Datenschutz und Datensicherheit

in Bezug auf Unternehmensnetze und Cloud-Dienste

1. Zusammenfassung

Gesetzliche Grundlage

In der Schweiz und der Europäischen Union ist der Datenschutz und die Datensicherheit von personenbezogenen Daten genau definiert in entsprechenden Gesetzen und Verordnungen.
In der Schweiz im Bundesgesetz über den Datenschutz (DSG) und in der EU in der Datenschutz-Grundverordnung (DSGVO). Am 25.09.2020 wurde vom Parlament das totalrevidierte Schweizer Datenschutzgesetz (DSG) angenommen.

Demnach darf keine Übermittlung und kein Transfer personenbezogener Daten in ein Land vorgenommen werden, welches in der definierten Länderliste nicht als Land mit angemessenem Datenschutz definiert ist, sofern nicht mit technischen Massnahmen ein adäquates Schutzniveau hergestellt ist.

Am 16.07.2020 erklärte der Europäische Gerichtshof die Regelung über den Schutz personenbezogener Daten zwischen der EU und der USA (Privacy Shield Abkommen) für ungültig.
Daraufhin hat in der Schweiz der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftrage (EDÖB) am 08.09.2020 eine Stellungnahme veröffentlicht zur Übermittlung von Personendaten in die USA und weitere Staaten ohne angemessenes Datenschutzniveau. Darin wird festgehalten, dass die **USA** die Anforderungen an das Datenschutzniveau verfehlen und nun auch in der Kategorie der Länder mit "ungenügendem Schutz" platziert sind, zusammen mit u.a. **China, Taiwan, Südkorea**, etc.

Unternehmens-Netzwerke und Cloud-Dienste

Netzwerkgeräte und Cloud-Dienstleistungen von Herstellern aus Ländern mit "ungenügendem Schutz" gemäss Länderliste, erfüllen die oben erwähnten gesetzlichen Vorgaben nicht, da diese Hersteller an die Gesetzgebung ihres Landes gebunden sind (z.B. Abhörbefugnissen der Behörden, FISA, Patriot Act). Dabei spielt es keine Rolle ob deren Rechenzentren in Europa oder der Schweiz stehen.

Betroffen sind u.a.:

- Cloud-Dienste
- SD-WAN Infrastrukturen
- Cloud managed WLANs
- Firewall (UTM Unified Threat Management)

Um das geforderte Schutzniveau herzustellen müssen bei Geräten und Dienstleistungen der oben erwähnten Hersteller entsprechende Massnahmen getroffen werden, wie z.B. die Erstellung einer Privat-Cloud beim Anwenderunternehmen selber oder das Deaktivieren der entsprechenden Funktionen in den Firewalls (UTM Deep Packet Inspection, Sandboxing, Machine Learning).

Strafbestimmungen und Sanktionen

Im totalrevidierten Schweizer Datenschutzgesetz (DSG), welches am 25.09.20 vom Parlament angenommen wurde, sind die Sanktionen massiv verschärft worden.
Darin ist neu festgehalten, dass natürliche Personen bei vorsätzlicher Verletzung der Informations- und Auskunftspflichten sowie der Sorgfaltspflichten neu mit Busse bis CHF 500'000.- bestraft werden. Die Strafbarkeit ist bereits gegeben, wenn eine tatsächlich eingetretene Verletzung in Kauf genommen wurde (Eventualvorsatz). Dies führt dazu, dass nach dem revidierten DSG Verantwortliche im Unternehmen wie CEOs, CIOs oder andere Funktionen direkt sanktioniert werden können. Die Zuständigkeit liegt dabei bei den kantonalen Staatsanwaltschaften.

2. Gesetzlich Referenzen EU – Europäische Union

(Die verwendeten Rechtsquellen sind jeweils im Text selber angegeben)

In der EU gilt bezüglich des Datenschutzes und der Datensicherheit die **EU Datenschutz-Grundverordnung (DSGVO)**

Gemäss DSGVO Art. 45 darf eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet.

Falls kein Beschluss nach Art. 45 vorliegt, darf gemäss Art 46 ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

EU - USA

Am 16.07.2020 erklärte der Europäische Gerichtshof die Regelung über den Schutz personenbezogener Daten zwischen der EU und der USA (Privacy Shield Abkommen) für ungültig.

Somit gelten nach diesem Urteil für alle Exporte von Personendaten aus der EU in die USA fortan die Vorschriften nach Art. 46 der EU Datenschutz-Grundverordnung (DSGVO). Gemäss dem Urteil stehen somit in erster Linie die Bearbeitungsverantwortlichen und in zweiter Linie die Datenschutzbehörden in den EU-Mitgliedländern in der Pflicht, von Fall zu Fall zu beurteilen, ob sich aufgrund der Standardvertragsklauseln (SCC14) gem. Art. 46 Abs. 2 DSGVO ein mit dem EU-Recht kompatibler Datenexport in die USA in der Praxis bewerkstelligen lasse. Falls dies verneint werden muss, seien Datenexporte aus der EU in die USA von den Verantwortlichen entweder in eigener Initiative oder auf Geheiss der Datenschutzaufsichtsbehörde des zuständigen EU/EWR -Mitgliedstaates einzustellen und bereits exportierte Personendaten zu löschen.

Länder ohne Einhaltung des Schutzniveaus

Drittländer, welche das vorgegebene **Schutzniveau nicht einhalten** gemäss DSVGO Art. 45, sind nun unter anderem: **China, USA, Taiwan**, etc.

3. Gesetzliche Referenzen Schweiz

(Die verwendeten Rechtsquellen sind jeweils im Text selber angegeben)

In der Schweiz gilt bezüglich des Datenschutzes und der Datensicherheit das **Bundesgesetz über den Datenschutz (DSG)**: https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/de

Gemäss DSG Art. 6 (Grenzüberschreitende Bekanntgabe) dürfen Personendaten nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.

Schweizer Unternehmen dürfen keinen Transfer personenbezogener Daten durchführen in Länder, welche den angemessenen Schutz nicht gewährleisten, sofern nicht mit technischen Massnahmen ein adäquates Schutzniveau hergestellt ist. Die Länder ohne angemessenen Schutz sind in der Länderliste aufgeführt.

Schweiz - USA

Nach dem Urteil des Europäischen Gerichtshof, bei welchem der Schutz personenbezogener Daten zwischen der EU und der USA (Privacy Shield Abkommen) für ungültig erklärt wurde, hat der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragen (EDÖB) am 08.09.2020 eine Stellungnahme veröffentlicht zur Übermittlung von Personendaten in die USA und weitere Staaten ohne angemessenes Datenschutzniveau i.S.v. Art. 6:

https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2020/Positionspapier_PS_%20ED%C3%96B_DE.pdf.download.pdf/Positionspapier_PS_%20ED%C3%96B_DE.pdf

Darin wird ausführlich beschrieben und begründet, dass die USA die Anforderungen an das Datenschutzniveau verfehlen und nun auch in der Kategorie der Länder mit "ungenügendem Schutz" platziert sind.

Länder ohne "angemessenen Schutz"

Vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragen (EDÖB) ist eine Liste der Staaten veröffentlicht, deren Gesetzgebung einen angemessenen Datenschutz gewährleistet (gemäss Art. 6 DSG): https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2020/staatenliste.pdf.download.pdf/20200908_Staatenliste_d.pdf

Gemäss dieser Länderliste bieten unter anderem folgende Staaten einen **ungenügenden Schutz**: **China, USA, Taiwan, Südkorea**, etc.

Direkte Auswirkung der DSGVO auf die Schweiz

Nach Art. 3 der DSGVO werden das Datenschutzrecht der EU und die darauf gestützte Rechtsprechung des EuGH jedoch von den Behörden und Gerichten der EU resp. des EWR auch gegenüber Schweizer Unternehmen angewendet, wenn Letztere in der dort genannten Weise Daten bearbeiten. Schweizer Unternehmen müssen deshalb davon ausgehen, dass diese ausländischen Behörden gegebenenfalls verlangen, dass sie sich beim Export von Personendaten unter Androhung von Bussen an die Vorgaben des EU-Rechts halten. Namentlich, wenn sie Daten von Einwohnern der EU resp. des EWR bearbeiten.

Totalrevision des Bundesgesetzes über den Datenschutz (DSG), 25.09.2020:

Zur Stärkung des Datenschutzes wurde am 25.09.2020 vom Parlament die Totalrevision des DSG verabschiedet. Die Vorarbeiten für die Revision der Verordnungen sind derzeit im Gange. Die Vernehmlassung zur Revision der VDSG wird voraussichtlich in der ersten Jahreshälfte 2021 eröffnet werden. (Vorentwurf DSG: https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/vorentw-d.pdf.download.pdf/vorentw-d.pdf)

Im revidierten DSG sind folgende vier Aspekte zentral:

- Erhöhung der Transparenz (Information über Datenbearbeitungen) und Stärkung der Rechte der betroffenen Personen
- Förderung der Prävention und der Eigenverantwortung der Datenbearbeiter
- Stärkung der Datenschutzaufsicht (durch EDÖB)
- Ausbau der Strafbestimmungen

Gemäss Art. 50 und 51 können natürliche Personen bei vorsätzlicher Verletzung der Informations- und Auskunftspflichten sowie der Sorgfaltspflichten neu mit Busse bis CHF 500'000.- bestraft werden, bei fahrlässiger Verletzung mit Busse bis 250'000.-. Ausreichend ist der Eventualvorsatz, weshalb die Strafbarkeit bereits gegeben ist, wenn eine tatsächlich eingetretene Verletzung in Kauf genommen wurde. Dies führt dazu, dass – im Gegensatz zur DSGVO bei der lediglich Unternehmen oder Organisationen im Fokus stehen – nach dem revidierten DSG Verantwortliche im Unternehmen wie CEOs, CIOs oder andere Funktionen direkt sanktioniert werden können. Die Zuständigkeit liegt dabei bei den kantonalen Staatsanwaltschaften.