ATTORNEYS AT LAW

Revision der Datenschutz-gesetzgebung

Nicht ohne den europäischen Daten-schutz

RA Dr. Michael Reinle, LL.M., Zürich
Bühlmann Rechtsanwälte AG
www.br-legal.ch

Themenübersicht

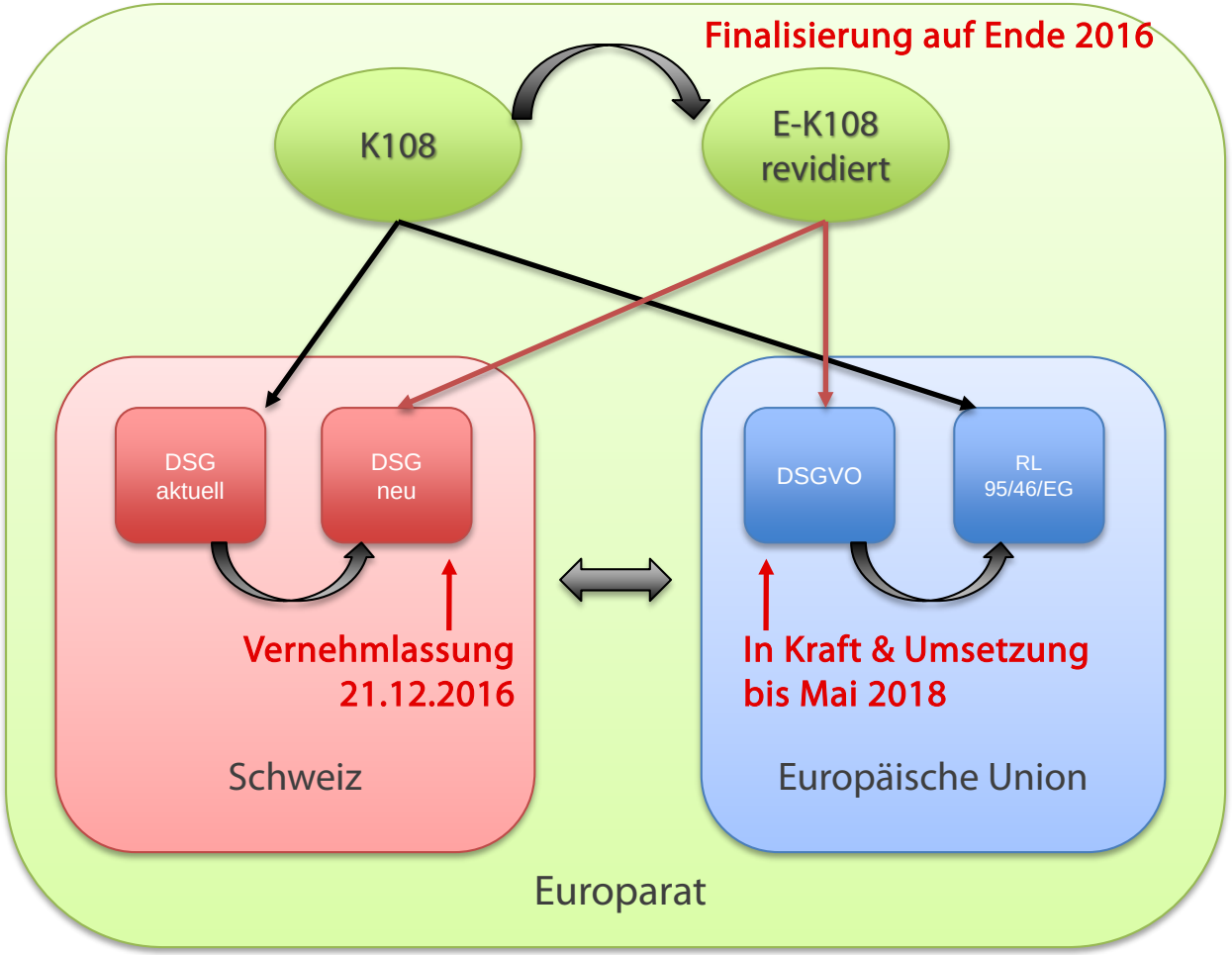
- Wo stehen wir? Laufende Reformen auf europäischer Ebene mit Relevanz für die Schweiz
- Regelungen im Überblick
- Räumlicher Geltungsbereich
- Einwilligung
- Profiling
- Informationspflichten
- Datenschutzfolgeabschätzung
- Kompetenzen der Aufsichtsbehörden

Revision der Datenschutzgesetzgebung

Wo stehen wir?

- DSG-Revision nicht im luftleeren Raum
  - Modernisierung der Datenschutzkonvention SEV 108 des Europarates (E-K108)
  - EU-Datenschutzgrundverordnung
- Starker Einfluss der E-K108
  - Aber: keine Revolution notwendig
  - Adäquanz mit internationalem Standard für grenzüberschreitende Datentransfers (vgl. Art. 6 DSG)
- EU-Datenschutzgrundverordnung
  - Keine Notwendigkeit der eins-zu-eins Übernahme
  - Angemessenheit genügt
  - Aber: Bilaterales Übereinkommen Schweiz-EU betreffend Anwendbarkeit der EU-DSGVO

Laufende Reformen mit Relevanz für die Schweiz



Wichtige Bestimmungen

E-K108: Regelungen im Überblick

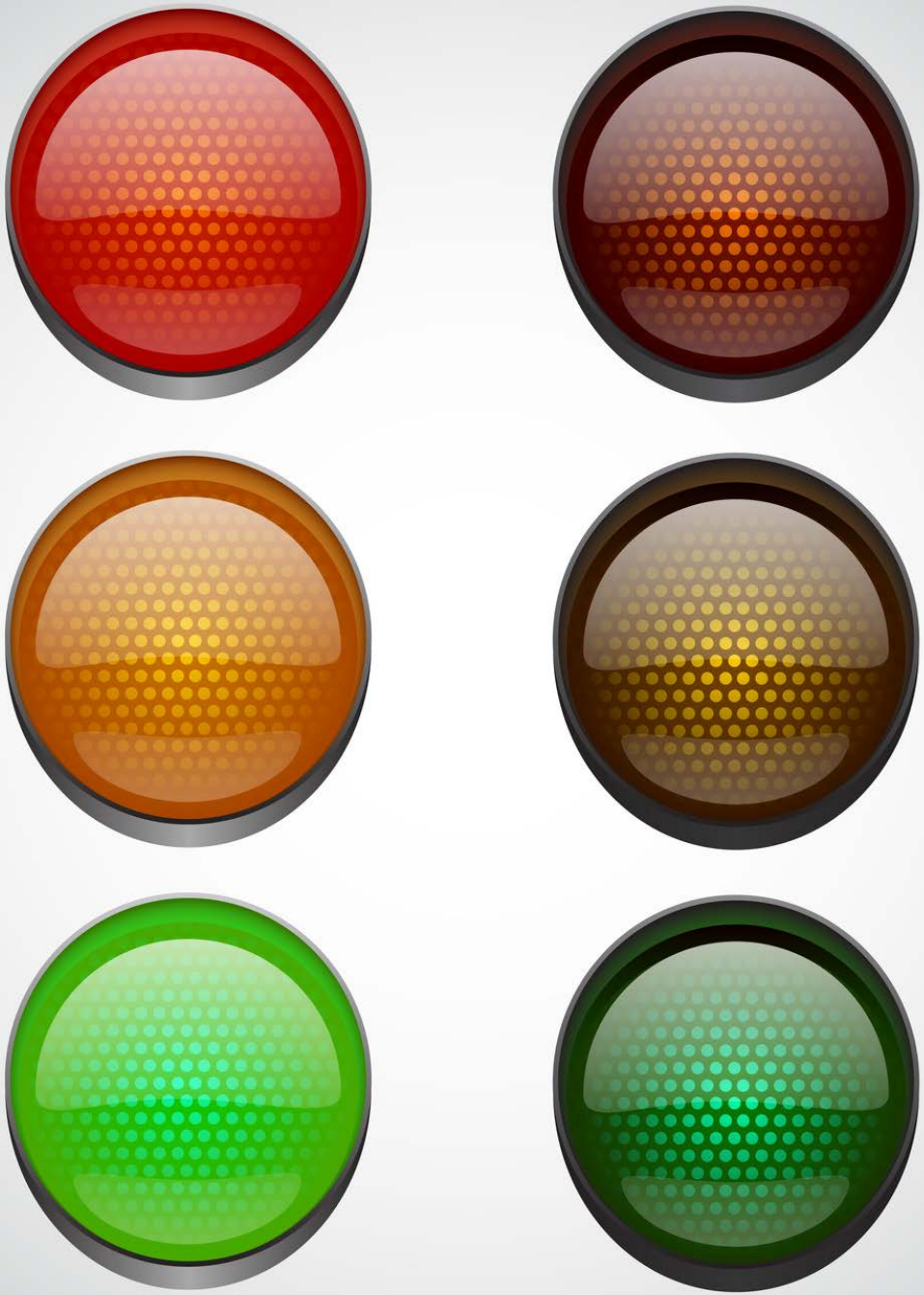
- Definitionen (z.B. Personendaten, Verantwortlicher, Bearbeiter, Empfänger; Art. 2 E-K108)
- Datenbearbeitungsgrundsätze (Art. 5 E-K108)
- Rechtmässigkeit der Datenbearbeitung (Art. 5 Ziff. 3 E-K108)
- Einwilligung (Art. 5 Ziff. 2 E-K108)
- Spezialkategorien von Personendaten (Art. 6 E-K108)
- Datensicherheit (Art. 7 E-K108)
- Informationspflicht bei direkter Datenbeschaffung (Art. 7bis Ziff. 1 und 1bis E-K108)
- Informationspflicht bei indirekter Datenbeschaffung (Art. 7bis Ziff. 2 E-K108)
- Recht, nicht einer automatisierten Einzelfallentscheidung unterworfen zu sein (Art. 8 Ziff. 1 lit. a E-K108)
- Auskunftsrecht (Art. 8 Ziff. 1 lit. b E-K108)
- Widerspruchsrecht (Art. 8 Ziff. 1 lit. d E-K108)
- Berichtigungs- und Löschungsrecht (Art. 8 Ziff. 1 lit. e E-K108)
- Pflicht zum Nachweis der Datenschutz-Compliance (Art. 8bis Ziff. 1 E-K108)
- Datenschutzfolgeabschätzung (Art. 8bis Ziff. 2 E-K108)
- Data Protection by Design / Default (Art. 8bis Ziff. 2 und 3 E-K108)
- Notifikation von Datenschutzpannen an die Aufsichtsbehörden (Art. 7 Ziff. 2 E-K108)
- Sanktionen und Rechtsbehelfe (Art. 10 E-K108)
- Auslandtransfers (Art. 12 E-K108)
- Kompetenzen der Aufsichtsbehörden (Art. 12bis E-K108)

EU-DSGVO: Regelungen im Überblick

- Extraterritoriale Anwendung (Art. 3 DSGVO)
- Definitionen (z.B. Profiling und Pseudonymisierung; Art. 4 DSGVO)
- Datenbearbeitungsgrundsätze (Art. 5 DSGVO)
- Rechtmässigkeit der Datenbearbeitung (Art. 6 DSGVO)
- Einwilligung (Art. 7 DSGVO)
- Spezialkategorien von Personendaten (Art. 9 DSGVO, „besonders schützenswerte Daten")
- Informationspflicht bei direkter Datenbeschaffung (Art. 13 DSGVO)
- Informationspflicht bei indirekter Datenbeschaffung (Art. 14 DSGVO)
- Auskunftsrecht (Art. 15 DSGVO)
- Berichtigungsrecht (Art. 16 DSGVO)
- Löschungsrecht (Art. 17 DSGVO)
- Recht einer Datenbearbeitung zu widersprechen (Art. 21 DSGVO)
- Verantwortung der verantwortlichen Stelle (Art. 24 DSGVO)
- Data Protection by Design / Default (Art. 25 DSGVO)
- Benennung eines Vertreters durch Nicht-EU-Unternehmen, falls DSGVO auf diese anwendbar (Art. 27 DSGVO)
- Auftragsdatenbearbeitung (Art. 28 f. DSGVO)
- Pflicht, alle Datenbearbeitungen zu dokumentieren (Art. 30 DSGVO)
- Notifikation von Datenschutzpannen an die Aufsichtsbehörden (Art. 33 DSGVO)
- Notifikation von Datenschutzpannen an betroffene Personen (Art. 34 DSGVO)
- Datenschutzfolgeabschätzung (Art. 35 DSGVO)
- Benennung eines Datenschutzverantwortlichen (Art. 37 DSGVO)
- Auslandsdatentransfer (Art. 44 ff. DSGVO)
- Administrativbussen (Art. 83 DSGVO)

Ausgewählte Kernthemen zur Diskussion…..

- Anwendungsbereich DSGVO
- Einwilligung
- Profiling
- Informationspflichten
- Datenschutzfolgeabschätzung
- Kompetenzen der Aufsichtsbehörden



Räumlicher Geltungsbereich

Art. 3 DSGVO: Anwendung auch auf Nicht-EU-Unternehmen

1. Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.
2. Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht
   - betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;
   - das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

…

Konstellationen

- Bearbeitung von Daten durch **EU-Niederlassung eines CH-Unternehmens** oder **Teilnahme an Datenbearbeitungen** von EU-Unternehmen (z.B. in Konzernverhältnissen)

- **Verkauf von Waren oder Dienstleistungen** eines CH-Unternehmens an EU-Kunden oder **Überwachung des Verhaltens** von Personen, sofern sich das Verhalten in der EU abspielt – z.B. Trackingtools in Webshop, der auch auf EU-Kunden ausgerichtet ist

- CH-Unternehmen beauftragt EU-Unternehmen zur **Auftragsdatenverarbeitung** (z.B. Cloud-Anbieter) – auch bei **Sub-Processing** des EU-Verarbeiters an Unternehmen ausserhalb der EU oder Bearbeitung von Personendaten durch CH-Unternehmen **im Auftrag** eines EU-Unternehmens (z.B. einer EU-Niederlassung)

Einwilligung

Einwilligung DSGVO

Art. 6 Abs. 1 Satz 1 lit. a, 7 DSGVO

- Definition (Art. 4 Nr. 11 DSGVO)
  - freiwillig
  - für den bestimmten Fall
  - in informierter Weise und
  - unmissverständlich abgegebene Willensbekundung
  - in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung
- Form
  - eindeutige bestätigende Handlung
  - schriftliche Erklärung, die auch elektronisch erfolgen kann
  - „Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen." (EG 32) → kein Opt-Out

Einwilligung E-K108

- Art. 5 Ziff. 2 E-K108
  - Free, specific, informed and unambigous consent
  - Abgabe eines klaren Statements (given by a statement), z.B. schriftlich, auf elektronischem Weg oder mündlich; oder
  - Klare, affirmative Handlung, welche im betreffenden Kontext klar zum Ausdruck bringt, dass die betroffene Person die beabsichtigte Datenbearbeitung akzeptiert
  - Stillschweigen, Inaktivität oder vorangekreuzte Formulare oder Boxen sollen nicht als Zustimmung gelten („Mere silence, inactivity or pre-validated forms and boxes should not, therefore constitute consent“)
  - Zustimmung soll alle Datenbearbeitungen für denselben Zweck oder dieselben Zwecke erfassen
  - Bei unterschiedlichen Zwecken soll die Zustimmung für jeden einzelnen Zweck gegeben werden („in the case of multiple purposes, consent should be given for each different purpose“)

Profiling

- Art. 4 DSGVO
  - **Definition «Profiling»**: jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen
  - Keine generelle ausdrückliche Zustimmung für das Profiling; es gilt Art. 6 DSGVO
  - Ausdrückliche Zustimmung wird nur in Art. 22 DSGVO im Zusammenhang mit Profiling erwähnt. Dort geht es jedoch um automatisierte Entscheidungen im Einzelfall – inklusive Profiling – mit rechtlicher Wirkung oder erheblicher Beeinträchtigung

- E-K108
  - Keine Definition und spezifische Regelung des Profilings

Informationspflichten

Direkte Datenbeschaffung (DSGVO)

- **Informationspflicht bei allen Datenbearbeitungen**
  1. Namen und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters
  2. Kontaktdaten des Datenschutzbeauftragten
  3. Zwecke und Rechtsgrundlage
  4. Ggf. die berechtigten Interessen an einer Datenverarbeitung
  5. Ggf. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
  6. Ggf. die Absicht einer Übermittlung in Drittstaaten oder an eine internationale Organisation
  7. Weitere Informationen, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten
  8. Dauer der Datenspeicherung bzw. Kriterien für die Festlegung der Dauer
  9. Bestehen von Betroffenenrechten wie Auskunft, Berichtigung, Löschung, Sperrung, Widerspruchsrecht oder Datenübertragbarkeit
  10. Widerrufsrecht bei einwilligungsbasierter Datenverarbeitung
  11. Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
  12. Ggf., ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben ist oder für den Vertragsschluss erforderlich ist
  13. Bestehen einer automatisierten Entscheidungsfindung einschliesslich Profiling sowie aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person

Indirekte Datenbeschaffung (DSGVO)

- Aktive Informationspflicht (Art. 14 DSGVO)
  - Gilt auch bei der Beschaffung von Daten aus Drittquellen
  - Spätestens einen Monat nach Datenerhebung aus Drittquelle
  - Ausnahme: Information ist unmöglich, unverhältnismässig oder würde den verfolgten Zweck vereiteln

- Inhalt der Information
  - Namen und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters
  - Kontaktdaten des Datenschutzbeauftragten
  - Bearbeitungszwecke und Rechtsgrundlage für Datenbearbeitung
  - Kategorien der bearbeiteten Personendaten
  - Empfänger oder Kategorien von Empfängern der Personendaten
  - …

Informationspflicht E-K108

- Aktive Informationspflicht (Art. 7bis E-K108)
  - Identität und Kontaktadresse des Verantwortlichen
  - Rechtliche Grundlage und Zweck der Datenbearbeitung
  - Kategorie der bearbeiteten Personendaten
  - Empfänger oder Kategorie der Empfänger bei Weitergabe der Personendaten
  - Informationen betreffend die Rechte der Betroffenen nach Art. 8 E-K108 sowie deren Geltendmachung
  - Alle anderen Informationen, die notwendig sind, um eine faire und transparente Datenbearbeitung zu gewährleisten (z.B. Aufbewahrungsdauer etc.)
- Indirekte Beschaffung (Art. 7bis Ziff. 2 E-K108)
- Form: jede angemessene Form (z.B. Datenschutzerklärung auf Website); **aber**: leicht zugänglich, lesbar und verständlich sein
- Aufschub der Information („(…) it can be done at a later stage, for instance when the controller is put in contact with the data subject for any new reason“)

Datenschutzfolgeabschätzung

- Art. 35 DSGVO
  - «Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein **hohes Risiko** für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch»

Datenschutzfolgeabschätzung DSGVO

- Beispiele
  - systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die auf automatisierter Verarbeitung einschliesslich Profiling gründet **und** die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen
  - Umfangreiche Bearbeitung besonders schützenswerter Daten

- Notifikation Aufsichtsbehörde (Art. 36 DSGVO)
  - Der Verantwortliche konsultiert vor der Verarbeitung die Aufsichtsbehörde, **wenn aus einer Datenschutzfolgeabschätzung gemäss Artikel 35 DSGVO hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte**, sofern der Verantwortliche **keine Massnahmen zur Eindämmung des Risikos trifft**

Datenschutzfolgeabschätzung E-K108

- Art. 8bis Ziff. 2 E-K108
  - **Grundsatz:** Datenschutzfolgeabschätzung bei jeder Datenbearbeitung
  - **Aber:** Art. 8bis Ziff. 4 E-K108 – Ausnahmen von der Pflicht mit Blick auf die Natur und den Umfang der bearbeiteten Daten, die Natur, den Umfang und den Zweck der Datenbearbeitung und, falls angemessen, die „Grösse“ des Verantwortlichen oder Bearbeiters (i.e. KMU oder Grossunternehmen)

Kompetenzen Aufsichtsbehörden

- DSGVO
  - Art. 58 DSGVO: Untersuchungs- und direkte Verfügungskompetenzen
  - Art. 83 DSGVO: Sanktionskompetenz (Geldstrafen von 10‘000 bis zu 20‘000 EUR oder im Falle eines Unternehmens von 2% bis 4% des weltweiten Jahresumsatzes des vorangegangen Geschäftsjahres)

- E-K108
  - Art. 10 sowie Art. 12bis E-K108
  - Untersuchungs- und direkte Verfügungskompetenzen („powers of investigation and intervention and the powers to issue decisions with respect to violations of the provisions of the Convention“)
  - Sanktionen: Umsetzungsspielraum, aber: „effective, proportionate and dissuasive“
  - Sanktionen: „(…) may involve the imposition of administrative sanctions, including fines. Where the legal system of the Party does not provide for administrative sanctions, (…) may be applied in such a manner that the sanction is proposed by the competent supervisory authority and imposed by the competent national courts“
  - Alte Fassung: „(…) to issue decisions and impose administrative sanctions (…)“

Take Home Message

- Neuerungen von E-K108 angetrieben
- Schweiz muss Bestimmungen der E-K108 umsetzen
- Umsetzung der E-K108 garantiert grundsätzlich freien Datentransfer in andere Vertragsstaaten der E-K108 (Art. 12 Ziff. 1 E-K108) – Stichwort „Angemessenheit“
- DSGVO muss nicht eins-zu-eins übernommen werden. **Aber**: DSGVO auch auf Nicht-EU-Unternehmen anwendbar (Art. 3 DSGVO)

ATTORNEYS AT LAW

Vielen Dank für die Aufmerksamkeit.

- Dr. Michael Reinle, LL.M. Zürich
- Bühlmann Rechtsanwälte AG
- www.br-legal.ch