Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Str. 22, 20459 Hamburg

Herrn Staatsrat Pörksen
Senatskanzlei der Freien und Hansestadt Hamburg
Rathausmarkt 1
20095 Hamburg

Ludwig-Erhard-Str. 22, 7. OG
20459 Hamburg
Telefon: 040 - 428 54 - 40 40
Telefax: 040 - 428 54 - 40 00
Ansprechpartner: Herr Prof. Dr. Caspar

E-Mail*: Johannes.Caspar@datenschutz.hamburg.de

Hamburg, den 05.03.2021

Nutzung von Zoom und Microsoft 365 in der FHH

Sehr geehrter Herr Staatsrat, lieber Herr Pörksen,

in Ihrer Antwort vom 6. Juli 2020 auf mein Schreiben zum Koalitionsvertrag betonen Sie, dass der Senat in seiner Digitalpolitik die bestmögliche IT-Unterstützung für die Mitarbeiterinnen und Mitarbeiter zu wirtschaftlich vertretbaren Kosten anstrebt sowie eine unangemessene Abhängigkeit von einzelnen Lieferanten vermeiden und die Einhaltung des Datenschutzes sicherstellen wird. Zudem stellen Sie Prüfungen in Aussicht, die zum Ziel haben, Mechanismen im vorwettbewerblichen Bereich zu fördern und somit die Anbieterbasis zu verbreitern. Unter diesen Gesichtspunkten darf ich aktuell auf Berichte meiner Mitarbeiter aus dem Jour fixe zwischen HmbBfDI und SK ITD 31 am 17.02.2021 zu sprechen kommen. Darin wurde angekündigt, dass die Senatskanzlei an der Einführung der Software Zoom für die Abwicklung von Videokonferenzen sowie Microsoft 365 zum Zwecke der Ablösung bisheriger Office-Anwendungen in der FHH arbeite.

Diese Entwicklungen besorgen uns vor dem Hintergrund, dass beide Systeme erhebliche datenschutzrechtliche Fragestellungen aufwerfen. Insofern möchte ich Sie bereits vorab über unsere kritische Einschätzung dieser Ankündigung unterrichten.

Das pandemiebedingte Erfordernis der Aufrechterhaltung des dienstlichen Betriebes führte bislang dazu, dass der datenschutzrechtlich problematische Einsatz vieler Systeme bisher ohne aufsichtsbehördliche Beanstandungen oder Prüfschritte verlaufen konnte. Meine Behörde wird hierbei auch in den kommenden Monaten mit dem erforderlichen Augenmaß agieren. Zugleich darf ich jedoch darauf hinweisen, dass viele der heute bestehenden Probleme bereits vor einem Jahr erkennbar waren und von mir auch gegenüber den unterschiedlichen Stellen angesprochen wurden. Die perspektivische Planung digitaler Entwicklungen gerade für den Regelbetrieb darf auch unter der gegenwärtigen Situation nicht auf der Strecke bleiben. An ihr bemisst sich die Fähigkeit von Politik, rationale und nachhaltige Lösungen für die Zukunft zu gestalten.

Wenn nun der Einsatz von Zoom und Microsoft 365 als eine dauerhafte Lösung in der FHH erwogen wird, begegnet dies jedenfalls aus Datenschutzsicht erheblichen Bedenken.

Mit Blick auf Videokonferenzsysteme hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit jüngst ihre Untersuchung aus dem letzten Jahr aktualisiert.[1] Für die Produkte Zoom sowie Microsoft Teams bleibt es insoweit nach wie vor bei einer äußerst kritischen datenschutzrechtlichen Bewertung mit einer roten Ampel[2]. Dieser Einschätzung schließen wir uns nach hiesiger Prüfung der Untersuchungskriterien und -methodik an. Gern stehen wir in diesem Zusammenhang für eine vertiefte Beratung zur Verfügung und geben Ihnen nähere Informationen. Gleichzeitig gehe ich davon aus, dass uns die schriftlichen Ausführungen bzw. Zusagen seitens Zoom gegenüber der Senatskanzlei zeitnah vorgelegt werden. Diese wurden anlässlich des Jour Fixe zwar angesprochen, ohne dass jedoch mehr als eine Überprüfung der Herausgabe an die Aufsichtsbehörde in Aussicht gestellt wurde.

Mit den bisherigen On-Premise-Installationen von Microsoft Office bietet Dataport die Möglichkeit an, Datenflüsse an externe Server zu analysieren und diese bei Bedarf zu unterbinden. Für den Fall, dass nun eine Umstellung auf Software-as-a-Service-Angebote in den Rechenzentren von Microsoft erfolgt, besteht diese Möglichkeit so nicht mehr. Eine manuelle Anpassung von Datenflüssen wie im bisherigen Rahmen ist dann nicht möglich. Die Nutzung von Diensten als Software-as-a-Service bzw. in Form einer Cloud-Lösung führt stattdessen zur Weitergabe von Daten auch personenbezogener Art an die Anbieter digitaler Dienste. Hier ist die Rechtsprechung des EuGH in Sachen „Schrems II“ (Urteil vom 16. Juli 2020 zu C-311/18) zur Datenweitergabe an Drittstaaten für die FHH als verantwortliche Stelle einschlägig und zu beachten. Ohne die Verwendung behördeneigener Systeme bzw. die Beibehaltung der bisherigen Lösung bleibt fraglich, wie sichergestellt werden soll, dass eine Übertragung personenbezogener Daten an Drittländer, für die im Sinne der Art. 44 ff DSGVO keine Rechtsgrundlage besteht, vermieden wird. Zudem kann durch die Verwendung behördeneigener System sichergestellt werden, dass öffentliche Stellen der FHH durch die Auswirkungen der Rechtsprechung des EuGH zu Art. 26 DSGVO (vgl. EuGH, Urteil vom 29.07.2019 zu C 14/17 „Fashion-ID“) nicht in eine gemeinsame Verantwortlichkeit für die Erhebung und Weiterleitung von personenbeziehbaren Meta- bzw. Telemetriedaten zusammen mit kommerziellen Dienstanbietern rutschen, die letztere für eigene kommerzielle Zwecke weiter verarbeiten. Eine Rechtsgrundlage für die Erhebung und Weiterleitung dieser Daten dürfte sich für die öffentlichen Stellen nämlich nicht ergeben. Im Zusammenhang mit der in Betracht gezogenen Nutzung von Microsoft 365 darf ich im Übrigen auf die Beschlusslage der Datenschutzkonferenz des Bundes und der Länder (DSK) vom 22.09.2020 verweisen, die derzeit eine rechtmäßige Nutzung von Microsoft 365 in Abrede stellt[3]; und dies ohne Berücksichtigung der sich durch die –Entscheidung des EuGH zu Schrems II ergebenen Folgen. Ich gehe davon aus und bin sicher, dass diese Aspekte gerade im Bereich der gesetzesgebundenen Exekutive in gebührender Weise Beachtung finden.

Jenseits der datenschutzrechtlichen Implikationen, die durch eine Umsetzung der Überlegung der Senatskanzlei aufgeworfen würden, darf ich die Gelegenheit nutzen, die derzeitigen Pläne der Senatskanzlei auch noch einmal vor dem Hintergrund der datenschutzpolitischen Ausführungen im Koalitionsvertrag zu würdigen. Der Koalitionsvertrag enthält ein klares Bekenntnis zur Entwicklung der FHH in Richtung auf mehr digitale Souveränität und Transparenz. Digitale Abhängigkeiten von außereuropäischen Dienstleistern werden immer deutlicher. Das zeigen exemplarisch die Entscheidungen des EuGH zu Schrems II für den Export personenbezogener Daten. Zuletzt machte der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom) deutlich, dass „eine überwiegende Mehrheit […] ihr Unternehmen für "nur kurzzeitig

---

[1] *Pressemitteilung „Mehr ‚Grün‘: Berliner Datenschutzbeauftragte veröffentlicht aktualisierte Hinweise zu datenschutzgerechten Videokonferenzdiensten“*
https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/20210218-PM-Videokonferenzdienste.pdf

[2] *Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten*
https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf

[3] *3. Zwischenkonferenz der DSK vom 22.09.2020, vgl. insbesondere Anlage 1*
https://www.datenschutzkonferenz-online.de/media/pr/20201030_protokoll_3_zwischenkonferenz.pdf

überlebensfähig" [hält], sollten digitale Dienstleistungen oder Technologien aus dem Ausland unvorhergesehen nicht mehr verfügbar sein. 94 Prozent der Befragten gaben an, dass ihr Unternehmen im Kern abhängig sei von digitalen Importen.“[4] Trotz vielfältiger Bekenntnisse zum vermehrten Einsatz von freien und offenen Softwarelösungen ist dieses Problem gerade auch im Bereich der öffentlichen Verwaltung immanent[5]. Das Bekenntnis im Koalitionsvertrag, als Vorreiter der digitalen Souveränität aufzutreten und Abhängigkeiten gegenüber Drittunternehmen zu vermeiden, insbesondere wenn überaus zweifelhaft ist, dass deren Datenverarbeitung nicht den europäischen Standards entsprechen, ist zu begrüßen. Eine solche Entscheidung würde jedoch bei Umsetzung der derzeit diskutierten Pläne in diametraler Weise konterkariert. Mitunter vorgetragene Bedenken gegen die Performanz quelloffener Systeme sind nach unserem Dafürhalten mit der entsprechenden Hardwareausstattung auszuräumen. Erfahrungswerte aus Schleswig-Holstein und bei öffentlichen Stellen in Hamburg wie der Polizei, die eine eigene Jitsi-Infrastruktur für ihre Weiterbildungen an der Akademie der Polizei aufgebaut hat, zeigen, dass mit dem entsprechenden Willen und der dazugehörigen Leistung in den Rechenzentren durchaus umsetzbar ist, quelloffene Dienste auch in der Verwaltung erfolgreich einzusetzen.

Für den weiteren Austausch sowie die datenschutzrechtliche Beratung mit Ihnen und der Senatskanzlei im Zusammenhang mit strategischen IT-Entscheidungen steht der Hamburgische Beauftrage für Datenschutz und Informationsfreiheit mit seinen Mitarbeiterinnen und Mitarbeitern auch weiterhin gern zur Verfügung.

Mit freundlichen Grüßen

Johannes Caspar

[4] *Digital unsouverän: Deutsche Wirtschaft "zu abhängig von Technologie-Importen", heise online* - https://www.heise.de/news/Digital-unsouveraen-Deutsche-Wirtschaft-zu-abhaengig-von-Technologie-Importen-5059145.html

[5] *Abhängigkeit der öffentlichen Verwaltung von Microsoft & Co ist "gigantisch", heise online* - https://www.heise.de/news/Abhaengigkeit-der-oeffentlichen-Verwaltung-von-Microsoft-Co-ist-gigantisch-5058500.html