbeitet, speichert oder überträgt. Wenn der Mutterkonzern Ihre Systeme betreibt, sind diese Systeme covered contractor information systems, und die Umgebung des Mutterkonzerns liegt innerhalb Ihres CMMC-Geltungsbereichs. Davon getrennt: Ein Administrator, der ein Passwort zurücksetzen kann, kann den Zugriff auf das ermöglichen, was dieses Passwort schützt, und das ist der Weitergabemaßstab nach 22 CFR 120.56(a)(3). Die praktikable Antwort ist in der Regel eine Administration der Enklave durch US-Persons, während der Konzern alles außerhalb behält.

Erlaubt die Ausnahmeregelung für Kanada unserem kanadischen Mutterkonzern den Zugriff auf die technischen Daten unserer US-Tochtergesellschaft?

Nein, und das ist die häufigste Fehllesart im Kanada-Korridor. Die Ausnahme in 22 CFR 126.5 erlaubt die lizenzfreie Ausfuhr nicht klassifizierter Güter der US Munitions List und entsprechender Dienstleistungen aus den Vereinigten Staaten an eine in Kanada registrierte Person oder zur Endverwendung durch die kanadische Regierung, mit Ausschlüssen, und mit vorheriger Genehmigung der Directorate of Defense Trade Controls für Wiederausfuhr oder Weiterverbringung. Sie erlaubt eine Ausfuhr, in eine Richtung, unter Bedingungen. Sie gewährt einem kanadischen Mutterkonzern kein dauerndes Recht, auf ITAR-kontrollierte technische Daten zuzugreifen, die seine US-Tochtergesellschaft vorhält. Genau wegen dieser Fehllesart wird die auf US-Persons beschränkte Datengrenze gebaut. Was die Ausnahme auf Ihren Sachverhalt abdeckt, bestätigt Ihr Rechtsbeistand für Exportkontrolle.

Brauchen wir FOCI-Minderungsmaßnahmen, bevor wir ITAR-kontrollierte technische Daten vorhalten dürfen?

Das sind zwei Fragen auf zwei verschiedenen Zeitplänen. Die FOCI-Minderung ist das, was die Defense Counterintelligence and Security Agency verlangt, wenn ein Unternehmen in ausländischem Besitz die Berechtigung zum Zugang zu klassifizierten Informationen braucht, ausgehandelt mit der DCSA über Ihren auf sicherheitsermächtigte Betriebe spezialisierten Rechtsbeistand. Der Großteil der Zulieferfertigung im Verteidigungsbereich ist nicht klassifizierte Arbeit mit CUI und ITAR-Kontrolle, die niemals eine facility clearance braucht, sodass die FOCI-Minderung möglicherweise nie in Ihren Geltungsbereich fällt. Die auf US-Persons beschränkte Datengrenze funktioniert anders. Wenn Sie kontrollierte technische Daten vorhalten, gilt sie vom ersten Tag an, an dem Sie sie vorhalten. Zu wissen, welche Auftragsklasse Sie anstreben, entscheidet, ob FOCI überhaupt im Gespräch ist.

Verlangt CMMC US-Staatsbürger?

Diese Frage entscheidet CMMC nicht. Die Zugriffskontrollen nach NIST SP 800-171 fragen, ob ein Nutzer befugt ist, nicht, welchen Pass der Nutzer hält. ITAR ist das Regelwerk, das entscheidet, wer für exportkontrollierte technische Daten befugt werden kann, und eine foreign person braucht eine Lizenz oder eine Ausnahmeregelung. Die beiden setzen aufeinander auf, statt zu konkurrieren: ITAR zieht die Linie, die Kontrollen nach 800-171 setzen sie durch und protokollieren sie, und das Assessment für CMMC Level 2 bewertet, ob sie echt ist. Genau deshalb funktioniert es, sie als ein Programm zu bauen, und genau deshalb erzeugt es drei Antworten, die sich am Tor widersprechen, wenn man sie als drei Anbietergespräche baut.

Quellen

1. ITAR 22 CFR 120.63, foreign person (eCFR). Der Gründungstest, der einen ausländischen Mutterkonzern gegenüber seiner eigenen US-Tochtergesellschaft zu einer foreign person macht
   https://www.ecfr.gov/current/title-22/section-120.63
2. ITAR 22 CFR 120.62, U.S. person (eCFR). Jede Einheit, die in den Vereinigten Staaten zur Geschäftstätigkeit gegründet ist
   https://www.ecfr.gov/current/title-22/section-120.62
3. ITAR 22 CFR 120.50, export, einschließlich des deemed export technischer Daten an eine foreign person in den Vereinigten Staaten in (a)(2) (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.50
4. ITAR 22 CFR 120.33, technical data. Die funktionale Definition, die ohne Kennzeichnung greift (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.33
5. ITAR 22 CFR 120.54, Tätigkeiten, die keine Ausfuhr sind, einschließlich der Ausnahme für Ende-zu-Ende-Verschlüsselung in (a)(5) und ihrer Definition in (b) (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.54
6. ITAR 22 CFR 120.55, access information. Entschlüsselungsschlüssel, Netzwerkzugangscodes und Passwörter (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.55
7. ITAR 22 CFR 120.56, release. Die Nutzung von access information, um einer foreign person den Zugriff auf unverschlüsselte technische Daten zu ermöglichen (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.56
8. ITAR 22 CFR 120.65, ausländisches Eigentum und ausländische Kontrolle, wie ITAR sie für seine eigenen Zwecke definiert (eCFR)
   https://www.ecfr.gov/current/title-22/section-120.65
9. ITAR 22 CFR 126.5, Ausnahmeregelungen für Kanada (eCFR) und ihre Grenzen beim Zugriff eines ausländischen Mutterkonzerns auf kontrollierte technische Daten
   https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-126/section-126.5
10. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (acquisition.gov, Klausel datiert Mai 2024, Stand DFARS Change 5/7/2026)
    https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.
11. NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, an der Stelle, die DFARS 252.204-7012(b)(2)(i) zitiert
    https://csrc.nist.gov/publications/sp800
12. DoD CIO, About CMMC: die Aussetzung der Anforderungen der Phase II am 13. Juli 2026, die Pause in Phase 1 und CMMC Level 2 als Selbstbewertung alle drei Jahre anhand der 110 Anforderungen nach NIST SP 800-171 Revision 2 mit jährlicher Bestätigung im SPRS, unter der DFARS-Klausel 252.204-7012
    https://dodcio.defense.gov/CMMC/About/

13. DFARS 225.003 Definitions, qualifizierte Länder (acquisition.gov, Stand DFARS Change 5/7/2026)
https://www.acquisition.gov/dfars/225.003-definitions.

14. DCSA, Foreign Ownership, Control, or Influence (FOCI) und Minderungsmaßnahmen im Rahmen der facility clearance
https://www.dcsa.mil/Industrial-Security/Entity-Vetting-Facility-Clearances-FOCI/Foreign-Ownership-Control-or-Influence/

15. DoD-CIO Standards Guide for Foreign Partners (2023), das Kontroll-Overlay für US-Betriebe in ausländischem Besitz
https://dodcio.defense.gov/Portals/0/Documents/Library/StandardsGuideForeignPartners.pdf

16. American Rheinmetall erreicht CMMC Level 2 für seine US-Produktionsstandorte (14.04.2026)
https://www.rheinmetall.com/en/media/news-watch/news/2026/04/2026-04-14-american-rheinmetall-has-achieved-cmmc-level-2-certification-for-its-us-production-facilities

17. Standard Work 2.0, die operative Methode aus vier Säulen, und die Säule Sovereign Tier, in der die Datengrenzen gesetzt werden
/method

18. Das Playbook für den US-Markteintritt verbündeter Verteidigungshersteller, die vollständige Abfolge des operativen Aufbaus, in der dieses Papier steht
/resources/us-market-entry-playbook

19. Die Landezone Neuengland, wo verbündete Verteidigungszulieferer ihren US-Betrieb aufbauen
/resources/new-england-landing-zone

20. IT/OT-Konvergenz für Verteidigungshersteller: warum MES, ERP und SCADA drei Compliance-Risiken sind, bis sie eines sind
/blog/it-ot-convergence-defense-manufacturers

21. Onshoring-Playbook für ausländische Hersteller: den US-Fertigungsbetrieb im Verteidigungsbereich in 90 Tagen aufbauen
/blog/foreign-manufacturer-onshoring-90-day-playbook

NÄCHSTER SCHRITT

Ein strategisches Gespräch anfragen

garrettpartridge.com/booking