Luther.

Erste-Hilfe-Paket „Schrems II“-Compliance

Nachdem der Europäische Gerichtshof (EuGH) den EU-US Privacy Shield in der Sache „Schrems II“ für ungültig erklärt hat, stehen Unternehmen nun vor der Frage, wie sie mit diesem Urteil umgehen. Die Entscheidung hat bereits jetzt erhebliche Auswirkungen auf die datenschutzrechtliche Bewertung von Datentransfers außerhalb der EU/des EWR – insbesondere in die USA. Eine Rechtfertigung über den Privacy Shield ist nicht mehr möglich. Aber auch Standarddatenschutzklauseln sind, trotz ihrer Wirksamkeit, zunehmend kritisch zu sehen. Nach Ansicht einiger Datenschutzaufsichtsbehörden sind sie nicht mehr ohne Weiteres dazu geeignet, internationale Datentransfers zu rechtfertigen. Eine schnelle Abhilfe ist nicht in Sicht, da die kritischen Punkte sich überwiegend auf die Ausgestaltung des Privacy Shields sowie die geltende Rechtslage in den USA beziehen.

Unternehmen sollten daher ihre Datenübermittlungen, u. a. in die USA und andere sog. unsichere Drittstaaten (z. B. China, Russland, Mittlerer Osten), überprüfen und zusätzliche Maßnahmen treffen, um ein ausreichendes Datenschutzniveau herzustellen. Wenn keine ausreichenden Vorkehrungen getroffen werden können, könnten ggf. auch Exit-Strategien erforderlich sein. Zur Vermeidung solcher möglicherweise schwerwiegenden Konsequenzen und bis zu einer konkreten Hilfestellung der Datenschutzaufsichtsbehörden bietet sich das folgende, vorläufige Maßnahmenpaket an, um Datentransfers zu evaluieren, Risiken zu identifizieren und zu adressieren:

Schritt 1

- Identifizierung internationaler Datentransfers und eingesetzter Drittstaaten-Dienstleister
- Differenzierung US-Privacy Shield/Standarddatenschutzklauseln
- Kategorisierung des jeweiligen Datentransfers nach Risikopotenzial anhand der Self Assessment Checkliste (siehe anbei)

Schritt 2

- Prüfung der vorhandenen Vereinbarungen und getroffenen Maßnahmen
- Vendor Due Diligence: Befragung der Datenimporteure zu Safeguards und Risikoeinschätzung (insbesondere ob dieser seine Pflichten nach den Standarddatenschutzklauseln einhalten kann)

Schritt 3

- **Zusätzliche** technisch-organisatorische Maßnahmen, z. B. stärkere Verschlüsselung, umsetzen
- **Zusätzliche** Pflichten/Absicherungen umsetzen bzw. vereinbaren (Informationspflichten, Ergänzung Standarddatenschutzklauseln)

Schritt 4

- Prüfung von Alternativen zur Legitimierung von internationalen Datentransfers (z. B. BCR, Erweiterung der Einwilligung etwa bei Cookies)
- Dokumentation und Evaluation

Schritt 5

- Erstes Maßnahmenpaket zur Absicherung von internationalen Datentransfers
- Nachweisbarkeit gegenüber Datenschutzaufsichtsbehörden sicherstellen (= Verringerung des Risikos von Auflagen und Bußgeldern)
- Allgemein: Überblick über internationale Datentransfers und Risiken, Compliance-Nachweis
- Entscheidungsgrundlage für Risikobewertungen und Exit-Strategien
- Prozessoptimierungen für Beauftragung und regelmäßige Kontrolle eingesetzter Dienstleister

Self Assessment Checkliste - Risikobewertung Internationaler Datentransfer nach Schrems II

Risikofaktoren (Beispiele)

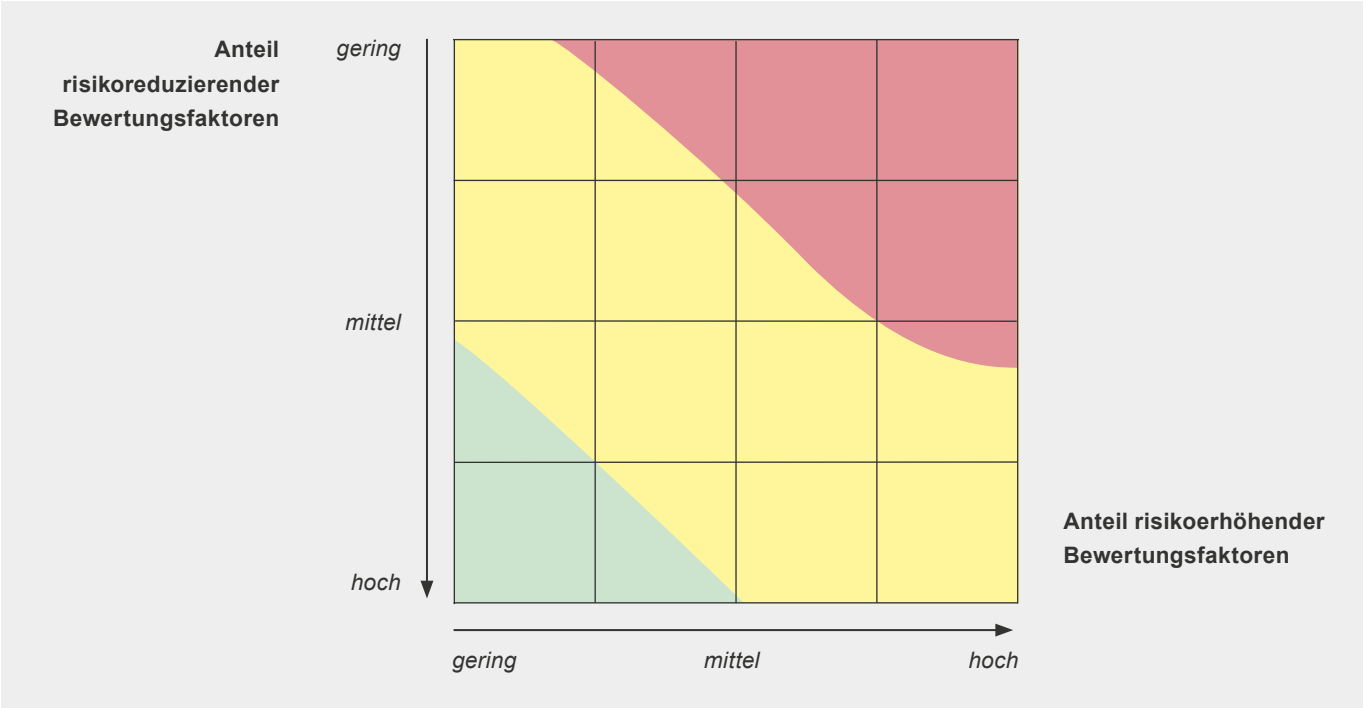
	Risikofaktor „Zielland“	Auswirkung Risiko*
Risikoerhöhende Faktoren / Maßnahmen	Kritisches Drittland wie bspw. USA, China, Russland, Mittlerer Osten (ggf. zukünftig auch UK)	
	Besondere Risiken für staatliche Zugriffe aufgrund nationaler Sicherheitsgesetze (z. B. FISA 702, EO 12333)	
	Eingeschränkte Rechtsschutzmöglichkeiten für EU-Betroffene	
	Risikofaktor „Dienstleister/Datenimporteur“	
	Telekommunikationsdiensteanbieter	
	Anbieter elektronischer Kommunikationsleistungen (E-Mail, Video, Messenger, etc.)	
	Cloud-Provider	
	Dienstleister/Datenimporteur war in der Vergangenheit bereits Adressat staatlicher Zugriffsmaßnahmen	
	Analyse-/Trackingdienstleister (z. B. Webseiten-Tracking)	
	Anbieter nachrangiger IT-Services (Wartung/Pflege, Support, etc.)	
	Gruppeninterner Datentransfer / Dienstleister	
	Risikofaktor „Art der Daten“	
	Besondere Kategorien personenbezogener Daten (Gesundheit, Religion, etc.)	
	Sensible Bank- und Finanzdaten	
	HR-Daten	
	Bestandsdaten von Arbeitnehmern oder Endkunden (Kontaktdaten, E-Mail-Adresse, User-Name)	
	Nutzungsdaten (LogIn-Daten, Webtracking-Daten, ohne Standortlokalisation)	
Risikoreduzierende Faktoren / Maßnahmen	Standarddatenschutzklauseln mit erweiterten Verpflichtungen/Sicherungsmaßnahmen, insb. transparente Information und ggf. Genehmigung durch Datenexporteur bei behördlichen Zugriffen	
	Erweiterung Betroffenenrechte / Ausgleich Rechtsschutzdefizite	
	Compliance-Bestätigung Dienstleister	
	Zertifizierungen des Dienstleisters zu Datenschutz/Datensicherheit	
	Einbindung Betroffener - Einwilligungslösung	
	Binding Corporate Rules (BCR)	
	Verhaltensregeln/Code of Conducts	
	Beschränkung auf pseudonyme Daten / Tokenization	
	Datenlokalisation EU/EWR (Container-Lösung, Treuhänder-Modell)	
	Verschlüsselungsmaßnahmen	
	Sonstige technische oder organisatorische Sicherheitsvorkehrungen zur Einschränkung von Zugriffen	

* Legende Risikoauswirkung	- risikoerhöhend -	- risikoneutral - Risiko vorhanden, aber nicht erhöht	- risikoreduzierend -

Die Einstufung der Risikoauswirkungen erfolgt auf Grundlage von Best Practices und ohne Übernahme einer Haftung.

Matrix Ergebnisauswertung – Kategorisierung des Risikopotenzials

Die ermittelten Risikofaktoren können anhand dieser Matrix den risikoreduzierenden Maßnahmen gegenübergestellt und so das Risikopotential für den jeweiligen internationalen Datentransfer leicht bestimmt werden. Auf dieser Basis sind sodann ggf. weitere Maßnahmen je nach Risikoklassifizierung abzuleiten.



Risikokategorie 1	Risikokategorie 2	Risikokategorie 3
Exit-Strategie/Alternative zum Drittlandtransfer erforderlich	Einsatz Standarddatenschutzklauseln mit Anpassungen vertretbar	Einsatz Standarddatenschutzklauseln grds. unbedenklich

Ihre Ansprechpartner

Dr. Michael Rath
Rechtsanwalt, Partner
Fachanwalt für IT-Recht
Köln
T +49 152 016 25745
michael.rath@
luther-lawfirm.com

Silvia C. Bauer
Rechtsanwältin, Partnerin
Köln
T +49 221 9937 25789
silvia.c.bauer@
luther-lawfirm.com

Dr. Stefanie Hellmich, LL.M.
Rechtsanwältin, Partnerin
Frankfurt a.M.
T +49 69 27229 24118
stefanie.hellmich@
luther-lawfirm.com

Christian Kuß, LL.M.
Rechtsanwalt, Partner
Köln
T +49 221 9937 25686
christian.kuss@
luther-lawfirm.com