BAKER & MCKENZIE

Die Datenschutz-Grundverordnung ist da – was ändert sich?

Dr. Matthias Scholz, LL.M. | Partner, Frankfurt/Main

10. November 2016

Datenschutztagung der GDD

GDD ERFA-KREIS Hessen

Hintergrund und Zweck

Hintergrund und Zweck (1)

1.) Datenschutz-Richtlinie 95/46/EG von 1995

- Grds. nicht direkt anwendbar, sondern durch die 28 EU-Mitgliedstaaten in nationales Recht umgesetzt. Der damit zusammenhängende Verwaltungsaufwand wird auf EUR 2,3 Mrd. jährlich geschätzt
- Meldepflichten in fast allen EU-Mitgliedstaaten kosten die Unternehmen jährlich geschätzte EUR 130 Mio

2.) Ziel der Datenschutz-Grundverordnung (DSGVO)

- Ein einheitliches und direkt anwendbares Datenschutzrecht in der ganzen EU, das die meist beschwerlichen Verwaltungsanforderungen und uneinheitliche Anwendung von „europäischem“ Datenschutzrecht aufheben soll
- Räumlicher Anwendungsbereich: Gleiche Anforderungen an alle Unternehmen, unabhängig von ihrem Sitz innerhalb und außerhalb der EU
- Aber: Keine Vollharmonisierung durch DSGVO!

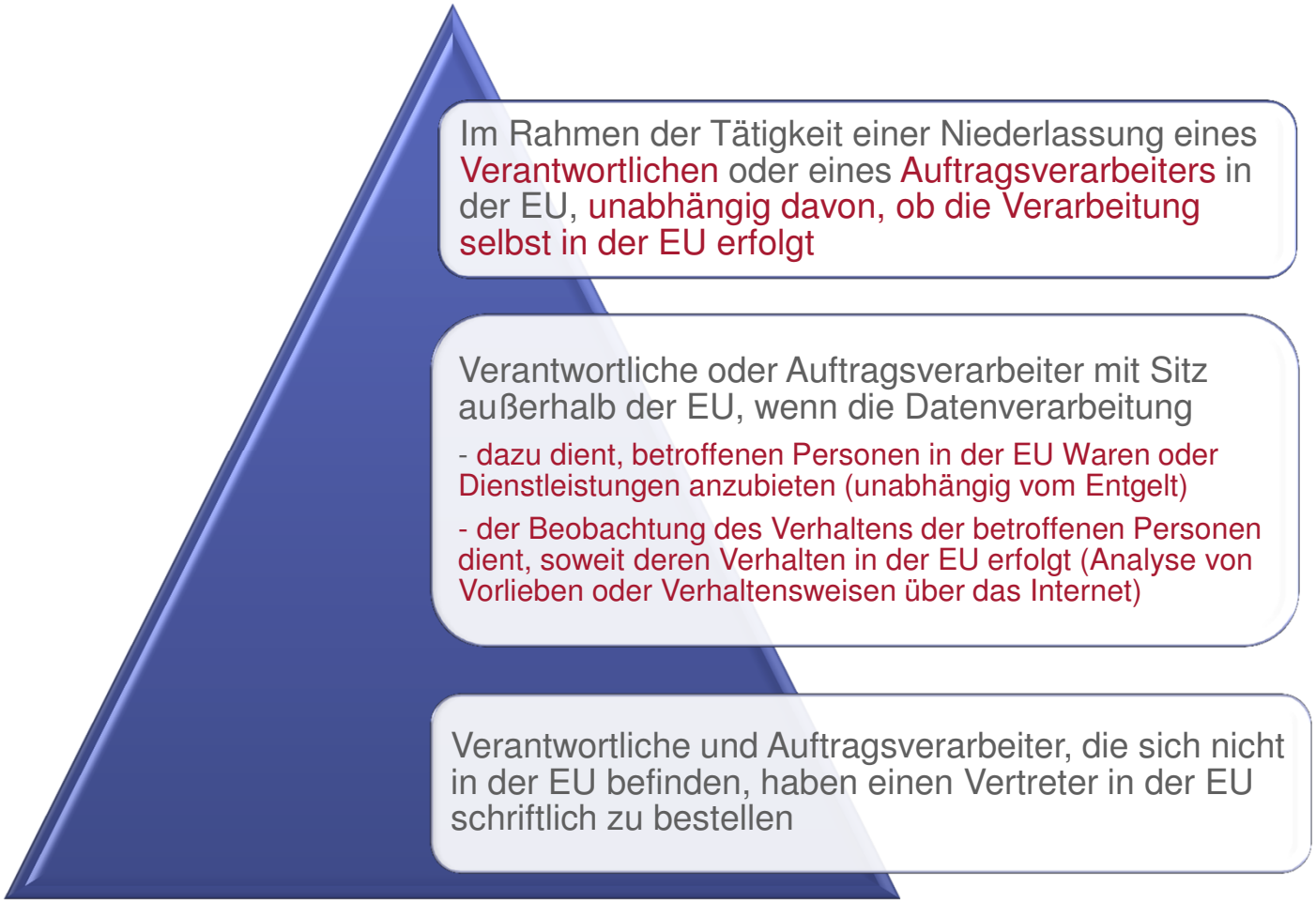
Hintergrund und Zweck (2)

3.) Entwicklung / Gegenwärtiger Stand

- Kommissionsvorschlag zur DSGVO wurde im Januar 2012 veröffentlicht
- Europäisches Parlament veröffentlichte Änderungen zum Kommissionsvorschlag am 12. März 2014
- Der Rat der Europäischen Union veröffentlichte Änderungsvorschläge zwischen Dezember 2014 und März 2015
- Trilog-Verhandlungen (Kommission, Parlament, Rat) bis Dezember 2015
- Annahme der DSGVO durch das Parlament und durch die Kommission am 27. April 2016
- Veröffentlichung im Amtsblatt der Europäischen Union am 4. Mai 2016
- Inkrafttreten 20 Tage nach Veröffentlichung, d.h. am 25. Mai 2016
- Zweijährige Übergangsfrist: Geltung der DSGVO ab 25. Mai 2018

Wesentliche Neuerungen

1. Räumlicher Anwendungsbereich



2. „One-Stop-Shop“ (1)

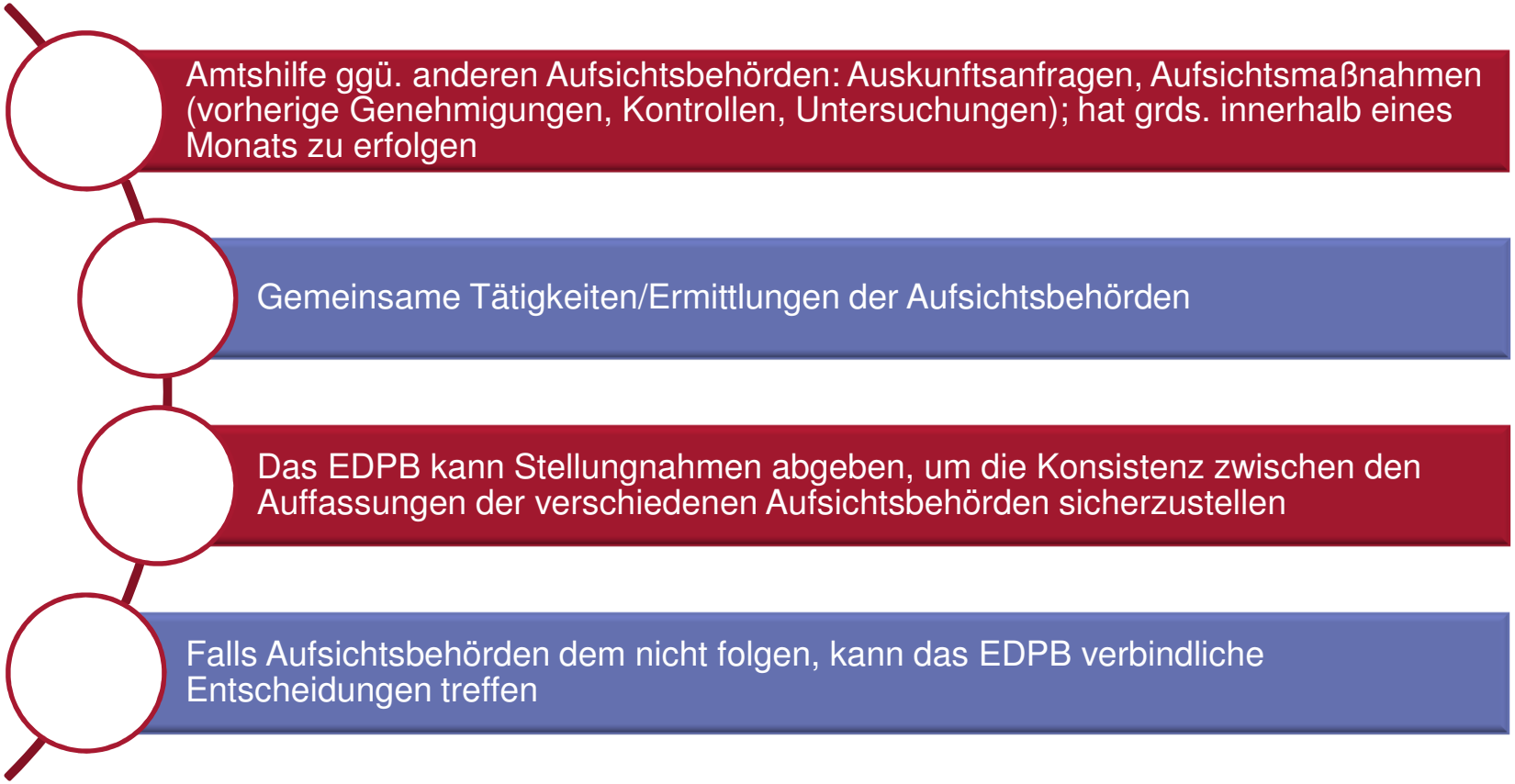
Jeder Mitgliedstaat hat eine Aufsichtsbehörde zu benennen. Wenn mehrere Aufsichtsbehörden bestehen, ist durch den Mitgliedstaat eine Aufsichtsbehörde zu benennen, die den Mitgliedstaat vor dem EDPB vertritt

Federführende Aufsichtsbehörde (*Lead Authority*) für grenzüberschreitende Verarbeitung: Hauptniederlassung (Art. 4 Nr. 16: Ort der Hauptverwaltung oder dort, wo die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung getroffen werden)

Jede Aufsichtsbehörde kann bei sich eingereichte Beschwerden annehmen (federführende Aufsichtsbehörde muss informiert werden)

Federführende Aufsichtsbehörde kooperiert/berät sich mit betroffenen Aufsichtsbehörden; der Auffassung der betroffenen Aufsichtsbehörden ist weitestgehend Rechnung zu tragen

2. „One-Stop-Shop“ (2)



3. Datenschutzbeauftragter (1)

- Verantwortliche und Auftragsverarbeiter haben einen Datenschutzbeauftragten zu benennen, wenn
  - die Kerntätigkeiten eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen;
  - die Kerntätigkeiten die umfangreiche Verarbeitung besonderer Arten personenbezogener Daten oder Daten über Straftaten betreffen; oder
  - das Recht der EU oder des Mitgliedstaats dies vorsieht.
- Eine Unternehmensgruppe kann einen Datenschutzbeauftragten ernennen, sofern der Datenschutzbeauftragte von jedem Standort aus leicht erreichbar ist.

3. Datenschutzbeauftragter (2)

- Kontaktdaten müssen der Aufsichtsbehörde gemeldet werden
- Kontaktdaten müssen veröffentlicht werden
- Aufgaben des Datenschutzbeauftragten gemäß DSGVO:
  - Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten zu Pflichten aus der DSGVO sowie anderer Datenschutzvorschriften der EU oder der Mitgliedstaaten
  - Überwachung der Einhaltung der DSGVO sowie anderer Datenschutzvorschriften der EU oder der Mitgliedstaaten
  - Schulung der Mitarbeiter
  - Beratung im Zusammenhang mit der Datenschutzfolgeabschätzung (Privacy Impact Assessment) und Überwachung der Durchführung
  - Ansprechpartner für die Aufsichtsbehörde(n)

4. Data Breach Notification

Der Verantwortliche hat die zuständige Aufsichtsbehörde nach Möglichkeit binnen 72 Stunden nach Feststellung der Verletzung über den Data Breach zu informieren, es sei denn, der Data Breach führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten von Personen

Hat der Data Breach voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge, muss der Verantwortliche die betroffene Person unverzüglich von der Verletzung unterrichten (Ausnahmen sind möglich)

Verantwortliche müssen alle Data Breaches intern dokumentieren

„Risiko für die Rechte und Freiheiten von Personen“ ist in der DSGVO nicht weiter definiert

Nach Feststellung eines Data Breaches durch den Auftragsverarbeiter hat er diese dem Verantwortlichen unverzüglich zu melden

5. Verzeichnis von Verarbeitungstätigkeiten (1)

- Der Verantwortliche und der Auftragsverarbeiter müssen ein Verzeichnis aller Verarbeitungsaktivitäten führen.
- Das Verzeichnis muss folgende Angaben enthalten:
  - Name und Kontaktdaten des Verantwortlichen, des Vertreters (soweit einschlägig) sowie eines etwaigen Datenschutzbeauftragten
  - Zwecke der Verarbeitung
  - Beschreibung der Kategorien von betroffenen Personen und der Kategorien der personenbezogenen Daten
  - Kategorien von Empfängern
  - Übermittlungen von Daten in ein Drittland einschließlich der geeigneten Garantien
  - Aufbewahrungsfrist
  - Beschreibung der technischen und organisatorischen Maßnahmen

5. Verzeichnis von Verarbeitungstätigkeiten (2)

– Die genannten Pflichten gelten nicht, wenn weniger als 250 Mitarbeiter beschäftigt sind, kein Risiko für die Rechte und Freiheiten der betroffenen Personen besteht, die Verarbeitung nur gelegentlich erfolgt und keine Verarbeitung von sensiblen Daten oder von Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten erfolgt.

6. Datenschutzfolgenabschätzung (Privacy Impact Assessment)

- Wenn aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung (insb. bei neuen Technologien) ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht, muss der Verantwortliche ein Privacy Impact Assessment (PIA) durchführen.
- Stellungnahme des Datenschutzbeauftragten ist einzuholen
- Die Aufsichtsbehörden erstellten eine Liste der Verarbeitungsvorgänge, für die ein PIA durchzuführen ist.
- PIA hat zumindest Folgendes zu enthalten:
  - Systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, einschließlich der vom Verantwortlichen verfolgten berechtigten Interessen
  - Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
  - Bewertung der Risiken in Bezug für die Rechte und Freiheiten der betroffenen Personen
  - Vorgesehene Maßnahmen im Hinblick auf die Risiken, einschließlich der Garantien, Sicherheitsvorkehrungen und Verfahren

7. Internationale Datenübermittlungen (1)

a) Sämtliche von der Kommission auf der Grundlage von Artikel 25 (6) der Datenschutz-Richtlinie erlassenen Beschlüsse (angemessenes Datenschutzniveau eines Landes = White List Countries; EU-US Privacy Shield)

➔ bleiben so lange in Kraft, bis sie von der Kommission durch eine Entscheidung geändert, ersetzt oder aufgehoben werden.

b) Sämtliche von einer Aufsichtsbehörde auf Grundlage von Artikel 26 (2) der Datenschutz-Richtlinie erteilten Genehmigungen (Binding Corporate Rules oder Ad-Hoc-Verträge) und von der Kommission auf der Grundlage von Artikel 26 (4) der Datenschutz-Richtlinie erlassenen Beschlüsse (angemessene Sicherheitsvorkehrungen wie EU-Standardverträge)

➔ bleiben so lange in Kraft, bis sie von der Kommission durch eine Entscheidung geändert, ersetzt oder aufgehoben werden.

7. Internationale Datenübermittlungen (2)

c) Neue Grundlagen eines Angemessenheitsbeschlusses

- Kommission kann feststellen, dass ein Drittland bzw. ein Gebiet oder ein oder mehrere spezifische Sektoren dieses Drittlands oder die betreffende internationale Organisation einen angemessenen Schutz bietet
- Derartige Datenübermittlungen bedürfen keiner besonderen Genehmigung
- Die Kommission kann, soweit dies erforderlich ist, derartige Beschlüsse widerrufen, ändern oder aussetzen, allerdings ohne Rückwirkung

d) Neue geeignete Garantien

- Binding Corporate Rules
- Standard Contractual Clauses der Kommission (Prüfverfahren)
  - ➔ Prüfverfahren: Ein Gremium von Repräsentanten der Mitgliedsstaaten entscheidet gemeinsam über die Annahme
- Standard Contractual Clauses der Aufsichtsbehörde mit Genehmigung durch Kommission (Prüfverfahren)
- Genehmigte Verhaltensregeln (Code of Conducts)
- Genehmigter Zertifizierungsmechanismus
- Durch die Aufsichtsbehörde genehmigte Ad-Hoc-Verträge (Kohärenzverfahren erforderlich)

7. Internationale Datenübermittlungen (3)

e) Ausnahmen

- Ausdrückliche Einwilligung
- Für die Erfüllung eines Vertrags mit der betroffenen Person erforderlich
- Zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person geschlossenen Vertrages
- Aus wichtigen Gründen des öffentlichen Interesses notwendig
- Für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
- Lebenswichtige Interessen der betroffenen Person
- Übermittlung erfolgt aus einem Register, das zur Information der Öffentlichkeit oder aller Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht

7. Internationale Datenübermittlungen (4)

e) Ausnahmen

- Interessensabwägung
  - Wenn es sich um eine einmalige Übermittlung handelt, die eine begrenzte Anzahl von betroffenen Personen betrifft und
  - zur Wahrung zwingender berechtigter Interessen des Verantwortlichen erforderlich ist, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen und
  - soweit der Verantwortliche alle Umstände beurteilt hat, die bei einer Datenübermittlung eine Rolle spielen und auf der Grundlage dieser Beurteilung geeignete Garantien zum Schutz personenbezogener Daten vorgesehen hat.
- Der Verantwortliche hat die Aufsichtsbehörde über die Übermittlung zu unterrichten.
- Der Verantwortliche hat die betroffene Person über die Übermittlung und seine zwingenden berechtigten Interessen zu unterrichten.

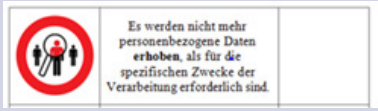
8. Datenschutzerklärung / Privacy Statement (1)

Inhalt		Vergleich zu deutschem Datenschutzrecht
▪ Name und Kontaktdaten des Verantwortlichen sowie ggf. des Vertreters		→
▪ Ggf. Kontaktdaten des Datenschutzbeauftragten		↗
▪ Zwecke, für die die personenbezogenen Daten verarbeitet werden, sowie die Rechtsgrundlage für die Verarbeitung		↗
▪ Vorrangiges berechtigtes Interesse des Verantwortlichen oder eines Dritten bei Interessenabwägung als Rechtfertigungsgrund		↗
▪ Empfänger oder Empfängerkategorien der personenbezogenen Daten		→
▪ Übermittlung in ein Drittland sowie Vorhandensein oder Fehlen eines Angemessenheitsbeschlusses oder Verweis auf Garantien und deren Verfügbarkeit		↗
▪ Aufbewahrungsfrist oder Kritierien für Fristfestlegung		↗

8. Datenschutzerklärung / Privacy Statement (2)

Inhalt		Vergleich zu deutschem Datenschutzrecht
▪ Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Datenübertragbarkeit)		↗
▪ Ggf. Information über das Recht, die Einwilligung jederzeit widerrufen zu können		→
▪ Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde		↗
▪ Ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob Verpflichtung zur Bereitstellung besteht und mögliche Folgen der Nichtbereitstellung		→
▪ Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling		↗
Falls nicht beim Betroffnen erhoben, zudem:		
▪ Datenkategorien		→
▪ Quellen, aus denen die personenbezogenen Daten stammen		↗

8. Datenschutzerklärung / Privacy Statement (3)

Form		Vergleich zu deutschem Datenschutzrecht
▪ Präzise, transparente, verständliche und leicht zugängliche Form sowie klare und einfache Sprache		↗
▪ Schriftliche oder elektronische Übermittlung, wobei Bereitstellen auf der Website genügt		→
▪ ggf. in Kombination mit Bildsymbolen wie von Kommission vorgeben 		↗
Zeitpunkt		
▪ Zum Zeitpunkt der Erhebung der Daten, wenn personenbezogene Daten beim Betroffenen erhoben werden		→
▪ Innerhalb angemessener Frist nach Erlangung der Daten, längstens jedoch innerhalb eines Monats, wenn personenbezogene Daten nicht beim Betroffenen erhoben werden		↘
Mögliche Sanktionen		
▪ Geldbuße bis 20 mio. EUR oder 4% des weltweit erzielten Jahresumsatzes		↗

9. Einwilligung (1)

Anforderungen		Vergleich zu deutschem Datenschutzrecht
▪ Freiwillig, d.h. echte oder freie Wahl. Fehlt in der Regel, wenn:		
▪ zwischen betroffener Person und Verantwortlichem ein klares Ungleichgewicht besteht		↗
▪ die Vertragserfüllung trotz fehlender Erforderlichkeit von der Erteilung abhängig gemacht wird		↗
▪ Spezifisch, d.h. verschiedene Datenverarbeitungszwecke erfordern separate Einwilligungen		↗
▪ Informiert, d.h. zumindest wissen, wer der Verantwortliche ist und zu welchen Zwecken Daten verarbeitet werden		→
▪ Unmissverständlich: in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, z.B. durch Anklicken eines Kästchens (unzureichend: vorangekreuzte Kästchen oder Untätigkeit)		↗
▪ Jederzeitige Widerrufsmöglichkeit und Belehrung hierüber vor Abgabe der Einwilligung		→

9. Einwilligung (2)

Form		Vergleich zu deutschem Datenschutzrecht
▪ Elektronische Erklärung ausreichend		→
▪ Nachweisbarkeit der Einwilligung		→
▪ Besondere Anforderungen bei vorformulierter Einwilligungserklärung		→
Sonstiges		
▪ Ggf. ausdrückliche Einwilligung erforderlich, z.B. für die Verarbeitung von sensiblen Daten oder für Profiling		↗
▪ Dienste der Informationsgesellschaft für Kinder unter 16: Einwilligung nur rechtmäßig, wenn und insoweit die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind erteilt wird		↗
→ Nach einzelstaatlichem Recht auch für jüngere Kinder möglich, soweit diese nicht unter 13 Jahren sind		
▪ bereits erteilte Einwilligungen gelten fort, wenn sie den Bedingungen der DSGVO entsprechen		→

9. Einwilligung (3)

Mögliche Sanktionen		Vergleich zu deutschem Datenschutzrecht
▪ Geldbuße bis 20 mio. EUR oder 4% des weltweit erzielten Jahresumsatzes		↗

10. Betroffenenrechte (1)

Auskunftsrecht		Vergleich zu deutschem Datenschutzrecht
Inhalt, z.B.:		
▪ Verarbeitungszwecke, Kategorien personenbezogener Daten, Empfänger oder Kategorien von Empfängern, inbesondere bei Empfängern in Drittländern		→
▪ Geplante Speicherdauer oder falls nicht möglich Kriterien für Festlegung der Dauer; alle verfügbaren Informationen über die Herkunft der Daten, wenn nicht bei betroffener Person erhoben; Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und bei Übermittlung an ein Drittland, Unterrichtung über geeignete Garantien		↗
Form:		
▪ Kopie der personenbezogenen Daten, d.h. ggf. Auszüge aus Datenbank mit E-Mail-Korrespondenz. Einschränkung: Erhalt der Kopie darf Rechte anderer Personen nicht beeinträchtigen		↗
▪ In gängigem elektronischem Format, falls Antrag elektronisch gestellt, z.B. per E-Mail		→
▪ Erste Kopie kostenlos, für weitere Kopien kann angemessenes Entgelt verlangt werden		→
Frist: keine ausdrückliche Regelung, aber § 271 BGB?		→

10. Betroffenenrechte (2)

Recht auf Löschung („Recht auf Vergessenwerden“)		Vergleich zu deutschem Datenschutzrecht
▪ Löschung personenbezogener Daten kann verlangt werden, wenn z.B. nicht mehr notwendig für Zwecke, für die sie erhoben wurden, oder Widerruf der Einwilligung und Fehlen einer anderweitigen Rechtsgrundlage		→
▪ Unverzüglich		↘
▪ Wurden die Daten öffentlich gemacht und besteht eine Löschungsverpflichtung, so trifft der Verantwortliche unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um Verantwortliche darüber zu informieren, dass eine betroffene Person die Löschung aller Links oder von Kopien oder Replikationen verlangt hat		↗
▪ Gilt nicht, wenn Verarbeitung erforderlich ist, z.B. zur Ausübung des Rechts auf freie Meinungsäußerung oder zur Erfüllung einer Verpflichtung		→
▪ Mitteilungspflicht gegenüber allen Empfängern, es sei denn, unmöglich oder mit unverhältnismäßigem Aufwand verbunden		↗

10. Betroffenenrechte (3)

Recht auf Datenübertragbarkeit		Vergleich zu deutschem Datenschutzrecht
▪ Recht auf Erhalt der von einem Betroffenen einer verantwortlichen Stelle zur Verfügung gestellten personenbezogenen Daten in einem üblichen, maschinenlesbaren Format, und		↗
▪ Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem sie beretigestellt wurden, zu übermitteln (auch direkt, soweit technisch machbar)		↗
▪ Voraussetzung: Datenverarbeitung beruht auf Einwilligung oder Vertrag		
▪ Einschränkung: Keine Beeinträchtigung von Rechten anderer		
Verbandsklage		
▪ Art. 80 DSGVO: Betroffene Person kann eine gemeinnützige Vereinigung mit der Wahrnehmung seiner Rechte beauftragen, z.B. Beschwerde bei Aufsichtsbehörde sowie Anspruch auf Schadensersatz		↗

11. Auftragsverarbeitung

- Ausweitung der Verantwortung: Auftragsverarbeiter ist auch für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich, z.B. für Einhaltung der TOMs, Meldung von Data Breaches, Bestellung eines Datenschutzbeauftragten. Verstöße sind bußgeldbewehrt
- Der Auftragsverarbeiter ist nicht Dritter (Art. 4 (11)); Aber: „Offenlegung durch Übermittlung“ setzt keine Weitergabe an Dritte voraus
  - ➔ keine ausdrückliche Privilegierung mehr aber evtl. Rechtfertigung gemäß Art. 6 Nr. 1 (f) „zur Wahrung der berechtigten Interessen des Verantwortlichen“
- Durchführung der Verarbeitung erfolgt auf Grundlage eines Vertrages in dem unter anderem Gegenstand, Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen, die Pflichten und Rechte des Verantwortlichen sowie weitere Anforderungen festgelegt sind (die Kommission und die Aufsichtsbehörde können diesbzgl. Standardvertragsklauseln festlegen)

12. Befugnisse der Aufsichtsbehörden

Untersuchungs-befugnisse der Aufsichts-behörden

- Verantwortliche, Auftragsverarbeiter und/oder ggf. der Vertreter können angewiesen werden, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind
- Untersuchungen in Form von Datenschutzüberprüfungen
- Zugriff auf alle personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind
- Zugang zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräte

Abhilfe-befugnisse der Aufsichts-behörden, z.B.

- Warnungen, dass beabsichtigte Verarbeitungsvorgänge möglicherweise gegen die DSGVO verstoßen
- Anweisung zur Erfüllung von Rechten der Betroffenen (z.B. Auskunft, Datenportierung, Löschung, Information)
- Anordnung zur Aussetzung von Datenverarbeitungsprozessen und Datenübermittlungen

13. Sanktionen (1)

Verhängung von Geldbußen

Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag werden bestimmte Faktoren berücksichtigt (z.B. Art, Schwere und Dauer des Verstoßes, Zahl der Betroffenen und das Ausmaß des von ihnen erlittenen Schadens, Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes, getroffene Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens, Grad der Verantwortung unter der Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen, etwaige einschlägige frühere Verstöße).

- „Geringfügige“ Verstöße: EUR 10 Mio. oder bis zu 2% des gesamten weltweiten Jahresumsatzes des abgelaufenen Finanzjahres, je nachdem, was höher ist.
    - Einwilligungserfordernisse bei Kindern
    - Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen
    - Ernennung eines Vertreters und/oder eines Datenschutzbeauftragten
    - Einsetzen von Auftragsverarbeitern
    - Interne Aufzeichnung von Verstößen und Datenschutzfolgeabschätzung
    - Sicherheitsvorkehrungen (TOMs)
    - Meldungen von Verletzungen des Schutzes personenbezogener Daten

13. Sanktionen (2)

Verhängung von Geldbußen

- „Schwerwiegende“ Verstöße: EUR 20 Mio. oder bis zu 4% des gesamten weltweiten Jahresumsatzes des abgelaufenen Finanzjahres, je nachdem, was höher ist.
  - Einfache Verarbeitungsgrundsätze, wie z.B. Fairness, Rechtmäßigkeit, Transparenz, Datensparsamkeit, Zweckbegrenzung, Gründlichkeit, Aufbewahrungsfristen, Einwilligung, Rechtmäßigkeit der Verarbeitung bei Daten besonderer Datenkategorien
  - Betroffenenrechte
  - Internationale Datenübermittlungen
  - Nichteinhaltung einer Anordnung der Aufsichtsbehörde

Baker & McKenzie has been global since inception.
Being global is part of our DNA.

BAKER & MCKENZIE

Dr. Matthias Scholz, LL.M.
Partner

Baker & McKenzie
Partnerschaft von Rechtsanwälten,
Wirtschaftsprüfern und Steuerberatern mbB

Bethmannstrae 50-54
60311 Frankfurt/Main

T: +49 69 2 99 08 203
M: +49 172 70 63 559
matthias.scholz@bakermckenzie.com