RA Jonas Breyer und Anja Hirschel*

Zehn Rechtsverstöße beim DPA für Microsoft 365 vom 2. 1. 2024 („DPA“) – Teil 1

Über die Wertlosigkeit der „Data Boundary“ und die Mitverantwortung der Aufsichtsbehörden

Kurz und Knapp

Es ist nicht ernsthaft zu bestreiten, dass Microsoft 365 von Unternehmen nicht DSGVO-konform eingesetzt werden kann. Die Datenschutzkonferenz (DSK) hat dies offiziell bestätigt,[1] ebenso aus ähnlichen Gründen jüngst der Europäische Datenschutzbeauftragte.[2] Und doch wird das angeblich alternativlose Microsoft 365 zu Lasten minderjähriger Schüler und anderer betroffenen Personen breitflächig eingesetzt. Unternehmen begehen flächendeckend kalkulierten Rechtsbruch.

I. Übersicht der Verstöße

Der Einsatz von Microsoft 365 unter Zugrundelegung des DPA-Zusatzes vom 2. 1. 2024 – der einen AV-Vertrag im Sinne des Art. 28 DSGVO darstellt – geht mit Verstößen mindestens gegen folgende Vorschriften einher:

a) Art. 28 Abs. 3 S. 1 DSGVO (Datenarten in AV-Vertrag, Nr. IV),
b) Art. 6 Abs. 1, Art. 9 Abs. 1 DSGVO (Datenarten und Behördenzugriffe, Nr. IV, VI, VII, XIII),
c) Art. 13, 14 DSGVO (Transparenz und Informationspflichten, Nr. IV)
d) Art. 28 Abs. 1 DSGVO (Reichweite des AV-Vertrags, Nr. V),
e) Art. 44 DSGVO (Offenlegungen und Drittlandübermittlungen, Nr. VII, VIII),
f) Art. 28 Abs. 3 lit. a DSGVO (Weisungsbindung, Nr. IX),
g) Art. 28 Abs. 3 lit. h DSGVO (Inspektionsrecht, Nr. X),
h) Art. 28 Abs. 3 lit. g DSGVO (Löschanweisung, Nr. XI),
i) Art. 28 Abs. 2 DSGVO (Subunternehmer, Nr. XII) und
j) Art. 28 Abs. 3 lit. c DSGVO (Datensicherheit, Nr. XIV).

II. Übersicht risikomitigierender Maßnahmen

Als (ungenügende) risikomitigierende Maßnahmen, wenn Microsoft 365 dennoch eingesetzt werden soll, sind zu nennen:

a) *Eingeschränkte Nutzung*: Verwendung von Microsoft 365 für – gerade sensible – personenbezogene Daten (und Geschäftsgeheimnisse) so wenig wie möglich. Denkbar wäre beispielsweise ein Anknüpfen an im Unternehmen bereits bestehende Schutzklassen, etwa aus der Informationssicherheit;
b) *Alternativen*: Nutzung alternativer Software für möglichst viele Bereiche, welche sich durch Quelloffenheit, Transparenz, Kontrollfähigkeit und Anpassbarkeit etwa im Hinblick auf Cloudformen und Speicherorte auszeichnet, gegebenenfalls unter Beauftragung von Dienstleistern (etwa Linux als Betriebssystem, LibreOffice als lokale Office-Suite, Nextcloud zum Dateiaustausch, Nextcloud Collabora oder Onlyoffice als cloudbasierte Office-Suite, Nextcloud Talk für Chats, Jitsi Meet oder Nextcloud Talk für Videokonferenzen, Lineage als Smartphone-Betriebssystem usw.);
c) *Haftung*: Verlagerung der rechtlichen Haftung auf eigenverantwortliche Dienstleister, soweit möglich;
d) *Kollektivvereinbarung*: Für Betriebs- und Personalräte: Verlagerung der Haftung auf den Arbeitgeber per Betriebs- und Personalvereinbarung;
e) *Verschlüsselung*: eigene Verschlüsselung von Daten, soweit möglich (bedingt wirkungsvoll, wenn auf den Endgeräten ebenfalls Microsoft-Betriebssysteme laufen);[3]
f) *Richtlinien*: Reduzierung einiger unnötiger Datenverarbeitungen durch Microsoft-Richtlinien zur administrativen Steuerung von Rechten;
g) *Vollzugsdefizit*: Die Aufsichtsbehörden (DSK) haben beschlossen, dass Microsoft 365 nicht rechtmäßig zu nutzen sei,[4] entfalten aber keine effektive Tätigkeit, sodass Unternehmen momentan von einem Vollzugsausfall ausgehen können.

III. Weitere Microsoft-Vertragsteile

Da die Microsoft-Verträge modular aufgebaut sind und das DPA nur eines davon ist, ist es im Kontext mit anderen Vertragsteilen zu prüfen.

1. DPA

Bei Microsofts „DPA“ handelt es sich um eine Vereinbarung zur Auftragsverarbeitung (AVV) im Sinne des Art. 28 DSGVO. Sie bestimmt, dass Microsoft personenbezogene Daten des Kunden auf Weisung verarbeitet. Umfasst ist insbesondere das Produkt „Microsoft 365“, das unter anderem folgende Dienste beinhaltet: Word, Excel, Powerpoint, Sharepoint, Teams, Outlook, Exchange, Publisher, Access, Intune, Defender, Entra (vormals Azure AD), Azure Information Protection und Azure Virtual Desktop.

2. MBSV

Das DPA als Vertragsmodul regelt nicht die Hauptleistung. Es ist im Zusammenhang mit dem Hauptvertrag zu lesen. Dies ist bei vielen Unternehmen der Microsoft Business- und Service-Vertrag (MBSV).

Aus diesem ergibt sich unter anderem die Information, dass irisches Recht und ein irischer Gerichtsstand Gegenstand der Vereinbarung seien.[5] Solche Vereinbarungen sind im B2B-

* Mehr über den Autor und die Autorin erfahren Sie am Ende des Beitrags.
Alle zitierten Internetquellen wurden zuletzt abgerufen am 7. 8. 2024.
1 DSK, Festlegung vom 24. 11. 2022 zu Microsoft 365.
2 EDSB, Pressemeldung vom 11. 3. 2024, https://www.edps.europa.eu/system/files/2024-03/EDPS-2024-05-European-Commission_s-use-of-M365-infringes-data-protection-rules-for-EU-institutions-and-bodies_EN.pdf.
3 Verschlüsselungsoptionen bei Microsoft 365: www.computerweekly.com/de/tipp/Microsoft-Office-365-bietet-mehrere-Verschluesselungsoptionen.
4 DSK, Festlegung vom 24. 11. 2022 zu Microsoft 365.

Verkehr prinzipiell wirksam.[6] Daraus folgt, dass sich Kunden auf den Schutz der §§ 305 ff. BGB in Bezug auf unzulässige AGB nicht berufen können, es sei denn, diese wären in irischem Recht vorgesehen. Zumindest die europäische Klausel-Richtlinie verpflichtet den irischen Gesetzgeber hierzu aber lediglich im B2C-Verkehr.[7]

Darüber hinaus ergibt sich aus dem MBSV die Information, welche Gesellschaft des Microsoft-Konzerns Vertragspartner ist. Dies ist die Microsoft Ireland Operations Ltd., Dublin.

3. Datenschutz-Zusätze

Weitere Vertragsteile sind je nach Unternehmen teils Microsofts Datenschutzzusätze M471 und M803. Diese sind dem DPA ähnlich und Vorläufer. Soweit ersichtlich, wurden sie nie formal abgelöst. Allerdings beansprucht das DPA Geltungsvorrang.[8] Das Vertragsmodul M803 entspricht Anhang C des neuen DPAs. Es enthält ergänzende Maßnahmen im Zusammenhang mit Drittlandexporten, die infolge der Schrems-II-Rechtsprechung des EuGH ergänzt wurden.

4. Finanzzusätze

Schließlich wurden von einigen Finanzunternehmen die Finanzzusätze M399 und M411 vereinbart. Sie dienen der Informationssicherheit, wie sie von der BaFin gefordert (und auch geprüft und durchgesetzt) wird, und räumen diesen Behörden ein direktes Kontrollrecht bei den Microsoft-Gesellschaften ein.[9]

Sie können Risiken des Datenschutzrechts in geringem Umfang mitigieren. So wird dort auch dem Kunden ein direktes, über das DPA hinausgehendes Prüfungsrecht eingeräumt und zwar im Hinblick auf „die Einhaltung aller geltenden gesetzlichen und vertraglichen Anforderungen“.[10] Jedoch wird das Recht sogleich wieder insofern entwertet, als der Kunde „sämtliche Kosten“ trägt, einschließlich einem ungenannten, dem Vernehmen nach hohen Tagessatz für Microsoft-Mitarbeiter sowie Reisekosten.[11] Da Microsoft sich in seinen Standardklauseln weltweite Datenverarbeitungen vorbehält, können für Prüfungen weltweite Reisen notwendig werden. Alternativ ermöglicht Microsoft dort sogenannte Gruppen-Audits, bei denen sich mehrere Microsoft-Kunden zwecks Audit zusammenschließen können. Dies wird aber ebenfalls entwertet, da Beanstandungen nur einstimmig mit allen weiteren Teilnehmern geltend gemacht werden können.[12] Außerdem kann Microsoft verlangen, dass Teilnehmer eines Gruppen-Audits das „Customer Compliance Program“ entgeltpflichtig abonniert haben, welches eine Teilnahme des Kunden an einem „Webcast“ undefinierten Inhalts gewährt.[13] Schließlich stehen alle Kundenkontrollen unter dem wenig konturierten Vorbehalt, dass der jeweils zu prüfende Dienst für „wichtige Funktionen des Geschäftsbetriebs des Kunden“ genutzt wird,[14] wobei die Beweislast beim Kunden liegt.

5. Produktbestimmungen

An verschiedenen Stellen führt Microsoft aus, es gälten gegebenenfalls noch „Online Services Terms“ („OST“). Es ist nicht nachvollziehbar, unter welchem rechtlichen Gesichtspunkt diese jemals verbindlicher Vertragsteil geworden sein sollten. Eine Zustimmung der Kunden ist regelmäßig nicht bekannt. Inzwischen wurden sie nach Behauptungen Microsofts durch „Produktbestimmungen“ abgelöst. Diese enthalten für Online-Services – wie Microsoft 365 – vor allem lizenzrechtliche und keine datenschutzrelevanten Regelungen, weswegen diese Frage für Zwecke dieses Beitrags nicht abschließend geklärt werden muss.

IV. Risiko „Datenarten“

Ein Risiko des Verantwortlichen liegt darin, dass Microsoft die verarbeiteten Datenarten nur kursorisch definiert. Im Gegensatz zu früheren DPA- beziehungsweise AV-Fassungen spricht Microsoft neuerdings insbesondere von „Kundendaten“, die vom Kunden „bereitgestellt“ werden. Daneben spricht Microsoft von „personenbezogenen Daten“.[15] Diese beiden Datenmengen werden im DPA teils gleich, teils unterschiedlich behandelt. Da Kundendaten regelmäßig ebenfalls personenbezogen im Sinne der DSGVO sind und der Definition eine klare Abgrenzung fehlt, überschneiden sich beide Datenmengen. Die Größe der Schnittmenge ist unklar, weil weitere Verarbeitungen von Kundendaten durch Microsoft graduell denkbar sind.

Beispiel: Wenn Microsoft Kundendaten, wie im DPA beschrieben, aggregiert, bis zu welchem Abstraktionsgrad werden sie noch als Kundendaten angesehen?

Diese Schwierigkeit erkennt Microsoft in anderem Zusammenhang selbst, wenn es heißt: „Personenbezogene Daten, die Microsoft von oder im Namen des Kunden durch die Verwendung des Onlinediensts zur Verfügung gestellt werden, sind ebenfalls Kundendaten.“[16] Eine Konkretisierung soll durch Anhang B erfolgen, der aber ebenfalls nur unkonturierte Regelbeispiele aufführt und zum Schluss anführt, Gegenstand könnten auch „alle anderen in Art. 4 DSGVO genannten personenbezogenen Daten“ sein. Was Microsoft unter personenbezogenen Daten versteht, bleibt im Dunklen, nachdem der EuGH den Personenbezug von „vernünftigerweise“ zur Identifizierung verfügbaren Mitteln abhängig gemacht hat.[17]

Dass Microsoft die Datenarten wesentlich genauer angeben könnte, zeigt eine detailliertere Dokumentation der mit Entra (ehemals Azure AD) synchronisierten Datenarten.[18] Diese Liste kann allerdings immer noch nicht vollständig sein, da beispielsweise Inhaltsdaten und personenbezogene Metadaten jedenfalls tieferer Protokollschichten völlig fehlen, obwohl diese technisch zwangsläufig verarbeitet werden. Die Bezeichnungen der Kategorien sowie der Zweck der Veröffentlichung (Syncronisierung Entra) deuten darauf hin, dass auch Verbindungsdaten fehlen, die etwa bei Anrufen anfallen.

Des Weiteren veröffentlicht Microsoft eine über 300-seitige Liste (Auszug siehe folgende Tabelle) mit sogenannten Diagnosedaten, die verarbeitet werden.[19] Laut Microsofts Datenschutzerklärung sind diese „required diagnostic data“ für „Produktverbesserungen“ bestimmt und „mindestens erforderlich“, „um Anwendungen zu schützen, auf dem neuesten Stand zu halten und dafür zu sorgen, dass sie ordnungsgemäß auf

5 MBSA, Nr. 13h und Nr. 13e und iii.
6 Art. 3 VO (EG) 593/2008 – Rom I; Art. 25 VO (EU) 1215/2012 – Brüssel Ia.
7 Art. 1 RL 93/13/EWG – mißbräuchliche Klauseln in Verbraucherverträgen.
8 DPA, S. 3, „Einleitung“, zweiter Absatz.
9 Vertragszusatz M399, Nr. 3.
10 Vertragszusatz M399, Nr. 4.
11 Vertragszusatz M399, Nr. 4a, 1, ii.
12 Vertragszusatz M399, Nr. 4a, 2, iv.
13 Vertragszusatz M399, Nr. 4a, 2, iv.
14 Vertragszusatz M399, Nr. 4a, 2, vii.
15 DPA, S. 4, „Definitionen“.
16 DPA, S. 7, „Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeiten“.
17 EuGH, 19. 10. 2016 – C-582/14, K&R 2016, 811 ff., Rn. 45 – Breyer.
18 https://learn.microsoft.com/de-DE/entra/identity/hybrid/connect/reference-connect-sync-attributes-synchronized.
19 https://learn.microsoft.com/en-us/deployoffice/privacy/required-diagnostic-data.

dem Gerät, auf dem sie installiert sind, funktionieren".[20] Der EuGH hat im Fall „Meta" entschieden, dass jedenfalls invasive Datenverarbeitungen zur Produktverbesserung nicht mehr nach Art. 6 Abs. 1 lit. f DSGVO zulässig sind,[21] wobei dieser Tatbestand für öffentlich-rechtliche Stellen ohnehin ausscheidet. Exemplarisch erhebt Microsoft nach eigenen Angaben beim Verfassen einer E-Mail (Abschnitt „send.message") unter anderem folgende Datenarten, die etwa erfassen, wie lange sich ein User in einem bestimmten Adressfeld aufgehalten hat. Die Felder stellen eine Verhaltensüberwachung im Sinne von § 87 Abs. 1 Nr. 6 BetrVG dar, für Office 365 wurde eine Mitbestimmungspflicht bereits bejaht.[22] Eine auch datenschutzrechtlich wirkende Betriebsvereinbarung ist zwar möglich, unterläge aber laut einer Entscheidung des EuGH aus dem Jahr 2023 den hohen Anforderungen des Art. 88 DSGVO in Bezug auf die Spezifizierung der Verarbeitung.[23] Die vorgenommene Zählung der Tastenanschläge („key_stroke_count") kommt der Funktionalität eines Keyloggers nahe, welcher vom BAG für gänzlich unzulässig befunden[24] wurde.

Feldname	*Erläuterung Microsoft*
account	account that performed the action
compose_addressing_duration	total time user spends on To/Cc/Bcc fields
compose_duration	total time user took to compose the message
draft_message_id	message ID
key_stroke_count	tracks the keystrokes count for the message that is being sent
message_ordering_mode	tracks how the user orders their messages in the reading pane (for example, newest on bottom or newest on top) so we can analyze the impact this has on the send rate and the type of send
thread_id	indicates thread ID of the conversation

Dass bei Microsofts E-Mail-Online-Dienst „Exchange" sämtliche E-Mail-Verbindungs- und Inhaltsdaten an Microsoft weitergegeben werden und funktional bedingt Microsoft auch Zugriff auf ihren Klartext innehat, etwaige Verschlüsselungen also nicht gegenüber Microsoft wirken, liegt auf der Hand. Exchange verwendet bloß eine Transportverschlüsselung von Server zu Server.[25]

Ähnliche Datentypen sind auch für weitere Dienste aus Microsoft 365 verzeichnet.

Der Europäische Datenschutzausschuss (EDSA) hat bestimmt, dass Datenarten in der AVV vertraglich hinreichend zu konkretisieren seien und auch eine ungleiche Verteilung der Marktmacht zwischen den Vertragsparteien eine Abweichung hiervon nicht zu rechtfertigen vermöge.[26] Der EDSA ist ein unabhängiges, bei der EU-Kommission angesiedeltes Organ, das aus den Datenschutz-Aufsichtsbehörden aller Mitgliedstaaten besteht. Er ist gesetzlich berechtigt und verpflichtet, Leitlinien zur Auslegung der DSGVO zu erlassen, um eine europaweit harmonisierte Anwendung sicherzustellen (Art. 70 Abs. 1 lit. e DSGVO).

Auch alle deutschen Datenschutz-Aufsichtsbehörden, organisiert in der Datenschutzkonferenz („DSK"), sehen in ihrer Festlegung vom 24. 11. 2022 in diesem Informationsgefälle einen Verstoß gegen die Spezifizierungspflicht des Art. 28 Abs. 3 DSGVO („Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen…").[27] Der Kunde kann ohne Kenntnis der Datenarten die Einhaltung der Datenschutz-Grundsätze gemäß Art. 5 Abs. 1 DSGVO nicht prüfen: die Zulässigkeit der Verarbeitung, die Transparenz (etwa Datenschutzerklärungen gegenüber Kunden und Beschäftigten), die Zweckbindung, die Datenminimierung, die Richtigkeit, die Speicherbegrenzung sowie die von der Datenqualität abhängende Datensicherheit. Erst recht kann der Kunde als Verantwortlicher die Einhaltung dessen nicht nachweisen und somit seiner Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO nicht genügen.[28]

Aus den oben genannten Datenarten ergeben sich auch Verstöße gegen Art. 6 Abs. 1 lit. f DSGVO (berechtigte Interessen). Beispielsweise ist die Übermittlung eines Thumbnail-Fotos auf Vorrat an Microsoft im Rahmen von Teams funktional nicht zur Nutzung erforderlich. Gerade im Arbeitsverhältnis sind wegen der arbeitsrechtlichen persönlichen Abhängigkeit des Arbeitnehmers Einwilligungen als mögliche Rechtsgrundlage problematisch. Entsprechendes gilt je nach Datenart für Art. 9 Abs. 1 DSGVO. Einmal hochgeladen, hat der Nutzer entgegen Art. 17 Abs. 1 DSGVO auch oft keine praktikable Möglichkeit der Löschung (siehe unten).

V. Risiko „Reichweite der AVV"

Die AVV weist einen Geltungsbereich auf, der Art. 28 Abs. 1 DSGVO nicht genügt. So umfasst sie ausdrücklich keine Daten, „die in den Räumlichkeiten des Kunden oder in vom Kunden ausgewählten Betriebsumgebungen von Drittanbietern verbleiben".[29] Merkmal einer Auftragsverarbeitung ist aber nicht, dass die Verarbeitung an einem bestimmten Ort stattfindet, sondern lediglich, dass eine vom Auftraggeber abweichende Stelle (insbesondere ein anderes Unternehmen) personenbezogene Daten im Auftrag verarbeitet.[30] Ob Microsoft seine Software so gestaltet, dass Microsoft die Datenverarbeitung beim Kunden (etwa lokal im Browser) oder online vornimmt, ist daher rechtlich unerheblich.

VI. Risiko „zweckfremde Datenverarbeitungen"

Ein Verstoß gegen Art. 28 Abs. 10 DSGVO, hiermit verbunden auch gegen Art. 6, 9 DSGVO (Offenlegung), liegt vor, soweit Microsoft sich im DPA vorbehält, „Statistiken" aus „Kundendaten" zu erstellen. Diese sollen unter anderem Microsofts „Geschäftsmodellierung", „Umsatz" und „Produktstrategie" dienen.

Wie die DSK feststellt, handelt es sich dabei um eigene Zwecke Microsofts. Microsoft konnte den Aufsichtsbehörden auf An-

20 https://privacy.microsoft.com/de-de/privacystatement?PrintView=true, Abschnitt „Microsoft 365, Office und andere Produktivitäts-Apps".
21 EuGH, 4. 7. 2023 – C-252/21, K&R 2023, 492 ff., Rn. 123 – Meta.
22 Zur Mitbestimmungspflicht bei Office 365 BAG, 8. 3. 2022 – 1 ABR 20/21, K&R 2022, 643 ff. = NZA 2022, 1134.
23 EuGH, 30. 3. 2023 – C-34/21, K&R 2023, 340 ff., Rn. 75 – Hauptpersonalrat.
24 BAG, 27. 7. 2017 – 2 AZR 681/16, K&R 2017, 745 = NJW 2017, 3258.
25 https://www.computerweekly.com/de/tipp/Microsoft-Office-365-bietet-mehrere-Verschluesselungsoptionen.
26 EDSA, Leitlinien 7/2020 zur Auftragsverarbeitung, Rn. 110 - 114.
27 DSK, Festlegung vom 24. 11. 2022 zu Microsoft 365, Anlage, S. 7 – 10.
28 DSK, Festlegung vom 24. 11. 2022 zu Microsoft 365, Anlage, S. 7 – 10.
29 DPA, S. 5, „Umfang".
30 EDSA, Leitlinien 7/2020 zur Auftragsverarbeitung, Rn. 76.