

Financial institutions  
Energy  
Infrastructure, mining and commodities  
Transport  
Technology and innovation  
Life sciences and healthcare

---

 **NORTON ROSE FULBRIGHT**

# EU-Datenschutzreform: Neue Pflichten für Kunden und Datacenter-Provider

Dr. Christoph Ritzer  
Norton Rose Fulbright LLP  
4. November 2015



# Agenda

- Stand, Verfahrensablauf und Zeitplan
- Was ändert sich?
- Aktuell: EuGH zu Safe Harbor und Konsequenzen
- Zusammenfassung und Fazit für Kunden und Datacenter Provider

# Stand, Verfahrensablauf und Zeitplan

# Aktueller Stand

- Europäische Kommission: Kommissar Věra Jourová
  - Kommission verabschiedet eigenen Vorschlag im Jan 2012
- Europäisches Parlament: Jan Philipp Albrecht MEP (rapporteur)
  - Liebe-Ausschuss einigt sich auf Text im Nov 2013
  - angenommen von der Vollversammlung im März 2014
- Rat der Europäischen Union: Luxemburg hat Präsidentschaft inne
  - Derzeitiger Vorsitzender ist Felix Braz, Justizminister (Luxemburg)
  - Einigung auf eigenen Entwurf im Juni 2015
- Wo stehen wir?
  - Zusage eine Einigung bis Ende des Jahres zu erreichen
  - DRPJ: Stellt eine weitere Herausforderung im Hinblick auf den Zeitplan dar
  - Politische Einigung ist im Januar zu erwarten, Verzögerung wegen formeller Verabschiedung und EiF



# Welche Gesetze werden sich ändern?

## Neues Recht

- Datenschutz-Grundverordnung (DGV) - Vorschlag für Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
- Datenschutzrichtlinie für Polizei und Justiz (DRPJ) - Vorschlag für Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr.

## Auswirkungen auf bestehender Recht

- EU-Datenschutzrichtlinie (95/46/EG) – wird aufgehoben
  - Folge: Deutsches Bundesdatenschutzgesetz wird weitgehend durch EU-Recht ersetzt
- ePrivacy-Richtlinie (2002/58/EG) – wird angepasst
  - Folge: Anpassungen in einigen Deutschen Gesetzen

# Überblick über den Verlauf des Trilogs

## Bisherige Sitzungen:

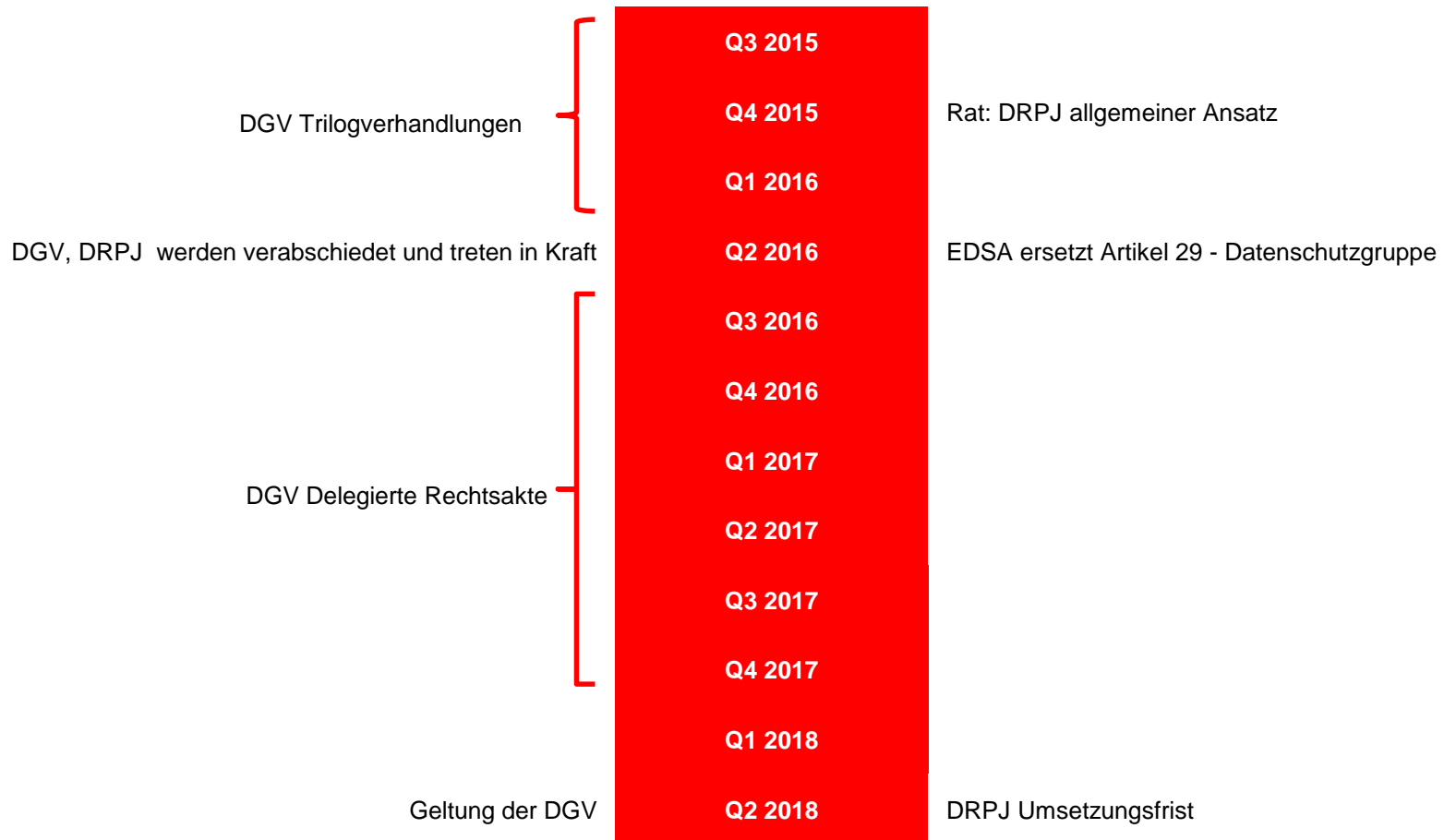
- **15. Juni, Luxemburg – Rat der Justizminister**
  - Einigung auf eigenen Entwurf im June 2015
- **24. Juni, Brüssel – 1. Trilogsitzung**
  - [Festlegung des Rates hinsichtlich Datenschutzrichtlinie für Polizei und Justiz]
  - Einigung auf grundsätzlichen Zeitplan der Verhandlungen des Trilogs
  - Allgemeiner Ansatz hinsichtlich delegierter Rechtsakte und Durchführungsakte
- **14. Juli, Brüssel – 2. Trilogsitzung**
  - Räumlicher Anwendungsbereich (Art. 3)
  - Internationale Datenübermittlungen (Kapitel V)
- **16. und 29. September – 3. und 4. Trilogsitzung**
  - Grundsätze (der Datenschutzgrundverordnung) (Kapitel II)
  - Rechte der betroffenen Personen (Kapitel III)
  - **Verantwortliche Stelle und Auftragsdatenverarbeiter (Kapitel VI)**

- **15. und 28. Oktober – 5. und 6. Trilogsitzung**
  - Aufsichtsbehörden (Kapitel VI)
  - Zusammenarbeit und Kohärenz (Kapitel VII)
  - Rechtsbehelfe, Haftung und Sanktionen (Kapitel VIII)

## Weiterer Zeitplan des Trilogs:

- **11. und 25. November – 7. und 8. Trilogsitzung**
  - Ziele und sachlicher Anwendungsbereich (Kapitel I)
  - Spezialvorschriften (Kapitel IX)
- **Dezember – 9. Trilogsitzung**
  - Delegierte Rechtsakte und Durchführungsakte (Kapitel X)
  - Schlussbestimmungen (Kapitel XI)
  - Sonstige offene Fragen

# DGV - Zeitplan



# Einzelne Änderungen



# Überblick: Wesentliche Änderungen

- Räumlicher Anwendungsbereich
- Harmonisierung und „one stop shop“
- Haftung und Sanktionen
- Änderungen hinsichtlich dem angemessenen Umgang mit Daten und der Einwilligung
- Erstellung von Profilen und “Big Data”
- Betroffenenrechte (z.B. Recht zum Vergessenwerden)
- Umsetzung im Alltag und Datenschutzbeauftragte
- Benachrichtigungspflichten bei Datenschutzverletzungen
- Haftung des Auftragsdatenverarbeiters
- Datenexport

# Räumlicher Anwendungsbereich

- **Wie bisher:** Wie bei der Richtlinie 95/46 gilt die DGV, wenn Verarbeitung im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen erfolgt.
- **NEU:** Anwendungsbereich wird ausgeweitet auf Unternehmen außerhalb der EU:

Zurückgreifen auf Mittel in der EU wird ersetzt durch:

- Anbieten von Waren oder Dienstleistungen an betroffenen Personen in der Union; oder
- Beobachtung ihres Verhaltens, soweit ihr Verhalten in der Europäischen Union erfolgt
- Ernennung eines Vertreters in einem EU-Mitgliedstaat, in dem die maßgeblichen EU-Bürger ansässig sind (Art. 25); sonst droht eine Geldbuße

Vertreter muss

- (i) Aufzeichnungen zu der Verarbeitung seiner Stelle führen;
- (ii) beauftragt werden, bei allen Fragen an Stelle der Verarbeiters als Anlaufstelle zu dienen;
- (iii) sich Durchsetzungsmaßnahmen gegen die verantwortliche Stelle unterwerfen
- Vertreter muss über relevante Verarbeitungstätigkeiten in Kenntnis gesetzt und von der Haftung freigestellt werden,

# Harmonisierung

- Verordnung – gilt unmittelbar in allen 28 MS, kein Umsetzungserfordernis hört sich deutlich einfacher an...ist es die Lösung?
- Vereinheitlichung bedeutet mehr Einfluss für Europäischen Datenschutzausschuss (EDSA) und die Kommission
- Einheitlichkeit bedeutet grundsätzlich der größte gemeinsame Nenner
- Verleiht jedoch MS die Befugnis in einigen Bereichen unterschiedliche Regelungen einzuführen
  - Möglichkeit spezifischere Vorschriften hinsichtlich der Verarbeitung von Arbeitnehmerdaten im Beschäftigungskontext zu erlassen (Art. 82)
  - Ausnahmen für Meinungs- und Pressefreiheit (Art. 81)
  - Ausnahmen für im öffentlichen Interesse liegende Archivzwecke und für wissenschaftlichen, statistischen und historischen Zwecken (Art. 83)
  - Betroffenenrechte können eingeschränkt werden aus Gründen der nationalen und öffentlichen Sicherheit, der Strafverfolgung, des Schutzes der betroffenen Person und der Rechte und Freiheiten anderer Personen, etc.
- Die Kommission, der EDSA und die Aufsichtsbehörden (AB) werden diesbezüglich Leitlinien vorgeben,.

# Rechtsbehelfe, Haftung und Sanktionen

- Vielfache Befugnisse der Aufsichtsbehörden (AB) zur Sanktionierung
- **Deutlich höhere Geldbußen**, die je nach Verstoß verhängt werden können:
  - € 0,25 Mio. oder bis zu 0,5% des weltweiten Jahresumsatzes
  - € 0,5 Mio. oder bis zu 1% des weltweiten Jahresumsatzes
  - € 1 Mio. oder bis zu 2% des weltweiten Jahresumsatzes
- Die Höhe hängt ab von: Art, Schwere und Dauer des Verstoßes; Vorsatz/ Fahrlässigkeit; früheren Verstöße; Grad der Verantwortlichkeit; Ergreifen von technischen und organisatorischen Maßnahmen und Bereitschaft zur Zusammenarbeit mit den AB
- Recht von Betroffenen bei unrechtmäßiger Datenverarbeitung für materielle und immaterielle Schäden entschädigt zu werden
- Neu: **Gesamtschuldnerische Haftung** zwischen verantwortlicher Stelle und Auftragsdatenverarbeiter

# Pflichten der Auftragsdatenverarbeiter

- Gesetzliche Pflichten der Auftragsdatenverarbeiter
  - Keine Unterauftragsdatenverarbeitung ohne Zustimmung der verantwortlichen Stelle sowie Informationspflicht bei Änderungen
  - Muss für jede verantwortlichen Stelle Aufzeichnungen hinsichtlich der verarbeiteten Datenkategorien und des Datenexportes führen
  - Verantwortlich für die Bestimmung der angemessenen Datensicherheitsmaßnahmen, sofern diese Aufgabe nicht ausdrücklich der verantwortlichen Stelle zugewiesen wurde
  - Muss Verantwortliche Stelle bei Verletzung “ohne gebührende Verzögerung” benachrichtigen
- Die meisten Verstöße können mit einer Geldbuße bis zu 2% sanktioniert werden: auch gegenüber dem Auftragsdatenverarbeiter
- Weil nach der Verordnung eine gesamtschuldnerische Haftung ausgeschlossen ist, wenn eine Partei beweisen kann, dass sie nicht verantwortlich ist, sollte im Detail vertraglich festgelegt werden, wer für was verantwortlich ist
- Wird den Inhalt sowie die Ausgewogenheit von Cloud-, Datenverarbeitungs-, Datenspeicherungs- und sonstigen Auftragsdatenverarbeitungsverträgen beeinflussen

# Änderungen hinsichtlich der Datenschutzerklärungen

## Neue Anforderungen:

- Kontaktinformationen des Datenschutzbeauftragten (falls vorhanden)
- Zusätzliche Informationen, welche notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten (im Text des Rates wird ein gewisser Freiraum zugestanden; nicht im EP Text zu finden)
  - falls Verarbeitung auf Einwilligung gestützt wird, muss ein Hinweis auf die jederzeitige Widerrufsmöglichkeiten erfolgen
  - falls Verarbeitung auf berechnigte Interessen gestützt wird, muss spezifiziert werden, welche dies sind
- Erläutern, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist; ob die betroffene Person verpflichtet ist, die Daten bereitzustellen und welche mögliche Folgen die Nichtbereitstellung hätte
- Betroffenenrechte und das Recht zur Beschwerde bei den Aufsichtsbehörden müssen hervorgehoben werden

# EP Entwurf: standardisierte Datenschutzerklärung

- Verpflichtende Hervorhebung von je notwendigen Datenverarbeitung; m wenn online (kann nur durch die Kc
- Dauer der Speicherung von Daten, Datensicherheit
- Wurden Daten in den letzten zwölf übermittelt?
- Welche Schutzvorkehrungen existiti Datenexporten?
- Angaben über das Profiling (falls vc die Logik einer automatisierten Dat

Anhang – Darstellung der Hinweise nach Artikel 13a

1) Unter Berücksichtigung der Proportionen, auf die unter Punkt 6 verwiesen wird, sehen die Hinweise wie folgt aus:

SYMBOL	WESENTLICHE INFORMATIONEN	ERFÜLLT
	Es werden nicht mehr personenbezogene Daten <b>erhoben</b> , als für die spezifischen Zwecke der Verarbeitung erforderlich sind.	
	Es werden nicht mehr personenbezogene Daten <b>gespeichert</b> , als für die spezifischen Zwecke der Verarbeitung erforderlich sind.	
	Personenbezogene Daten werden nicht zu anderen als den Zwecken <b>verarbeitet</b> , für die sie erhoben wurden.	
	Es werden keine personenbezogenen Daten an gewerbliche Dritte <b>weitergegeben</b> .	
	Es werden keine personenbezogenen Daten <b>verkauft oder verpachtet</b> .	
	Es werden keine personenbezogenen Daten <b>unverschlüsselt</b> aufbewahrt.	

DIE EINHALTUNG DER BESTIMMUNGEN IN BEZUG AUF ZEILE 1-3 IST NACH EU-RECHT VORGESCHRIEBEN

# Einwilligung

- Einwilligung – neue Anforderungen
  - Nicht sensible personenbezogene Daten: Unmissverständliche Einwilligung
  - Besondere Arten von personenbezogenen Daten: Ausdrückliche Einwilligung
  - Keine ausdrückliche Schriftform mehr – aber Verantwortliche Stelle muss nachweisen können, dass Einwilligung erteilt wurde
  - Bei schriftlicher Einwilligung muss eine Unterscheidung zwischen dem Datenschutzteil und dem Rest erfolgen
  - Vor Erteilung der Einwilligung muss Betroffener über das Widerrufsrecht informiert werden
  - Online-Einwilligungen von Kindern müssen durch die Eltern erfolgen, wobei verhältnismäßiger Aufwand betrieben werden muss, um dies zu verifizieren
  - Ungültig, wenn ein “klares Ungleichgewicht” zwischen Betroffenen und verantwortlicher Stelle besteht (umstrittener Erwägungsgrund 34)



# Umsetzungspflichten im Alltag (1)

Benachrichtigungspflicht (war in vielen EU-Staaten relevant) abgeschafft, aber ersetzt durch:

- **Rechenschaft:** Art. 22 verlangt von der verantwortlichen Stelle, dass sie geeignete Maßnahmen durchführt und den Nachweis dafür erbringt, dass personenbezogene Daten in Übereinstimmung mit der Verordnung verarbeitet werden.
- **Dokumentierung:** Art. 28 erfordert dass verantwortliche Stelle (zu einem gewissen Grad auch Auftragsdatenverarbeiter) ihre Verarbeitungsvorgänge aufzeichnen und – auf Nachfrage – der AB zur Verfügung stellen, einschließlich Angaben über die Zwecke der Verarbeitung einschließlich des berechtigten Interesses und Löschungsfristen
- **Sicherheit:** Art. 30 & Erwägungsgrund 66 erfordern, dass die verantwortliche Stelle oder der Auftragsdatenverarbeiter eine Bewertung des Sicherheitsrisikos vornimmt, bevor technische und organisatorische Maßnahmen hinsichtlich der bestehenden Risiken implementiert werden
- **Datenschutz-Folgenabschätzung (PIA):** Muss nach Art. 33 von der verantwortlichen Stelle durchgeführt werden, wenn die Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen bedeutet, etwa Diskriminierung, Identitätsdiebstahl, finanzielle Verluste oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile

# Umsetzungspflichten im Alltag (2)

- **Datenschutzbeauftragter**

- Ernennung nicht verpflichtend nach DGV; eventuell Verpflichtung durch MS oder anderes EU-Gesetz
- Datenschutzwissen, direkter Kontakt zur Geschäftsführung, angemessen ausgestattet, führzeitig bei Datenschutzfragen eingebunden & unabhängig
- Ein Beauftragter kann auch für eine Unternehmensgruppe ernannt werden
- Kann auch extern besetzt werden
- Muss informieren, sensibilisieren, ausbilden und überwachen

- **Codes of Conduct & Zertifizierung**

- Angemessene Maßnahmen könnten durch genehmigte Codes of Conduct, Zertifizierungen oder EDSA-Richtlinien vorgegeben werden
- Branchenverhaltensregeln arbeiten die Anforderungen aus – können von den AB genehmigt werden, wenn sie den Anforderungen der DGV entsprechen; Überwachung der Einhaltung kann von den AB akkreditierten Zertifizierungsstellen überlassen werden; bei Verletzung ist ein Ausschluss der verantwortlichen Stelle möglich

- Obwohl ein **risikobasierender Ansatz** eingeführt wird, wurde die “*best practice*” hinsichtlich dem Umgang mit Daten letztlich umfassend in der Verordnung geregelt, wobei Sanktionen von bis zu 2% des weltweiten Jahresumsatzes bei Verstößen drohen


# Meldung von Verletzungen

- **Meldungserfordernis** gegenüber Behörde:
  - Verletzungen, die voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge haben, wie etwa Diskriminierung, Identitätsdiebstahl oder Betrug, finanzielle Verluste, [...] oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile (gleiche Anforderungen wie bei PIA),
  - aber nicht wenn Maßnahmen erfolgten, welche das Risiko ausschließen
- **Frist:**
  - Auftragsdatenverarbeiter muss verantwortliche Stelle “ohne gebührende Verzögerung” benachrichtigen
  - Meldung muss eine vernünftige Begründung enthalten, wenn sie erst nach 72 Stunden erfolgte
  - Meldung zur AB muss eine Beschreibung der Art der Verletzung, Angabe der ungefähren Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Datenkategorien und der ungefähren Zahl der betroffenen Datensätze, Folgen, ergriffenen oder vorgeschlagenen Maßnahmen
  - Verantwortliche Stelle muss derartige Verletzungsvorfälle dokumentieren
- Meldungserfordernis bezüglich Betroffenen: Gleiches Erfordernis wie bei Behörde

# Datenexport (Kapitel V)


- Auftragsdatenverarbeiter können bei unrechtmäßigem Datenexport haften
- Kein Auslaufen von Angemessenheitsentscheidungen (“White list”, Standardvertragsklauseln) & Möglichkeit für die Kommission weitere Angemessenheitsentscheidungen zu treffen, einschließlich sektorspezifische Angemessenheitsentscheidungen
- Derzeit genutzte EU-Standardvertragsklauseln müssen erneuert werden
- Binding Corporate Rules werden formalisiert und von der Leitbehörde bewilligt (muss EDSA einbeziehen)
- Verhaltensregeln und Zertifizierungen könnten dazu genutzt werden, um Datenexport ohne weitere Genehmigung zu rechtfertigen
- Geldbuße von 2% des weltweiten Jahresumsatzes bei unrechtmäßigem Datenexport

# EuGH zu Safe Harbor und Konsequenzen



„Insbesondere verletzt eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des durch Art. 7 der Charta garantierten **Grundrechts auf Achtung des Privatlebens**“

„Desgleichen verletzt eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Art. 47 der Charta verankerten **Grundrechts auf wirksamen gerichtlichen Rechtsschutz**.“



# EuGH vom 6. Oktober 2015 (C-362/14 - Schrems)

- Safe Harbor Entscheidung der EU-Kommission wird **aufgehoben**
- **Keine Übergangsfristen**: Bisher auf Safe Harbor gestützte Datenübermittlung ist damit rechtswidrig – Datenschutzbehörden gewähren Frist bis Ende Januar 2016 vor Durchsetzung
- **Alternativen?**  
Es bleiben theoretisch noch die EU-Standardvertragsklauseln und Binding Corporate Rules (BCRs) – und auch das eingeschränkt
- EuGH zieht aber auch andere Maßnahmen wie EU-Standardvertragsklauseln indirekt in Frage...
- Stellungnahme der Art. 29 Datenschutzgruppe und der deutschen Datenschutzkonferenz (d.h. die Aufsichtsbehörden der Länder)
- BCRs werden derzeit nicht mehr genehmigt
- EU-Standardvertragsklauseln in Frage gezogen

# Zusammenfassung und Fazit für Kunden und Datacenter Provider



# Zusammenfassung der wesentlichen Auswirkungen

- Deutlich höhere Sanktionen
- **Für Kunden:** Formelle Anforderungen an die Datenverarbeitung werden größer und müssen implementiert werden
- **Für Provider:** Neue Haftung, wenn sie Zugriff auf personenbezogene Daten haben
- **Empfehlungen:**
  - Klare Regelungen der Verantwortung in den Verträgen
  - Fokus auf Codes of Conducts & Zertifizierungen
  - Risiken und Pflichten werden eingepreist werden müssen
  - Bestehende Auftragsdatenverarbeitung-Verträge müssen überprüft werden
- Die neu vorgesehenen Rechte werden Geschäftsbeziehung verkomplizieren – effektives System einführen, um hierauf zu reagieren

The logo consists of a stylized, upward-pointing chevron shape in a gold color, positioned above the first letter of the text.

**NORTON ROSE FULBRIGHT**