Baker McKenzie.

Datenschutzrecht

17. General Management MBA, 26. Mai 2017

RA Dr. Lukas Feiler, SSCP CIPP/E

1 Grundlagen

Datenschutz als Grundrecht

- Europäische Menschenrechtskonvention
  - Schützt Privatsphäre (Artikel 8)
- EU Grundrechtscharta
  - Schützt das Grundrecht auf Datenschutz (Artikel 8)
- Österreich: § 1 Datenschutzgesetz 2000
- USA
  - 4. Verfassungszusatz: Schutz vor unreasonable searches & seizures; gilt aber nur wenn "reasonable expectation of privacy" (Katz v. United States, 389 U.S. 347 (1967))
    → secrecy paradigm

Wozu Datenschutz-Compliance?

- Bisher:
  - In Österreich: Datenschutzgesetz 2000 (DSG 2000)
- Ab 25. Mai 2018: Datenschutz-Grundverordnung der EU (DSGVO)
  - Geldstrafen von bis zu 20 Millionen Euro oder vier Prozent des gesamten, weltweit erzielten Jahresumsatzes
- Haftung der Geschäftsleitung
  - Für Verwaltungsstrafen haften Mitglieder der Geschäftsleitung grds solidarisch mit der Gesellschaft
  - Haftung gegenüber der Gesellschaft aus Dienstvertrag

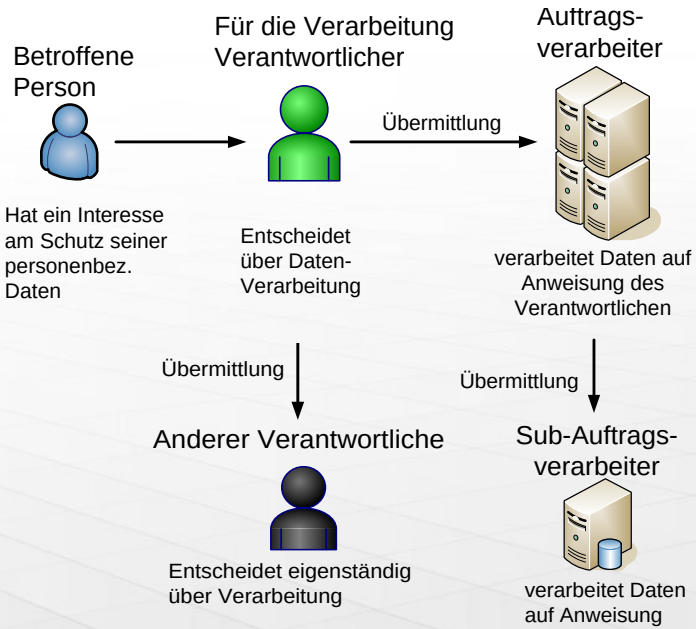
2 Rechte und Pflichten nach der DSGVO

Akteure im Bereich des Datenschutzrechts

- Betroffene Person
  - identifizierte oder identifizierbare natürliche Person
- Verantwortlicher
  - (idR juristische) Person, die über Mittel und Zwecke der Datenverarbeitung entscheidet
- Auftragsverarbeiter
  - Verarbeitet personenbezogene Daten im Auftrag und auf Anweisung eines Verantwortlichen
- Datenschutzbehörde (DSB)

Aktualisierte Terminologie

Die neuen Akteure



Entstehungsgeschichte

Hintergrund

- EU-Datenschutzrichtlinie von 1995:
  - Nicht direkt anwendbar → 28 unterschiedliche nationale Datenschutzgesetze → der damit verbundene Verwaltungsaufwand kostet Unternehmen ca. EUR 2,3 Mrd. pro Jahr
  - Datenschutzrechtliche Meldungen in fast allen EU-Mitgliedstaaten kosten Unternehmen ca. EUR 130 Mio. pro Jahr

- EU-Datenschutz-Grundverordnung:
  - Eine einheitliche und unmittelbar anwendbare Datenschutz-Rechtsvorschrift, die die meisten umständlichen Verwaltungsanforderungen abschafft

Entstehungsgeschichte

Rechtsetzungsprozess

- Der Rechtsetzungsprozess dauerte lange und war komplex
  - Fast 4000 Änderungen wurden von Mitgliedern des EP eingebracht
  - Die Abstimmung des EP wurde zweimal vertagt
- Zeitlicher Ablauf
  - Januar 2012: Die Kommission bringt einen ersten Vorschlag ein
  - März 2014: EP nimmt den Entwurf in einer Plenarabstimmung (1. Lesung) an
  - Juni 2014: Der Rat verabschiedet eine gemeinsame Position zu einigen Aspekten
  - 15. Dezember 2016: Politische Einigung im Trilog
  - 25. Mai 2018: DSGVO tritt in Geltung

Anwendungsbereich

Welche Datenverarbeitungen erfasst sind

- Jede Verarbeitung personenbezogener Daten ist erfasst
- Verarbeiten: jede Handhabung personenbezogener Daten (auch das Gespeichert-Halten)
- Personenbezogene Daten: Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen
  - DSG 2000: natürliche und juristische Personen
  - DSGVO: nur natürliche Personen

Anwendungsbereich

Wo die Datenschutz-Grundverordnung gilt

- DSGVO gilt für Verantwortliche/Auftragsverarbeiter
  - mit Sitz in der EU bzw EWR;
  - ohne Sitz in der EU/EWR aber mit einer Niederlassung in der EU/EWR, wenn Verarbeitung im Rahmen der Tätigkeiten der Niederlassung;
  - ohne Sitz in der EU, aber
    - Waren oder Dienstleistungen werden in der EU/EWR angeboten
    - Verhalten von Betroffenen in der EU/EWR wird beobachtet

Verhältnis zu nationalem Recht

Einheitliche Rechtsvorschrift mit Ausnahmen

- Unmittelbare Anwendbarkeit der DSGVO
  - Kein Fortbestehen der nationalen Datenschutzgesetze nach dem 25. Mai 2018
  - Prinzip der einheitlichen Auslegung
- Außerhalb des Anwendungsbereichs der DSGVO
  - Spielraum des nationalen Gesetzgebers
  - 69 Öffnungsklauseln
- Europäische Kommission kann „delegierte Rechtsakte“ erlassen
  - Vorschlag der Kommission: 26 Kompetenzen
  - EP-Abstimmung: 10 Kompetenzen
  - Endgültige Vereinbarung: 2 Kompetenzen

Verhältnis zu nationalem Recht

Öffnungsklauseln für nationale Gesetzgeber

- DSGVO überlässt viele Fragen den nationalen Gesetzgebern (u.a.):
  - Alter für eine wirksame Einwilligung eines Kindes: 16, 15, 14 oder 13?
  - Wann ist wirksame Einwilligung in Verarbeitung sensibler Daten ausgeschlossen?
  - Verarbeitung von strafrechtlich relevanten Daten möglich?
  - Ausnahmen vom Profiling-Verbot?
  - Unterliegen Betroffenenrechte zusätzlichen Beschränkungen?
  - Muss ein Datenschutzbeauftragter bestellt werden?
  - Können Behörden Geldbußen auferlegt werden?
  - Können Datenschutz-NGOs im Namen der betroffenen Personen Schadenersatz fordern? Können sie selbst eine einstweilige Verfügung erwirken?

Verhältnis zu nationalem Recht

Rechtsdurchsetzung durch nationale Behörden

- Durchsetzung durch die nationalen Aufsichtsbehörden
  - Europäische Kommission hat keine Durchsetzungsbefugnis
  - Europäischer Datenschutzausschuss
    - Ersetzt Artikel-29-Datenschutzgruppe
    - Nur zuständig für Streitigkeiten zwischen Aufsichtsbehörden

Grundsätze der Datenverarbeitung

- Rechtmäßigkeit (Rechtsgrundlage für Verarbeitung erforderlich)
- Treu und Glauben
- Transparenz
- Zweckfestlegung
- Zweckbindung
- Richtigkeit
- Datenminimierung
- Speicherbegrenzung
- Sicherheit
- Rechenschaftspflicht

Rechtmäßigkeit der Datenverarbeitung

Datenschutzrechtliche Rechtsgrundlagen

1. Einwilligung der betroffenen Person (informierte und freiwillige Zustimmung)
2. Erforderlichkeit für die Erfüllung des mit betroffener Person geschlossenen Vertrages
3. Gesetzliche Verpflichtung des Verantwortlichen
4. Lebenswichtige Interessen der betroffenen Person
5. Erforderlichkeit für Aufgabe im öffentlichen Interesse oder Ausübung öffentlicher Gewalt
6. Überwiegende berechtigte Interessen des Verantwortlichen oder eines Dritten

Rechtmäßigkeit der Datenverarbeitung

Neue Grenzen für die elektronische Einwilligung

- Schlüssige oder ausdrückliche Zustimmung
- Checkbox darf nicht per Default angehakt sein
- Zustimmung durch AGB?
  - in verständlicher und leicht zugänglicher Form
  - in klarer und einfacher Sprache
  - von anderen Regelungsgegenständen der AGB klar zu unterscheiden

Rechtmäßigkeit der Datenverarbeitung

Einwilligung von Personen unter 16 Jahren

- Zustimmung von Minderjährigen für Online-Dienste grds erst gültig ab 16 Jahren
- < 16 Jahre: Zustimmung der Erziehungsberechtigten erforderlich
  - Verantwortlicher muss „angemessene Anstrengungen unter Berücksichtigung der vorhandenen Technologie“ unternehmen
- Praktische Umsetzung
  - Angebot nicht auf Unter-16-Jährige ausrichten
  - Registrierung nur zulassen, wenn Geburtsdatum angegeben
- Nationales Recht: Altersgrenze kann auf bis zu 13 Jahre herabgesetzt werden

Rechtmäßigkeit der Datenverarbeitung

Herausforderung für Gratis-Dienste

- Viele „Gratis“-Dienste im Internet setzen Zustimmung zur Datenerhebung voraus
- Zustimmung nur gültig, wenn sie „frei“ ist
- Grds nicht „frei“, wenn

die Durchführung eines Vertrages von Zustimmung zur Datenverarbeitung abhängig gemacht wird und

  - die Datenverarbeitung für die Vertragserfüllung nicht erforderlich ist

- Stehen die datengestützten Geschäftsmodelle auf dem Spiel?
  - Die Einwilligung kann für die Vertragserfüllung (wirtschaftlich) notwendig sein
  - Alternativ anbieten:
    - keine Gebühr + datenschutzrechtliche Einwilligung oder
    - angemessene Gebühr

Rechtmäßigkeit der Datenverarbeitung

Einwilligung bei sensiblen Daten

- Als sensible Daten gelten: Daten aus denen
  - rassische und ethnische Herkunft,
  - politische Meinungen,
  - religiöse oder weltanschauliche Überzeugungen oder
  - Gewerkschaftszugehörigkeit hervorgeht

  und
  - genetische und biometrische Daten zur Identifizierung einer natürlichen Person
  - Gesundheitsdaten sowie Daten zum Sexualleben

→ überwiegendes berechtigtes Interesse ist nicht ausreichend

→ Einwilligung muss ausdrücklich erfolgen

Transparenz

Erweiterte Datenschutzerklärung

- Die Datenschutzerklärung muss folgende Angaben enthalten
  1. die Identität des Verantwortlichen
  2. den Datenschutzbeauftragten
  3. die Verarbeitungszwecke
  4. die rechtliche Grundlage der Verarbeitung
  5. die Empfänger
  6. die internationalen Datenübermittlungen
  7. die Dauer der Datenspeicherung
  8. das überwiegende berechtigte Interesse (sofern als Rechtsgrundlage genutzt)
  9. Betroffenenrechte
  10. Möglichkeit, die Einwilligung zu widerrufen
  11. Bestehen eines Beschwerderechts
  12. Bei Profiling: Entscheidungslogik

Neue Betroffenenrechte

Datenübertragbarkeit, Vergessenwerden

- Recht auf Datenübertragbarkeit
  - Recht auf Übermittlung der Daten in einem wiederverwendbaren Format an den Betroffenen oder Dritten
  - gilt nur gegenüber Verantwortlichen
  - gilt nur, wenn Daten vom Betroffenen bereitgestellt wurden
  - gilt nur, wenn Verarbeitung mit Einwilligung oder zur Vertragserfüllung
- Recht auf Vergessenwerden

  = Recht auf Löschung

Neue Betroffenenrechte

Einschränkung der Verarbeitung

- Recht der betroffenen Person auf Einschränkung der Verarbeitung wenn:
  - die Richtigkeit der Daten von betroffener Person bestritten wird – für Dauer der Überprüfung der Richtigkeit
  - die Verarbeitung unrechtmäßig ist, die betroffene Person jedoch eine Löschung ablehnt
  - der Verantwortliche die Daten nicht länger benötigt; aber die betroffene Person benötigt diese zur Geltendemachung, Ausübung oder Verteidigung von Rechtsansprüchen
  - die betroffene Person Widerspruch eingelegt hat – bis über diesen entschieden wurde

Melde- und Dokumentationspflichten

Verzeichnis der Verarbeitungstätigkeiten

- Dokumentationspflichten bisher:
  - Österreich: grds keine
  - Deutschland: Führung eines Verfahrensverzeichnisses
- DSGVO: Führung eines „Verzeichnisses der Verarbeitungstätigkeiten“
  - auf Anfrage der Aufsichtsbehörde bereitzustellen
  - keine Pflicht, Verzeichnis betroffenen Personen zur Verfügung zu stellen
- Mindestinhalt des Verzeichnisses nach DSGVO:
  - Name und Kontaktdaten des Verantwortlichen und eines etwaigen Datenschutzbeauftragten
  - Verarbeitungszwecke, Kategorien betroffener Personen, personenbezogener Daten und Empfänger
  - Informationen zu Datenübermittlungen in Drittländer
  - Speicherdauer
  - Datensicherheitsmaßnahmen

Privacy Impact Assessments

- Privacy Impact Assessment verpflichtend, wenn voraussichtlich ein hohes Risiko für Betroffene durch Datenverarbeitung besteht, insbesondere bei
  - Profiling;
  - umfangreicher Verarbeitung sensibler oder strafrechtlich relevanter Daten;
  - systematischer, umfangreicher Überwachung öffentlicher Bereiche
- Inhalt des Privacy Impact Assessments
  - Beschreibung der Verarbeitungsvorgänge und Zwecke
  - Bewertung der Notwendigkeit und Verhältnismäßigkeit
  - Beschreibung allfälliger Abhilfemaßnahmen
  - Risikobewertung (niedrig/mittel/hoch) unter Berücksichtigung der Abhilfemaßnahmen

Melde- und Dokumentationspflichten

Bisherige Meldepflichten

- Derzeit geltende EU-Datenschutzrichtlinie: Ausnahmen von der Meldepflicht für Mitgliedstaaten nur auf folgender Grundlage möglich:
  - Bestellung eines betrieblichen Datenschutzbeauftragten
  - Datenverarbeitungsverfahren mit niedrigem Risiko
- In Österreich: Jede Datenanwendung ist vorab an Datenschutzbehörde zu melden
  - Ausnahme: sog. „Standard-Datenanwendung“ (z.B. Personalverwaltung für privatrechtliche Verhältnisse)
  - Wenn sensible Daten oder strafrechtlich relevante Daten betroffen (z.B. Videoüberwachung): Genehmigungsvorbehalt

Melde- und Dokumentationspflichten

DSGVO reduziert Meldepflichten

- Keine allgemeine Meldepflicht
- Aber vorherige Konsultation der Aufsichtsbehörde
  - wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung mit einem hohen Risiko verbunden ist, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.
  - ist die Aufsichtsbehörde der Auffassung, dass der Verantwortliche das Risiko nicht ausreichend eingedämmt hat, unterbreitet sie innerhalb von acht Wochen entsprechende Empfehlungen.

Privacy by Design & Privacy by Default

- Privacy by Design (Datenschutz durch Technik)
  - technische Maßnahmen zur Umsetzung der Datenschutzgrundsätze

  z.B. Minimierung von Art und Umfang der Daten und Pseudonymisierung der Daten
- Privacy by Default (Datenschutz durch datenschutzrechtliche Voreinstellungen)
  - personenbezogene Daten sollten durch Voreinstellungen nicht ohne Eingreifen der betroffenen Person veröffentlicht werden
- Relevanz für Softwarehersteller?

Datensicherheitspflichten

Vertraulichkeit, Verfügbarkeit, Integrität

- Daten sind zu schützen vor
  - Verlust der Vertraulichkeit
  - Verlust der Verfügbarkeit
  - Verlust der Integrität
- Risikoangemessene Sicherheitsmaßnahmen unter Berücksichtigung
  - des Stands der Technik,
  - der Implementierungskosten,
  - der Art, des Umfangs, der Umstände & Zwecke der Verarbeitung und
  - der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

Datensicherheitspflichten

Sicherheitsmaßnahmen

- Angemessene Maßnahmen umfassen laut DSGVO insb.:
  - Pseudonymisierung und Verschlüsselung;
  - die Fähigkeit, die Sicherheit der Systeme sicherzustellen;
  - die Fähigkeit, die Verfügbarkeit nach einem Zwischenfall rasch wiederherzustellen → Incident Response Capabilities;
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Sicherheitsmaßnahmen → Audits
- Technische Standards ausreichend?
  - z.B. „Critical Security Controls für Effective Cyber Defense“ des Center for Internet Security (CIS) oder ISO/IEC 27001

Typen von Sicherheitsmaßnahmen

- Nach der Art der Maßnahme: Technische, organisatorische und physische Maßnahmen
- Nach der Wirkungsweise: präventive, detektive, reaktive oder absreckende Maßnahmen

Beispiele	Technical	Organizational	Physical
Präventiv	Firewall	4-Augen-Prinzip	Stahltür
Detektiv	Intrusion Detection System	Verpflichtender Log Review	Brandmelder
Reaktiv	(Backup &) Restore	Incident Response Policy	Feueralarm
Abschreckend	Warnmeldung	Disziplinarordnung	Hung

Melde- und Dokumentationspflichten

Meldung von Datensicherheitsverstößen

- auch Pflicht zur „Data Breach Notification“
- Eine Verletzung des Schutzes personenbezogener Daten muss der Aufsichtsbehörde unverzüglich und spätestens binnen 72 Stunden gemeldet werden
- Pflicht zur Notifikation gegenüber betroffenen Personen nur, wenn das bestehende Risiko hoch ist

Der Datenschutzbeauftragte

Bestellung

- DSG 2000: Keine Regelungen
- Mit der DSGVO verpflichtend, wenn
  - Verarbeitung durch Behörde oder öffentliche Stelle

    oder
  - Daten-getriebenes Geschäftsmodell
    - Kerntätigkeit des Unternehmens ist umfangreiche regelmäßige und systematische Überwachung von Betroffenen
    - Kerntätigkeit des Unternehmens ist die umfangreichen Verarbeitung sensibler oder strafrechtlich relevanter Daten

    oder
  - nach nationalem Recht vorgeschrieben (voraussichtlich nicht in Österreich)

Persönliche Voraussetzungen

- Persönliche Voraussetzungen
  - berufliche Qualifikation und Fachwissen auf dem Gebiet des Datenschutzrechts
  - kann, muss aber nicht Arbeitnehmer des Verantwortlichen sein
  - es darf kein Interessenskonflikt vorliegen
- Bestellung eines externen Datenschutzbeauftragten ist möglich

Der Datenschutzbeauftragte

Stellung im Unternehmen

- weisungsfrei
- genießt Kündigungsschutz
- unmittelbare Berichterstattung an die höchste Managementebene
- Einbindung in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen
- muss über alle notwendigen Ressourcen verfügen
- hat Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen
- Anlaufstelle für betroffene Personen
- Verschwiegenheitsverpflichtung
- Grds keine Haftung nach der DSGVO

Outsourcing an Auftragsverarbeiter

- Verantwortlicher kann sich zur Datenverarbeitung eines Auftragsverarbeiters bedienen
  - Auftragsverarbeiter muss ausreichende Gewähr für rechtmäßige und sichere Datenverwendung bieten
- Auftragsverarbeitervereinbarung muss Pflichten des Auftragsverarbeiters festlegen:
  - Verarbeitung nur auf dokumentierte Weisungen des Verantwortlichen;
  - Vertraulichkeit von zur Verarbeitung befugter Personen gewährleisten;
  - muss notwendige Sicherheitsmaßnahmen umsetzen;
  - nach Abschluss der Leistungserbringung personenbezogene Daten löschen/zurückgeben;
  - Einsatz von Sub-Auftragsverarbeitern nur mit Genehmigung des Verantwortlichen;
  - Duldung und Unterstützung von Audits;
  - stellt dem Verantwortlichen sämtliche Informationen zum Nachweis der Einhaltung zur Verfügung

Internationale Datenübermittlungen

- Unproblematisch bei Empfängern
  - in der EU oder dem EWR;
  - in einem Drittland mit adäquatem Datenschutzniveau
    - z.B. Kanada, Schweiz
    - U.S.-Privacy-Shield: angemessener Datenschutz, wenn sich der Empfänger nach Privacy Shield selbst-zertifiziert hat
- Wenn in Drittland kein adäquates Datenschutzniveau
  - grundsätzlich „Standardvertragsklauseln“ erforderlich
    - DSG 2000: genehmigungspflichtig
    - DSGVO: keine Genehmigung erforderlich
  - Ausnahme: Einwilligung der Betroffenen

Zuständigkeit der nationalen Behörden

- Die Durchsetzungsbefugnis liegt bei den nationalen Aufsichtsbehörden
- Welche Aufsichtsbehörde ist zuständig?
  - Kein echter One-Stop-Shop (Verfahren der Zusammenarbeit und Kohärenz) für Konzerne
  - Allgemein gilt: jede Aufsichtsbehörde ist im Hoheitsgebiet ihres Mitgliedstaats zuständig

Fehlendes Kollisionsrecht

- Das nationale Recht welches Mitgliedstaats ist anwendbar?
- DSGVO enthält (bis auf eine Ausnahme) keine Regelungen zu Gesetzeskonflikten in Bezug auf Öffnungsklauseln
  - Das Recht des Landes, in dem der für die Verarbeitung Verantwortliche niedergelassen ist?
  - Das Recht des Landes, in dem die betroffene Person ihren Wohnsitz hat?
  - Das Recht des Landes, in dem die Daten verarbeitet werden?
  - Wendet jede Aufsichtsbehörde ihre eigenen Rechtsvorschriften an?
  - Das Recht welches Mitgliedstaats wenden die Gerichte an?

    Wird die Beschwerde einer betroffenen Person abgewiesen, entscheidet die Aufsichtsbehörde, bei der die Beschwerde eingelegt wurde; wird der Beschwerde stattgegeben, entscheidet die federführende Aufsichtsbehörde → kollisions- und zuständigkeitsrechtliches Paradox

Befugnisse der Aufsichtsbehörden

- Untersuchungsbefugnisse
- Abhilfebefugnisse
  - Warnungen über voraussichtliche Verstöße gegen Verordnung erteilen
  - Verwarnungen bei Verstößen gegen Verordnung erteilen
  - Einhaltung anordnen und Verarbeitungsverbote/-einschränkungen verhängen
- Genehmigungsbefugnisse

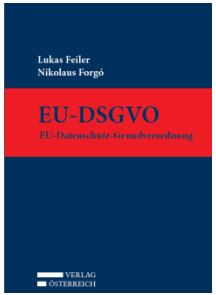
Verhängung und Bemessung von Geldstrafen

- Strafrahmen nach DSGVO: bis zu 20 Millionen Euro oder vier Prozent des weltweiten, jährlichen Umsatzes des Unternehmens
- Unionskartellrechtlicher Unternehmensbegriff
  - Bemessung der Strafe: weltweiter Umsatz des gesamten Konzerns maßgeblich
  - Strafe kann auch über Konzernmutter verhängt werden
    - Mitverantwortung der Konzernobergesellschaft, wenn Tochtergesellschaft Verhalten nicht autonom bestimmt
    - widerlegliche Vermutung bei 100%-igen Tochtergesellschaften (EuGH C-107/82 – AEG)

Private Rechtsdurchsetzung

- Betroffene Person kann klagen,
  - wo sie ihren Wohnsitz hat;
  - wo der Verantwortliche/Auftragsverarbeiter eine Niederlassung hat
- Mögliche Ansprüche:
  - Betroffenenrechte (Auskunft, Löschung, …)
  - Materieller und immaterieller Schadenersatz
- Rechtsdurchsetzung durch NGOs:
  - NGOs können im Namen von Betroffenen klagen
  - Schadenersatzansprüche nur, wenn nach nationalem Recht zugelassen (nach welchem?)
  - Betroffenenrechte unabhängig von Auftrag eines Betroffenen einklagen (je nach Gerichtsstand)

Baker McKenzie.



Dr. Lukas Feiler, SSCP CIPP/E
Senior Associate
Leiter des Teams für IT-Recht in Wien

Schottenring 25
1010 Vienna

T: +43 1 24 250
lukas.feiler@bakermckenzie.com

Lukas Feiler ist Co-Autor des ersten österreichischen Kommentars zur Datenschutz-Grundverordnung und begleitet Unternehmen auf www.digitalwave.at bei der digitalen Transformation

www.bakermckenzie.com