DSK
DATENSCHUTZKONFERENZ

Vorsitz 2020
Sächsischer
Datenschutzbeauftragter

Dresden, 29. September 2020

3. Zwischenkonferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

Videokonferenz am 22. September 2020

- Protokoll -

TOP 1 - Begrüßung und Organisatorisches

Der **Vorsitzende** begrüßt die Teilnehmerinnen und Teilnehmer der 3. Zwischenkonferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, die als Videokonferenz durchgeführt wird, und stellt den geplanten Ablauf der Konferenz dar.

Der Vorsitzende stellt fest, dass der BfDI und die Aufsichtsbehörden aller Bundesländer entweder per Video oder per Telefon trotz anfänglicher technischer Probleme an der Konferenz teilnehmen.

Der Vorsitzende dankt Mecklenburg-Vorpommern für die technische Organisation der Konferenz.

TOP 2 - Tagesordnung und Protokoll

Der **Vorsitzende** verweist auf die allen Teilnehmern zur Verfügung gestellte Tagesordnung. Auf Antrag **Niedersachsens** wird unter TOP 17 – Sonstiges der Punkt „Informationsaustausch der Aufsichtsbehörden zur Anwendung des Bußgeldkonzeptes der DSK" aufgenommen.

Das Protokoll der 2. Zwischenkonferenz wurde im Umlaufverfahren Nr. 24/2020 beschlossen und liegt vor.

TOP 3 - Information zu Umlaufverfahren der DSK

Durch den **Vorsitzenden** wird festgestellt, dass alle Umlaufverfahren abgeschlossen werden konnten. Eine aktuelle Übersicht der Umlaufverfahren in 2020 wurde den Teilnehmenden mit E-Mail vom 17. September zur Verfügung gestellt.

Es erfolgt die zustimmende Kenntnisnahme durch die Konferenz.

[17, 0, 0] (Zustimmung, Ablehnung, Enthaltung)

TOP 4 - Bericht aus dem Europäischen Datenschutzausschuss (EDSA)

Der **BfDI** berichtet, dass der EDSA seit der 2. Zwischenkonferenz der DSK insgesamt 7x per Videokonferenz u. a. mit folgenden Themenschwerpunkten getagt habe:

- 16. Juni 2020

  Stellungnahme zu Covid19-Maßnahmen bei Grenzöffnungen, Stellungnahmen zur Interoperabilität von Kontaktnachverfolgungsanwendungen Covid-19 als Ergänzung der Stellungnahme zu Corona-Warn-Apps; Telekom und SAP werden noch voraussichtlich in diesem Jahr das Gateway herstellen, das den Datenaustausch zwischen den Apps verschiedener Anbieter ermöglichen soll.

- 30. Juni 2020

  Arbeitsplanung der Subgroups und Strategieplanung des EDSA;

  Am 29. September 2020 werde ein Workshop auf Commissioners-Ebene zum Entwurf eines Strategiepapiers eines Draftingteams, in dem auch Deutschland vertreten gewesen sei, stattfinden. Schwerpunkte werden sein: Stärkere Harmonisierung der Rechtseinhaltung und effektiver Rechtsdurchsetzung sowie Zusammenarbeit der Aufsichtsbehörden.

- 17. Juli 2020

  Stellungnahmen zur SCHREMS II-Entscheidung des Europäischen Gerichtshofs; Leitlinien für das Zusammenspiel zwischen Zweiter Zahlungsdienstleistungsrichtlinie (EU) 2015/2366 (PSD2) und DSGVO

- 22. Juli 2020

  Auswirkungen des Brexit auf BCRs und das Management von ICO-geführten BCRs

- 23. Juli 2020

  Erste FAQ (häufig gestellte Fragen) zur Klärung der Folgen des Schrems-II-Urteils;

  Es sei noch einmal festgehalten worden, dass es keine Übergangsfrist für Datenverarbeitung geben wird.

- 2. September 2020

  Die Leitlinien zu den Begriffen des Verantwortlichen und des Auftragsverarbeiters seien angenommen worden.

  Des Weiteren seien zwei Task Forces - eine zu den 101 Beschwerden von NOYB und eine zu Schrems II: Nächste Schritte und Folgemaßnahmen eingerichtet worden.

- 14. September 2020

  Interne Leitlinien für das Verfassen von Plenarprotokollen durch das Sekretariat; Task Force 101 Beschwerden;

Hamburg ergänzt, dass eine stärkere Transparenz des Gremiums EDSA angeregt und auch durchgesetzt worden sei, u.a. durch die Veröffentlichung der Sitzungsprotokolle. Des Weiteren berichtet Hamburg über die Rundmail der Irischen Aufsichtsbehörde (IDPC) im Hinblick auf Maßnahmen gegen Facebook bzgl. Datentransfer in die USA an das EDSA-Plenum vom 14. September 2020. Hamburg sagt zu, im Nachgang der 3. Zwischenkonferenz die Rundmail der IDPC sowie das Antwortscheiben Hamburgs den Aufsichtsbehörden zur Verfügung zu stellen.

Hamburg berichtet, dass sich die 101 Beschwerden, die bei einzelne Aufsichtsbehörden eingegangen seien, sich insbesondere gegen Webseiten-Betreiber richten würden, die unzulässig Tracking-Tools einsetzen und Daten in die USA übermittelten. Die Zuständigkeit für die Befassung mit diesen Beschwerden lege auf Länderebene. Der EDSA habe hier keine direkten Kompetenzen. Jedoch sei es sinnvoll, ein einheitliches Vorgehen abzustimmen. Die deutschen Aufsichtsbehörden unterstützen die Task Force „101 complaints" des EDPB durch die Mitarbeit von Hamburg, Berlin, Bayern, Nordrhein-Westfalen und Baden-Württemberg.

Darüber hinaus informiert **Hamburg** über das Artikel 65 Verfahren in Sachen Twitter. Das Verfahren, dessen Gegenstand mehrere Einsprüche verschiedener Aufsichtsbehörden sind, soll durch eine einheitliche Entscheidung bis November abgeschlossen werden. Dabei komme es in diesem Verfahren auch auf die Frage an, was unter dem Begriff „maßgebliche und begründete Einsprüche" verstanden werde. Hierzu laufe die Diskussion.

TOP 5 - EuGH-Urteil „Schrems II" (C-311/18)

Der **Vorsitzende** führt in den TOP mit einer Zusammenfassung der Aktivitäten auf nationaler Ebene ein. Auf europäischer Ebene seien, wie bereits durch den BfDI unter TOP 5 berichtet, zwei Task Forces des EDSA eingerichtet.

Hessen ergänzt, dass das 1. Treffen der Task Force „101 complaints" (teilnehmende Aufsichtsbehörden: Baden-Württemberg, Berlin) voraussichtlich am 2. Oktober 2020 sein wird. Die Task Force „Supplementary Measures" hätte bereits die Arbeit aufgenommen. Es sei schon ein erster Entwurf zu Hilfestellungen für Verantwortliche bei Umsetzung des Urteils diskutiert worden. Ggf. werde auch eine Art Entscheidungsbaum für die Verantwortlichen erstellt. Auf deutscher Ebene werde die Arbeit dieser Subgroup durch mehrere Kollegen und Kolleginnen unterstützt, die sich bereit erklärt haben, bei verschiedenen Schwerpunktthemen mitzuwirken. Es sei erfreulich gewesen, dass sich viele Aufsichtsbehörden zu einer Mitarbeit bereit erklärt haben. Bereits Ende Oktober soll im EDSA-Plenum ein Papier verabschiedet werden.

Die Aufsichtsbehörden halten fest, dass es Ziel sein sollte, sich auf ein einheitliches Vorgehen zu verständigen. Deutschland könne nur durch aktive Mitarbeit Einfluss auf die Ergebnisse der Task Forces nehmen.

Im Ergebnis der sich anschließenden Diskussion trifft die Datenschutzkonferenz folgende Festlegung:

1. Die Datenschutzkonferenz richtet eine Task Force „Schrems II" ein (teilnehmende Aufsichtsbehörden: LDA Bayern, Baden-Württemberg, BfDI, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Thüringen). Aufgabe dieser Task Force ist es, zum einen eine Strategie sowie konkrete Vorschläge für ein gemeinsames Vorgehen der deutschen Aufsichtsbehörden zur Umsetzung des EuGH-Urteils „Schrems II" zu erarbeiten und zum anderen die nationalen Vertreter in der Task Force „101 complaints" des EDPB zu unterstützen.

2. Mit dem Vorsitz der Task Force „Schrems II" werden Hamburg und Berlin beauftragt. Hierbei ist Hamburg federführend für den Themenbereich „Gemeinsames Vorgehen der deutschen Aufsichtsbehörden" und Berlin federführend im Themenbereich „Unterstützung der nationalen Vertreter der Task Force „101 complaints" des EDPB".

[17, 0, 0] (Zustimmung, Ablehnung, Enthaltung]

TOP 6 - Anwendung der DSGVO auf Datenverarbeitungen von Parlamenten

Der BfDI führt in den TOP ein. Der Bundestag habe hierzu eine Arbeitsgruppe beim Ältestenrat eingerichtet. Es sei festzustellen, dass auf Grundlage des EuGH-Urteils vom 9. Juli 2020 die bisherige Haltung nicht mehr aufrechterhalten werden könne.

Die unterschiedlichen Auffassungen der Aufsichtsbehörden zur Auslegung des EuGH-Urteils und dessen Konsequenzen werden kontrovers diskutiert. Im Ergebnis der Diskussion fasst die Datenschutzkonferenz folgenden Beschluss:

> Anlässlich des Urteils des EuGH vom 9. Juli 2020 (C-272/19) wird der Beschluss der DSK vom 5. September 2018 „Anwendung der DSGVO im Bereich von Parlamenten, Fraktionen, Abgeordneten und politischen Parteien" bis zur Neuformulierung eines Beschlusses ausgesetzt.

[13, 2, 2] (Zustimmung, Ablehnung, Enthaltung]

Die Datenschutzkonferenz trifft zum weiteren Vorgehen folgende Festlegung:

1. Der AK Grundsatz wird beauftragt, bis zur 100. DSK in Auswertung des Urteils des EuGH vom 9. Juli 2020 (C-272/19) den Beschluss der DSK vom 5. September 2018 „Anwendung der DSGVO im Bereich von Parlamenten, Fraktionen, Abgeordneten und politischen Parteien" zu überprüfen und ggf. anzupassen bzw. neu zu formulieren.

2. Der DSK-Vorsitz wird beauftragt, die Konferenz der Landtagsdirektoren über den Beschluss und die Festlegung zu Ziffer 1 zu informieren.

[17, 0, 0] (Zustimmung, Ablehnung, Enthaltung]

TOP 7 - Entschließung zur vorgesehenen Streichung des § 41 Abs. 1 Satz 3 BDSG (erstinstanzliche Zuständigkeit der Landgerichte ab Geldbußen von einhunderttausend Euro)

Berlin führt in den TOP ein und stellt den gemeinsamen Entschließungsentwurf von Berlin und dem BfDI vor.

Auf Grundlage der sich anschließenden Diskussion u. a. über die Besetzung der Kammern bei Amts- und Landgerichten der Länder, über die Erfahrungen im Umgang mit datenschutzrechtlichen Bußgeldverfahren durch die zuständigen Gerichte sowie über die Zielsetzung der öffentlichen Stellungnahme der Datenschutzkonferenz zum Gesetzesentwurf des Bundesrates (Drs. 107/20) zur Streichung des § 41 Abs. 1 Satz 3 BDSG werden Änderungsvorschläge zum Entschließungsentwurf eingebracht. Die im Ergebnis der Diskussion abgestimmten Änderungen werden in den Entschließungsentwurf eingearbeitet.

Sachsen-Anhalt informiert, dass der Bundesrat den Gesetzesentwurf am 3. Juli 2020 beschlossen habe.

Die Datenschutzkonferenz stimmt der vorliegenden geänderten Fassung der Entschließung zu.

[16, 0, 1] (Zustimmung, Ablehnung, Enthaltung]

TOP 8 - Entschließung zur digitalen Souveränität

Mecklenburg-Vorpommern stellt den in den Arbeitskreisen Grundsatz, Verwaltung und Technik parallel abgestimmten Entschließungsentwurf vor. Neben der konsolidierten Fassung des Entschließungsentwurfes liegt eine Fassung mit weiteren umfangreichen Anmerkungen und Änderungsvorschlägen aus Baden-Württemberg vor. Es wäre nun festzulegen, ob die Datenschutzkonferenz erst über die konsolidierte Fassung der Arbeitskreise oder über die baden-württembergische Fassung abstimmen solle.

Baden-Württemberg äußert Unverständnis darüber, dass diese Anmerkungen und Änderungsvorschläge seitens der Arbeitskreise vor der Zwischenkonferenz nicht bewertet wurden und ggf. Berücksichtigung gefunden haben. Jedoch würde sich Baden-Württemberg einer Mehrheitsentscheidung nicht entgegenstellen.

Sachsen-Anhalt stimmt für die konsolidierte Fassung vor allem unter Berücksichtigung der auf der Sondersitzung des IT-Planungsrates beschlossenen Investitionen für eine digitale Verwaltung (3 Mrd. Euro aus dem Konjunkturpaket).

Niedersachsen unterstützt ausdrücklich die Ausführungen Sachsen-Anhalts und weist daraufhin, dass die Datenschutzkonferenz vertreten durch Niedersachsen im IT-Planungsrat eine Beratungsfunktion innehabe. Der Bezug zum IT-Planungsrat solle demnach im Entschließungsentwurf beibehalten werden.

Die Datenschutzkonferenz stimmt der vorliegenden Fassung der Entschließung vom 22. September 2020 zu.

[14, 1, 2] (Zustimmung, Ablehnung, Enthaltung]

TOP 9 - Datenschutzrechtliche Bewertung der Auftragsverarbeitung bei Microsoft Office 365

Der **Vorsitzende** stellt die Ergebnisse der Umlaufverfahren Nr. 23/2020 („Datenschutzrechtliche Bewertung der Auftragsverarbeitung bei Microsoft Office 365") und Nr. 26/2020 (Abbruch des Umlaufverfahrens Nr. 23/2020) dar. Er weist noch einmal darauf hin, dass der vorliegenden Bewertung des Einsatzes des Produktes von Microsoft Office 365 durch den AK Verwaltung vom 15. Juli 2020 die Online Service Terms (OST) sowie die Datenschutzbestimmungen für Microsoft-Onlinedienste (Data Processing Addendum / DPA) – mit dem jeweiligen Stand: Januar 2020 – zu Grunde liegen.

Nach kontroverser Diskussion stimmt die Datenschutzkonferenz die Punkte des Festlegungsentwurfs einzeln ab. In der Diskussion wurde darauf hingewiesen, dass eine öffentliche Äußerung der DSK notwendig sei, außerdem sei der Text des Arbeitskreises bereits öffentlich. Bayern zog daraufhin die Nr. 5 der Vorlage (Nichtveröffentlichung der Dokumente) zurück.

Die Datenschutzkonferenz trifft folgende Festlegungen:

1. Die Datenschutzkonferenz nimmt die Bewertungen des AK Verwaltung[1] der dem Einsatz des Produktes Microsoft Office 365 zu Grunde liegenden Online Service Terms (OST) sowie die Datenschutzbestimmungen für Microsoft-Onlinedienste (Data Processing Addendum / DPA) – jeweils Stand: Januar 2020 –hinsichtlich der Erfüllung der Anforderungen von Artikel 28 Absatz 3 Datenschutz-Grundverordnung (DS-GVO) zustimmend zur Kenntnis.

   [9, 8, 0] (Zustimmung, Ablehnung, Enthaltung]

   Nachfolgende Aufsichtsbehörden haben gebeten, ihr abweichendes Votum kenntlich zu machen: Baden-Württemberg, Bayern, Hessen, Rheinland-Pfalz, Saarland, Sachsen.

2. Die Datenschutzkonferenz bittet eine Arbeitsgruppe (teilnehmende Aufsichtsbehörden: BfDI, Mecklenburg-Vorpommern, Sachsen und Schleswig-Holstein) unter Federführung Brandenburgs und des LDA Bayern u. a. auf Grundlage dieser Bewertungen Gespräche mit dem Hersteller aufzunehmen, um zeitnah daten-schutzgerechte Nachbesserungen sowie Anpassungen an die durch die Schrems II-Entscheidung des EuGH aufgezeigten Maßstäbe an Drittstaatentransfers für die Anwendungspraxis öffentlicher und nicht öffentlicher Stellen zu erreichen.

   [13, 2, 2] (Zustimmung, Ablehnung, Enthaltung]

3. Die Arbeitsgruppe wird gebeten, der Datenschutzkonferenz bis zur 100. Sitzung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder einen Zwischenbericht zu erstatten.

   [17, 0, 0] (Zustimmung, Ablehnung, Enthaltung]

Der Vorsitzende erklärt auf Nachfrage, dass er vor Veröffentlichung der Bewertungen des AK Verwaltung Kontakt mit Microsoft aufnimmt und die Bewertungen sowie die Festlegung der Datenschutzkonferenz übersendet. Er wird bei Presseanfragen ggf. die Festlegung zusammen mit der Anlage herausgeben und sie im Rahmen des Protokolls veröffentlichen. Bayern erklärt, seine Gegenposition auch öffentlich darstellen zu wollen.

Des Weiteren wird festgelegt, dass der AK Grundsatz beauftragt wird, die Rahmenbedingungen aufsichtsbehördlicher Produktwarnungen, insbesondere Rechtsgrundlagen, Anforderungen an Beweiserhebung und Verfahren sowie Haftungsfragen zu analysieren und der Datenschutzkonferenz möglichst bis zur 100. Sitzung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu berichten.

[13, 1, 3] (Zustimmung, Ablehnung, Enthaltung]

TOP 10 - Datenschutzrechtliche Positionierung zu Windows 10

Der zwischen BfDI und LDA Bayern abgestimmte und eingereichte Beschlussvorschlag wird an den AK Technik zurück verwiesen. Der AK Technik wird beauftragt, in seiner nächsten Sitzung am 30. September 2020 über diesen Beschlussvorschlag abschließend zu beraten.

---

[1] Anlage 1: Bewertung des AK Verwaltung vom 15.07.2020

Der konsolidierte und abgestimmte Beschlussvorschlag soll dann im Umlaufverfahren in der Datenschutzkonferenz abgestimmt werden.

TOP 11 - Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur

Der **BfDI** berichtet über den aktuellen Sachstand. Am 19. August 2020 habe zu dem Themenkomplex eine Bundespressekonferenz stattgefunden, an der neben BfDI auch Baden-Württemberg, Brandenburg und Niedersachsen teilgenommen haben.

Mit der Entschließung zum Patientendaten-Schutz-Gesetz, die im Umlaufverfahren durch die Datenschutzkonferenz abgestimmt wurde, werde der Bundesrat aufgefordert, die abschließende Beratung des PDSG zu nutzen, um den Vermittlungsausschuss anzurufen und notwendige datenschutzrechtliche Verbesserungen des PDSG noch im Gesetzgebungsverfahren zu erwirken.

Er weist daraufhin, dass zum 01.01.2021 ein nicht ausreichendes Authentifizierungsverfahren implementiert sein und ein unzureichendes Frontend für die Versicherten zur Nutzung bereitstehen werde.

Die Aufsichtsbehörden informieren ihrerseits über die Kontaktaufnahme mit den Krankenkassen und berichten über die jeweiligen Gesprächsergebnisse.

TOP 12 - Begleitung der Umsetzung des Onlinezugangsgesetzes durch die DSK

Der **DSK-Vorsitz** wird beauftragt, zur Abstimmung des Festlegungsentwurfs zur Begleitung der Umsetzung des OZG durch die DSK, der durch den AK Verwaltung vorgelegt wurde, ein Umlaufverfahren einzuleiten.

TOP 13 - Weiterer Umgang mit Ziffer 3 der Festlegung zu TOP 24 der 97. DSK: Vereinheitlichung von Publikationsformaten

Der TOP kann aus zeitlichen Gründen nicht mehr behandelt werden und wird auf die 100. DSK vertagt.

TOP 14 - Anfrage der Redaktion netzpolitik.org „Regelmäßige Veröffentlichung von DSGVO-Kennzahlen" vom 26. Mai 2020

Der TOP kann aus zeitlichen Gründen nicht mehr behandelt werden und wird auf die 100. DSK vertagt.

TOP 15 - Bericht der Aufsichtsbehörden zur Verarbeitung personenbezogener Daten bei der Bewältigung der Corona-Pandemie

Aus zeitlichen Gründen kann der TOP nicht mehr behandelt werden. Der **DSK-Vorsitz** wird beauftragt, die Berichte der Aufsichtsbehörden in schriftlicher Form einzuholen und diese auf dem BSCW-Server zur Verfügung zu stellen.

TOP 16 - Bericht des DSK-Vorsitzenden

1. Der **Vorsitzende** informiert, dass der Workshop des AK DSK 2.0 vom 13. bis 14. Oktober 2020 in Berlin durch einen externen Moderator begleitet werden wird. Dies ermöglicht dem Vorsitzenden sich inhaltlich stärker in die Diskussion einbringen zu können.

2. Aus zeitlichen Gründen wird der **Vorsitzende** schriftlich über die Anhörung des Beirates Beschäftigtendatenschutz informieren.

TOP 17 - Sonstiges

1. Auf Nachfrage von **Niedersachsen** tauschen sich die Aufsichtsbehörden über die Anwendung des DSK-Bußgeldkonzepts aus.

2. Der **BfDI** wird gebeten, den Sachstand zum Entwurf eines Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien (TTDSG) schriftlich mitzuteilen, insbesondere darüber, ob noch in diesem Jahr mit entscheidenden Schritten im Gesetzgebungsverfahren zu rechnen sei.

3. Auf Grund der Stellungnahme der BRAK prüft der AK Technik derzeit die Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail".

TOP 18 - Einsatz von Videokonferenzsystemen

Mecklenburg-Vorpommern als Vorsitz des AK Technik berichtet, dass auch zur 5. konsolidierten Fassung des Positionspapiers umfangreiche Anmerkungen der Aufsichtsbehörden eingegangen seien, die noch nicht abschließend bewertet und eingearbeitet werden konnten.

Mecklenburg-Vorpommern empfiehlt, das Positionspapier an den AK Technik zur Beschlussfassung in seiner nächsten Sitzung (voraussichtlich in der 40. KW) zu verweisen. Die abschließende Einbeziehung des AK Grundsatz solle durch interne Absprache zwischen den Vertretern des AK Technik und des AK Grundsatz in den jeweiligen Dienststellen erfolgen. Der **DSK-Vorsitz** wird gebeten, das Positionspapier dann im Umlaufverfahren beschließen zu lassen. Seitens der Teilnehmenden gibt es keine Einwände gegen dieses Vorgehen.

[17, 0, 0] (Zustimmung, Ablehnung, Enthaltung]

TOP 19 - Kurzpapier Nr. 14 der DSK „Beschäftigtendatenschutz"

Niedersachsen führt in den TOP ein und erläutert das Kurzpapier.

Der **BfDI** regt an, den letzten Absatz „Ausblick" des Kurzpapieres im 2. Satz „[...]Fragerecht bei der Einstellung von Bewerberinnen und Bewerbern, die Problematik eines Pre-Employment-Screenings" zu ergänzen. Das Pre-Employment Screening werde zur Profilbildung genutzt. Somit würden Bewerberangaben sowie Hintergründe der sich Bewerbenden intensiv überprüft. Der **BfDI** berichtet, dass auch im Beirat Beschäftigtendatenschutz angesprochen worden sei, dass das Thema Profilbildung bei sich Bewerbenden durch die DSGVO nicht ausreichend abgedeckt sei.

Die Datenschutzkonferenz stimmt der durch den Arbeitskreis Beschäftigtendatenschutz erarbeiteten Neufassung des Kurzpapiers Nummer 14 der DSK „Beschäftigtendatenschutz" einschließlich der Ergänzung durch den BfDI und dessen Veröffentlichung auf der Webseite der DSK zu.

[16, 0, 1] (Zustimmung, Ablehnung, Enthaltung]

Der **Vorsitzende** dankt dem AK Beschäftigtendatenschutz für die geleistete Arbeit.

i. V. Baumann

Andreas Schurig
Sächsischer Datenschutzbeauftragter

Bewertung des AK Verwaltung vom 15.07.2020

Sachverhalt:

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat die dem Einsatz des Produktes Microsoft Office 365 zu Grunde liegenden Online Service Terms (OST) sowie die Datenschutzbestimmungen für Microsoft-Onlinedienste (Data Processing Addendum / DPA) – jeweils Stand: Januar 2020 – geprüft und hinsichtlich der Erfüllung der Anforderungen von Artikel 28 Absatz 3 Datenschutz-Grundverordnung (DS-GVO) bewertet. Sie kommt zu dem Ergebnis, dass auf Basis dieser Unterlagen kein datenschutzgerechter Einsatz von Microsoft Office 365 möglich ist.

Dies ergibt sich aus den nachfolgenden Gründen:

1.) Art und Zweck der Verarbeitung, Art der personenbezogenen Daten

Auch unter der Berücksichtigung der Klassifizierung des Dienstes MS Office 365 als cloud-spezifischer Dienst, wonach es ggf. sachdienlich ist, die Arten personenbezogener Daten und deren Verarbeitungszweck verallgemeinert zu benennen, muss es dem Auftraggeber dennoch möglich sein, beides näher zu beschreiben und ggf. zu konkretisieren.

Dies betrifft insbesondere die Beschreibung personenbezogener Daten hinsichtlich der gesonderten datenschutzrechtlichen Anforderungen und Risikostufen, bspw. bei Daten nach Art. 9 DS-GVO, als auch der für den Auftraggeber maßgeblichen Zwecke.

Seitens des Auftragsverarbeitungsvertrages muss es ersichtlich sein, in welchem Umfeld (Fachverfahren) die Datenverarbeitung stattfindet und für welche Zwecke die Daten im Auftrag verarbeitet werden sollen. In diesem Zusammenhang wird Microsoft empfohlen, den Abstraktionsgrad zu verringern und Freifelder, welche erforderlichenfalls angepasst werden können, einzusetzen. Ggf. ist dadurch sogar eine konkrete Benennung im Einzelfall möglich.

2.) Eigene Verantwortlichkeit Microsofts im Rahmen der Verarbeitung für legitime Geschäftszwecke

Microsoft verweist innerhalb der Datenschutzbestimmungen für Microsoft Online-Dienste (Data Processing Agreement (DPA)) darauf, dass soweit es personenbezogene Daten im Zusammenhang mit legitimen Geschäftstätigkeiten von Microsoft verwendet oder anderweitig verarbeitet, Microsoft ein unabhängiger Datenverantwortlicher für diese Verwendung und für die Einhaltung aller geltenden Gesetze sowie der Erfüllung der Verpflichtung als Verantwortlicher verantwortlich ist.

Auch wenn nunmehr eine Aufzählung dieser legitimen Geschäftstätigkeiten erfolgt, ist weiterhin nicht eindeutig ersichtlich, welche weiteren personenbezogenen Daten in

diesem Rahmen verarbeitet werden. Dies betrifft insbesondere die Verarbeitung personenbezogener Daten in Bezug auf die Aktivitäten Microsofts unter den Punkten 3), 4), 5) und 6) der Definition der „legitimen Geschäftstätigkeit".[2]

Zudem besteht für die Übermittlung weiterer personenbezogener Daten vom Verantwortlichen an Microsoft, z.B. im Rahmen der Telemetrie, neben dem Auftragsverarbeitungsvertrag keine weitere Rechtsgrundlage.

Soweit Verantwortliche für die Übermittlung an Microsoft als eigenständig Verantwortlichem für die Verarbeitung der Daten vom Verantwortlichen und Dritten für „legitime Geschäftszwecke" ein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 lit. f) DS-GVO darlegen könnten, gilt dies gemäß Art. 6 Abs. 1 Satz 2 DS-GVO nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung. Es bedarf daher einer eigenen Rechtsgrundlage, die es der öffentlichen Verwaltung erlaubt, Daten von Beschäftigten oder Bürgerinnen und Bürgern für diese Zwecke zur Verfügung zu stellen.

Die jeweiligen Regelungen zur Zulässigkeit der Verarbeitung personenbezogener Daten durch öffentliche Stellen (gemäß Art. 6 Abs. 3 lit. b DS-GVO) können dabei wegen des (aufgrund der Grundrechtsrelevanz) strengen Erforderlichkeitsgrundsatzes nur bedingt als Rechtsgrundlage herangezogen werden. Nur unter der Voraussetzung, dass z.B. ein nachhaltig sicherer Einsatz der Software lediglich möglich ist, wenn der Anbieter bestimmte personenbezogene Systemdaten verarbeiten kann, kann die entsprechende Datenverarbeitung auch zur Erfüllung der Aufgaben erforderlich sein.

Jedenfalls für öffentliche Stellen sind daher nicht alle Anwendungsfälle der „legitimen Geschäftszwecke" abgebildet.

3.) Offenlegung verarbeiteter Daten – Cloud Act

In den Datenschutzbestimmungen für Microsoft Onlinedienste verweist Microsoft darauf, dass verarbeitete Daten außerhalb der Weisung des Kunden auch offengelegt werden können, wenn die Datenschutzbestimmungen es vorsehen oder dies gesetzlich vorgeschrieben wird.

Diese Beschreibung ist nicht hinreichend konkret und bestimmt nicht die durch den Auftraggeber vertraglich zu definierenden Rechte. Die Ausnahme darf sich ausschließlich auf das Recht der Union oder einzelstaatliches Recht eines Mitgliedsstaates beziehen, wobei nicht ausgeschlossen ist, dass zu diesem Recht auch Rechtshilfeabkommen gelten, die die Union oder einzelne Mitgliedsstaaten mit Drittstaaten schließen.

---

[2] (3) interne Berichterstattung und Modellierung (z. B. Prognose, Umsatz, Kapazitätsplanung, Produktstrategie); (4) Bekämpfung von Betrug, Cyberkriminalität oder Cyberangriffen, die Microsoft oder Microsoft-Produkte betreffen könnten; (5) Verbesserung der Kernfunktionalität in Bezug auf Barrierefreiheit, Datenschutz oder Energieeffizienz; und (6) Finanzberichterstattung und Einhaltung gesetzlicher Verpflichtungen

Die konkrete Umsetzung und die Auswirkungen des Cloud Acts, dem Microsoft als US-amerikanischer Hersteller unterliegt, auf die datenschutzrechtliche Frage zur rechtlich zulässigen Weitergabe personenbezogener Daten in diesem Kontext, sind nicht abschließend geklärt.

4.) Umsetzung technischer und organisatorischer Maßnahmen nach Art. 32 DS-GVO

Seitens der Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder besteht Konsens, dass der Auftraggeber grundsätzlich die Umsetzung und Beschreibung der technischen und organisatorischen Maßnahmen durch die Online-Service-Terms, die Datenschutzbestimmungen sowie weiterer durch Microsoft bereitgestellter Dokumentation prüfen und ausreichend (Zusatz-) Informationen einholen können muss. Zwar ist eine entsprechende IT-Sicherheitsrichtlinie in den DPA erwähnt (nicht in den OST), diese liegt jedoch vor Vertragsschluss nicht vor.

Grundsätzlich ist daher festzuhalten, dass in den Standard-OST seitens Microsoft keine ausreichende Darstellung erfolgt, welche dem Risiko angemessenen Maßnahmen der angebotene Onlinedienst für die Verarbeitung von personenbezogenen Daten bietet. Microsoft stellt darauf ab, dass der Verantwortliche allein für die unabhängige Entscheidung verantwortlich ist, ob die technischen und organisatorischen Maßnahmen für einen bestimmten Onlinedienst seinen Anforderungen entsprechen, einschließlich seiner Sicherheitsverpflichtungen gemäß geltenden Datenschutzvorschriften. Die derzeitigen Darstellungen zu den technischen und organisatorischen Maßnahmen in den Vertragsunterlagen allein reichen für den Verantwortlichen nicht aus (und sind durch den Verantwortlichen auch kaum zu prüfen), um eine objektive Einschätzung zu treffen, ob die Maßnahmen dem Risiko angemessen sind.

5.) Löschung und Rückgabe personenbezogener Daten

Microsoft differenziert im Rahmen der Verarbeitung zwischen den Kundendaten, die sich aus dem Auftragsverhältnis ergeben und Daten, die zur Erbringung „professioneller Dienstleistungen" und der Verarbeitung für „legitime Geschäftszwecke" eigenverantwortlich verarbeitet werden.

Seitens Microsoft werden entsprechend der Rolle als „Verantwortlicher" Daten, die zu eigenen Zwecken verarbeitet werden, nicht gelöscht.

Es ist zwar nachzuvollziehen, dass diese Daten gem. Definition nicht Teil der Auftragsverarbeitung sind und demnach aufgrund einer anderen Rechtsgrundlage verarbeitet werden, dennoch ist zu hinterfragen, wie lange die Daten für eigene Zwecke vorgehalten werden. Hierzu äußert sich Microsoft nicht.

6.) Information über Unterauftragsverarbeiter

In Bezug auf die Weitergabe personenbezogener Daten an Unterauftragnehmer ist die „vorherige schriftliche Zustimmung des Kunden zur Weitervergabe der Verarbeitung von Kundendaten und personenbezogenen Daten durch Microsoft" nur dann ausreichend, wenn eine Übersicht der zum Zeitpunkt der Unterzeichnung des Auftragsverarbeitungsvertrages vom Verantwortlichen (Kunden / Auftraggeber) genehmigten Unterauftragnehmer aufgenommen wird (siehe dazu auch 3.2.7 der Opinion 14/2019 des Europäischen Datenschutzausschusses).

Der zur Information über Hinzuziehung oder Ersetzung von Unterauftragnehmern vorgesehene „Mechanismus zur Benachrichtigung des Kunden über dieses Update" durch das Abonnement von Push-Benachrichtigungen ist dementsprechend proaktiv durch Microsoft einzusetzen.