An alle Interessierten

MICROSOFT 365 – SERVICES AUS DER MS-CLOUD ANALYSE UND EMPFEHLUNGEN ZUM RRB ZH NR. 2022-0542 - RISIKOGESICHTSPUNKTE

Lukas Fässler
lic.iur.Rechtsanwalt[1,2], Informatikexperte
faessler@fsdz.ch

Milica Stefanovic
MLaw Rechtsanwältin[2]
stefanovic@fsdz.ch

Zugerstrasse 76b
CH-6340 Baar
Tel.: +41 41 727 60 80
Fax: +41 41 727 60 85
www.fsdz.ch
sekretariat@fsdz.ch
UID: CHE-349.787.199 MWST

Carmen De la Cruz
Rechtsanwältin und Notarin 1,2
Eidg. dipl. Wirtschaftsinformatikerin
Industriestrasse 7
6300 Zug
delacruz@lexcellence.swiss

Partnerkanzleien:

Böhni Rechtsanwälte GmbH
Roman Böhni
MLaw Rechtsanwalt[1,2]
BSc Wirtschaftsinformatik

Zugerstrasse 76b
CH-6340 Baar
Tel.: ++41 41 541 79 60
info@boehnilaw.ch
www.boehnilaw.ch

[1] Mitglied des Schweizerischen Anwaltsverbandes
[2] Eingetragen im Anwaltsregister des Kantons Zug

Baar, 20. Mai 2022
Von: Rechtsanwalt Lukas Fässler

/Users/martinamurer/Desktop/Microsoft 365 - Cloudservices - Analyse und Empfehlungen zu RRB ZH 2022-0542 - 20-05-2022.docx

01. Ausgangslage

Nach der Veröffentlichung des Beschlusses Nr. 2022-0543 vom 30. März 2022 des Regierungsrates des Kantons Zürich über eine Risikobeurteilung hinsichtlich des Einsatzes von MS365 in der Verwaltung des Kantons ZH sind verschiedene Interpretationen zum Inhalt und der Bedeutung dieses RRB gemacht worden. Einzelne Anfragen gehen soweit, ob es anderen öffentlich-rechtlichen Körperschaften unbesehen weiterer Risikoabklärungen möglich sei, sich auf diesen RRB des Kantons ZH zu stützen und die Auslagerung und den Betrieb gewisser bisher auf internen Servern betriebenen Office-Anwendungen von Microsoft in eine cloud-basierte Umgebung von Microsoft auf diese Risikobeurteilung zuzulassen.

Als Unterlagen haben wir den RRB Nr. 2022-0542, ein Memorandum von VISCHER Rechtsanwälte vom 24.3.2022 (Bischof und Rosenthal) zuhanden des Amtes für Informatik des Kantons Zürich sowie weiterführende und in diesem Dokument verwiesene Entscheidungen mitanalysiert und in unsere Betrachtungen einbezogen.

02. Rahmenbedingungen und Einflussfaktoren

02.01 Grundlagen

Aus dem RRB ZH Nr. 2022-0542 sowie weiteren Kommentaren in der IT-Fachpresse ist zu entnehmen, dass die vom Regierungsrat des Kantons ZH vorgenommene Risikobeurteilung auf folgenden Grundlagen basiert:

- Separate Lieferantenrisikobeurteilung;
- Separate spezielle Zusatzrisikobeurteilung «lawfull access»;
- Vertrag des Kantons ZH mit Microsoft auf der Basis der SIK-Vertragsgrundlagen, datiert von Juni 2021;
- Zusatzvertrag zum SIK-Microsoft-Basisvertrag, datiert von Juni 2021;
- Separate Beurteilung und Genehmigung dieser Zusatzvereinbarung durch die kantonale Datenschutzbeauftragte;
- Anwendung des Risikobeurteilungsmodells von David Rosenthal;

- Durchführung eines internen Workshops zur Risikobeurteilung mit juristischen und technischen Fachexpertinnen und Experten aus dem Amt für Informatik, der Staatsanwaltschaft, dem kantonalen Steueramt, der Staatskanzlei und der Kantonspolizei Zürich;
- Beizug von statistischen Zahlen des Bundesamtes für Justiz aus der US-Rechtshilfe, ergänzt mit Erfahrungswerten der dortigen Spezialistinnen und Spezialisten im Zusammenhang mit abgelehnten oder nicht gestellten Gesuchen von US-Behörden.

02.02. Massgebliche Überlegungen RR Kanton ZH

- Der RRB ZH Nr. 2022-0542 betrifft ausschliesslich die **Risikobeurteilung des besonderen Bereichs des «lawful-access»** und dies – entgegen oft gehörter Argumente – nicht wegen des im Jahre 2018 erlassenen *US Clarifying Lawful Overseas Use of Data Act* (CLOUD Act) oder des *US Stored Communications Act* (SCA), sondern wegen des aus der **Section 702 des US Foreign Intelligence Surveillance Act (FISA) sowie der Executive Order (EO) 12.333** fliessenden **Rechts der amerikanischen Behörden auf Massenüberwachung von durch US-Provider abgewickelter Kommunikation von Nicht-US-Personen**.
- Die aufgrund der bestehenden (und auch künftig neuen) Datenschutzgesetze gesetzlich verankerte **Datenschutzfolgeabschätzung** bleibt davon unberührt und ist weiterhin von den verantwortlichen Verwaltungsstellen im Rahmen ihrer Projektumsetzungen und ihres ISDS-Konzeptes abzuklären und zu dokumentieren. Dies nicht zuletzt auch deshalb, weil in der öffentlichen Verwaltung nicht nur Personendaten, sondern auch vom Amtsgeheimnis erfasste Daten oder weitere geheimzuhaltende Informationen in eine Risikobeurteilung einzubeziehen sind.

02.03 Entscheid der österreichischen Datenschutzbehörde vom 22. April 2022

In einer Entscheidung vom 22. April 2022 (bei noyb abrufbar) in einem Parallelverfahren zu Google Analytics I hat die österreichische Datenschutzbehörde die Fragen nach einer risikobasierten Beurteilung von Cloud-Services beantwortet und zwar im Sinne der grundrechtlichen Konzeption des Datenschutzes.

Die DSB fragt dabei **nicht nach der Wahrscheinlichkeit**, dass problematisches US-Recht tatsächlich zur Anwendung kommt. Die Tatsache, dass lokale Behörden durch die Standardvertragsklauseln nicht gebunden sind und von problematischen Zugriffsrechten Gebrauch machen können, genügt. Dadurch **lehnt** die DSB den sog. "**risikobasierten Ansatz**" ab. Für die DSB gilt damit der "risikobasierte Ansatz" bei der Übermittlung in Drittstaaten nicht.
Rechtsschutzlücken im lokalen Recht dürfen demnach grundsätzlich nicht hingenommen werden und stellen somit keine Frage einer Risikobeurteilung dar**.** Es genügt nicht, dass eine Anwendung von relevanten Datenschutzverletzungen nur «ausreichend unwahrscheinlich» ist oder das durch sie für die betroffenen Personen bewirkte Risiko ausreichend niedrig ist.

Es stelle sich in diesem Zusammenhang die Grundsatzfrage, wie die von nationalen Nachrichtendiensten (in concreto: US-Nachrichtendienste) auf der Grundlage des eigenen nationalen (US-)Rechts tatsächlich zuässigen Zugriffe auf Personendaten und die damit einhergehende Verletzung elementarer Schutzrechte der Betroffenen verhindert oder eingeschränkt werden können. Solange [Google] selbst die Möglichkeit habe, auf Daten im Klartext zuzugreifen, könnten technische Maßnahmen nicht als effektiv im Sinne der obigen Überlegungen betrachtet werden
https://datenrecht.ch/dsb-oesterreich-google-analytics-ii-singularisierung-reicht-keine-individuellkonkrete-bestimmung-der-angemessenheit/?utm_source=datenrecht&utm_campaign =25cb8e0939-datenrecht-Mailchimp&utm_medium=email&utm_term=0_15155ce73b-25cb8e0939-90792857.

03 Entscheidpunkte

Auf der Basis von umfassenden (risikobasierten) Vorarbeiten und Abklärungen entschied der Regierungsrat des Kantons ZH im Zusammenhang mit dem Einsatz von M365 und insbesondere von Exchange Online sowie Teams, welche als on-premise-Lösungen gar nicht existieren und mit zunehmender Verbreitung

daher zum Gang in die Cloud zwingen, in Bezug auf den besonderen Risikobereich des lawful-access was folgt:

- Das Risikobeurteilungsmodell von David Rosenthal wird in der kantonalen Verwaltung **als Standardmodell** für die Einschätzung des **lawful-access-Risikosbereichs bei Cloudlösungen** eingesetzt. Diesem Vorgehen und Entscheid stehen die Beurteilungen der österreichischen Datenschutzbehörden diametral entgehen.
- Liegt die **Eintretenswahrscheinlichkeit** eines erfolgreichen Lawful-Access so niedrig, dass eine Wahrscheinlichkeit von **90% erst bei einem Beobachtungszeitraum von über 100 (!!) Jahren erreicht wird** (prognostizierte Wahrscheinlichkeit eines erfolgreichen ausländischen Behördenzugriffs in Bezug auf Geschäftsfalldaten (d.h. Daten aus hoheitlichen Geschäften) in einer Betrachtungsperiode von 5 Jahren liegt bei 0.74 Prozent), wird der Einsatz der Cloud-Lösungen von Microsoft aus der Warte des Regierungsrates des Kantons ZH zugelassen. Dieser Berechnungsmethodik wird entgegengehalten, dass sie eine Risikenbewertung in das zukünftige Verhalten eines Staates vorwegnehme, was angesichts der jeweils massgeblichen konkreten Lagen (z.B. Kriegszustände, Katastrophen etc.) gar nie zutreffend beurteilt werden könne.
- In einer Beobachtungsperiode über 5 Jahre entspricht dies nach der in den gängigen Lehrterminologien definierten Schwere von «sehr tief» oder «tief», jedoch noch nicht «mittel». Diese Bewertungsterminologie ist für die Argumentation der österreichischen Datenschutzbehörde nicht massgeblich, da gar keine Risikobewertung vorgenommen werden könne.
- Wenn das Risiko für einen lawful-access jedoch höher liegt, führt das dazu, dass eine entsprechende Cloud-Lösung vom Regierungsrat im Einzelfall zugelassen werden muss.
- Die Übernahme der Argumentation im RRB Nr. 2022-0542 setzt hinisichtlich der beurteilten vertraglichen Grundlagen zu Microsoft-Cloudservices auch voraus, die entsprechende Körperschaft über die gleichen vertraglichen Grundlagen im Bereich der Lizenzierung von Microsoft-Produkten verfügt wie der Kanton ZH. Dieser basiert auf dem Standardvertrag der SIK mit Microsoft aus Juni 2021.

04 Folgen für andere öffentlich-rechtliche Körperschaften

Auf der Basis dieser Überlegungen und der kontroversen Beurteilung zu dieser Frage können in Bezug auf die Uebernahme dieser Risikobeurteilung für einen lawful-access sowie für die notwendige Datenschutzfolgeabschätzung (Art. 22 neues Bundesdatenschutzgesetz; Art. 8 kantonales, Datenschutz-, Informations- und Archivgesetz vom 28.4.2019) folgende Schlüsse gezogen werden:

- Eine Übernahme des RRB Nr. 2022-0542 ist per se in Bezug auf ein **Risikobeurteilung im besonderen Risikobereich eines «lawful-access» für M365-Produkte** zwar möglich, jedoch nur dann statthaft, wenn nicht der fundiert begründeten Ansicht und Argumentation der österreichischen Datenschutzbehörden gefolgt wird.
- Eine so vorgenommene Risikobeurteilung ist nicht mit der gesetzlich geforderten allgemeinen Datenschutzfolgeabschätzung nach dem jeweiligen kantonalen Datenschutzgesetz identisch, sondern sie ist eine Zusatzrisikobeurteilung, welche aus dem Umstand geschuldet ist, dass die US-Behörden bei der Beurteilung im Fokus standen (FISA und EO mit Zwang zur Datenherausgabe von Nicht-US-Personen an US-Strafverfolgungsbehörden).
- Diese Risikobeurteilung eines lawful-access deckt somit nur einen Teilaspekt der zu klärenden Fragen im Zusammenhang mit der Auslagerung der Bearbeitung von Personendaten und dem Amtsgeheimnis unterliegenden Verwaltungsdaten ab. Sie bezieht sich ausschliesslich auf die im Rahmen der IKT-Grundversorgung im Kanton ZH zum Einsatz gelangenden Microsoft-Produkte der M365-Produktefamilie.
- Andere öffentlich-rechtliche Körperschaften (Kantone, Städte, Gemeinden etc.) müssen die Anwendung des Risikobeurteilungsmodell von David Rosenthal als Standardmodell explizit je für sich beschliessen, weil sich daraus auch für spätere und andere als die Microsoft-Cloudservices herzuleitende Risikobeurteilungen abgeleitet werden müssen. Wer den Ansatz der österreichischen Datenschutzbehörden teilt, legt jedenfalls für seinen Zuständigkeitsbereich kein

Standardisierungsvorgaben fest, schon gar nicht auf dem Risikobeurteilungsmodell von David Rosenthal, weil solche Betrachtungen unter der österreichischen Argumentation keinen Platz haben können.

- Wird ein risikobasierter Ansatz gewählt und zusätzlich ein Standardisierungsentscheid bezüglich der Risikobeurteilung von «lawfull access» gefällt, hat die zuständige öffentlich-rechtliche Körperschaft weiter zu entscheiden, ob die spezifischen Risikoabklärungen des Kantons ZH für seine Körperschaft und die organisatorisch nachgeordneten Verwaltungseinheiten überhaupt einschlägig und plausibel sind oder nicht.
- Mithin kann der RRB Nr. 2022-0542 also nur für Microsoft-Produkte M365 und vorerst auch nur bezüglich einer Risikobeurteillung für «lawful-access» als Diskussionsbasis, nicht aber als generell-abstrakt anzuwendender Risikobeurteilungsansatz herangezogen werden. Es bleibt die Grundsatzfrage zu klären, ob man «lawfull access» überhaupt als Risiko bewerten kann oder nicht.
- Jede auszulagernde Applikation muss seitens der Verantwortlichen (Amtsstelle, Dienststelle, Gemeinde etc.) einer **Datenschutzfolgeabschätzung nach der jeweils einschlägigen kantonalen Datenschutzgesetzesgebung** unterzogen werden, welche sich zusätzlich auch mit dem Faktum des «lawfull access» als besonderer Risikobereich auseinanderzusetzen hat und festzulegen hat, ob man solche Datenverwendungen, Datenbenutzungen oder Datenherausgabemöglichkeiten ausländischer Staaten aufgrund ihrer nationalen Gesetzgebung hinnehmen will oder nicht. Auszuschliessen sind sie jedenfalls auch nicht durch die Anwendung von Muster- oder Standardvertragsklauseln, welche in der Regel nachgeordnete staatliche Organisationseinheiten gar nicht rechtsverbindlich binden können.
- Dort wo Applikationen in eine andere Rechenzentrums-Infrastruktur eines nicht öffentlich-rechtlichen, nicht in der Schweiz (oder der EU, welche gleiches Datenschutzniveau garantiert) niedergelassenen Service-Providers ausgelagert werden (Drittländer ausserhalb EU; aber auch Länder der EU, die bekanntlich auch gesetzliche Grundlagen für nachrichtendienstliche Tätigkeiten geschaffen haben), muss **zusätzlich eine Auseinandersetzung und eine Entscheidung bezüglich des Umgangs mit dem Faktum «lawful-access» eines Fremdstaates vorgenommen werden.**
- Der Kanton Zürich hat das zu beurteilende Vertragswerk mit Microsoft mit einer von der kantonalen Datenschutzbeauftragten gestützten Beurteilung ergänzt. Es ist daher ebenfalls zu empfehlen, dass die jeweils zuständige kantonale Datenschutzaufsicht eine entpsrechende Ergänzungserklärung zu den Microsoft-Vertragsgrundlagen abgibt, die – analog zur Ergänzungserklärung der Datenschutzbeauftragten des Kantons Zürich – in das Vertragswerk mit Microsoft (Schweiz resp. Irland) eingebunden werden muss.
- Dort, wo Personendaten und dem Amtsgeheimnis unterliegende Daten in Cloud-Lösungen von Anbietern gespeichert und betrieben werden, auf welche gestützt auf nationale Gesetze ausländischer Staaten staatliche oder andere Institutionen einen Herausgabezwang gegenüber dem Cloud-Serviceprovider ausüben können, muss immer zur ordentlichen **Datenschutzfolgeabschätzung** und den daraus abgeleiteten technischen und organisatorischen Schutz- und Sicherheitsmassnahmen eine **zusätzliche lawful-access Risikobeurteilung durchgeführt werden**. Diese Risikobeurteilung ist ebenfalls im Rahmen des jeweiligen ISDS-Konzeptes der verantwortlichen Verwaltungseinheit auszuweisen.
- Die Verantwortung für den Schutz von Personendaten und dem Amtsgeheimnis unterliegenden Daten durch angemessene organisatorische und technische Massnahmen liegt bei den einzelnen Verwaltungseinheiten, auch bezüglich des besonderen Aspektes des «lawful access».
- Die Verantwortung für die ISDS-Konzept im Bereich der IKT-Grundversorgung liegen bei der zentralen Informatik, welche die standardisierte IKT-Grundversorgung bereitstellt. Dazu sind verschiedene rechtliche, organisatorische und technische Sicherheitsmassnahmen wirksam einzusetzen.
- Die hohe Veränderungsgeschwindigkeit im Bereich des Angebotes von Cloud-Lösungen in der IKT-Grundversorgung, aber auch in den Fachapplikationsbereichen der einzelnen Verwaltungseinheiten erfordert aus der Sicht des Datenschutzes und der Informationssicherheit ein **fortdauerndes Überwachen** sowie ein **stetiges Beurteilen aller Risiken, auch des besonderen Aspektes des «lawfull access»**.

- Der Kanton ZH hat angesichts der sich enorm rasch wandelnden Risiken sowie des schnellen Wandels hin zu Applikationen aus der Cloud eine Stelle eines Cloud-Sicherheitsbeauftragten im direkten Kontext des RRB Nr. 2022-0542 geschaffen. Ob sich eine solche Massnahme auch für die anderen Verwaltungseinheiten aufdrängt, haben diese in eigener Verwantowrtung zu entscheiden.
- Es ist aber klar, dass sowohl die ISDS-Konzepte, die Datenschutzfolgenabschätzungen, die besonderen lawful-access-Beurteilungen sowie die eingesetzen rechtlichen, organisatorischen und technischen Massnahmen einer permanenten Überprüfung und Anpassung bedürfen. Bestehende Cloud-Lösungen müssen daher in kurzen Abständen – mindestens einmal jährlich – bezüglich Veränderungen der Risikosituation im Bereich Informationssicherheit und Datenschutz sowie des besonderen Aspektes des «lawful access» überprüft werden.
- Die entsprechenden jährlichen Prüfberichte sind von den verantwortlichen Verwaltungseinheiten zu dokumentieren und nach den gesetzlichen Aufbewahrungs- und Archivbestimmungen aufzubewahren.
- Ob für den besonderen Aspekt des «lawful access» eine verschärfte Prüf-, Vorlage- und Dokumentationspflicht eingeführt werden soll, liegt ebenfalls in der Verantwortung der zuständigen Körperschaften.

FSDZ Rechtsanwälte & Notariat AG
Rechtsanwalt Lukas Fässler

Rechtsanwalt
CH-6340 Baar (Schweiz), 20.05.2022

Qualifizierte elektronische Signatur · Schweizer Recht
Signiert auf Skribble.com