

● DSGVO ante portas: Bin ich bereit für die neuen Regeln des Datenschutzes?

●
Cloud 2017 Infrastruktur & Security
Seedamm Plaza, Pfäffikon SZ, 26. Oktober 2017

Dr. Rolf Auf der Maur, Rechtsanwalt, VISCHER AG
Dr. Thomas Steiner, LL.M., Rechtsanwalt, VISCHER AG

● Übersicht

- Was die DSGVO verlangt
- Warum Schweizer Unternehmen handeln müssen
- Worauf Auftragsverarbeiter achten müssen
- Worauf Verantwortliche achten müssen
- Gap Analyse / Was zu tun ist
- Fragen / Diskussion

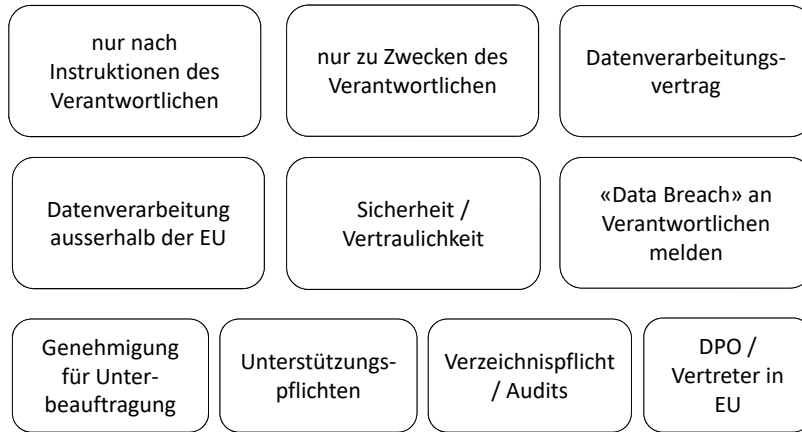
● Was die DSGVO verlangt



● Warum Schweizer Unternehmen handeln müssen

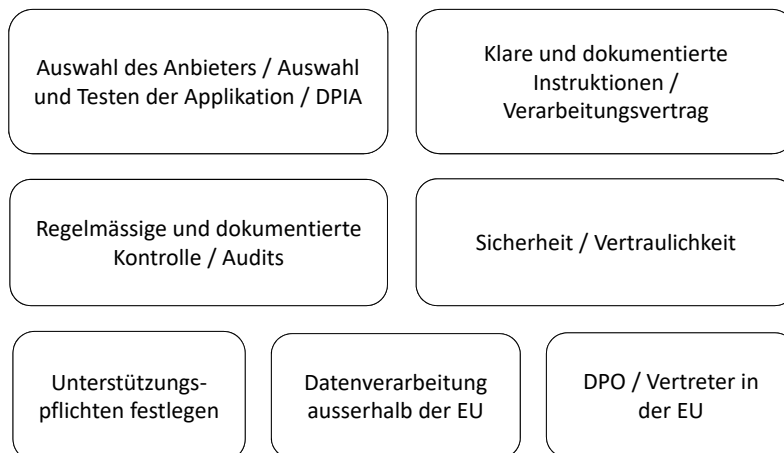
- Betroffen sind Schweizer Unternehmen, die:
 - natürlichen Personen in der EU Produkte oder Dienstleistungen anbieten (entgeltlich oder unentgeltlich)
 - das Verhalten von Nutzern ihrer Plattform (Website/App) analysieren, die sich in der EU befinden
 - an der Datenverarbeitung von EU-Unternehmen teilnehmen (z.B. als Auftragsverarbeiter oder als Schweizer Konzerngesellschaft)
- Bussenrisiko: bis zu EUR 20 Mio. oder 4% des weltweiten Umsatzes
- Reputationsrisiko

● Worauf Auftragsverarbeiter achten müssen



Aber nicht: Auskunfts-, Berichtigungs- und Löschungspflicht

● Worauf Verantwortliche achten müssen



→ vgl. FINMA Rundschreiben 17/xx Outsourcing – Banken und Versicherer

● Mindestinhalt des Datenverarbeitungsvertrags

- Nur nach dokumentierten Instruktionen des Verantwortlichen
- Nur zu Zwecken des Verantwortlichen
- Zusicherung der Vertraulichkeit (NDA auch für Mitarbeiter)
- Zusicherung der Sicherheit
- Unterstützung bei Anfragen (von Betroffenen oder Behörden) an Verantwortlichen
- Mitwirkung bei Audits durch oder im Auftrag des Verantwortlichen
- Unterbeauftragung nur mit Zustimmung
- Rückgabe- oder Löschungspflichten bei Beendigung

● Gap Analyse Auftragsverarbeiter (I)

- ✓ Für welche Kunden sind wir als Auftragsverarbeiter im Sinne der DSGVO tätig?
- ✓ Enthalten die Kundenverträge den Mindestinhalt von Art. 28(3) DSGVO?
- ✓ Sind die Instruktionen des Kunden betreffend die Datenverarbeitung, einschliesslich Vertraulichkeit und Sicherheit von Daten genügend klar und dokumentiert?
- ✓ Entsprechen die vom Auftragsverarbeiter zugesicherten organisatorischen und technischen Sicherheitsmassnahmen den Vorgaben der DSGVO und anderer Regulierungen, denen wir unterstehen?
- ✓ Wo speichern wir die Daten unserer Kunden? Halten wir uns an die Regelungen für Transfers in schutzunsichere Länder?
- ✓ Haben wir Prozesse für die Meldung eines «Data Breach» an den Kunden definiert? Sind unsere Mitarbeiter in diesen Prozessen genügend geschult?

● Gap Analyse Auftragsverarbeiter (II)

- ✓ Sind Prozesse dafür definiert und implementiert, wie wir Kunden bei Anfragen von Betroffenen oder Behörden unterstützen?
- ✓ Sind die Prozesse betreffend Audits durch Verantwortliche definiert und implementiert?
- ✓ Ist das Vorgehen nach Beendigung der Auftragsverarbeitung (Erfüllung allfälliger Rückgabe- oder Löschungspflichten bei Beendigung) intern und mit dem Kunden geregelt?
- ✓ Unterstehen wir der neuen Verzeichnispflicht gemäss Art. 30 Abs. 2 DSGVO? Wenn ja, wo besteht Handlungsbedarf?
- ✓ Besteht für uns die Pflicht, einen Datenschutzbeauftragten zu ernennen? Wenn nein, welches sind für uns die Vorteile, wenn wir dies freiwillig tun?
- ✓ Besteht für uns die Pflicht, einen Vertreter in der EU zu ernennen?

● Gap Analyse Verantwortlicher (I)

- ✓ Welche Datenverarbeitungen haben wir ausgelagert?
- ✓ Haben wir die sorgfältige Auswahl von Applikationen und Auftragsverarbeiter dokumentiert?
- ✓ Sind betroffene Personen über die Auslagerung genügend informiert?
- ✓ Haben wir allenfalls notwendige Einwilligungen der betroffenen Personen dokumentiert?
- ✓ Haben wir die Auftragsverarbeiter klar und dokumentiert instruiert?
- ✓ Wo speichern und verarbeiten die Auftragsverarbeiter die Daten unserer Kunden? Halten wir uns an die Vorgaben betreffend Transfers in schutzunsichere Länder?

● Gap Analyse Verantwortlicher (II)

- ✓ Kontrollieren wir unsere Auftragsverarbeiter regelmässig? Sind die Kontrollen / Audits dokumentiert?
- ✓ Genügen die uns vom Auftragsverarbeiter zugesicherten Sicherheitsmassnahmen den Anforderungen der DSGVO an die Datensicherheit?
- ✓ Sind Prozesse betreffend Unterstützung durch Auftragsverarbeiter bei Anfragen von Behörden oder Betroffenen definiert?
- ✓ Sind Prozesse definiert, wie uns unsere Auftragsverarbeiter einen «Data Breach» melden?
- ✓ Besteht für uns die Pflicht, einen Datenschutzbeauftragten zu ernennen? Wenn nein, welches sind für uns die Vorteile, wenn wir dies freiwillig tun?
- ✓ Besteht für uns die Pflicht, einen Vertreter in der EU zu ernennen?

● Was zu tun ist (Auswahl)

- In Gap Analyse identifizierte Anforderungen risikobasiert priorisieren
- Umsetzung gemäss Risikoeinschätzung / Priorisierung
- Verhandlungen von Verarbeitungsverträgen frühzeitig beginnen / ggf. eigene Muster für Vertragszusätze erstellen
- Sicherheit / Vertraulichkeit sicherstellen
- Verantwortliche: Prozesse für Auswahl, Instruktion und Kontrolle definieren
- Dokumentation und Verzeichnisse erstellen / interne Prozesse definieren
- Prozesse für die Meldung von «Data Breaches» definieren
- Datenaufbewahrungs- und Löschkonzepte implementieren
- ggf. Datenschutzbeauftragten (DPO) ernennen
- ggf. Vertreter in der EU ernennen



Fragen / Diskussion



Ihr Kontakt bei VISCHER



Dr. Rolf Auf der Maur
Rechtsanwalt, Partner

ram@vischer.com

+41 58 211 34 00



Dr. Thomas Steiner, LL.M.
Rechtsanwalt, Senior Associate

tsteiner@vischer.com

+41 58 211 34 00

●
VISCHER: Your Team for Swiss Law



● Roundtable - Cloud 2017

15

VISCHER

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