Datenschutz: Umstellung auf Microsoft 365 Was Non-Profit-Organisationen beachten müssen, um ihre Daten in der Cloud zu schützen

Thomas Althammer, Hannover*/Dietrich Branscheid, Hannover**

Covid19 hat ein Schlaglicht auf die Themen Homeoffice, Videokonferenzen und Cloud-Computing geworfen. Non-Profit-Organisationen, Vereine, Stiftungen und Sozialunternehmen (insgesamt im Folgenden NPOs genannt) standen diesen Bereichen bisher eher restriktiv gegenüber. Allerdings mussten auch sie sich öffnen, um Minimalbetrieb im Lockdown aufrecht zu erhalten.

Video-Calls und besonders Cloud-Computing spielen dabei eine wichtige Rolle. Sie sind für Wirtschaft, NPOs und Privatkunden extrem relevante Zukunftstechnologien. Datenverarbeitung in der Wolke zeichnet sich durch jederzeitige Verfügbarkeit von überall auf der Welt aus, dynamische Ressourcenverwaltung und stets aktuelle Software. Für Datenschützer dagegen kann sie ein Problemfall sein. Die Risiken der Umstellung auf Cloud-Lösungen wie Microsoft 365 können und müssen kritische bewertet und Risiken minimiert werden. Einen Überblick bietet der folgende Beitrag.

I. Zukunft des Cloud-Computings

Microsoft hat mit der *Office-Suite* einen hohen Marktanteil in Deutschland. Basierend auf der „Cloud-first" Strategie werden nach und nach immer mehr Dienste aus der Cloud angeboten. Das heißt, dass ein großer Teil der privaten Nutzer, Unternehmen, Vereine und Verbände sich künftig mit dem Umzug der Daten in die Wolken auseinandersetzen muss. Denn klassische Desktop-Anwendungen von Microsoft und auch anderen Anbietern werden nach und nach aus der Wartung fallen. Am Beispiel von *Microsoft* als Marktführer in Deutschland wollen die Autoren aufzeigen, wo die Vorteile und Risiken des Cloud-Computings liegen und wie die datenschutzkonforme Migration der Daten in die Wolke gelingen kann.

II. Auftragsverarbeitung in der DSGVO geregelt

Beim Cloud-Computing werden im Auftrag des Verantwortlichen organisationseigene Daten auf IT-Systemen externer Dienstleister verarbeitet (zum Beispiel von *Microsoft* sowie weiteren Subunternehmen). Das nennt man Auftragsverarbeitung. Dafür gelten in der Europäischen Union strenge gesetzliche Regeln. In der Datenschutzgrundverordnung (DSGVO) sind insbesondere Artikel 28 und 32 relevant. Demgegenüber finden sich Regelungen zur rechtskonformen Auftragsverarbeitung für die evangelische Kirche und Einrichtungen der Diakonie in den §§ 27 und 30 des Kirchengesetzes über den Datenschutz der evangelischen Kirche (DSG-EKD) oder für die katholische Kirche und Organisationen der Caritas in den §§ 26 und 29 des Gesetzes über den kirchlichen Datenschutz (KDG).

Unternehmen, NPOs und weitere Nutzer müssen den beauftragten Dienstleister zusätzlich hinsichtlich der notwendigen technisch-organisatorischen Maßnahmen überprüfen. Die Überprüfung hat erstmals vor der Beauftragung zu erfolgen und ist regelmäßig (in der Regel jährlich) zu wiederholen. Die Datenübermittlung in das Ausland ist getrennt zu überprüfen. Unabhängige Sicherheitszertifizierungen, z.B. gemäß ISO 27001[1], können teilweise als Ersatz für persönliche Kontrollen herangezogen werden.

In der Praxis wird Cloud-Computing von den verschiedenen Datenschutzbehörden teils als problematisch eingestuft. Die Übermittlung personenbezogener Daten ist unter anderem nur dann zulässig, wenn die hohen datenschutzrechtlichen Anforderungen der Auftragsverarbeitung auch tatsächlich erfüllt werden. Besonders problematisch ist die Datenübermittlung an Server im Nicht-EU-Ausland oder der Zugriff auf Daten in Drittstaaten.

III. Zur Datenübermittlung in Drittländer bedarf es eines Angemessenheitsbeschlusses der EU oder des Abschlusses der Standardvertragsklauseln

Speicherort der *Microsoft*-Cloud-Dateien sind inzwischen unter anderem zwar Server in Deutschland oder der EU, allerdings müssen US-amerikanische Unternehmen im Rahmen der Auftragsverarbeitung gegebenenfalls US-Behörden aufgrund des CLOUD Acts[2] Zugriff auf diese Daten gewähren.

Beim Cloud-Computing werden oft Rechenzentren auf der ganzen Welt verwendet. Das bedeutet, dass personenbezogene Daten „in der Cloud", also zum Beispiel in Indien, China oder eben den USA verarbeitet werden, ohne dass der Auftraggeber über den tatsächlichen Ort, an dem sich seine Daten befinden, Kenntnis hat. Auch der Zugriff eines *Microsoft*-Mitarbeiters im Rahmen des Kunden-Supports, kann einen Auslandsbezug darstellen. Beispielsweise wird der Support für *Microsoft Office 365* aus Ägypten durchgeführt, inklusive Zugriff per Fernwartung (nach vorheriger Freischaltung durch den Anwender).

* Thomas Althammer ist Geschäftsführer Althammer & Kill GmbH & Co. KG, Hannover.

** Dietrich Branscheid ist Berater für Datenschutz Althammer & Kill GmbH & Co. KG, Hannover.

1 Bundesamt für Sicherheit und Informationsschutz über Zertifizierung und Anerkennung: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/GS_Zertifizierung_node.html (Stand 09.07.2020).

2 Heise Medien GmbH „US Cloud Act regelt internationalen Zugriff": https://www.heise.de/select/ix/2018/7/1530927567503187 (Stand 09.07.2020).

Die datenschutzrechtlichen Voraussetzungen der Auftragsverarbeitung inklusive Drittlandsbezug werden durch *Microsoft* vertraglich zugesichert. Das heißt aber nicht, dass der Auftraggeber dadurch von einer schutzbedarfsorientierten Risikoanalyse bezüglich der konkreten Verarbeitung von personenbezogenen Daten in der Wolke befreit wird. Insbesondere Sozial- und Gesundheitsorganisationen und Non Profits verarbeiten regelmäßig besonders schützenswerte Daten und müssen bei der Migration in die Cloud zusätzliche Maßnahmen ergreifen, um den europäischen Standard des Datenschutzes zu gewährleisten.

IV. *Europäischer Gerichtshof* kippt Datentransfer in die USA

Grundlage der Datenübermittlung in die USA waren bisher das EU-US Privacy Shield sowie die EU-Standard-Vertragsklauseln. Mitte Juli 2020 hat nun der *Europäische Gerichtshof* (*EuGH*) die Vereinbarung der EU mit den USA für ungültig erklärt. Der strenge europäische Datenschutz erlaubt den Transfer von Daten ins EU-Ausland nur, wenn dort das gleiche Schutzniveau sichergestellt ist, wie in der EU. Das sah der *Europäische Gerichtshof* in den USA nicht als gegeben an. Nun bedarf es einer neuen Vereinbarung zwischen der EU und den USA.

V. Welche Arten des Cloud-Computings gibt es und wie werden sie aus Datenschutzsicht bewertet?

Innerhalb der Cloud-Angebote wird grundsätzlich zwischen drei Services unterschieden:

- **Infrastructure as a Service (IaaS):** Dieser Service ermöglicht, das komplette Rechenzentrum vollends virtuell abzubilden und in die Cloud zu verlegen. Beispiel: Miete von Computern beziehungsweise virtuellen Maschinen
- **Plattform as a Service (PaaS):** Hier werden nur bestimmte Bereiche virtuell abgebildet. *Microsoft* stellt vollständige Betriebssysteme und virtuelle Server zur Verfügung und wartet diese. Beispiel: Speicherdienste wie *OneDrive* oder *DropBox*
- **Software as a Service (SaaS)**: Dies ist der bekannteste Service beim Cloud-Computing. Hierbei werden Web-basierte Programme direkt gestellt. Vorteil des SaaS-Modelles ist, dass dem Servicenehmer die Anschaffungs- und Betriebskosten teilweise erspart werden, weil der Cloud-Anbieter die komplette IT-Administration und weitere Dienstleistungen wie Wartungsarbeiten und Softwareaktualisierungen übernimmt. Beispiel: *Microsoft* Office Produkte im Browser oder *Google* Apps

Die Cloud-Lösung über *Microsoft 365* bezeichnet also zunächst das Anbieten einer virtuellen Dienstleistung im Bereich des Hostings für Anwendungen und Speicherressourcen. Während Unternehmen oder Organisationen früher üblicherweise selbst lokal Computer-Server betrieben, boten in den letzten 15 Jahren immer mehr IT-Dienstleister professionelles Server-Hosting an. Auf das Betreiben eines eigenen Servers konnten NPOs oder Unternehmen daher bereits verzichten.

Anders als beim klassischen Hosting kann der Cloud-Anbieter die länderübergreifende Infrastruktur seiner Rechenzentren im Rahmen der rechtlichen Möglichkeiten und vertraglicher Vereinbarungen frei wählen. Das heißt, er ist dazu berechtigt, Systeme in verschiedenen Rechenzentren zu hosten. Der Endkunde kann jedoch eine Speicherregion, zum Beispiel in Deutschland oder der Europäischen Union bestimmen, insofern dort ein Rechenzentrum verfügbar ist und dies vom jeweiligen Dienst unterstützt wird.

Der größte Vorteil des Cloud-Computings – die permanente Erreichbarkeit von Daten überall auf der Welt – ist gleichzeitig das größte Risiko, dessen sich Organisationen und Unternehmen bewusst sein müssen. Sie müssen Vor- und Nachteile gegen die Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität der eigenen Daten und damit der potentiell Betroffenen abwägen und Maßnahmen treffen, um die Risiken zielgerichtet reduzieren zu können.

VI. Verfügbarkeit

Gerade die Corona-Pandemie hat gezeigt, wie wichtig es ist, dass die eigenen Daten für Mitarbeiterinnen und Mitarbeiter verfügbar bleiben. Zwar sorgt das Cloud-Computing prinzipiell für jederzeitige Verfügbarkeit, doch der Internetzugang ist hier oft der Flaschenhals. Besitzt das Personal im Homeoffice beispielsweise die IT-Infrastruktur, um über das Internet Informationen zu verarbeiten?

VII. Vertraulichkeit

Non-Profit-Organisationen, Vereine und Verbände arbeiten in der Regel mit besonders schützenswerten Daten – man denke nur an die Jugend- und Familienhilfe, die Altenpflege oder Sozialdienste. Der Vertrauensverlust durch Verstöße gegen die Vertraulichkeit lässt sich nicht umkehren und ist im Hinblick auf den Datenschutz gravierend[3].

VIII. Integrität

Wenn Informationen manipuliert oder ungewollt verändert werden – zum Beispiel in Patientenakten –, kann erheblicher Schaden entstehen. Deshalb gilt der Integrität der Daten besonderes Augenmerk, wenn personenbezogenen Daten in der Cloud verarbeitet werden sollen.

IX. Wie gelingt die datenschutzkonforme Cloud-Migration für NPOs?

Um die Schutzziele nicht zu gefährden, müssen NPOs vor der Migration von Daten in die Wolke die Möglichkeiten und Risiken des Cloud-Computings für den jeweiligen Anwendungsfall genau prüfen. Es gibt diverse technische und organisatorische Möglichkeiten, die einzelnen Verarbeitungsvorgänge sowie die Nutzerrechte auf das Nötigste zu begrenzen, zum Beispiel in dem die an *Microsoft* übermittelten Telemetrie- und Diagnosedaten auf das Nötigste beschränkt werden. Welche Optionen und Maßnahmen sich hier anbieten, hängt auch von den erforderlichen Diensten und der Situation im Einzelfall ab.

3 Vgl.Schweigepflicht nach § 203 StGB.

WICHTIG: Zu jedem Zeitpunkt bleibt die Pflicht des Verantwortlichen bestehen, für eine rechtmäßige Verarbeitung von personenbezogenen Daten in *Microsoft 365* oder anderen Cloud-Angeboten Sorge zu tragen.

X. Wer braucht eine Datenschutz-Folgeabschätzung?

Für einige Verfahren, insbesondere bei der Verarbeitung besonderer Arten personenbezogener Daten (beispielsweise Gesundheitsdaten) sind Datenschutz-Folgeabschätzungen zwingend vorgeschrieben. Sie werden über sogenannte White- und Blacklists definiert. IT-Verantwortliche müssen im Rahmen des Prozesses Verfahren beschreiben, Risiken identifizieren und überprüfen, ob die getroffenen Schutzmaßnahmen angemessen sind.
VORSICHT: Maßnahmen, die im Falle des Falles von Behörden nicht als „angemessen" eingestuft werden, bergen Risiken auf Schadenersatz oder Bußgeldverfahren. Entsprechen die eigenen Lösungen dem Stand der Technik und sind sie im Hinblick auf die Risiken ausreichend?
EMPFEHLUNG: Auch wer nicht zu Datenschutz-Folgeabschätzungen verpflichtet ist, sollte trotzdem den risikobasierten Ansatz nutzen, um geeignete Maßnahmen zu treffen.

XI. Fazit

Auch wenn es auf dem Weg in die Cloud viele Fragen zum Datenschutz zu beachten gibt, so kann der Aufwand für viele Organisationen lohnen: In Zeiten der Digitalisierung sind neuartige Dienste und verbesserte Formen der Zusammenarbeit gefragt. Die Corona-Krise hat gezeigt, dass auch mit verteilten Standorten und Arbeit aus dem Homeoffice der Informations- und Kommunikationsfluss gewährleistet sein muss. Viele Cloud-Angebote halten hierfür gute Antworten bereit.
Checkliste für die Datenmigration in die Wolke

✔ **Strukturen analysiert und Zielkonzept erarbeitet?**
- Lizenzmodell und nötige Dienste identifiziert
- Bestandsaufnahme des Status quo
- Vertragliche Fragen und rechtliche Prüfung geklärt (Interessenabwägung hinsichtlich Auftragsverarbeitung formuliert)

✔ **Datenschutz-Folgeabschätzung durchgeführt?**
- Datenschutzkonzept erstellt und Verfahren dokumentiert
- Risiken identifiziert, analysiert und mit Datenströmen abgeglichen
- Maßnahmen zur Datenschutzkonformität ergriffen

✔ **Berechtigungen angepasst, Schutzmaßnahmen implementiert?**
- Konfigurationen / Gruppenrichtlinien betrachtet
- technische und organisatorische Maßnahmen implementiert
- Restrisiko ermittelt und Datenschutz-Folgeabschätzung ergänzt

✔ **Gesamtkonfiguration regelmäßig überprüft?**
- IT-Sicherheitsanalyse der Konfiguration vorgenommen
- laufende Anpassung an technische und rechtliche Weiterentwicklung
- regelmäßige Kontrolle durch Penetrationstests

Die Anpassung der Satzung an die tatsächlichen Verhältnisse des Vereinslebens

Dominik Nast, Stuttgart

Lässt in Vereinen das tatsächliche Engagement der Mitglieder nach, spiegelt sich dieser Umstand auch in einer geringen Teilnahme an der Mitgliederversammlung wider. Selbst in mitgliederstarken Vereinen sind niedrige Versammlungspräsenzen leider keine Seltenheit mehr. Wenn in diesem Fall die Satzung hohe Anforderungen an die Beschlussfassung stellt, kann dies zu einem echten Problem für das Vereinsleben werden, wie die Entscheidung des OLG München vom 30.1.2020[1] verdeutlicht. Aus diesem Grund sollten Vereine ihre Satzung regelmäßig überprüfen und, falls notwendig, an aktuelle Vereinsstrukturen anpassen. Wurde die Satzung nicht sukzessive aktualisiert, stellt sich die Frage, ob und inwieweit nachträglich noch Korrekturen möglich sind.

I. Einführung

Nach § 33 Abs. 1 S. 1 BGB bedürfen Satzungsänderungsbeschlüsse einer Mehrheit von drei Vierteln der abgegebenen Stimmen. Diese Vorschrift greift aber nur ein, soweit und solange die Satzung keine abweichenden Erfordernisse aufstellt, § 40 S. 1 BGB. Es besteht daher weitgehend Einigkeit, dass über die Mehrheitsanforderungen grundsätzlich frei disponiert werden kann,[2] wovon in der Praxis auch rege Gebrauch

* Dominik Nast ist Rechtsanwalt bei der HAVER & MAILÄNDER Rechtsanwälte Partnerschaft mbB, Stuttgart.

1 OLG München Beschl. v. 30.1.2020 – 31 Wx 371/19, ZStV 2020, 127.

2 MünchKommBGB/*Leuschner*, 8. Aufl. 2018, BGB § 33 Rz. 23 mwN.