Data Protection – eine Utopie?

«Das Recht hinkt der Entwicklung hinterher.» Was wohl auf viele Rechtsgebiete zutreffen mag, galt bisher insbesondere für das Schweizer Datenschutzrecht. «Cloud Storage», informationelle Selbstbestimmung, Onlineshop usw. waren 1993 bei der Redaktion des bis heute geltenden Datenschutzgesetzes (DSG) noch kein Thema.

Die Bedeutung des Schutzes der persönlichen Daten nimmt mit den täglich besser werdenden Algorithmen und der exponentiell steigenden Datenmenge rasant zu. Das Parlament verabschiedete deshalb am 25. September 2020 die erste Totalrevision des DSG.

Niemand ist von einer Verletzung der Persönlichkeit durch ungerechtfertigte Bearbeitung der Personendaten gefeit; die Weitergabe von Personendaten an Dritte ist nur eines der vielen Beispiele. Der Gesetzgeber wollte deshalb die Rechte des Einzelnen stärken. Dies gilt jedoch nicht für juristische Personen, denn deren Daten sind neu generell vom Anwendungsbereich des DSG ausgenommen. Voraussetzung für die Abwehr einer Persönlichkeitsverletzung ist die Auskunft darüber, inwiefern überhaupt persönliche Daten bearbeitet wurden. Das Auskunftsrecht wird deshalb von einer momentan abschliessenden Liste an Pflichtinformationen auf «jede Information, die für eine betroffene Person erforderlich ist, um ihre Rechte nach DSG geltend zu machen», erweitert.

Den erwähnten Herausforderungen wird auch mit erweiterten Compliance-Vorgaben für die sogenannte «Datenbearbeiter» (insbesondere auch KMUs) begegnet. So sind diese neu zum Führen eines Verzeichnisses aller Bearbeitungstätigkeiten verpflichtet, welches unter Anderem den Bearbeitungszweck und die Aufbewahrungsdauer der Personendaten beinhalten muss. Weiter wird eine Meldepflicht bei Datenverlusten bzw. Datensicherheitsverletzungen eingeführt. Das revidierte Gesetz wird voraussichtlich anfangs 2022 in Kraft treten, wobei keine Übergangsfristen vorgesehen sind. Eine frühzeitige Auseinandersetzung mit den Folgen für das eigene Unternehmen ist deshalb unumgänglich. Dies gilt aufgrund Abweichungen des neuen DSG von der europäischen Datenschutz-Verordnung (DSGVO), auch für bereits DSGVO-konforme Unternehmen.

Ob das neue DSG einen effektiven Beitrag zu einem griffigeren Persönlichkeitsschutz zu leisten vermag, muss sich in der Anwendung noch weisen.

www.h-h.ch

HAFNER & HOCHSTRASSER
RECHTSANWÄLTE ATTORNEYS AT LAW

ANZEIGE

WIRD GROUP

IBM Platinum Business Partner TM

Was passiert bei einem Ausfall kritischer Systeme in der Schweiz?

In den vergangenen Jahren hat der Bund viel in den Schutz kritischer Infrastrukturen (SKI) investiert: von der ersten SKI-Strategie 2012, der Überarbeitung 2017 bis zur laufenden Umsetzung 2018 - 2022.

Aber wie sieht es mit den Unternehmern und deren Mitarbeitern aus, wie mit der Bevölkerung? Wer hat die Strategie gelesen und wann fand die letzte Simulation statt? Wer wusste vor der laufenden Pandemie, wie auf einen Lockdown zu reagieren ist? Wo stand, dass es zu Grenzschliessungen kommen kann? Wir stellen uns zur Zeit viele Fragen, oft im Kontext von harten Interessenskonflikten.

Die aktuelle Krise macht Krisenszenarien greifbar. Was früher nur einem kleinen Kreis transparent war, spürt heute jeder im täglichen Leben. Eine Frage geht unter: Wie binden wir Unternehmen und Bevölkerung in die Umsetzung der SKI-Strategie ein, um auf zukünftige grosse Ausfälle unserer SKI vorbereitet zu sein, besser vorbereitet als auf die Pandemie?

Was müssen und können wir tun, wenn es zu einem flächendeckenden grossen Cyber-Incident kommt? Ein Szenario, von dem wir seit Jahren reden, das wir allerdings ausserhalb der SKI-Arbeitsgruppen nie wirklich zu Ende gedacht haben. Nun wäre die Zeit reif. Jeder ist sensibilisiert.

Sind wir alle auf den grossen Cyber-Shutdown vorbereitet?

Wenn wir heute von kritischen Infrastrukturen sprechen, dann sind diese weitgehend abhängig von einer funktionierenden IT-Infrastrukur, sowie IT-gesteuerten Netzinfrastrukturen (Strom, Wasser, etc.). Eine Abhängigkeit, deren sich heute weder Unternehmer, noch Bevölkerung tatsächlich in aller Konsequenz bewusst sind – bis zu dem Tag, an dem das Mobile Phone nicht mehr funktioniert, die Onlineshops innert eines Sekundenbruchteils verschwunden sind und Zahlsysteme nicht mehr reagieren.

Unternehmen und Mitarbeiter waren im Lockdown der Pandemie (weitgehend) erstaunlich flexibel in der Umstellung auf das Arbeiten im Homeoffice. Digitalisierung sei Dank. Im Cyber-Shutdown dürfte es dann schwierig werden. Man muss schon sehr genau nachdenken, um zu identifizieren welcher Service dann noch verfügbar ist.

Der Vorteil des Pandemie-Szenarios ist, dass es sich langsam entwickelt – man sieht es kommen, anfangs fast unbeachtet, doch stetig. Ein Cyber-Shutdown entwickelt sich in wenigen Minuten bis Stunden und im Extremfall instantan. Auch das Recovery verläuft nach komplett anderen Mustern.

Lässt uns die Cloud im Stich?

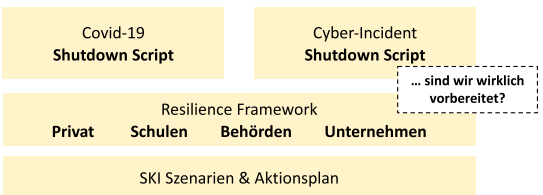
Die fortschreitende Digitalisierung unserer Gesellschaft geht einher mit einer nicht mehr umkehrbaren und rasant zunehmenden Abhängigkeit von Cloud-Diensten. Nun sind gerade diese besonders anfällig, sollte es zu einem Cyber-Shutdown kommen. Wenn wir also von Resilienz-Massnahmen sprechen, dann müssen diese insbesondere im Bereich der Cloud-Service-Nutzung wirken. Dabei gilt es einiges zu bedenken, was wir in der Vergangenheit in grossen Teilen vernachlässigt haben. Interessant ist, dass Cloud-Dienste oberflächlich betrachtet sehr anfällig wirken, allerdings aufgrund der zugrundeliegeneden Architektur gerade auch eine Lösung für Resilienz-Optimierungen bieten. Cloud-Dienste können über Geo-Zonen hinweg resilient verfügbar sein. Funktioniert mein Mobile Phone in der Schweiz nicht, gehe ich ins Nachbarland und kommuniziere weiter.

Wir müssen die Cloud-Anbieter eng in die Pflicht nehmen und auch über Notfall-Szenarien nachdenken, wo wir aus anderen Geo-Zonen auf unsere Daten und Services zugreifen können. Das wird für Schulen nicht funktionieren, sicher aber für private Dienste und Unternehmen.

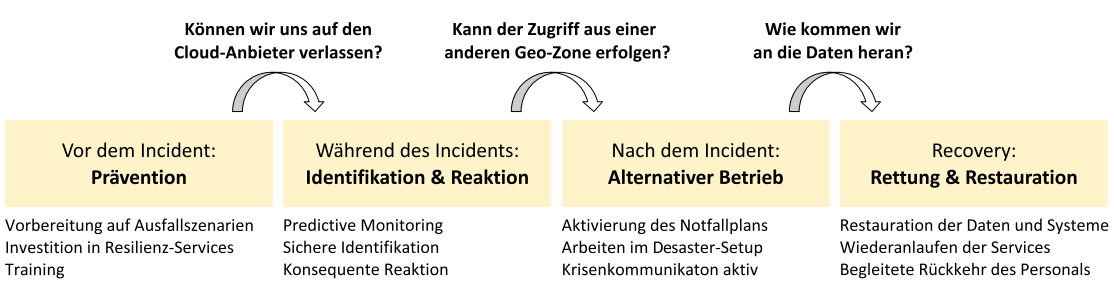
Wie setzen wir das Gelernte um?

Wir haben durch Covid-19 vieles zu Krisenbewältigungsszenarien gelernt und jeden Tag kommt Neues dazu. Nun gilt es das Erlernte auch konkret umzusetzen. Wir kennen alle das im Covid-19 Fall aktivierte Shutdown-Skript. Die meisten waren völlig unvorbereitet und hatten Mühe mit der Entwicklung Schritt zu halten.

Es sind nun alle gefordert, das bisher Vernachlässigte nachzuholen. Auf einen grossen Cyber-Shutdown müssen wir alle vorbereitet sein. Jeder, ob privat, in der Schule oder im Unternehmen sollte sein Cyber-Incident-Shutdown-Script kennen und aktivieren können. Für zukünftige Szenarien reicht es nicht mehr, in Facharbeitsgruppen an SKI Aktionsplänen zu arbeiten. Es gilt alle einzubeziehen und jeder sollte auch seinen Beitrag leisten.



Beruhigend ist, dass Schulen und Gastrobetriebe im Cyber-Shutdown nach alten Mustern weitgehend weiter funktionieren werden. Unternehmen und Behörden werden praktisch ausgeschaltet, sollten sie nicht vorbereitet sein.



Über BearingPoint

BearingPoint ist eine unabhängige Management- und Technologieberatung mit europäischen Wurzeln und globaler Reichweite, die von 178 Partnern geführt wird. Das Unternehmen agiert in drei Bereichen: Consulting, Business Services und Software.

Für weitere Informationen:
www.bearingpoint.com

Kontakt
Herr Jürgen Stückle, Cybersecurity Advisor

Data Protection – eine Utopie?

«Das Recht hinkt der Entwicklung hinterher.» Was wohl auf viele Rechtsgebiete zutreffen mag, galt bisher insbesondere für das Schweizer Datenschutzrecht. «Cloud Storage», informationelle Selbstbestimmung, Onlineshop usw. waren 1993 bei der Redaktion des bis heute geltenden Datenschutzgesetzes (DSG) noch kein Thema.

Die Bedeutung des Schutzes der persönlichen Daten nimmt mit den täglich besser werdenden Algorithmen und der exponentiell steigenden Datenmenge rasant zu. Das Parlament verabschiedete deshalb am 25. September 2020 die erste Totalrevision des DSG.

> **“ Niemand ist von einer Verletzung der Persönlichkeit durch ungerechtfertigte Bearbeitung der Personendaten gefeit.**

Niemand ist von einer Verletzung der Persönlichkeit durch ungerechtfertigte Bearbeitung der Personendaten gefeit; die Weitergabe von Personendaten an Dritte ist nur eines der vielen Beispiele. Der Gesetzgeber wollte deshalb die Rechte des Einzelnen stärken. Dies gilt jedoch nicht für juristische Personen, denn deren Daten sind neu generell vom Anwendungsbereich des DSG ausgenommen. Voraussetzung für die Abwehr einer Persönlichkeitsverletzung ist die Auskunft darüber, inwiefern überhaupt persönliche Daten bearbeitet wurden.

Das Auskunftsrecht wird deshalb von einer momentan abschliessenden Liste an Pflichtinformationen auf «jede Information, die für eine betroffene Person erforderlich ist, um ihre Rechte nach DSG geltend zu machen», erweitert.

Den erwähnten Herausforderungen wird auch mit erweiterten Compliance-Vorgaben für die sogenannte «Datenbearbeiter» (insbesondere auch KMUs) begegnet. So sind diese neu zum Führen eines Verzeichnisses aller Bearbeitungstätigkeiten verpflichtet, welches unter Anderem den Bearbeitungszweck und die Aufbewahrungsdauer der Personendaten beinhalten muss. Weiter wird eine Meldepflicht bei Datenverlusten bzw. Datensicherheitsverletzungen eingeführt. Das revidierte Gesetz wird voraussichtlich anfangs 2022 in Kraft treten, wobei keine Übergangsfristen vorgesehen sind. Eine frühzeitige Auseinandersetzung mit den Folgen für das eigene Unternehmen ist deshalb unumgänglich. Dies gilt aufgrund Abweichungen des neuen DSG von der europäischen Datenschutz-Verordnung (DSGVO), auch für bereits DSGVO-konforme Unternehmen.

Ob das neue DSG einen effektiven Beitrag zu einem griffigeren Persönlichkeitsschutz zu leisten vermag, muss sich in der Anwendung noch weisen.

www.h-h.ch

HAFNER & HOCHSTRASSER
RECHTSANWÄLTE ATTORNEYS AT LAW