



TECHNOLOGIETRANSFER ZWISCHEN UNTERNEHMEN

Was unter Technologietransfer zu verstehen ist

Im exportkontrollrechtlichen Kontext bezeichnet Technologietransfer die Weitergabe von technischem Wissen, Daten oder Know-how an Empfänger außerhalb der Europäischen Union. Dabei spielt es keine Rolle, **auf welchem Weg die Information übertragen wird**. Entscheidend ist allein, dass kontrollierte Technologie einem Empfänger im Ausland zugänglich gemacht wird. Typische Formen des Technologietransfers sind beispielsweise:

- 🌐 Versand technischer Dokumentationen oder Baupläne per E-Mail, Bereitstellung von Entwicklungsdaten in Cloud-Systemen, Video-Konferenzen oder Telefonate mit technischen Erläuterungen, Versand von Datenträgern mit Konstruktionsunterlagen, Schulungen oder technische Beratungen für ausländische Partner

Schon ein einzelnes technisches Detail kann exportkontrollrechtlich relevant sein, wenn es sich auf kontrollierte Technologien bezieht.

Rechtlicher Rahmen in Deutschland und der EU

Der rechtliche Rahmen ergibt sich aus 3 zentralen Regelwerken: Das Außenwirtschaftsgesetz (AWG) definiert Ausfuhr ausdrücklich nicht nur als physischen Warenexport, sondern auch als „nicht gegenständliche Übermittlung von Software oder Technologie“ – etwa per E-Mail oder Cloud. Die Außenwirtschaftsverordnung (AWV) konkretisiert die genehmigungspflichtigen Güter und Technologien in der Ausfuhrliste. Auf EU-Ebene ergänzt die Dual-Use-Verordnung (EU) 2021/821 diese Vorgaben mit einer europaweit gültigen Liste für Güter mit doppeltem Verwendungszweck. Zuständige Genehmigungsbehörde ist das BAFA.

Wann ein Technologietransfer genehmigungspflichtig ist

Eine Genehmigungspflicht entsteht immer dann, wenn kontrollierte Technologie ins Ausland übertragen wird. Das betrifft nicht nur klassische Dokumente oder Datenträger. Auch digitale Übertragungen oder Gespräche können eine genehmigungspflichtige Ausfuhr darstellen. Typische Beispiele sind:

- 🌐 Versand einer Konstruktionszeichnung an einen Partner außerhalb der EU
- 🌐 Zugriff eines ausländischen Mitarbeiters auf Entwicklungsdaten
- 🌐 Präsentation technischer Details auf einer internationalen Konferenz
- 🌐 Nutzung einer Cloud, deren Server außerhalb der EU stehen

Besonders kritisch sind Fälle, in denen Technologie für militärische Zwecke oder für sensible Anwendungen genutzt werden könnte. In solchen Fällen greifen zusätzliche Vorschriften, beispielsweise im Zusammenhang mit Rüstungsgütern oder Dual-Use-Technologien.

Cloud, Homeoffice und digitale Zusammenarbeit

Die Digitalisierung hat das Thema Technologietransfer erheblich komplexer gemacht. Viele Unternehmen speichern Entwicklungsdaten heute in Cloud-Systemen oder arbeiten in internationalen Projektteams. Dadurch können technische Informationen automatisch über Ländergrenzen hinweg verfügbar werden. *Ein Beispiel:*

Wird eine technische Datei in eine Cloud hochgeladen, deren Server sich außerhalb der EU befinden, kann bereits dies als Technologietransfer gelten. Gleiches gilt, wenn ein Mitarbeiter aus einem Drittland auf diese Daten zugreift.

Unternehmen müssen daher genau prüfen,

- 🌐 wo ihre Daten gespeichert werden,
- 🌐 wer Zugriff auf diese Daten hat, und
- 🌐 aus welchen Ländern auf diese Daten zugegriffen wird.

Technische Unterstützung als Sonderfall

Neben der Weitergabe von Daten wird auch **technische Unterstützung** exportkontrollrechtlich erfasst. Darunter fallen beispielsweise:

- 🌐 technische Schulungen
- 🌐 Wartungsanleitungen
- 🌐 Beratung zur Entwicklung oder Nutzung eines Produkts
- 🌐 Unterstützung bei Installation oder Betrieb

Wenn solche Leistungen für Unternehmen oder Personen in bestimmten Ländern erbracht werden oder sich auf kontrollierte Technologien beziehen, kann ebenfalls eine Genehmigungspflicht bestehen.

Ausnahmen von der Exportkontrolle

Nicht jede technische Information unterliegt der Exportkontrolle. Bestimmte Kategorien sind ausdrücklich ausgenommen, insbesondere:

- 🌐 **allgemein zugängliche Informationen**, etwa veröffentlichte Fachliteratur
- 🌐 **Grundlagenforschung**, die nicht auf konkrete Anwendungen ausgerichtet ist
- 🌐 **Informationen im Rahmen von Patentanmeldungen**

Sobald Informationen jedoch vertraulich sind oder konkrete technische Anwendungen betreffen, können sie exportkontrollrechtlich relevant werden.

Typische Risiken in der Unternehmenspraxis

In der Praxis entstehen Verstöße häufig nicht durch bewusste Umgehung, sondern durch fehlendes Bewusstsein. Viele Mitarbeiter verbinden Exportkontrolle ausschließlich mit physischen Waren. Dass auch ein E-Mail-Anhang oder eine Präsentation auf einer Konferenz exportkontrollrechtlich relevant sein kann, ist oft nicht bekannt. Zu den häufigsten Risiken gehören daher:

- 🌐 Versand technischer Dokumente ohne Exportkontrollprüfung
- 🌐 Zugriff ausländischer Mitarbeiter auf Entwicklungsdaten
- 🌐 unkontrollierte Nutzung von Cloud-Diensten
- 🌐 Schulungen oder Beratungen ohne vorherige Prüfung der Genehmigungspflicht

Hinzu kommt, dass die Kontrolllisten immer umfangreicher werden – etwa in Bereichen wie KI, Mikroelektronik oder Quantentechnologie.

Was Unternehmen jetzt tun sollten

Um Risiken zu vermeiden, sollten Unternehmen ein funktionierendes **Exportkontroll-Compliance-System** aufbauen. Dazu gehören insbesondere:

- 🌐 Definieren Sie klare interne Zuständigkeiten für die Exportkontrolle und schulen Sie Ihre Mitarbeiter regelmäßig.
- 🌐 Klassifizieren Sie Ihre Produkte und Technologien eindeutig und prüfen Sie Empfänger, Länder und Endverwendungen sorgfältig.
- 🌐 Sichern Sie Ihre IT-Strukturen für den Umgang mit sensiblen Daten.

Ein solches System hilft nicht nur, Verstöße zu vermeiden, sondern kann im Ernstfall auch bußgeldmindernd berücksichtigt werden. Technologietransfer ist heute ein zentraler Bestandteil internationaler Zusammenarbeit – gleichzeitig aber auch ein sensibles Feld der Exportkontrolle. Für Sie als Unternehmen bedeutet das: Nicht nur Güterlieferungen müssen geprüft werden, sondern auch der Austausch von technischem Wissen.