DATENSCHUTZ IN ZEITEN VON MS TEAMS, VIDEOVERHANDLUNGEN & HOME OFFICE

Ltd. Ministerialrat Gregor Eisenhuth
Bayerisches Staatsministerium der Justiz

27. September 2022
Amberger Congress Centrum

Die Datenschutz-Grundverordnung (DSGVO)…
ist – für viele völlig überraschend – am 25. Mai 2018 in Kraft getreten:

- Dauer des Gesetzgebungsverfahrens: Sechs Jahre
- Inkrafttreten: Mai 2016
- Seit 25. Mai 2018 unmittelbar geltendes Recht in allen EU-Mitgliedstaaten
- 99 Artikel mit 173 Erwägungsgründen regeln das Datenschutzrecht insbesondere
  - Die Grundsätze der Verarbeitung personenbezogener Daten
  - Die Rechte der betroffenen Personen,
  - Die Verantwortlichkeit für die Datenverarbeitung (DV) und
  - Die Befugnisse der Aufsichtsbehörden und Sanktionsmöglichkeiten
- Ergänzend gelten das Bundesdatenschutzgesetz sowie das Bayerische Datenschutzgesetz, die Teilbereiche des Datenschutzes regeln, soweit die DSGVO diese für die nationalen Gesetzgeber offen gelassen hat.
- Grundlage ist das europäische Grundrecht auf Schutz personenbezogener Daten gem. Art. 8 der Charta der Grundrechte der EU (GRCh)
- Die DSGVO verpflichtet auch private Unternehmen und zwar auch solche mit Sitz außerhalb der EU,
  - wenn diese Daten von EU-Bürgern verarbeiten oder
  - eine Niederlassung in der EU haben.

Die Justiz und der Datenschutz:

Bereits vor den erheblichen Veränderungen des justiziellen Arbeitens hatte die eingesetzte Digitalisierung einen Perspektivwechsel bei der Datenverarbeitung bedingt:

Spätestens mit der Einführung der elektronischen Akte und des elektronischen Rechtsverkehrs – nicht vorrangig durch die DSGVO und ihre Umsetzung im nationalen Recht – musste sich die Justiz ihre eigene Rolle als datenverarbeitende Organisation bewusst machen.

Die Justiz erhebt selbst in erheblichem Umfang nicht selten sensible personenbezogenen Daten von Beteiligten wie auch von Unbeteiligten. Die zunehmende Möglichkeit der strukturierten Durchsuchung und Analyse von elektronisch gespeicherten Daten steigert zugleich das Bedürfnis nach der Gewährleistung datenschutzrechtlicher Grundsätze.

Corona – Ansteckungsgefahr für den Datenschutz

Telearbeit, Home Office und Mobiles Arbeiten

Telearbeit = Arbeit an vom Arbeitgeber fest eingerichteten Bildschirmarbeitsplätzen im Privatbereich der Beschäftigten

Mobile Arbeit = Von anderen Orten als dem regulären Arbeitsplatz in der Dienststelle im Privatbereich der Beschäftigten aus geleistete Arbeit, soweit es sich nicht um Telearbeit handelt.

Datenverarbeitung im Arbeitsverhältnis

- Art. 4 Nr. 7 DSGVO: Verantwortlicher ist die Behörde, vertreten durch ihre(n) jeweilige(N) Leiter(in)
- Dies gilt auch uneingeschränkt bei Telearbeit und mobiler Arbeit
- Mitarbeiter(innen) dürfen personenbezogene Daten ausschließlich gemäß Weisung des Verantwortlichen verarbeiten

Telearbeit, Home Office und Mobiles Arbeiten

Hieraus folgt eine **Organisationsverpflichtung**, die insbesondere folgende Punkte beinhaltet:

- Regelung:
  - ✓ **Dienstvereinbarung** über Telearbeit und Mobile Arbeit im nichtrichterlichen und nichtstaatsanwaltlichen Dienst bei den Gerichten und Staatsanwaltschaften im Geschäftsbereich des Bayerischen Staatsministeriums der Justiz, Ziffer 9 (**schriftliche Verpflichtung!**)
  - ✓ Ergänzt durch **Datenschutzhinweise** zur Telearbeit und zum mobilen Arbeiten, JMS vom 4. Juli 2022 Gz. B5 – 1552E – VI – 4574/2022
- Schulung der Mitarbeiter(innen)
- Kontrollpflicht

Ziel der datenschutzrechtlichen Regelungen und Hinweise zur Telearbeit bzw. zur mobilen Arbeit

- Der Datenschutz steht Telearbeit und Mobilem Arbeiten nicht grundsätzlich entgegen. Vielmehr gebietet der risikobasierte Ansatz des geltenden Datenschutzrechts bei der Ausübung von Telearbeit bzw. beim mobilen Arbeiten für die Verarbeitung personenbezogener Daten ein vergleichbares Schutzniveau herzustellen wie bei der Verarbeitung der entsprechenden Daten am Büroarbeitsplatz, an dem v.a. die vorhandenen Zutrittskontrollen die Vertraulichkeit der Datenverarbeitung gewährleisten.

- Die Regelungen in der DV und die ergänzenden Hinweise sollen bei der vorzunehmenden Prüfung unterstützen, ob und ggf. wie bestimmte dienstliche Aufgaben bzw. Tätigkeiten datenschutzkonform im Rahmen von Telearbeit bzw. Mobiler Arbeit wahrgenommen werden können.

- Sie können nicht von der stets im Einzelfall vorzunehmenden Risikoabwägung entbinden. Im Zweifel muss der jeweilige Verantwortliche nach Art. 4 Nr. 7 Datenschutz-Grundverordnung (DSGVO) oder - im Bereich der richterlichen Unabhängigkeit - die jeweilige Richterin bzw. der jeweilige Richter selbst entscheiden.

- Die Einbeziehung des örtlichen Datenschutzbeauftragten bei der Klärung von Zweifelsfragen wird empfohlen.

Der (sichere) Weg ist das Ziel

Ziffer 9.1. DV: „*Die Beschäftigten haben eigenverantwortlich für den datenschutzsicheren Transport der Akten und sonstigen notwendigen Arbeitsunterlagen zu sorgen. Auch im Rahmen der Telearbeit und Mobilen Arbeit müssen Personalakten in der Dienststelle verbleiben*“.

Ziffer 2 DS-Hinweise:

- Angemessener Transportschutz
- Eigentumskennzeichnung für den Verlustfall
- Getrennte Aufbewahrung von Passwörtern
- Medienbruch nach Möglichkeit vermeiden
- Nur dienstliche zur Verfügung gestellte Speichermedien nutzen (Verschlüsselung!)

My Home is my Castle – aber füllen Sie doch bitte noch den Wassergraben um Ihren heimischen Arbeitsplatz

Ziffer 9.2. DV: „*Für die Aufbewahrung der dienstlichen Unterlagen im privaten Bereich muss ein verschließbarer Schrank oder ein abschließbares Behältnis vorhanden sein; Familienangehörige und Dritte dürfen keinen Zugang zu den dienstlichen Unterlagen erhalten*“.

Ziffer 3 DS-Hinweise:

- Ausreichender Akustik- und Sichtschutz
- Keine Smart Home-Geräte (z.B. Alexa) im Homeoffice
- WLAN mit ausreichend komplexem Passwort schützen
- Vollständige Sicherheitsupdates garantiert (nur) die Verbindung per Dockingstation in der Dienststelle

Der Thingplatz lag immer unter freiem Himmel – bei der mobilen Arbeit mache ich mein Ding auch außerhalb der eigenen 4 Wände

Ziffer 3 DS-Hinweise:

- Verwenden von Sichtschutzfolien
- Öffentliche Aufladestationen meiden
- Keine Verbindung dienstlicher IT-Geräte über USB- oder Bluetoothschnittstellen mit Fahrzeugen
- Öffentliche WLANs nur vorübergehend nutzen, besser: mobiler WLAN-Hotspot oder entsprechende Funktion des Diensthandys
- Mobile Arbeit außerhalb der EU oder eines Drittstaats mit Angemessenheitsbeschluss (Art. 45 Abs. 3 DSGVO) kann besondere, im Zweifel nur schwer zu erfüllende datenschutzrechtliche Anforderungen begründen.

BYOD – Bitte nicht!

Ziffer 9.3. DV: „*Die von der Dienststelle zur Verfügung gestellten Rechner und Datenträger sind gegen den Zugriff Unberechtigter zu schützen.* ***Private Datenträger dürfen nicht verwendet werden****. Der Rechner ist mit einer Sicherheitskomponente gegen die Inbetriebnahme durch Unbefugte abzusichern.* ***Veränderungen an der Hard- und Software sind nicht gestattet****“.*

Ziffer 5 DS-Hinweise:

- Nutzen Sie zu dienstlichen Zwecken möglichst die vom Dienstherrn zur Verfügung gestellten elektronischen Geräte. Dies gilt insbesondere für den Laptop als zentrales Arbeitsmittel.
- Die Nutzung privater **netzwerkfähiger** Geräte wie etwa Drucker, Scanner, Faxgeräte oder sonstiger Multifunktionsgeräte (hierunter fallen regelmäßig nicht zusätzliche Monitore) ist möglichst zu vermeiden.
- Wenn Drucker: Bitte dienstlich zugelassene Geräte verwenden und diese per USB (nicht WLAN) mit dem Rechner verbinden.

Melden macht frei!

Selbst bei Anwendung größter Sorgfalt können bei den heutigen komplexen Datenverarbeitungsvorgängen bei der Telearbeit und beim Mobilen Arbeiten zahlreiche Dinge schief gehen. Scheuen Sie sich daher bitte nicht, Vorfälle und Auffälligkeiten zeitnah mitzuteilen. Mit einem umsichtigen Meldeverhalten leisten Sie den vielleicht wichtigsten Beitrag zu einer sicheren Arbeitsumgebung am Telearbeitsplatz bzw. beim Mobilen Arbeiten:

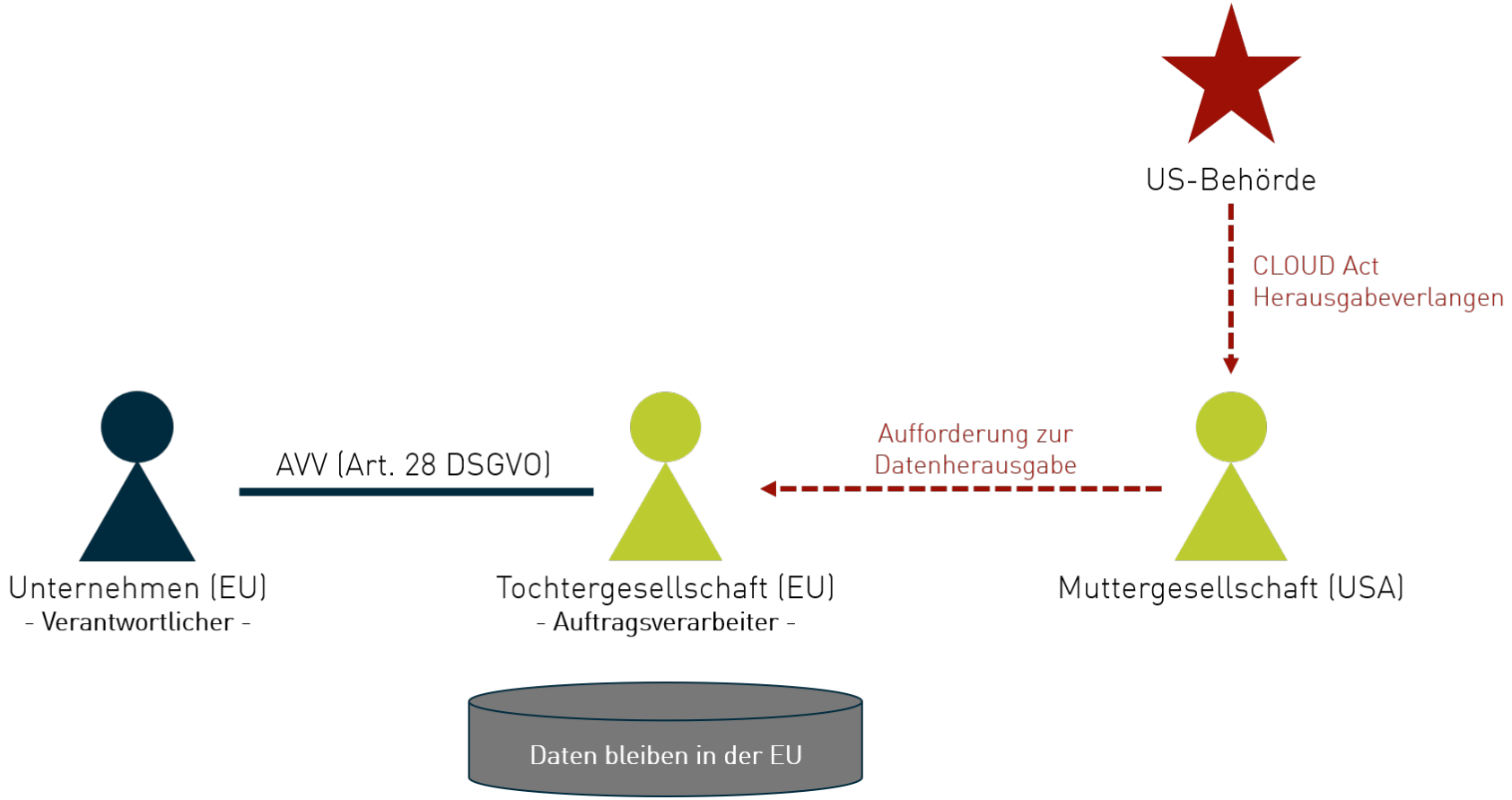
- Unterstützt den Verantwortlichen bei der Erfüllung von Meldepflichten gemäß Art. 33 DSGVO;
- Unterstützt das IT-Sicherheitsmanagement;
- Unterstützt den behördlichen Datenschutzbeauftragten;
- Unterstützt alle anderen Anwenderinnen und Anwender der bayerischen Justiz durch rechtzeitige Begrenzung möglicher Angriffe von außen!

Datenschutzrechtliche Herausforderungen bei Videoverhandlungen – Cloud Act vs DSGVO

- Ende März 2018 hat US-Präsident Donald Trump den sog. **CLOUD Act** (Clarifying Lawful Overseas Use of Data Act) noch vor Abschluss eines laufenden Supreme Court Verfahrens und ohne internationale Absprachen unterzeichnet. Dieses neue Gesetz erlaubt US-Behörden den Zugriff auf im Ausland gespeicherte Daten, solange die betroffenen **Server unter der Kontrolle von US-Unternehmen** sind. Eine vorherige Überprüfung durch Gerichte oder Behörden des Staates, in dem sich die Server befinden, ist nicht vorgesehen.

- Folge war nahezu zwangsläufig ein **Konflikt mit der** am 25. Mai 2018 in sämtlichen Mitgliedstaaten in Kraft getretenen **DSGVO**. Diese verbietet Unternehmen nämlich die Übergabe von in der EU gesicherten Daten ohne Rechtshilfeabkommen, Art. 48 DSGVO. Bei einem Verstoß gegen die Pflichten aus Artikel 48 drohen nach Art. 83 DSGVO empfindliche Bußgelder in Höhe von bis zu 20 Millionen Euro oder mindestens vier Prozent des weltweiten Jahresumsatzes.

Datenschutzrechtliche Herausforderungen bei Videoverhandlungen – Cloud Act vs DSGVO



Datenschutzrechtliche Herausforderungen – Ausgangssituation

- „**Schrems II-Entscheidung“ des EuGH vom 16. Juli 2020**: Aufhebung des Privacy Shield Abkommens, weil der sog. Cloud Act US-Sicherheitsbehörden in Einzelfällen Zugriff auch auf Daten amerikanischer Unternehmen ermöglicht, die auf Servern innerhalb der EU gespeichert sind => Vermutung für ein angemessenes Schutzniveau einer Datenverarbeitung in den USA ist entfallen.
- Das angemessene Schutzniveau kann jedoch weiterhin durch geeignete **Standardvertragsklauseln** nach dem Muster der Kommission **und** eine **Risikoabwägung** für die konkrete Vertragskonstellation sichergestellt werden.
- Eine datenschutzkonforme Nutzung von MS 365 – Produkten erfordert daher die vertragliche Einbeziehung der EU-Standardvertragsklauseln in der jeweils aktuellen Fassung **und** technisch-organisatorische Maßnahmen, die ein angemessenes Schutzniveau im Hinblick auf die konkret verarbeiteten Daten sicherstellen.

Datenschutzrechtliche Herausforderungen – vertragliche Maßnahmen

Übermittlungen auf Grundlage von Standarddatenschutzklauseln sind **nicht automatisch**, sondern nur zulässig, wenn Datenzugriffe durch drittstaatlichen Behörden nur in einem Umfang stattfinden können, der auch nach EU-Recht zulässig wäre (Maßstab ist Art. 52 EU-Grundrechtecharta).

Microsoft hat als Reaktion auf das bekannte Schrems II-Urteil bereits wichtige Anpassungen bei den verwendeten **Standardvertragsklauseln** vorgenommen, die auch zum Bestandteil der hiesigen Verträge gemacht wurden (Stand: 12/2020):

- die **Information** der betroffenen Person, wenn Microsoft eine Aufforderung von Dritten (insbesondere US-Sicherheitsbehörden) zur zwangsweisen Offenlegung von personenbezogenen Daten erhält;
- die Verpflichtung von Microsoft, den **Rechtsweg** zu beschreiten, um die behördliche Anordnung zur Herausgabe der Daten anzufechten;
- den Anspruch auf **Schadensersatz** für die betroffene Person, sofern diese durch die Offenlegung einen materiellen oder immateriellen Schaden erlitten hat.

Datenschutzrechtliche Herausforderungen – vertragliche Maßnahmen

Nunmehr sind die am 4. Juni 2021 von der Kommission veröffentlichten Standardvertragsklauseln in den Vertrag mit MS einzubeziehen:

Die neuen Standardvertragsklauseln sind an die **DSGVO angepasst**, **berücksichtigen die EuGH-Rechtsprechung zum Privacy Shield** und sind **modular aufgebaut.** Allerdings müssen alle bereits abgeschlossenen Standardvertragsklauseln, insbesondere mit US-Anbietern, innerhalb von 18 Monaten(27. Dezember 2022) aktualisiert werden.

Berücksichtigung der Schrems II-Rechtsprechung des EUGH zum Privacy Shield – Speziell die Klauseln 14 und 15 (Abschnitt III) enthalten spezielle Sicherheitsmaßnahmen, die einigen der Ergänzungen entsprechen, die von Datenschutzbehörden und dem Europäischen Datenschutzausschuss (“EDSA”) bereits zu den alten Standardvertragsklauseln vorgeschlagen wurden.

Vereinbarung der neuesten Standardvertragsklauseln setzt das **Produkt MS 365 E5** voraus.

Datenschutzrechtliche Herausforderungen – vertragliche Maßnahmen

- **15. September 2022:** Neue Version des "Microsoft Products and Services Data Protection Addendum" (DPA) geht auf Vorgaben der EU-Kommission ein und umfasst MS 365.
- Die nunmehr allein gültigen neuen SVK werden dabei in **Modul 3** zu Transfers von Auftragsverarbeitern abgeschlossen => Drittlandsübermittlungen erfolgen somit von Microsoft Irland als Datenexporteur
- Damit einher gehen erstmals Garantien, "um etwaige Auswirkungen der Gesetze des Bestimmungsdrittlands" auf die Einhaltbarkeit der Klauseln durch den Datenimporteur zu regeln.
- Dabei gilt es vor allem vorab zu klären, "wie mit verbindlichen Ersuchen von Behörden im Drittland nach einer Weitergabe der übermittelten personenbezogenen Daten umzugehen ist„.
- Nutzer der neuen SVK müssen zudem ergriffene Maßnahmen benennen, mit denen die Menge der persönlichen Daten vor einem Transfer möglichst gering gehalten, pseudonymisiert und verschlüsselt wird.

Datenschutzrechtliche Herausforderungen – technische und organisatorische Maßnahmen (Art. 32 DSGVO)

- Dateispeicherorte mit Rechnungsadresse werden bereits jetzt in Deutschland gehostet.
- Betrieb des Cloudmandanten für die wichtigsten Cloudanwendungen (Exchange Online, Teams) innerhalb der Europäischen Union. Rechenzentren ausschließlich in Amsterdam und Dublin. Ein Umzug in die deutschen Cloudzentren soll 2022 abgeschlossen werden.
- **Vorhaltung nur unbedingt notwendiger Daten in der Cloud**. Weitere Attribute werden ausschließlich lokal gehalten.
- Verschlüsselung aller Netzverbindungen von und zur Cloud nach dem Stand der Technik unter anderem durch den Einsatz von TLS und MTLS (in transit). Speicherung in FIPS 140-2 zertifizierten Hardware Security Modulen (HSM). Zusätzlich zur ohnehin obligatorischen Bitlocker-Verschlüsselung **Verschlüsselung gespeicherter Daten mittels Service Key**.

Datenschutzrechtliche Herausforderungen – technische und organisatorische Maßnahmen (Art. 32 DSGVO)

- Einrichtung einer sog. **„Customer Lockbox“,** um sicherzustellen, dass Microsoft nicht in die hiesige Datenhoheit eingreifen kann.
- **Deaktivierung** der Übertragung von **Telemetrie- und Diagnosedaten**. Cloudbasierte Anwendungen bzw. Zusatzdienste wurden zum Zwecke der Minimierung der Datenübertragung ebenfalls weitgehend deaktiviert.
  Schriftliche Zusicherung von Microsoft: Bei der Anmeldung für europäische „Tenants“ bzw. beim Lizenzabgleich findet keine Übermittlung von Echtdaten in Drittländer statt.
- Handlungsempfehlungen für die Anwender zu möglichst datenschutzkonformen und sicherheitstechnisch gebotenen Einstellungen.

Datenschutzrechtliche Herausforderungen – Anforderungen der bayerischen Datenschutzaufsicht

AKI 39 des Bayer. Landesbeauftragten für den Datenschutz betr. Office-Anwendungen aus Drittstaaten bei bayerischen öffentlichen Stellen (grob zusammengefasst):

- Erforderlich ist ein umfassendes **Datenschutz-Sicherheitskonzept** für die betroffenen Anwendungen;
- Die Zulässigkeit der Übermittlung von personenbezogenen Daten in ein Drittland ist an **Art. 44 ff. DSGVO** zu messen;
- Bei fehlendem **Angemessenheitsbeschluss** kommt es entscheidend auf die Einbeziehung der **EU-Standardvertragsklauseln** an;
- **Es reicht** jedoch **nicht allein die Einbeziehung** des Klauselwerks, vielmehr muss der Verantwortliche den **Nachweis erbringen**, dass die zu übermittelnden personenbezogenen Daten aus Rechtsgründen von vornherein nicht Gegenstand der betreffenden Zugriffsrechte US-amerikanischer Behörden werden können;
- Soweit dies nicht vollständig nachgewiesen werden kann, ist zusätzlich eine **Kompensation über Verschlüsselung und/oder Pseudonymisierung** erforderlich.

Datenschutzrechtliche Herausforderungen – Wesentliche Unterschiede zwischen Online-Gerichtsverhandlungen und Homeschooling

- Gerichtsverhandlungen sind grundsätzlich **öffentlich** (§ 169 GVG).
- **Freiwilligkeit** der Teilnahme an Online-Verhandlungen vs. staatlicher Schulpflicht (§ 128a ZPO).
- In Online-Gerichtsverhandlungen werden grundsätzlich **keine besonders sensiblen Daten von Minderjährigen** verarbeitet.

Datenschutzrechtliche Herausforderungen – Ausblick

Ankündigung von Microsoft zur Einführung einer EU-Datengrenze (**„EU-Boundary“**): Verarbeitung personenbezogener Daten europäischer Kunden inkl. sämtlicher Dienste ab Ende 2022 ausschließlich innerhalb der EU. Wesentliche Verbesserungen gemäß dem Stand einer Kundenveranstaltung vom 16.12.2021:

- Ausbau der Datenspeicherung und insbesondere der zugehörigen Dienste in der EU;
- Ausbau der VDI-Infrastruktur, um Wartung und Support ohne den physischen Transfer von Daten vornehmen zu können;
- Weniger Unterauftragsverarbeiter und wenn, bevorzugt aus der EU;
- Diagnosedaten verbleiben ab Dezember 2022 vollständig innerhalb der EU-Boundary;
- Über den MS Defender werden sämtliche von MS gesammelten Informationen als Dokument abrufbar sein (Transparenz).

Datenschutzrechtliche Herausforderungen – Ausblick

- Presse vom 3. Februar 2022 :

  „SAP und Arvato bauen Verwaltungs-Cloud mit Microsoft-Technik“

- Das Angebot soll auf der Cloud-Plattform Azure von Microsoft aufsetzen. Dabei erfolgen aber sowohl die Datenverarbeitung und Datenhaltung als auch der Betrieb sämtlicher Services in Deutschland.
- Um das souveräne Cloud-Angebot für den öffentlichen Sektor in Deutschland zur Verfügung zu stellen, ist ein neues deutsches Unternehmen, die **Delos Cloud**, gegründet worden. Das neue Unternehmen wird alleiniger Eigentümer der Plattform sein.
- Die Lösung umfasst das Software-Paket Microsoft 365. Das neue Angebot wird technisch, operativ und rechtlich souverän sein. Es erfolgt eine vollständige Trennung von den globalen Microsoft-Rechenzentren und der bestehenden Public-Cloud-Infrastruktur in Deutschland.

Datenschutzrechtliche Herausforderungen – Ausblick

Der Stand der Verhandlungen um ein Nachfolgeabkommen für den Privacy Shield:

- U.S.-Regierung und EU-Kommission arbeiten intensiv und konstruktiv an einem Privacy-Shield-Nachfolger. Entscheidend, insbesondere für die Kommission, ist, dass das Folgeabkommen diesmal Bestand vor dem EuGH haben muss.

- Wichtigster Knackpunkt ist der Zugang europäischer Betroffener zu Rechtmitteln in den USA.

- Sämtliche Parteien der neuen Bundesregierung betonen die Dringlichkeit eines neuen rechtssicheren Datenabkommens, verweisen aber grundsätzlich auf die Zuständigkeit von Brüssel.

Dieser Weg wird kein leichter sein…

6.10.2015: EuGH erklärt den **Safe-Harbour** Beschluss der EU-Kommission im **Schrems I-Urteil** für ungültig. Dieser bildete von 2000 – 2015 die rechtliche Grundlage für die Übermittlung personenbezogener Daten zwischen EU und USA.

16.7.2020: EuGH erklärt den nachfolgenden **Privacy Shield** Beschluss der EU-Kommission vom 1.8.2016 im **Shrems II-Urteil** für nichtig. Damit besteht wieder kein Angemessenheits-beschluss iSv Art. 45 DSGVO für Datenverarbeitungen in den USA.

16.12.2020: Microsoft verkündet massiven Ausbau der Rechenzentrumsinfrastruk tur in der EU („Data Boundary“) und stellt neue Vertragsklauseln mit weit reichenden Rechtschutzmöglichkeiten zur Verfügung.

2021 (fortlaufend): StMJ passt Konfigurationen der MS365-Produkte(inkl. Teams) datenschutzkonform an, bezieht die neuen Klauseln in Vertrag mit MS ein und gibt umfangreiche Anwendungshinweise an gerichtliche Praxis

4.6.2021: EU-Kommission erlässt Durchführungsbeschluss mit neuen Standardvertragsklausel n für Datenübermittlung in Drittländer. Microsoft übernimmt diese in der Folge inhaltsgleich in den Vertrag mit StMJ.

16.4.2021: Bayer. Kultusmini sterium gibt Umstieg von MS Teams auf Visavid bekannt.

3.2.2022: SAP und Microsoft kündigen Partnerschaft für den Aufbau einer souveränen Cloud-Plattform für öffentliche Verwaltung und Justiz in Deutschland an. Datenverarbeitung und Datenhaltung als auch der Betrieb sämtlicher Services erfolgen in Deutschland. Zur Umsetzung wird im **Mai 2022** die **Delos Cloud GmbH** von SAP gegründet.

1.12.2021: BayLfD erlässt Aktuelle Kurz-Information (AKI) 39 zu Office-Anwendungen aus Drittstaaten bei bayerischen öffentlichen Stellen. Danach ist unter best. Voraussetzungen datenschutzkonformer Einsatz von MS Office möglich. Wichtigste zusätzliche Anforderung: Erstellung eines Datenschutz-Sicherheitskonzepts (das hier im **August 2022** vollendet wurde).

12.4.2022: EU-Kommissar Didier Reynders vermutet öffentlich, dass das Nachfolgeabkommen des nichtigen Privacy Shield bis Ende 2022 abgeschlossen werden könnte. **Zwischenzeitlich** liegt der Kommission als wichtige Voraussetzung im Entwurf eine **Executive Order des US-Präsidenten** zur Prüfung vor, die Teile des Cloud Acts einer stärkeren Verhältnismäßigkeits-prüfung unterwerfen soll.

25.3.2022: Kommissions-Präsidentin von der Leyen und US-Präsident Biden verkünden politische Grundsatzeinigung beim transatlantischen Datenschutz als Grundlage für einen neuen (dritten) Angemessenheitsbeschluss mit mehr Rechtsschutzgarantien für EU-Bürger.

31.12.2022: Microsoft sagt Abschluss der vollständigen EU-Boundary zu mit der Folge, dass auch sämtliche in der privaten Azure Cloud gehosteten Daten ausschließlich in der EU verarbeitet und gespeichert werden (inkl. Diagnosedaten und von Drittunternehmen erbrachten Diensten).

24.6.2022: Delos gibt bekannt, dass die souveräne Cloud für öffentliche Kunden bis 2025 starten soll. Mit SAP und Microsoft wurde in Abt. B für Herbst 2022 ein entsprechendes Sachstandsmeeting vereinbart, um Ausschreibungen für justizielle Fachanwendungen rechtzeitig vorbereiten zu können.

Herzlichen Dank für Ihre Aufmerksamkeit!

Ihr Ansprechpartner:
Gregor.Eisenhuth@stmj.bayern.de