VISCHER

Das digitale China-Geschäft im Umbruch: Der Cybersecurity Act und seine Auswirkungen auf das ICT-Business

CEIBS Lakeside Chat

Horgen, 22. April 2017

Dr. Rolf Auf der Maur, Rechtsanwalt, VISCHER AG

Lukas Züst, Rechtsanwalt, VISCHER AG

Übersicht

- Digitalisierung und Datenrecht
- Tendenzen im internationalen Datenrecht
  - EU
  - Schweiz
  - USA
  - Asien
- Der Cybersecurity Act vom 7. November 2016
- Draft Measures for Security Review of Network Products and Services
- Beispiele aus der Praxis

Treiber des Datenschutzes in Europa: Schutz vor dem Fichenstaat

Treiber des Datenschutzes beim DSG 1992:

- Schutz der Persönlichkeit (Private und Unternehmen)
- Schutz vor dem Überwachungsstaat ("Fichenaffäre")
- Föderalismus (DSG für Private und Bund, kantonale Gesetze für kantonale Behörden)
- Technologischer Stand: Nachkriegszeit
- Schweiz 1992 als "Nachzügler" in Europa

Treiber der Gesetzesrevisionen: Angst vor Kontrollverlust bei Big Data Analytics

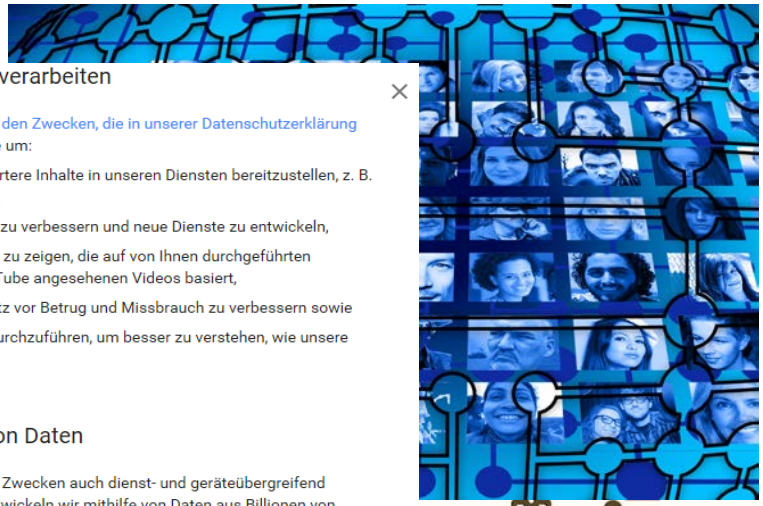
Treiber der DSG Revision 2017:

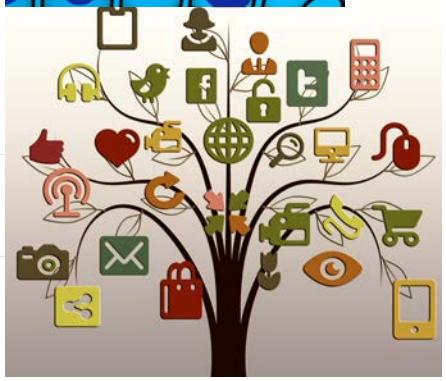
- Daten als Rohstoff für digitale Geschäftsmodelle
- Big Data und Data Analytics auf dem Vormarsch
- Migration von Daten in die "Cloud" (Bedeutungsverlust der nationalen Grenzen)
- Wachsende Risiken für Datensicherheit
- Algorithmen übernehmen Selektionen und führen automatisierte Entscheide aus: Forderung nach Transparenz und Einsprachemöglichkeiten
- EU DSGVO: Sanktionen bis 4% des Jahresumsatzes

Grundsätzliche Unterschiede Schweiz vs. EU

Schweiz	EU
• Datenbearbeitung erlaubt unter Einhaltung bestimmter Voraussetzungen (Zweckbindung, Verhältnismässigkeit, Rechtmässigkeit) • EDÖB heute ohne Verfügungs-kompetenz, soll diese aber neu erhalten (Sanktionskompetenz soll bei kanto-nalen Strafverfolgungsbehörden bleiben) • Nationale Wirkung für Bund und Private • DSG 39 Artikel / VE-DSG 60 Artikel auf 24 Seiten	• Verbotsgesetz mit Erlaubnisvorbehalt (Einwilligung, gesetzliche Pflicht oder überwiegendes Interesse – als Resultat einer Interessenabwägung) • Sanktionen bis 4% des weltweiten Jahresumsatzes oder EUR 20 Mio. bei Verletzungen gegen DSGVO Pflichten. Ausgestaltet als Verwaltungssanktionen. • Extraterritoriale Wirkung • 99 Artikel plus 173 Erwägungen auf 88 Seiten

Gemeinsame Herausforderungen ./. USA: "The Privacy Paradox" und Cybersecurity





Warum wir die Daten verarbeiten

Wir verarbeiten diese Daten zu den Zwecken, die in unserer Datenschutzerklärung aufgeführt sind, beispielsweise um:

- nützlichere und personalisiertere Inhalte in unseren Diensten bereitzustellen, z. B. relevantere Suchergebnisse,
- die Qualität unserer Dienste zu verbessern und neue Dienste zu entwickeln,
- interessenbasierte Werbung zu zeigen, die auf von Ihnen durchgeführten Suchanfragen oder auf YouTube angesehenen Videos basiert,
- die Sicherheit und den Schutz vor Betrug und Missbrauch zu verbessern sowie
- Analysen und Messungen durchzuführen, um besser zu verstehen, wie unsere Dienste genutzt werden.

Zusammenführung von Daten

Wir führen die Daten zu diesen Zwecken auch dienst- und geräteübergreifend zusammen. Beispielsweise entwickeln wir mithilfe von Daten aus Billionen von Suchanfragen Modelle zur Rechtschreibkorrektur, die in allen unseren Diensten zum Einsatz kommen. Außerdem können wir Sie und andere Nutzer mithilfe kombinierter Daten vor potenziellen Sicherheitsrisiken warnen.

Wie verwendet Google Daten zur Verbesserung der Nutzerfreundlichkeit?

Tipp: Wenn Sie sich mit einem Google-Konto anmelden, bevor Sie zustimmen, wird Ihre Auswahl auf allen Geräten und in allen Browsern gespeichert, bei denen Sie angemeldet sind.

WEITERE OPTIONEN ICH STIMME ZU

Datenrecht in den USA

- Fokus auf Datensicherheit: Data Breach Notification (Recht der Bundesstaaten)
- FTC Regeln für Bereiche mit besonderen Risiken:
  - Gesundheitsdaten
  - Daten von Kindern bis 13
- Selbstregulierung mit Zustimmung der Bundesregierung
  - EU/US Safe Harbour (durch EUGH 2015 annuliert)
  - EU/US Privacy Shield (seit 2016)
  - Parallele Abkommen mit der USA
- Homeland Security Act erlaubt Zugriff der NSA auf alle Kommunikationsdaten

Chinese Cybersecurity Act

- Cybersecurity Act vom 7. November 2016, angenommen in dritter Lesung durch den ständigen Ausschuss des Volkskongresses
- Inkrafttreten per 1. Juni 2017 (verhältnismässig lange Vorlaufzeit)
- Zweck:
  - Cybersecurity
  - Souveränität im Cyberspace
  - Nationale Sicherheit
  - Schutz natürlicher und juristischer Personen
  - Förderung der gesunden Entwicklung der Digitalisierung für Wirtschaft und Gesellschaft

National Security and Social Public Order – weite Begriffe

- «Overall National Security Concept»:
  - National Security Law
  - Anti-Terrorism Law
  - Desicion on Strengthening Network Information Protection
  - Decision on Internet Security Protection
  - Regulations for Safety Protection of Computer Information Systems,
  - Adminsitrativ Measures for Internet Information Services
  - Cybersecurity Law

- Kontrolle des Staates über das Internet als Teil des Nationalen Sicherheitskonzepts.

Begriffsdefinitionen

- Network Operator
  - «owners and administrators of network and network service providers»
- Critical Information Infrastructure Operator
  - Keine Definition im Gesetz
  - Industrien werden jedoch im Gesetz genannt: Telekommunikation, Energie, Transport, Wasserschutz, Finanzen, öffentliche Dienstleistungen, e-Government und andere wichtige Industrien und Schlüsselinformationsinfrastrukturen, dessen Zerstörung oder Beschädigung ernsthaften Schaden für die nationale Sicherheit, die nationale Volkswirtschaft und des öffentlichen Interesses zur Folge haben

Wirkung: Segregation des Internets

- «Critical Information Infrastructure» (CII) Betreiber müssen personenbezogene und wichtige Daten, welche im Geschäftsverkehr gesammelt oder generiert wurden, in China speichern
- Sofern die Daten – aus «legitimen Geschäftsgründen» ins Ausland übermittelt werden müssen, muss der Betreiber vorab einer «Sicherheitsprüfung» unterzogen werden.
- Im Ergebnis führt dies zu einer Segregation der Daten eines global tätigen CII Betreibers
- Potentiell und längerfristig Auswirkungen auch auf Patente möglich

Beispiele:

- WeChat:
  - Was ist WeChat?
  - Subscription account (corporate and individuals) vs Service account (corporate)
  - Domestic account vs. International account

- Tmall:
  - Was ist Tmall?
  - Tmall.com vs. Tmall Global

Wie wird die Kontrolle über das Internet versucht zu erreichen?

- Netzwerkbetreiber sind verpflichtet, technische Unterstützung und Hilfe der Behörden für öffentliche Sicherheit und Staatssicherheit für ihre Massnahmen für den Erhalt der nationalen Sicherheit und Strafverfolgung zu bieten
- Speicherung der «Logs» für mindestens sechs Monate
- Pflicht zur Schaffung von «Back Doors» darin enthalten?

Measures for the Security Review of Network Products and Services (Draft for Comment)

- Wichtige Netzwerkprodukte und –dienstleistungen, welche im Informationssystem im Zusammenhang mit der Nationalen Sicherheit und dem Öffentlichen Interesse benutzt werden, müssen einer Netzwerksicherheitsprüfung unterzogen werden bevor Sie zum Vertrieb in China zugelassen werden
- Betroffene Industrien sind insbesondere die Finanz-, Telekommunikations- und Energieindustrie
- Beispiel: ITC Hardware/Software-Supplier aus dem In- und Ausland werden betroffen sein:
- Pflicht der Supplier zur «Kooperation» bei der Prüfung: Potentiell muss mit der Pflicht zur Freigabe des «Source Codes» oder Entschlüsselung von Verschlüsselungsprogrammen gerechnet werden.

Sanktionen: was muss guter Datenschutz kosten?

Schweiz und EU

- DSGVO:
  - Busse in Höhe von 4% des letzten weltweiten Jahresumsatzes oder EUR 20 Mio. (höherer Betrag massgeblich) für alle Verstösse

- CH VE-DSG:
  - Verletzung administrativer Nebenpflichten als Straftatbestände mit Bussen bis CHF 500'000.– für die verantwortlichen Personen
  - Wenn verantwortliche Personen nicht identifizierbar: Busse bis CHF 100'000.– für das Unternehmen
  - Wirkung: Benachteiligung nationaler Unternehmen mit Dateninfrastruktur in der Schweiz

Verantwortlichkeit bei Verstössen gegen das Cybersecurity Law

- Aufforderungen auf Korrektur und Warnungen durch die zuständige(n) Behörde(n)
- Strafrechtliche Verantwortlichkeit bei Pflichtverletzungen:
  - Bussen von bis zu RMB 1 Mio für den Betreiber
  - Bussen von bis zu RMB 100’000 für die verantwortliche Person
  - Beschlagnahmung des illegal erzielten Gewinns
  - Busse bis zum 10-fachen des illegal erzielten Gewinns
  - Einstellung des Betriebes
  - Schliessung der Website
  - Entzug von Bewilligungen
  - Entzug der Business License
- Zivilrechtliche Verantwortung bei Pflichtverletzung:
  - Haftung gegenüber den betroffenen Personen

Mit welcher Umsetzung des Cybersecurity Gesetzes wird zu rechnen sein?

- Inkrafttreten am 1. Juni 2017
- Implementation Rules and Regulations müssen erst noch erlassen werden und in Kraft treten
- Erfahrung aus den Einführungen von grossen Gesetzesneuheiten (z.B. Anti-Monopoly Law 2008) oder wichtigen Revisionen (Gesellschaftsrechtsrevision 2013) in der Vergangenheit: das Gesetz wurde in einer ersten Phase (meist 6-12 Monate) nicht berücksichtigt bzw. die alten Regeln von den Behörden noch angewandt.
- Aber: Bei Internetsicherheitskontrolle könnte es jedoch anders sein, weil (i) diese faktisch bereits erfolgt und (ii) der Staat an einer strengen Umsetzung des Gesetzes ein grosses Interesse hat

Ihr Kontakt bei VISCHER

Dr. Rolf Auf der Maur

Rechtsanwalt, Partner

ram@vischer.com

+41 58 211 34 00

Lukas Züst

Rechtsanwalt, Head China Desk

lzuest@vischer.com

+41 58 211 34 35

Your Team for Swiss Law and navigation through the Chinese legal Environment

VISCHER

Herzlichen Dank.

Zürich
Schützengasse 1
CH-8021 Zürich
Tel +41 58 211 34 00
Fax +41 58 211 34 10

Basel
Aeschenvorstadt 4
CH-4010 Basel
Tel +41 58 211 33 00
Fax +41 58 211 33 10