NIEDERER KRAFT & FREY

Niederer Kraft & Frey Ltd
Bahnhofstrasse 13 · CH-8001 Zurich
Telephone +41 58 800 8000 · Telefax +41 58 800 8080
nkf@nkf.ch · www.nkf.ch

Cross-Border Outsourcing und Datenschutz

Clara-Ann Gordon

Seminar Cross-Border Outsourcing – Rechtsfragen und Lösungen
Europa Institut, 28. September 2016

NKF

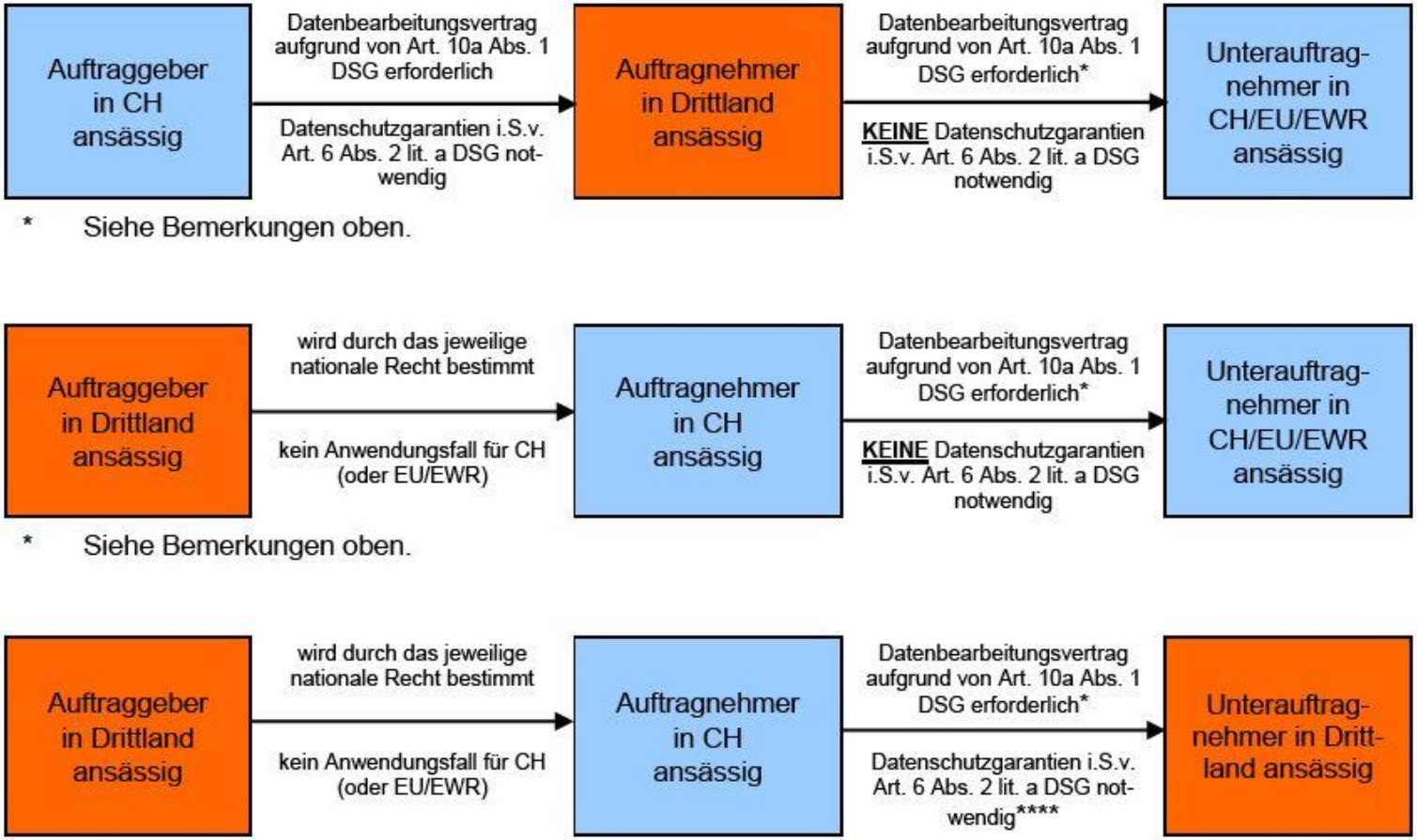
Thema

- **Outsourcing: je nach Rechtsgebiet andere Bedeutung und Anforderungen**
- **Überall sind Personendaten involviert und tangiert:**
  - Outsourcing von Betriebsteilen und –aufgaben
  - Inanspruchnahme von externen Dienstleistungen
  - Übertragung der Datenbearbeitung innerhalb des Konzerns oder durch Dritte
- **Gesetzliche Grundlagen:**
  - Art. 10a und 6 DSG: Übertragung der Datenbearbeitung
  - Kantonale Datenschutzgesetze: bei IT-Outsourcing von kantonalen und kommunalen Verwaltungen
- **Verantwortung bleibt beim Outsourcing-Bezüger**
- **Cloud Computing**

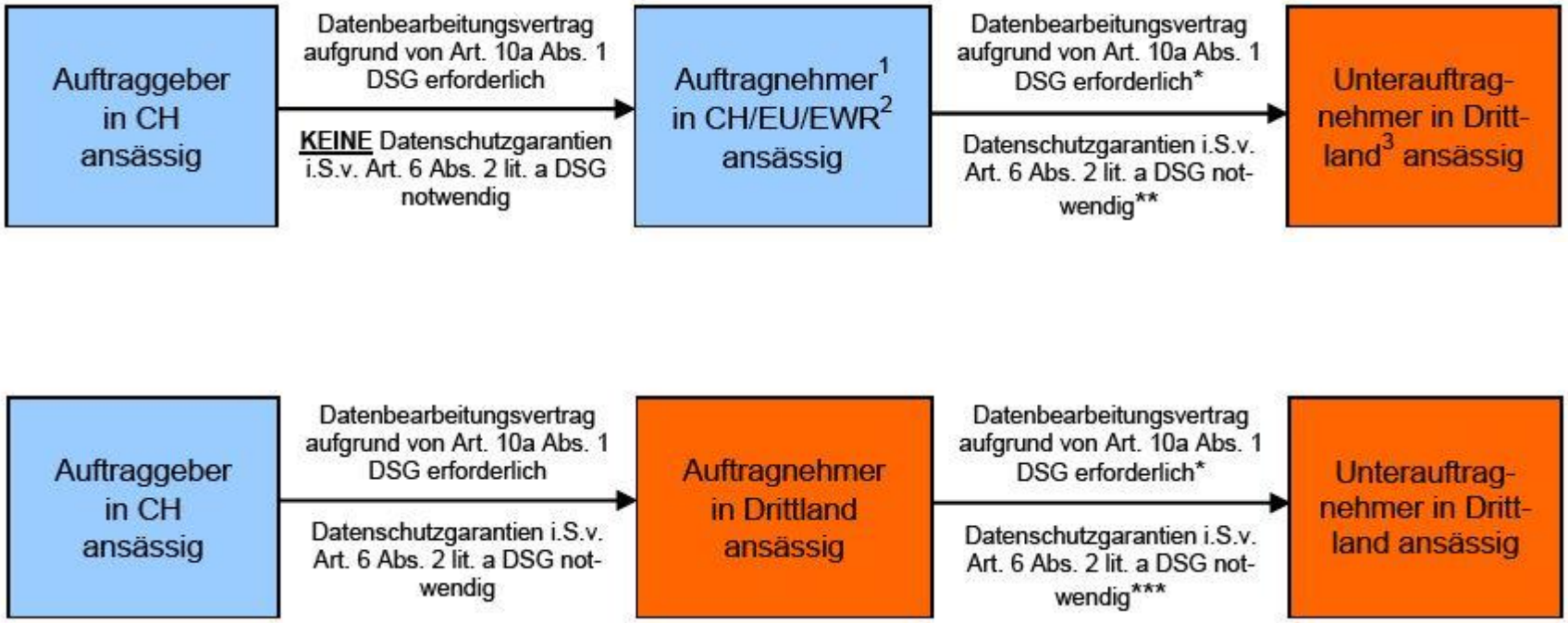
Übertragung der Datenbearbeitung ins Ausland

- **Offshoring, Farshoring oder Nearshoring?**
- **Wann kommt das DSG zur Anwendung?**
  - Territorialitätsprinzip: Datenbearbeitungen in CH und Zugriffe vom Ausland auf Server in CH
  - Jedoch Bekanntgabe von CH Personendaten vom Ausland aus in ein Drittland untersteht nicht mehr DSG
  - Keine Anwendung des DSG, wenn Personendaten direkt im Ausland erhoben werden (z.B. via Webserver)
- **Achtung: Geheimnispflicht (z.B. Bankgeheimnis, Berufsgeheimnis, etc.) oder Blocking Statutes können Export generell verbieten**
- **Kein Fall von grenzüberschreitender Bekanntgabe bei anonymisierten und verschlüsselten Personendaten**

Outsourcing Konstellationen I*



Outsourcing Konstellationen II*



Art. 10a DSG

- **Wortlaut von Artikel 10a DSG:**

[1] Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn:

a. die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte; und

b. keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.

[2] Der Auftraggeber muss sich insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet.

[3] Dritte können dieselben Rechtfertigungsgründe geltend machen wie der Auftraggeber.

Voraussetzungen Art. 10a DSG I

- **Auftraggeber (Outsourcing-Bezüger)**
  - Kann muss aber nicht Inhaber der Datensammlung sein
  - Achtung Unterscheidung in EU: controller und processor
- **Auftragsdatenbearbeitung**
  - Übertragung der Datenbearbeitung
  - Keine Mindestmenge an Daten oder Bearbeitungsvorgängen erforderlich
  - Es muss jedoch eine Bearbeitung von Personendaten vorliegen
- **Drittperson**
  - Jede vom Auftraggeber verschiedene Person
  - Nicht aber eigene Arbeitnehmer
  - Normallfall ist Auftragsbearbeitung innerhalb des Konzerns

Voraussetzungen Art. 10a DSG II

- **Subordinationsverhältnis**
  - Vereinbarung: Form unerheblich
  - von Gesetzes wegen: z.B. Auftrags- und Standesrecht beim Rechtsanwalt
  - oder anders: konzerninterne Verhältnisse, technische Kontrollmöglichkeit
- **Bearbeitung im gleichen Rahmen wie Auftraggeber**
  - Auftragnehmer (Provider) hat datenschutzrechtliche Schranken wie Auftraggeber (Outsourcing-Bezüger) zu beachten
  - Weisungsgebundene Datenbearbeitung

Voraussetzungen Art. 10a DSG III

- **Keine entgegenstehenden gesetzlichen oder vertraglichen Geheimhaltungspflichten**
  - Bankgeheimnis, Fernmeldegeheimnis, StGB 162, etc.
  - Bei vertraglichen Geheimhaltungspflichten: Einwilligung einholen, anonymisieren etc.
- **Einhaltung Datensicherheit**
  - Art. 7 DSG
  - Sorgfaltspflicht des Auftraggebers
  - Umfang der Sorgfaltspflicht hängt von den Umständen ab
  - Prüfstandards? ISO 27001?

Voraussetzungen Art. 10a DSG IV

- **Rechtfertigungsgründe**

  - Betroffene Person kann Auftraggeber und Auftragsbearbeiter in Anspruch nehmen
  - Beseitigungsansprüche, Schadenersatzforderungen, etc.
  - Achtung: in CH keine Unterscheidung zwischen Controller (verantwortlicher Datenbearbeiter) und Processor (Auftragsdatenbearbeiter)

IT-Outsourcing Vertrag

- **Notwendige, datenschutzrechtliche Klauseln**:

  - Verweis auf DSG-Bestimmungen
  - Zusicherung des Providers zur Einhaltung der DSG-Bestimmungen
  - Gewährleistung von datenschutzrechtlichen Ansprüchen von Datensubjekten
  - Zustimmung des Outsourcing-Bezügers für Beizug von Subprovidern durch Provider
  - Zweckbindung der Datenbearbeitung durch Provider
  - Verpflichtung des Providers zur Überbindung der DSG-Einhaltungsverpflichtungen an Mitarbeiter, Hilfspersonen und beigezogene Dritte
  - Verpflichtung des Providers zur Einhaltung von Sicherheitsstandards

Die zulässige Auftragsdatenbearbeitung

- **Folge der zulässigen Auftragsdatenbearbeitung ist das Bekanntgabeprivileg:**

  - Provider gilt nicht mehr als Dritter im Sinne des DSG
  - Keine Anmeldepflicht nach Art. 11a Abs. 3 lit. b DSG
  - Kein Rechtfertigungsgrund nach Art. 12 Abs. 2 lit. c DSG notwendig
  - Keine Einschränkung der Rechtfertigungsmöglichkeit nach Art. 9 Abs. 3 DSG
  - Keine Pflicht zur Information über Datenempfänger gemäss Art. 7a DSG
  - Keine Anwendung des Erkennbarkeitsgrundsatzes (Art. 4 Abs. 4 DSG) und Informationspflicht (Art. 7a DSG)

Spezialfragen Art. 10a DSG I

- **Konzerninterne Datenflüssen:**

  - Normalfall: Übertragung der Datenbearbeitung von einer Konzerngesellschaft an die andere (inter-company agreements)
  - Abgrenzungsfragen: Bearbeitung für eigene Zwecke und nicht für die auslagernde Konzerngesellschaft

- **Zugriff von mehreren Konzerngesellschaften auf Daten – Nutzung jedoch für eigene Zwecke (Shared Service Center)**

- **Gemeinsame Inhaberschaft einer Datensammlung – Nutzung jedoch für eigene Zwecke**

Spezialfragen Art. 10a DSG II

- **Kontrolle der Weisungen (Auditrecht):**

  - Auftraggeber ist für Oberaufsicht verantwortlich
  - Vorbehalt der zur Überwachung notwendigen Rechte:
    - Zugang für interne und externe Revisoren
    - Recht zur Inspektion der Infrastruktur
    - Recht über Art der Datenbearbeitung
  - Umfang des Auditrechts festlegen: jederzeit oder nur quartalsweise, mit oder ohne Vorankündigung etc.
  - In der Praxis: ein grosser Knackpunkt und im regulierten Bereich oft eine Voraussetzung für die Zulässigkeit des Outsourcings

Cross-border Datenbearbeitung

- **Zusätzlich Erfüllung der Voraussetzungen von Art. 6 DSG**
- **Anforderungen von Art. 10a und 6 DSG mit üblichen Standardverträgen in der Regel erfüllt**
- **Angemessener Schutz:**
  - Swiss Transborder Data Flow Agreement
  - EU-Musterklauseln
  - Privacy Shield CH?
- **Achtung Geheimnispflicht kann Übertragung ins Ausland generell untersagen**

Häufige Probleme im Outsourcing Alltag

- **Genaue Location der Cloud?**
- **Beizug von Subprovidern**
- **Auslagerung von gesetzlich geschützten Personendaten: Hilfspersonen-Problematik**
- **Rückgabe von Personendaten:**
  - Welches Format?
  - Rückgabeformalitäten vertraglich regeln
  - Konkurs des Providers / Cloud Anbieters: kein Anspruch auf Herausgabe von Daten

Auswirkungen revidiertes DSG auf Outsourcing I

- **Entwurf wird im Q4 erwartet**
- **Geplante Anpassungen:**
  - Begriff Processor wird eingeführt / Unterscheidung Processor/Controller
  - Informationspflicht muss inhaltlich ausgeweitet werden: Angaben über Controller, die bearbeiteten Daten, Rechtsgrundlage, Zweck, Empfängerkategorien, Betroffenenrechte
  - Ausweitung Auskunftsanspruch und Anhörungsrecht
  - Data Breach Notifications
  - Privacy Impact Assessment und Privacy by Design

Auswirkungen revidiertes DSG auf Outsourcing II

- EDÖB hat neu Sanktionsmöglichkeiten
- Bussen analog Kartellrecht: 10% des Dreijahresumsatzes

- **DSGVO hat zusätzliche Anforderungen:**

  - Inwiefern Anwendbarkeit für CH?
  - Bearbeitung von Daten über Kinder
  - Informationspflicht gegenüber Dritten bei Lösch- und Korrekturbegehren
  - Recht auf Datenportabilität
  - Pflicht zur Konsultation der Datenschutzbehörden
  - usw.

Schlusskommentare

- **Outsourcing-Sachverhalt und Übertragung der Datenbearbeitung gemäss Art. 10a DSG sind meistens nicht deckungsgleich**
- **DSG-Vorschriften sind oft nicht die Deal-Breakers – sondern die regulatorischen Vorgaben**
- **Bedingt durch DSG Revision bestehende Outsourcing Setups überprüfen – Hohe Bussen**
- **Neue Verschlüsselungstechniken ermöglichen Outsourcing in die Cloud und ins Ausland**

NIEDERER KRAFT & FREY

Contact

Niederer Kraft & Frey Ltd
Bahnhofstrasse 13
CH-8001 Zurich
Switzerland

Phone +41 58 800 8000
Fax +41 58 800 8080
Web http://www.nkf.ch

Clara-Ann Gordon
clara-ann.gordon@nkf.ch