



Forensic & Integrity Services

Denkanstöße

Haben Sie Ihre Datentransfers an
Drittländer im Griff?



Sechs Schritte, um die Compliance-Standards bei Datentransfers zu erfüllen

Haben Sie als Verantwortlicher oder Auftragsverarbeiter geprüft, ob bei einer Datenübermittlung die allgemeinen DSGVO-Voraussetzungen erfüllt sind und den Anforderungen nach Kapitel V der DSGVO entsprochen wird?



Faktoren, die zur Komplexität von Datentransfers beitragen

Datentransfers sind für Unternehmen aus mehreren Gründen komplex:

1. **Unterschiedliche Datenschutzgesetze:** Nicht jede länderspezifische Datenschutzregelung entspricht den Anforderungen der europäischen Datenschutz-Grundverordnung (DSGVO).
2. **Technische Herausforderungen:** Der sichere Transfer von Daten erfordert oft eine erhebliche technische Infrastruktur und technische Expertise.
3. **Vertragsrechtliche Aspekte:** Durch Standardvertragsklauseln, verbindliche Unternehmensregeln (Binding Corporate Rules) oder andere Instrumente ist eine DSGVO-konforme Datenverarbeitung sicherzustellen.
4. **Rechtsunsicherheit:** Gerichtliche Entscheidungen wie das Schrems-II-Urteil oder der EU-US-Angemessenheitsbeschluss vom 10. Juli 2023 zwingen Unternehmen, ihre Praktiken zur Datenübertragung regelmäßig zu prüfen und ggf. zu ändern.

Datentransfers erfordern von Unternehmen einen durchdachten und sorgfältig verwalteten Ansatz.

Dazu ein paar Denkanstöße ...

Kennen Sie Ihre internationalen Datentransfers?

#1

Erfassung und Klassifizierung von Daten

Wissen Sie, ...

- ▶ ... welche Arten von Daten Sie verarbeiten? Klassifizieren Sie Ihre Daten, um die Grundlage einer Datensicherheitsstrategie zu schaffen und sensible Daten zu identifizieren.
- ▶ ... wo diese Daten gespeichert werden? Stellen Sie sicher, dass nur autorisierte Personen darauf zugreifen können.
- ▶ ... welche Daten außerhalb der EU transferiert werden und wie diese geschützt sind? Führen Sie ein internes Assessment durch.

Länderübergreifende Unternehmen brauchen
länderübergreifende Lösungen

#2

Übertragungsmechanismen

Welche geeigneten Mechanismen nutzen Sie?

- ▶ Prüfen Sie das Vorliegen eines Angemessenheitsbeschlusses.

Am 10. Juli hat die EU-Kommission einen Angemessenheitsbeschluss für die Datenübertragung zwischen der EU und den USA erlassen. Das Data Privacy Framework enthält aber auch neue Verpflichtungen und jährliche Zertifizierungen für US-Unternehmen. Außerdem werden bereits jetzt Probleme mit der US-Überwachung und der Massendatenerfassung erwartet, sodass es fraglich ist, ob sich Unternehmen dem Data Privacy Framework anschließen werden.

- ▶ Nutzen Sie die Standardvertragsklauseln oder Binding Corporate Rules in Verbindung mit zusätzlichen Sicherheitsmaßnahmen und einem Transfer Impact Assessment und prüfen Sie ggf. andere rechtliche Instrumente wie beispielsweise Industrie-Kodizes als Basis.
- ▶ Regeln Sie die regelkonforme Datenverarbeitung bei Ihren Auftragsverarbeitern.

Regelkonform zu agieren setzt voraus zu wissen, was „regelkonform“ bedeutet

#3

Kenntnis der Datenschutzregelungen

Halten Sie geltende Datenschutzgesetze ein?

- ▶ Es gelten die eigenen Datenschutzgesetze wie auch die Datenschutzvorschriften der Länder, in die Sie Daten übertragen.
- ▶ Verstehen und interpretieren Sie die geltenden Datenschutzgesetze beim Transfer in Drittländer.
- ▶ Definieren Sie angemessene Maßnahmen, um die Datenschutzgesetze und -vorschriften einzuhalten.

Identifizieren Sie Ihr mögliches Problem

#4

Risikobewertung

Was soll bei einer Risikobewertung getan werden?

- ▶ Identifizieren Sie die möglichen Risiken im Rahmen der Datenübertragung in ein Drittland, insbesondere durch staatliche Eingriffe.
- ▶ Bewerten Sie das Risiko und die Risikoquellen nach Eintrittswahrscheinlichkeiten und der Schwere der Folgen für den Schutz der personenbezogenen Daten.
- ▶ Identifizieren Sie zusätzliche Maßnahmen, um ein im Drittland gleichwertiges Schutzniveau zu gewährleisten.
- ▶ Dokumentieren Sie Ihre Risikobewertung und schließen Sie diese mit einem nachvollziehbaren Urteil ab.

Schützen Sie die Ihnen anvertrauten
personenbezogenen Daten

#5

Implementierung von Sicherheitsmaßnahmen

Geben Sie Ihr Bestmögliches, um die Sicherheit der
Daten zu gewährleisten!

- ▶ Ergreifen Sie technische und organisatorische Maßnahmen.
- ▶ Schützen Sie Ihre Daten durch Verschlüsselung, Pseudonymisierung und Zugriffskontrollen.
- ▶ Führen Sie regelmäßig Sicherheitskontrollen durch.
- ▶ Fertigen Sie ein Notfallprotokoll an.

Entwicklungen und Veränderungen brauchen den Überblick

#6

Stetige Überwachung und Überprüfung

Sind Ihre Maßnahmen nachhaltig?

- ▶ Überprüfen Sie regelmäßig die vom Transfer betroffenen Datenverarbeitungsprozesse unter Einhaltung der Datenschutzgesetze und -vorschriften.
- ▶ Stellen Sie sicher, dass alte wie auch neue Auftragsverarbeiter in Drittländern datenschutzkonform sind, und führen Sie Third Party Risk Assessments durch.
- ▶ Schaffen Sie interne Prozesse, um Datentransfers bei beispielsweise Änderungen der Rechtslage auszusetzen oder zu beenden.

“

Ein sorgfältiger Datentransferprozess ist für Unternehmen unerlässlich. Er fördert die Einhaltung der gesetzlichen Vorschriften, schützt vor Sanktionen und bewahrt den guten Unternehmensruf.

Durch effektive Risikobewertungen, geeignete Sicherheitsmaßnahmen, sichere Verträge und kontinuierliche Überwachung verbessert ein solider Prozess die allgemeine Datensicherheit und minimiert Datenschutzverletzungen.

Insgesamt ist ein durchdachter Datentransferprozess unerlässlich für den Schutz personenbezogener Daten und das Vertrauen in das Unternehmen.



Meribeth Banaschik

Partner | Forensic & Integrity Services

Ihre Kontakte



Meribeth Banaschik

Partner | Forensic & Integrity Services |
EY's Europe West Chief Innovation Officer

Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft
Börsenplatz 1
50667 Köln

Telefon +49 160 939 14325
meribeth.banaschik@de.ey.com
[LinkedIn](#)



Gesa Pari Schatz

Senior Manager, CIPM, CFE
Forensic & Integrity Services

Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft
Graf-Adolf-Platz 15
40213 Düsseldorf

Telefon +49 160 939 13987
gesa.pari.schatz@de.ey.com
[LinkedIn](#)



Jenny Le

Senior Manager, Esq. FIP, CIPP/E, CIPM
Forensic & Integrity Services

Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft
Arnulfstraße 59
80636 München

Telefon +49 160 939 11436
jenny.w.le@de.ey.com
[LinkedIn](#)



Weitere Informationen finden Sie unter de.ey.com/infogov

Mit unserer Arbeit setzen wir uns für eine besser funktionierende Welt ein. Wir helfen unseren Kunden, Mitarbeitenden und der Gesellschaft, langfristige Werte zu schaffen und das Vertrauen in die Kapitalmärkte zu stärken.

In mehr als 150 Ländern unterstützen wir unsere Kunden, verantwortungsvoll zu wachsen und den digitalen Wandel zu gestalten. Dabei setzen wir auf Diversität im Team sowie Daten und modernste Technologien in unseren Dienstleistungen.

Ob Assurance, Tax & Law, Strategy and Transactions oder Consulting: Unsere Teams stellen bessere Fragen, um neue und bessere Antworten auf die komplexen Herausforderungen unserer Zeit geben zu können.

„EY“ und „wir“ beziehen sich in dieser Präsentation auf alle deutschen Mitgliedsunternehmen von Ernst & Young Global Limited (EYG). Jedes EYG-Mitgliedsunternehmen ist rechtlich selbstständig und unabhängig. Ernst & Young Global Limited ist eine Gesellschaft mit beschränkter Haftung nach englischem Recht und erbringt keine Leistungen für Mandanten. Informationen darüber, wie EY personenbezogene Daten sammelt und verwendet, sowie eine Beschreibung der Rechte, die Einzelpersonen gemäß der Datenschutzgesetzgebung haben, sind über ey.com/privacy verfügbar. Weitere Informationen zu unserer Organisation finden Sie unter ey.com.

In Deutschland finden Sie uns an 20 Standorten.

© 2023 Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft
All Rights Reserved.

ED None

ey.com/de