

BOARD - Zeitschriften Archiv > 2020 > BOARD 4/2020 > Das Aufsichtsratsbüro > Die Bedeutung von digitalen Board Portalen für Aufsichtsratsgremien

<b>Zeitschrift:</b>	BOARD
<b>Autor:</b>	Christopher Knabe
<b>Beitragstyp:</b>	Beitrag
<b>Ausgabe:</b>	4/2020

## Die Bedeutung von digitalen Board Portalen für Aufsichtsratsgremien

**Christopher Knabe**



Christopher Knabe MBL-HSG, Loomion AG

Eine Diskussion über die Vorteile solcher Portale und die Risiken bei der Auswahl des richtigen Anbieters vor dem Hintergrund der jüngsten Entscheidung des EuGH zum Privacy Shield vom 16. Juli 2020.

### Inhalt

- I. Board Portale in der Praxis
- II. Das Facebook-Urteil des EuGH
- III. Auswirkungen des Urteils auf die Auswahl eines Board Portals?
- IV. Fazit

### Keywords

Board Portal; Facebook-Urteil; Privacy Shield

### I. Board Portale in der Praxis

Digitale Board Portale haben mittlerweile bei 50 %<sup>1</sup> der Unternehmen mit einem Aufsichtsrat Einzug erhalten. Keines dieser Unternehmen kann sich die Arbeit im Gremium ohne ein solches Portal mehr vorstellen. Die

---

<sup>1</sup> Quelle: Dadael Research 2019.

Vorteile von Enterprise Level Board Portalen (es gibt in dieser Klasse eigentlich nur 3 bis 4 Anbieter) sind schon häufig diskutiert worden und werden hier nur noch stichpunktartig aufgezeigt:

- Extrem hohe Effizienzsteigerung für die Arbeit des Aufsichtsratssekretärs sowie auch der Mitglieder des Aufsichtsrates durch Real Time-Verfügbarkeit von Daten.
- Hochsichere Lösungen für die Speicherung, Langzeit-zur-Verfügungstellung und Distribution von Daten
- Vollständige Kontrolle über den Verlauf und Verbleib von Daten und Informationen.

Dass knapp 50 % der Unternehmen noch kein Board Portal nutzen, erscheint fahrlässig. Der Aufsichtsrat behandelt in seinen Sitzungen nicht nur Punkte, die als Geschäftsgeheimnisse eingeordnet werden müssen, sondern in vielen Fällen auch personenbezogene Daten, die ebenfalls einem besonderen Schutz unterstehen. Diese hochbrisanten und vertraulichen Informationen dann an die private Google Email-Adresse von Mitgliedern des Aufsichtsrates zu senden, macht immer wieder sprachlos.

Für beide Gruppen von Unternehmen, die, die schon ein Board Portal nutzen wie auch die, die sich in einem Auswahlprozess befinden, hat die Welt sich jedoch am 16. Juli 2020 gravierend verändert. Beide müssen die Auswahl ihres momentan genutzten oder zukünftigen Anbieters vollständig neu hinterfragen oder bewerten. Dazu nun im Einzelnen.

## **II. Das Facebook-Urteil des EuGH**

Fast auf den Tag genau hat der Europäische Gerichtshof mit dem Urteil in der Rechtssache C-311/18 am 16. Juli 2020, vier Jahre nach Inkrafttreten des EU-US Privacy Shield 2016/1250, den Beschluss der EU-Kommission kassiert und zum zweiten Mal für ungültig erklärt. Brisant ist hierbei, dass der EuGH den zuvor erwähnten Privacy Shield-Beschluss wegen den gleichen Mängeln wie den Safe Harbour-Beschluss in 2015 gekippt hat. In beiden Fällen hatte der österreichische Jurist und Datenschutzexperte Maximilian Schrems Facebook in Irland aufgefordert, seine auf irischen Facebook-Servern gespeicherten Daten nicht mehr auf Server von Facebook in die USA zu übermitteln. Dem wollte Facebook mit der Begründung des Privacy Shields nicht nachkommen, weshalb die irische Datenschutzbehörde den Fall dem EuGH zur Prüfung vorgelegt hat.

Der EuGH folgte den Bedenken Schrems' in Bezug auf die viel zu weitreichenden Zugriffsmöglichkeiten von US-Geheimdiensten nun weitgehend und löste mit seinem Urteil ein Erdbeben aus. „Die amerikanische Überwachungspraxis sei nicht auf das zwingend erforderliche Maß begrenzt“, betonten die Richter. Zudem könnten Betroffene ihre in der EU vorgesehenen Rechte nicht gerichtlich in den USA durchsetzen.

In einem weiteren Schritt rügte der EuGH die irische Datenschutzbehörde, die in diesem Fall für Facebook als Aufsichtsbehörde zuständig ist. Facebook wusste nämlich schon, was auf sie zukommt und versuchte mit den sogenannten Standardvertragsklauseln eine eigene gestaltete Rechtssicherheit zu schaffen. Standardvertragsklauseln werden immer dann angewandt, wenn keine ausreichende Rechtssicherheit aus Sicht des Anbieters, hier in diesem Fall Facebook, vorliegt, und man sich anhand bilateraler Verträge in Ermangelung eines Gesetzes absichern möchte. Der EuGH stellte in diesem Zusammenhang fest, dass die grundsätzliche Anwendung von Standardvertragsklauseln zulässig ist, die aber von Facebook gewählten Inhalte in ihren Standardvertragsklauseln ebenfalls viel zu mangelhaft und von der irischen Datenschutzbehörde ungenügend überwacht wurden.

## **III. Auswirkungen des Urteils auf die Auswahl eines Board Portals?**

Wie schon erwähnt gibt es im Bereich der Anbieter von Enterprise Level Board Portalen eigentlich nur 3 oder 4 Anbieter, je nachdem wie man die gesellschaftsrechtlichen Strukturen bewerten möchte. Drei der vier Provider sind US-amerikanische Anbieter, die ausschließlich ihre Portale als Cloud-Lösungen offerieren und damit den gleichen Status wie Facebook haben. Nur ein einziger Anbieter auf diesem Niveau von Board Portalen ist nicht

durch US-amerikanische Anteilseigner beherrscht und betreibt nachweislich auch keine Server in den USA. Es ist auch nicht verwunderlich, dass dieser europäische Anbieter als einziger im Markt neben seinen Cloud Servern auch eine sogenannte On-Premise-Variante anbietet, die es dem Kunden ermöglicht, sich dieser gesamten Diskussion zu entziehen und seine Aufsichtsratsdaten auf kundeneigenen Servern zu lagern und zu sichern.

Bisher konnten Nutzer von US-amerikanischen Board Portal-Anbietern sich auf den Privacy Shield berufen und damit wenigsten so tun, als hätten sie ihren Prüfungspflichten in Zusammenhang mit der DS-GVO und anderen Gesetzen zum Schutz ihrer Daten genüge getan. Die US-amerikanischen Anbieter haben bisher auch Mantra-artig immer versichert, dass sie ja einen Firmensitz sowie Server in Deutschland oder anderen EU-Mitgliedstaaten hätten und damit den lokalen, nationalen Datenschutzgesetzen unterliegen würden. Diese Aussage hat Facebook auch immer wieder betont und dennoch wurde nun erneut, nach 2015 und dem Scheitern des Safe Harbour-Abkommens, festgestellt, dass diese Aussagen einfach keinen Wert haben. Das Gericht stellte nach 2015 erneut fest, dass es eigentlich keine Möglichkeit für einen US Board Portal-Anbieter gibt, EU rechtskonform Daten auf ihren Servern in den USA, und bei genauerer Hinsicht, auch nicht auf Servern in Deutschland oder irgendwo in der Welt, zu speichern. In den USA gibt es schlichtweg kein Datenschutzgesetz, dass mit EU-Gesetzen vergleichbar oder kompatibel ist.

Es gibt eine ganze Batterie an Gesetzen in den USA, die einen US-amerikanischen Board Portal-Anbieter zwingen, mit den US-Behörden stillschweigend und unter Strafandrohung zu kooperieren, egal wo der Server in der Welt betrieben wird.

Dazu jeweils kurz im Einzelnen:

#### **Foreign Intelligence Surveillance Act, 2001 (FISA)**

Dieses Gesetz sieht unter anderem den Betrieb von geheimen Gerichten vor. Deren Verhandlungen sind niemals öffentlich und die eigentlich verhandelte Person oder Organisation ist auch niemals anwesend oder hat Kenntnis darüber, dass ein US-Gericht über sie verhandelt. Es ist daher auch nicht verwunderlich, dass die Anzahl der Beschlüsse seit Jahren ansteigt und noch keine einzige Entscheidung eines FISA-Gerichts den Antrag einer US-Behörde abgelehnt hat.

#### **National Security Letters**

Diese werden direkt von der Ermittlungsbehörde ausgestellt und unterliegen nicht der Genehmigung eines Gerichts, was aus rechtsstaatlicher Sicht sicherlich problematisch ist. National Security Letters sind in der Praxis verbreiteter als durch ein Gericht genehmigte, geheime Durchsuchungen. Gemäß einer Statistik des Electronic Privacy Information Center (EPIC) wurden im Jahre 2010 circa 1.600 Gerichtsbeschlüsse nach dem Foreign Intelligence Surveillance Act (FISA) erlassen, die Zahl der National Security Letters soll dagegen bei rund 24.000 liegen.<sup>2</sup>

#### **Stored Communications Act, 1986 (SCA)**

Dieses Gesetz sieht insbesondere die geheime Überwachung von Meta-Daten von Nutzern von elektronischen Kommunikationsgeräten im In- wie auch im Ausland vor. Es ermächtigt US-Behörden aber auch auf andere erweiterte Datensätze zuzugreifen, sollten die Meta-Daten den ersten Ursprungsverdacht, der sehr einfach und weit gefasst sein kann, erhärten.

#### **International Communications Privacy Act, 2017 (ICPA)**

Auch dieses Gesetz sieht vor, dass US-Behörden auf Daten von US-amerikanischen Unternehmen zugreifen dürfen, egal wo deren Server in der Welt stehen.

---

<sup>2</sup> Quelle: Arnd Böken, Patriot Act und Cloud Computing – Zugriff auf Zuruf?

#### **Clarifying Lawful Overseas Use of Data Act, 2018 (CLOUD Act.)**

Dieses neueste Meisterwerk kann datenschutzrechtlich definitiv als die Bazooka aller oben genannten Gesetze angesehen werden. Es sieht vor, dass jegliches nationale Datenschutzgesetz von den USA als ungültig angesehen wird und ein US-amerikanischer Cloud-Anbieter, zu dem US Board Portal-Betreiber ebenfalls gehören, sämtliche gewünschte Daten, egal auf welchem Server in der Welt gespeichert, stillschweigend herausgeben muss.

#### **IV. Fazit**

Es wird deutlich, dass die Auswahl eines US Board Portal-Anbieters ohne gültigen Rechtsrahmen (Ex-Privacy Shield) eigentlich unmöglich gemacht wurde. Aber auch mit der bisherigen Gesetzesgrundlage wurde nun zum zweiten Mal entschieden, dass so etwas nicht rechtskonform möglich ist. Das Unternehmen sollte nun in Eigenverantwortung ein sehr aufwändiges Data Protection Impact Assessment (DPIA) durchführen und seine Situation neu bewerten. Durch den Wegfall des Privacy Shields sollte das Unternehmen als nächstes mit dem Board Portal-Betreiber die zuvor genannten Standardvertragsklauseln vereinbaren, um eine gesetzeskonforme Vereinbarung über die Handhabung von Daten auf deutschen Servern mit dem Anbieter zu erhalten. Beides, dass DPIA wie auch die Verhandlung über Standardvertragsklauseln, dürfte in 100% aller Fälle scheitern, weil der Board Portal-Betreiber nicht in der Lage sein wird, die strengen rechtlichen Anforderungen des einzelnen Unternehmens sowie der Datenschutzbehörden abzubilden. Darüber hinaus sollte das Unternehmen durch ständige Überprüfung der Vereinbarung sich vergewissern, dass der Anbieter sich an die Standardvertragsklauseln hält. Auch das wird nicht gelingen und weiterhin erhebliche Rechtsunsicherheit zurücklassen, weil der Board Portal-Betreiber bei der Überprüfung selbst auf Nachfrage durch das Unternehmen ja nicht wahrheitsgemäß antworten darf, da er die Daten schließlich geheim weiterreichen muss.

Das Wissen des deutschen Unternehmens darüber, dass US Board Portal-Anbieter den oben genannten Gesetzen unterliegen und im Zweifel trotz Standardvertragsklauseln, besonders auch in Zeiten von „Make America Great Again“ (MAGA), Daten herausgeben müssen, führt zu erheblichem Aufwand und Risiken und macht eine Entscheidung unmöglich. Die positive Kenntnis der oben genannten Risiken im Vorhinein einer Beauftragung eines US Board Portal-Betreibers kann unter bestimmten Umständen sogar zu Konsequenzen in Zusammenhang mit § 85 GmbHG führen und den Tatbestand der Verletzung der Geheimhaltungspflicht erfüllen.

In den nächsten Tagen drohen Unternehmen im Europäischen Wirtschaftsraum (EWR), die weiterhin amerikanische Cloud-Dienste nutzen, Maßnahmen einschliesslich Sanktionen von Datenschutz-Aufsichtsbehörden sowie Abmahnungen von betroffenen Personen wie auch von Konkurrenten und Konsumentenschutzorganisationen.

Und für alle diejenigen Unternehmen die jetzt sagen, das betrifft uns nicht, wir sind nicht so wichtig, wir haben nichts zu verheimlichen, möchte ich nur sagen: Ich freue mich auf die Zusendung Ihres nächsten Sitzungsprotokolls, Sie haben ja nichts zu verheimlichen.