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

360°dcLounge meets CeBIT

Dr. Christoph Ritzer
17. März 2016

Agenda

- Stand, Verfahrensablauf und Zeitplan
- Was ändert sich?
- Zusammenfassung und Fazit

Stand, Verfahrensablauf und Zeitplan

SCHUTZ Status

Welche Gesetze werden sich ändern?

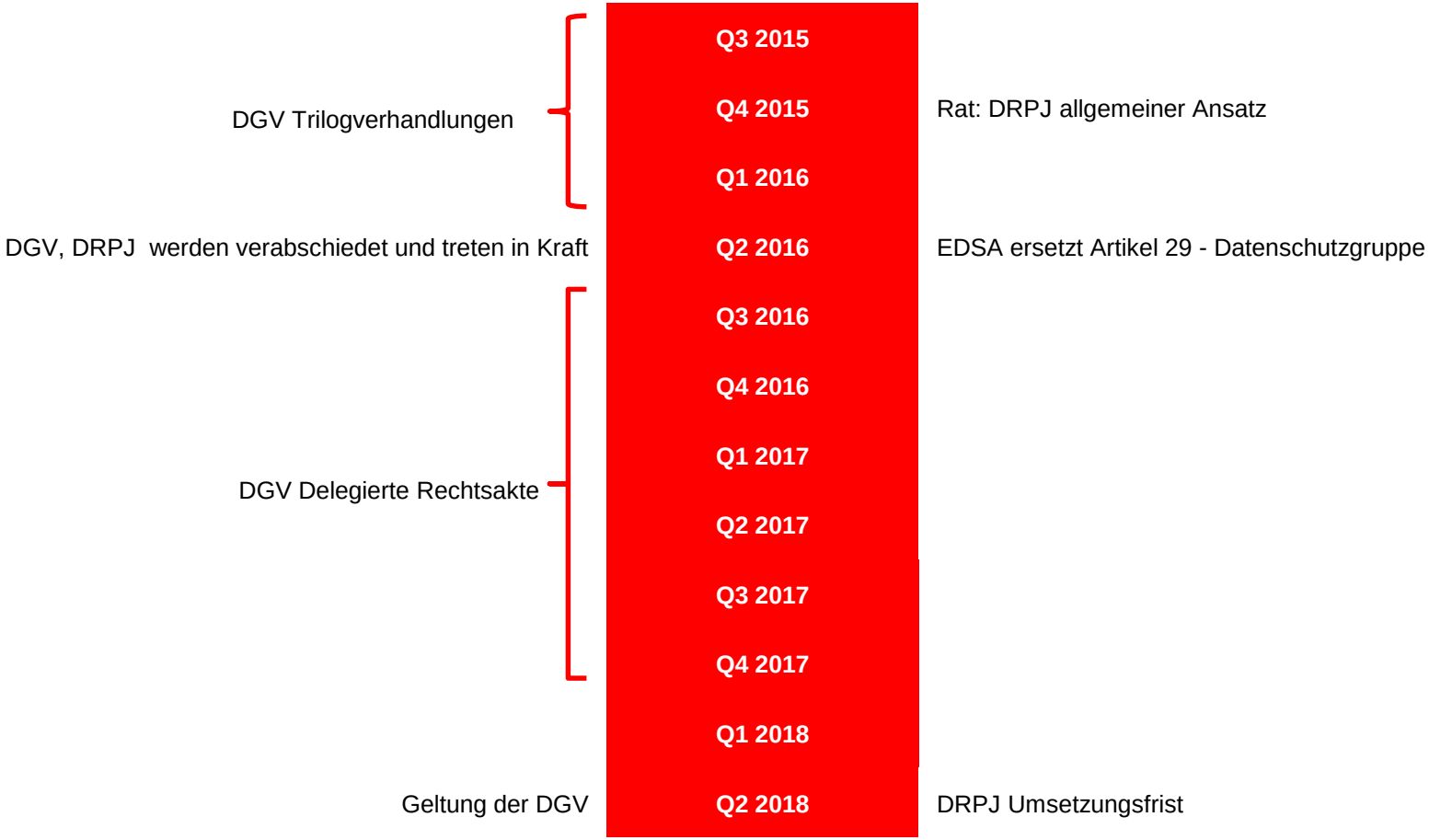
Neues Recht

- 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

DGV - Zeitplan



NORTON ROSE FULBRIGHT

Einzelne Änderungen

SCHUTZPunkte

Überblick: Wesentliche Änderungen

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

Grundsätzliches

SCHUTZRaum

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 größter gemeinsame Nenner
- Verleiht jedoch MS die Befugnis in einigen Bereichen unterschiedliche Regelungen einzuführen
  - Verarbeitung von Arbeitnehmerdaten im Beschäftigungskontext (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.

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

Umsetzungspflichten im Alltag

SCHUTZPflichten

Umsetzungspflichten im Alltag (1)

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

- **Rechenschaft** (*Accounability*): Verantwortliche Stelle muss
  - muss die Einhaltung der Datenschutzgrundsätze nachweisen können,
  - geeignete Maßnahmen durchführen, um die DSGVO einhalten zu können.
- **Dokumentierung**: Verantwortliche Stelle (zu einem gewissen Grad auch Auftragsverarbeiter) muss 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**: Verantwortliche Stelle oder der Auftragsverarbeiter müssen eine Bewertung des Sicherheitsrisikos vornehmen, bevor technische und organisatorische Maßnahmen hinsichtlich der bestehenden Risiken implementiert werden
- **Datenschutz-Folgenabschätzung** (PIA): Muss 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 immer verpflichtend nach DSGVO; eventuell Verpflichtung durch MS oder anderes EU-Gesetz
  - 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 4% des weltweiten Jahresumsatzes bei Verstößen drohen

Haftung und Sanktionen

SCHUTZFolgen

…wenn man die Regeln nicht einhält

Haftung und Sanktionen (1)

Geldbußen

- Deutlich höhere Geldbußen, die je nach Verstoß verhängt werden können:
  - € 10 Mio. oder bis zu 2% des weltweiten Jahresumsatzes
  - € 20 Mio. oder bis zu 4% des weltweiten Jahresumsatzes
- Die Höhe hängt ab von:
  - Art, Schwere und Dauer des Verstoßes;
  - Vorsatz/Fahrlässigkeit;
  - früheren Verstößen;
  - Grad der Verantwortlichkeit;
  - Ergreifen von technischen und organisatorischen Maßnahmen und
  - Bereitschaft zur Zusammenarbeit mit den AB

Haftung und Sanktionen (2)

Schadenersatz

- Recht von Betroffenen bei unrechtmäßiger Datenverarbeitung für materielle und immaterielle Schäden entschädigt zu werden
- Neu: Gesamtschuldnerische Haftung zwischen verantwortlicher Stelle und Auftragsdatenverarbeiter

Meldung von Verletzungen

- **Meldungserfordernis**
  - 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 gebührliche 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

Auftragsverarbeitung

SCHUTZ Delegation

Pflichten der Auftragsverarbeiter

- Gesetzliche Pflichten der Auftragsverarbeiter
  - 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 gebührliche Verzögerung” benachrichtigen
- Die meisten Verstöße können mit einer Geldbuße bis zu 2% sanktioniert werden: auch gegenüber dem Auftragsverabeiter
- 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

Einwilligung und Hinweise

SCHUTZFormen

Änderungen hinsichtlich der Datenschutzerklärungen

Neue Anforderungen:

- Zusätzliche Informationen:
  - falls Verarbeitung auf Einwilligung gestützt wird, muss ein Hinweis auf die jederzeitige Widerrufsmöglichkeiten erfolgen
  - falls Verarbeitung auf berechtigte Interessen gestützt wird, muss spezifiziert werden, welche dies sind
  - Hinweis auf Profiling
- 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
- Kontaktinformationen des Datenschutzbeauftragten
- Betroffenenrechte und das Recht zur Beschwerde bei den Aufsichtsbehörden müssen hervorgehoben werden

EP Entwurf: standardisierte Datenschutzerklärung

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

NORTON ROSE FULBRIGHT

Einwiligung

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 (Erwägungsgrund 34)
- Ungültig auch, wenn andere Zwangslage: auch zu prüfen, wenn die Erfüllung eines Vertrags von der Einwilligung abhängig gemacht wird

Übermittlung in Drittsaaten

Export SCHUTZ

Datenexport (Kapitel V)

- Auftragsdatenverarbeiter können bei unrechtmäßigen Datenexport haften
- Kein Auslaufen von Angemessenheitsentscheidungen, Möglichkeit für die Kommission weitere Angemessenheitsentscheidungen zu treffen, einschließlich sektorspezifische Angemessenheitsentscheidungen
- 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
- Aber: EuGH vom 6. Oktober 2015 (C-362/14 - Schrems)

„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…

Zusammenfassung und Fazit für Kunden und Datacenter Provider

SCHUTZ Fazit

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


NORTON ROSE FULBRIGHT