orka Newsletter | Commercial | IT-, KI- & Datenrecht | Öffentliches Wirtschaftsrecht und Vergaberecht

Cyber Resilience Act: Neue Cybersicherheitsanforderungen für vernetzte Produkte

Am 20. November 2024 wurde die Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates – **der sog. Cyber Resilience Act (CRA)** oder auf Deutsch: die Cyberresilienz-Verordnung – im Amtsblatt der Europäischen Union veröffentlicht. Der CRA ist eine produktrechtliche Vorschrift, die erstmals umfassende und unmittelbar geltende **Cybersicherheitsanforderungen für „Produkte mit digitalen Elementen"** auf EU-Ebene einführt.

Der CRA schließt damit eine bislang bestehende Regelungslücke: Während das bisherige Unionsrecht zwar sektorspezifische Cybersicherheitsvorschriften kannte, fehlte ein horizontaler Rechtsrahmen, der verbindliche Anforderungen an die Sicherheit von Hard- und Softwareprodukten über alle Branchen hinweg festlegt. Für **Unternehmen, die solche Produkte herstellen, einführen oder vertreiben**, besteht Handlungsbedarf – die zentralen Pflichten gelten ab dem 11. Dezember 2027.

Zielsetzung und zeitliche Anwendbarkeit

Der CRA verfolgt zwei zentrale Ziele:

- Zum einen sollen Produkte mit digitalen Elementen künftig mit **weniger**

Schwachstellen auf den Markt gebracht werden.
- Zum anderen sollen Hersteller **während des gesamten Produktlebenszyklus** konsequent für die Cybersicherheit ihrer Produkte Verantwortung übernehmen.

Flankierend soll mehr Transparenz für Nutzer geschaffen werden, damit diese bei der Auswahl und Verwendung von Produkten die Cybersicherheit besser berücksichtigen können.

Der CRA ist bereits am **10. Dezember 2024** in Kraft getreten. Für die Anwendbarkeit der einzelnen Regelungen gilt folgender gestaffelter Zeitplan:

- Ab dem **11. Juni 2026** gelten die Vorschriften über die Notifizierung von Konformitätsbewertungsstellen.
- Ab dem **11. September 2026** gelten die Meldepflichten der Hersteller für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle.
- Ab dem **11. Dezember 2027** gelten sämtliche übrigen Anforderungen des CRA, insbesondere die grundlegenden Cybersicherheitsanforderungen und die Herstellerpflichten.

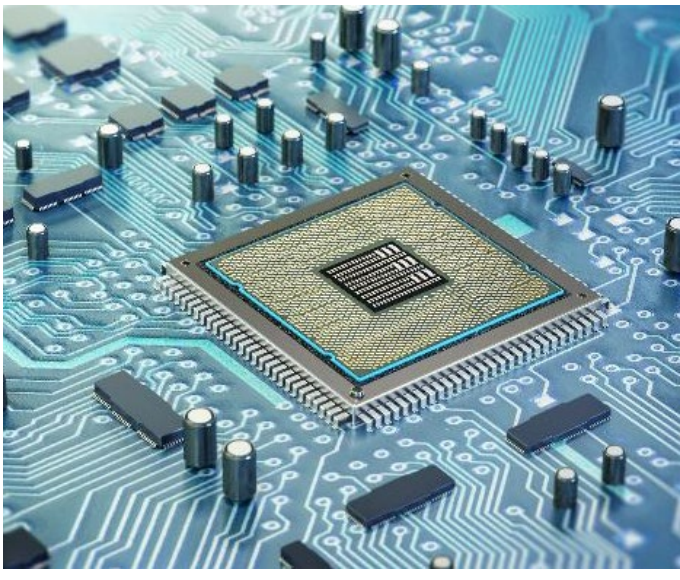
Wichtig für die Praxis: Produkte, die vor dem 11. Dezember 2027 in den Verkehr gebracht wurden, unterliegen den Anforderungen des CRA grundsätzlich nur dann, wenn sie nach diesem Datum einer wesentlichen Änderung unterzogen werden. Hiervon ausgenommen sind jedoch die **Meldepflichten nach Art. 14 CRA:** Diese gelten ab dem 11. September 2026 für alle in den Anwendungsbereich des CRA fallenden Produkte – also auch für solche, die bereits vor dem 11. Dezember 2027 in den Verkehr gebracht wurden.

Welche Produkte sind erfasst?

Der CRA gilt für auf dem Markt bereitgestellte „Produkte mit digitalen Elementen“, deren bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt.

„Produkte mit digitalen Elementen“ sind gemäß Art. 3 Nr. 1 CRA Software- oder Hardwareprodukte und deren Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in den Verkehr gebracht werden. Der Begriff ist bewusst weit gefasst:

- **Hardwareprodukte:** z.B. Router, Smartphones, industrielle Steuerungssysteme, vernetzte Maschinen, Mikrocontroller.
- **Softwareprodukte:** z.B. Betriebssysteme, mobile Apps, Firmware, Passwort-Manager, VPN-Software.
- **Komponenten:** z. B. Sicherheitsmodule oder Softwarebibliotheken, die separat auf dem Markt bereitgestellt werden.



Ebenfalls erfasst ist die **sog. „Datenfernverarbeitung“** (Art. 3 Nr. 2 CRA): Hierunter fällt eine entfernt stattfindende Datenverarbeitung, für die eine Software vom Hersteller selbst oder unter dessen Verantwortung konzipiert und entwickelt wird und ohne die das Produkt eine seiner Funktionen nicht erfüllen könnte.

Praktisches Beispiel: Eine Cloud-Funktion, die es Nutzern ermöglicht, ein smartes Haushaltsgerät aus der Ferne zu steuern, fällt als Datenfernverarbeitungslösung in den Anwendungsbereich des CRA.

Nicht erfasst sind hingegen Produkte ohne jegliche Datenverbindung (z.B. eine rein mechanische Maschine) sowie bestimmte Produktkategorien, für die Sonderregelungen gelten (z.B. Medizinprodukte, typgenehmigte Kraftfahrzeuge).

Besondere Konformitätsbewertungsanforderungen gelten für **zwei Sonderkategorien**:

- **Wichtige Produkte mit digitalen Elementen**: Produkte, bei denen die Ausnutzung von Schwachstellen besonders schwerwiegende Folgen haben kann, z.B. Firewalls, Betriebssysteme, Router, Passwort-Manager oder Mikrocontroller mit sicherheitsrelevanten Funktionen. Sie werden in Klasse I und Klasse II unterteilt.
- **Kritische Produkte mit digitalen Elementen**: Produkte mit besonders hohem Risikopotenzial, z.B. Hardware-Sicherheitsboxen oder Smart-Meter-Gateways. Für sie kann die Kommission per delegiertem Rechtsakt eine verpflichtende europäische Cybersicherheitszertifizierung vorschreiben.

Grundlegende Cybersicherheitsanforderungen

Produkte mit digitalen Elementen dürfen künftig nur dann auf dem Markt bereitgestellt werden, wenn sie die grundlegenden Cybersicherheitsanforderungen des Anhangs I CRA erfüllen. Diese gliedern sich in zwei Teile:

Produktbezogene Anforderungen (Anhang I Teil I CRA):

Produkte müssen so konzipiert, entwickelt und hergestellt werden, dass sie ein angemessenes Cybersicherheitsniveau gewährleisten. Konkret müssen sie – soweit **auf Basis der Risikoabwägung** anwendbar – insbesondere:

- ohne bekannte ausnutzbare Schwachstellen auf den Markt gebracht werden (z.B. durch Sicherheitstests vor dem Inverkehrbringen),
- mit einer sicheren Standardkonfiguration ausgeliefert werden (z.B. keine voreingestellten Standard-Passwörter, die für alle Geräte identisch sind),
- durch geeignete Authentifizierungs- und Zugangskontrollmechanismen vor unbefugtem Zugriff schützen,
- die Verfügbarkeit wesentlicher Funktionen auch nach einem Sicherheitsvorfall gewährleisten (z.B. Schutz vor Denial-of-Service-Angriffen).

Anforderungen an die Behandlung von Schwachstellen (Anhang I Teil II CRA)

Hersteller müssen während des gesamten Unterstützungszeitraums **aktiv Schwachstellen managen**. Dazu gehören insbesondere:

- unverzügliche Behebung von Schwachstellen und Bereitstellung von Sicherheitsaktualisierungen (soweit technisch möglich: getrennt von Funktionsupdates),
- kostenlose Bereitstellung von Sicherheitsaktualisierungen für Nutzer,
- regelmäßige Sicherheitstests und -überprüfungen,
- Einführung und Umsetzung einer Strategie für die koordinierte Offenlegung von Schwachstellen (Coordinated Vulnerability Disclosure Policy),
- Bereitstellung einer Kontaktadresse für die Meldung von Schwachstellen.

Der **Unterstützungszeitraum** muss die voraussichtliche Nutzungsdauer des Produkts widerspiegeln und beträgt grundsätzlich mindestens fünf Jahre. Bei Produkten, die erfahrungsgemäß länger genutzt werden (z.B. industrielle Steuerungssysteme, Router), ist ein entsprechend längerer Zeitraum vorzusehen.

Pflichten der Hersteller

Der CRA adressiert grundsätzlich **alle Wirtschaftsakteure in der Lieferkette** – also Hersteller, Bevollmächtigte, Einführer und Händler. Die umfangreichsten Pflichten treffen den Hersteller.

Hersteller müssen u. a.:

- eine Cybersicherheits-Risikoabwägung für ihr Produkt durchführen und deren Ergebnisse in sämtlichen Phasen – von der Planung über die Entwicklung bis zur Wartung – berücksichtigen,
- die technische Dokumentation gemäß Anhang VII CRA erstellen und mindestens zehn Jahre lang (oder für die Dauer des Unterstützungszeitraums, je nachdem, was länger ist) aufbewahren,
- eine EU-Konformitätserklärung ausstellen und die CE-Kennzeichnung anbringen,
- eine zentrale Anlaufstelle für Nutzer einrichten, über die Schwachstellen gemeldet werden können,
- das Enddatum des Unterstützungszeitraums klar und verständlich angeben (mindestens Monat und Jahr) sowie
- bei bekannt gewordener Nichtkonformität unverzüglich Korrekturmaßnahmen ergreifen oder das Produkt ggf. zurückrufen.

Meldepflichten der Hersteller

Hersteller sind außerdem verpflichtet, aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle, die die Sicherheit ihres Produkts beeinträchtigen, gleichzeitig dem zuständigen CSIRT (als Koordinator) und der ENISA über eine einheitliche Meldeplattform zu melden. Dabei gilt ein gestuftes Meldesystem:

- **Innerhalb von 24 Stunden:** Frühwarnung nach Kenntniserlangung,
- **Innerhalb von 72 Stunden:** Detaillierte Schwachstellen- bzw. Vorfallsmeldung,
- **Innerhalb von 14 Tagen** (bei Schwachstellen) **bzw. einem Monat** (bei Vorfällen): Abschlussbericht.

Achtung: Diese Meldepflichten gelten – abweichend von den übrigen CRA-Anforderungen – bereits ab dem 11. September 2026 und erfassen auch Produkte, die vor dem 11. Dezember 2027 in den Verkehr gebracht wurden.

Konformitätsbewertungsverfahren

Vor dem Inverkehrbringen müssen Hersteller ein Konformitätsbewertungsverfahren durchführen. Der CRA sieht **drei Module** vor:

- **Modul A (interne Kontrolle):** Selbstbewertung durch den Hersteller; grundsätzlich für alle Produkte der „Standardkategorie" zulässig sowie für wichtige Produkte der Klasse I, sofern harmonisierte Normen angewendet werden.
- **Modul B+C (EU-Baumusterprüfung):** Einbeziehung einer notifizierten Stelle; verpflichtend für wichtige Produkte der Klasse I ohne Anwendung harmonisierter Normen sowie für alle wichtigen Produkte der Klasse II.
- **Modul H (umfassende Qualitätssicherung):** Bewertung des gesamten Qualitätsmanagementsystems durch eine notifizierte Stelle; besonders geeignet für Hersteller mit vielen Produkttypen oder häufigen Updates.

Pflichten von Einführern und Händlern

Pflichten der Einführer

Einführer (Importeure) dürfen nur Produkte in den Verkehr bringen, die den grundlegenden Cybersicherheitsanforderungen des CRA entsprechen. Sie müssen vor dem Inverkehrbringen insbesondere sicherstellen, dass der Hersteller das vorgeschriebene Konformitätsbewertungsverfahren durchgeführt hat, die technische Dokumentation erstellt wurde und das Produkt die CE-Kennzeichnung trägt. Werden Schwachstellen bekannt, sind Einführer verpflichtet, den Hersteller unverzüglich zu informieren und bei erheblichen Cybersicherheitsrisiken auch die Marktüberwachungsbehörden zu unterrichten.

Pflichten der Händler

Händler müssen vor der Bereitstellung eines Produkts auf dem Markt prüfen, ob dieses die CE-Kennzeichnung trägt und ob die Informations- und Kennzeichnungspflichten des Herstellers und Einführers erfüllt sind. Auch Händler sind verpflichtet, bei bekannt gewordenen Schwachstellen oder Nichtkonformitäten den Hersteller zu informieren und ggf. Korrekturmaßnahmen zu veranlassen.

Erweiterung der Herstellerpflichten auf Einführer und Händler

Besondere Aufmerksamkeit verdient die Regelung der Art. 21 und 22 CRA: **Einführer und Händler werden kraft Gesetzes wie Hersteller behandelt** – mit der Folge, dass sie sämtliche Herstellerpflichten zu erfüllen haben –, wenn sie

- ein Produkt unter ihrem eigenen Namen oder ihrer eigenen Marke in den Verkehr bringen oder
- eine wesentliche Änderung an einem bereits in den Verkehr gebrachten Produkt vornehmen.

Praxishinweis: Unternehmen, die Produkte unter eigenem Label vertreiben (sog. White-Label-Produkte) oder bestehende Produkte modifizieren, sollten sorgfältig prüfen, ob sie dadurch in die Rolle des Herstellers im Sinne des CRA rücken – mit allen damit verbundenen Pflichten.

Sanktionen und Rechtsdurchsetzung

Der CRA sieht **empfindliche Sanktionen** vor, die den Druck zur Compliance erheblich erhöhen.

Verstöße können mit **Geldbußen von bis zu 15 Mio. EUR oder – bei Unternehmen – bis zu 2,5 % des weltweiten Jahresumsatzes** des vorangegangenen Geschäftsjahres geahndet werden (je nachdem, welcher Betrag höher ist).

Darüber hinaus eröffnet Art. 65 CRA die **Möglichkeit von Verbandsklagen**: Die Richtlinie (EU) 2020/1828 über Verbandsklagen findet auf Verstöße gegen den CRA Anwendung, die die Kollektivinteressen von Verbrauchern beeinträchtigen oder beeinträchtigen können. Verbraucherverbände und andere qualifizierte Einrichtungen können damit kollektive Rechtsschutzmaßnahmen gegen Wirtschaftsakteure einleiten, die ihren CRA-Pflichten nicht nachkommen.

Angesichts der **kurzen Umsetzungsfristen** – die ersten Pflichten (Meldepflichten) gelten bereits ab September 2026 – sollten betroffene Unternehmen jetzt mit der Analyse ihres Produktportfolios und der Vorbereitung auf die CRA-Anforderungen beginnen.

Ihre Ansprechpartner

Felix Meurer
Rechtsanwalt, Salary Partner

T +49 30 509320-117
felix.meurer@orka.law

Maria Najdenova
Rechtsanwältin, Salary Partnerin

T +49 211 60035-202
maria.najdenova@orka.law

Marieke Schwarz
Rechtsanwältin, Salary Partnerin

T +49 211 60035-422
marieke.schwarz@orka.law

Viktoria Gott, LL.M.
Rechtsanwältin, Senior Associate

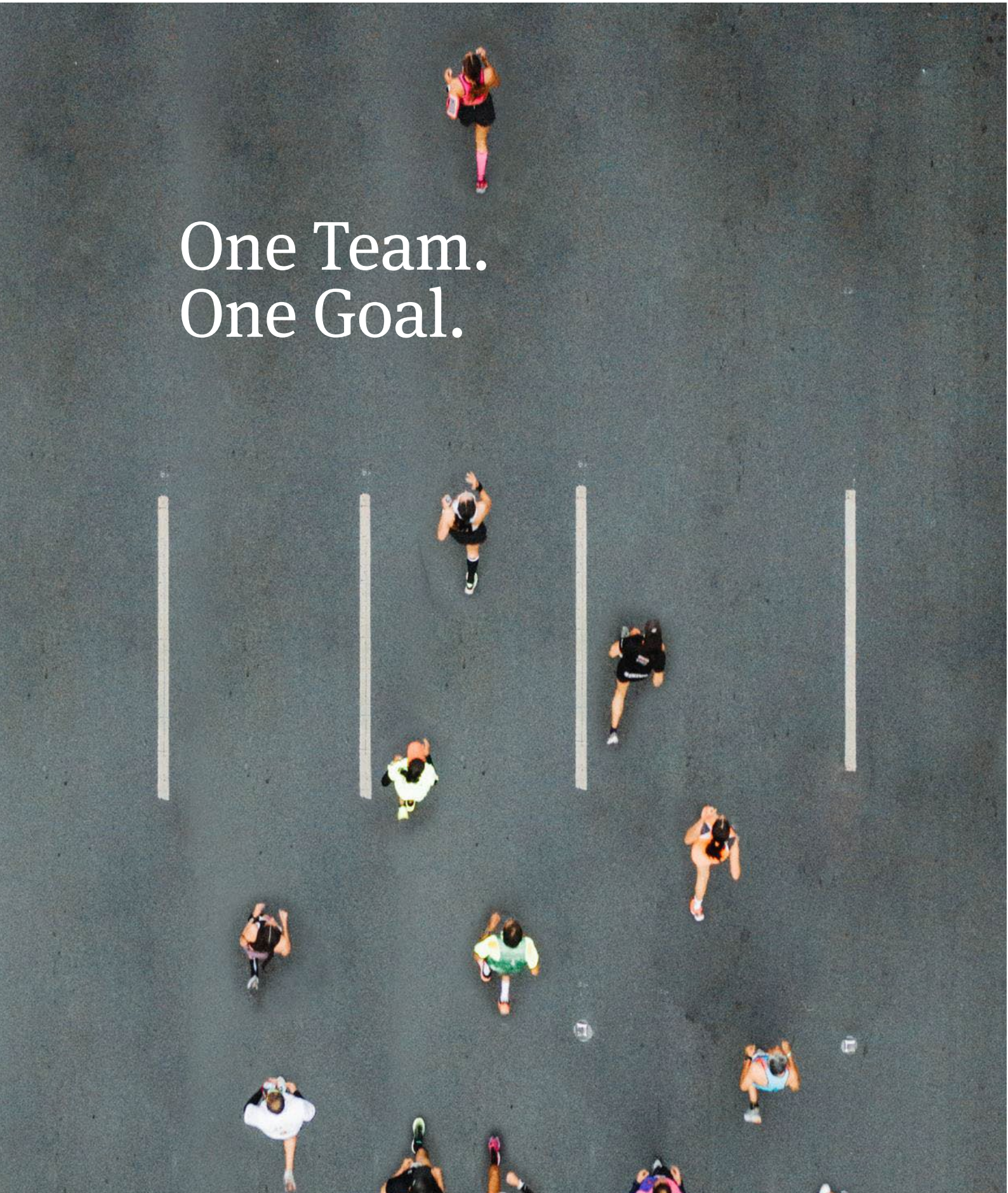
T +49 30 509320-144
viktoria.gott@orka.law

Gina Leder
Rechtsanwältin, Senior Associate

T +49 211 60035-256
gina.leder@orka.law

Nicola Lübke, LL.M.
Rechtsanwältin, Associate

T +49 211 60035-204
nicola.luebke@orka.law


One Team.
One Goal.