© Rudolpho / PIXELIO

Datenschutz in der Cloud - eine graue Wolke?

7. Kommunaler IT-Sicherheitskongress der kommunalen Spitzenverbände und des IT-Planungsrates

Dr. Christoph Lahmann

LfD Niedersachsen

03. Mai 2021

Cloud Computing aus datenschutzrechtlicher Sicht
- Risiken -

- **Risiken der Verarbeitung in der Cloud**
  - Sicherheit der Datenverarbeitung
  - Verfügbarkeit der Cloud
  - Transparenz der Datenverarbeitung in der Cloud
  - Integrität und Vertraulichkeit der Datenverarbeitung
  - Mangelnde Trennung verschiedener Nutzer einer Cloud
  - Löschung von Daten (Unsicherheit bei der Umsetzung)
  - Nachvollziehbarkeit durch Protokollierung und Dokumentation
  - Cyberangriffe auf die IT-Infrastruktur
  - Unerlaubter Datentransfer in Drittländer

- **IT Sicherheit in der Cloud**
  - C5 Anforderungskatalog des BSI
    „Cloud Computing Compliance Criteria Catalogue – C5“
    - Orientierungshilfe Cloud-Sicherheit für Anbieter, Nutzer und Prüfer
    - Die Kriterien sind aus etablierten Standards zur Informationssicherheit abgeleitet
  - Darauf aufsetzend sind die datenschutzrechtlichen Anforderungen zu erfüllen.

- **Datenschutzrecht**: Erhebung, Übermittlung oder Verarbeitung personenbezogener Daten („pb Daten“).
- **Personenbezogene Daten**: die verarbeiteten Einzelangaben können einer bestimmten oder bestimmbaren natürlichen Person – dem/r Betroffenen – zugeordnet werden können.
  z.B.:
  - Daten über Kundinnen und Kunden, Antragsteller, Lieferanten, sonstige Geschäftspartner
  - Daten zu Personen, die mit dem Cloud-Nutzer in keinem spezifischen Verhältnis stehen
  - Mitarbeiterdaten des Cloud Nutzers
- Das Datenschutzrecht bleibt im Falle einer bloßen Pseudonymisierung weiterhin anwendbar. Ebenso bei verschlüsselten Daten in der Cloud.
- Das Datenschutzrecht gilt nicht, wenn die Daten anonymisiert sind.

Rollen bei der Verarbeitung personenbezogener Daten
- datenschutzrechtliche Sicht -

- **Verantwortlicher**
  - Entscheidet über *Mittel* und *Zwecke* der Verarbeitung (Art. 4 Nr. 7 DSGVO)
  - Rechtsgrundlage nach Art. 6 DSGVO erforderlich

- **Auftragsverarbeiter**
  - Verarbeitet Daten „im Auftrag des Verantwortlichen“ (Art. 4 Nr. 8 DSGVO)
  - Keine eigene Rechtsgrundlage erforderlich
  - Wichtig: AV Vertrag; Vereinbarung nach Art. 28 DSGVO

- **Gemeinsam Verantwortlicher**
  - Zwei oder mehr Verantwortliche entscheiden gemeinsam über *Mittel* und *Zwecke* der Verarbeitung.
  - jeweils individuelle Rechtsgrundlage nach Art. 6 sowie Vereinbarung nach Art. 26 DSGVO erforderlich.

⟹ „wesentliche Mittel“ vs. „nicht-wesentliche Mittel“

- Bei Verarbeitung unter Nutzung von Cloud-Diensten bleibt die „verantwortliche Stelle“ verantwortlich für die Einhaltung der Vorgaben der DSGVO:
  - Datenschutzkonforme Einbeziehung des Cloud-Anbieters einschließlich dessen eventueller Subunternehmer
  - Vertrag über Auftragsverarbeitung
  - Gewährleistung eines angemessenen Sicherheitsniveaus („TOM“)
  - Erfüllung der Informationspflichten
  - Ermöglichung der Ausübung von Betroffenenrechten
  - Grenzüberschreitender Datenverkehr
    - Innereuropäischer Raum
    - Außereuropäischer Raum

Zulässigkeit von Datenexporten Drittländer

Wann ist ein Datentransfer ins Ausland zulässig?

- **Zweistufige Prüfung der Zulässigkeit**

1. Grundsätzlich: Ist die Verarbeitung von Daten überhaupt zulässig?
   Rechtsgrundlage nach Art. 6 DSGVO

2. Schritt: Ist die Übermittlung zulässig?
   - Besteht ein Angemessenheitsbeschluss der EU besteht (u.a. Argentinien, Kanada, UK)
   - Andernfalls handelt es sich um „unsichere Drittländer“. Dann existieren insbesondere folgende Optionen:
     - Standardvertragsklauseln
     - Einwilligung des Betroffenen
     - Konzernweite Verhaltensregeln (sog. Binding Corporate Rules)
     - Genehmigte Zertifizierungen
     - ***Privacy Shield (!)***

Urteil des EuGH „Schrems II“ zur Übermittlung personenbezogener Daten in Drittländer

- **EuGH** Urteil vom 16. Juli 2020**:**
  Angemessenheitsbeschluss der KOM zum DS-Niveau in den USA auf Grundlage Privacy Shield ist ungültig.
  - Im Anwendungsbereich der **US-Auslandsaufklärungsprogramme** kein gleichwertiges Schutzniveau
  - Betroffene sind ohne wirksame **Rechtsbehelfe** gegen Zugriffsbefugnisse der US-Behörden auf personenbezogene Daten
- Datenexporte auf der Grundlage des Privacy Shields sind **unzulässig** und müssen eingestellt werden.
- **Massive Auswirkungen** auf Nutzung von Cloud Diensten
  - Telemetriedaten-Übermittlung bei Win10 und Office 365
  - Videokonferenzlösungen wie Zoom, WebEx, MS Teams oder Skype
  - Einbindung von Social Media Tools in Webseiten, etwa Google Analytics, Facebook Fanpages, Twitter, Instagram oder YouTube.
  - CRM-Systeme, Personalmodule von ERP-Systemen, Reisemanagement-Systeme
  - Zusammenarbeit mit Fernwartungsdienstleistern

Konsequenzen des Urteils Schrems II für Datenexporte in Drittländer

Orientiert an der „Roadmap“ des Europäischen Datenschutzausschusses könnten Verantwortliche folgenden Ablaufplan durchgehen:

- **Bestandsaufnahme**
- **Überprüfung der „ Übermittlungsinstrumente“**
  insbesondere Angemessenheitsbeschluss der Kommission, Standardvertragsklauseln, BCR, Artikel 49 DS-GVO
- **Beurteilung der Rechtslage im Drittland:**
  Garantien gem. Art. 46 DS-GVO in der Praxis nach dem Recht des Drittlands effektiv?
  Haben die exportierten pb Daten im Drittland ein Schutzniveau, dass dem in EU/EWR garantierten Niveau gleichwertig ist?

! **<u>Auswahl und Anwendung zusätzlicher Maßnahmen:</u>**
  Kommen zusätzliche Maßnahmen zur Sicherstellung des Schutzniveaus in Betracht?

- **Zusätzliche Verfahrensschritte:**
  Änderungen der Übermittlungsinstrumente im VVT; Informationspflichten nach Art. 13 Abs. 1 Buchstabe f DS-GVO anpassen; ggf. Genehmigung erweiterter Standardvertragsklauseln bei der Aufsichtsbehörde einholen.
- **Monitoring:** Die Lage im Drittland muss in angemessenen Abständen auf neue Entwicklungen überwacht werden.

Roadmap EDSA: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Videokonferenzen in der Cloud 1/2
- Verantwortlichkeit -

Verantwortlich:

- Unternehmen/Behörde, das die Video-Konferenz durchführt

Pflichten:

- Beachtung der rechtlichen Anforderungen gewährleisten
- Dokumentation (!) deren Einhaltung

Betriebsmodelle:

- **Selbst betriebener Dienst**

  Die Verantwortlichen können die Umstände der Verarbeitung vollumfänglich selbst bestimmen

- **Betrieb durch einen externen IT-Dienstleister**
  Wer eine Software präferiert, sie aber nicht selbst betreiben kann, kann hierfür einen Dienstleister beauftragen. Es liegt eine Auftragsverarbeitung vor.

- **Cloud-Dienst**

  Der Verantwortliche hat die vom Online-Dienstanbieter vorgelegten Auftragsverarbeitungsverträge, Nutzungsbedingungen und Sicherheitsnachweise sowie dessen Datenschutzerklärung zu prüfen.

Videokonferenzen in der Cloud 2/2
- Technisch-organisatorische Maßnahmen -

- **TOM für Videokonferenz Systeme, u.a.:**
  - Verzicht auf nicht erforderliche Funktionalitäten, sichere Nutzerverwaltung und Konfiguration, Deaktivierung von Kamera und Mikrofon außerhalb von Konferenzen, usw.
  - Transportverschlüsselung (mindestens TLS 1.2, besser 1.3), Ende-zu-Ende-Verschlüsselung,

© T.Klostermeier / PIXELIO

- **Auswirkungen des Schrems II Urteils:**
  - Derzeit offen, ob und welche zusätzlichen Maßnahmen in Betracht kommen.
    - **Nutzdaten:** Ende-zu-Ende-Verschlüsselung
    - Aber: **Metadaten** (Verkehrsdaten) weiterhin unverschlüsselt, weil der Anbieter diese im Klartext zur Authentifizierung und zum Herstellen einer Verbindung benötigt.

➢ Nutzung von Videokonferenzprodukten US-amerikanischer Anbieter sorgfältig zu prüfen. Auch, wenn der Vertragspartner eine europäische Tochtergesellschaft ist.

➢ Umstieg auf europäische Anbieter oder auf eine „on premise“-Lösung in Betracht zeihen

Ergänzende Quellen zu Videokonferenzdiensten:

- Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK):
  - **Orientierungshilfe Videokonferenzsysteme**, Stand 23.10.2020;
  - **Checkliste** als Anlage dazu, Stand 11.11.2020

- FAQ der LfD Niedersachsen vom 21.08.2020 sind insb. folgende Dokumente verfügbar:

- Berliner Beauftragte für Datenschutz und Informationsfreiheit:
  - Checkliste für die Durchführung von Videokonferenzen während der Kontaktbeschränkungen, Version 1.4 vom 3. Juli 2020)
  - Berliner Datenschutzbeauftragte zur Durchführung von Videokonferenzen während der Kontaktbeschränkungen, Version 1.2 vom 3. Juli 2020
  - Empfehlungen für die Prüfung von Auftragsverarbeitungsverträgen von Anbietern von Videokonferenz-Diensten, Version 1.0 vom 3. Juli 2020
  - Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenz-Diensten, Version 2.0 vom 18.02.2021

Office 365 in der Cloud

- 2019 / 2020 wurde von der DSK geprüft, ob die **Datenschutzbestimmungen und Online-Geschäftsbedingungen** die Anforderungen des Art. 28 DSGVO zur Auftragsverarbeitung erfüllen
- Enge **Beteiligung Microsofts** im Rahmen der Prüfung
- Beschluss der Datenschutzkonferenz (DSK) vom 22.09.2020:
  derzeit „kein datenschutzgerechter Einsatz von Microsoft Office 365 möglich“
- **Weitere Gespräche** mit Microsoft laufen, um wichtige Nachbesserungen zu erwirken
  - Bezüglich der Defizite bei Datenschutzbestimmungen und Online-Geschäftsbedingungen
  - In Hinblick auf Anpassungen infolge der Schrems II-Entscheidung des EuGH
  - Frage der Telemetriedaten Übertragung

- Fazit: Einsatz von Microsoft Office 365 in der Cloud ist für öffentliche Stellen weiterhin mit einem erheblichen rechtlichen Risiko verbunden.

AG Cloud Computing und Digitale Souveränität des IT PLR

- AG Cloud wurde im Juni 2019 durch den IT-Planungsrat eingerichtet (Entscheidung 2019/38)

- **Länderoffene Arbeitsgruppe** unter Federführung Nordrhein-Westfalens und des Bundes (BMI) mit Vertretungen aus Kommunen, kommunalen Spitzenverbänden und des Datenschutzes

- **Zielsetzungen**:
  - Erarbeitung von Strategien und Maßnahmen zur Stärkung der Digitalen Souveränität
  - Entwicklung von Anforderungen an Softwarehersteller für den Betrieb von Anwendungen in der Cloud

- **Unterarbeitsgruppen**: Technik & Betrieb, Beschaffung, Kommunikation

- **Wesentliche Maßnahmen:**
  - Erarbeitung einer Deutschen Verwaltungscloud-Strategie
  - Formulierung von Anforderungen an Technologieanbieter
  - Proof-of-Concepts/ Machbarkeitsnachweise
  - Erarbeitung von Beschaffungsleitfäden für Ausschreibungen
  - Definition von rechtlich-regulatorischen Rahmenbedingungen

Fazit

- Cloud Dienstleistungen sind die **strategischen Geschäftsmodelle der Softwarehersteller** und Dienstleister. On-premise Lösungen laufen aus.

- Der **Wert des Datenschutzes** zeigt sich gerade im Umgang mit Cloud Diensten

- Verantwortliche Stelle muss die in DSGVO und LDSG geforderten
  - vertraglichen
  - organisatorischen
  - technischen

  Rahmenbedingungen gewährleisten

- Datenschutz- und Sicherheitsfragen beim Cloud Computing sind zumindest teilweise ungeklärt - Schrems II Entscheidung des EuGH bringt zusätzliche Unsicherheit

- Mehr **Rechtssicherheit** bei Nutzung europäischer Cloud Anbieter und/oder Private Cloud Lösungen

- Es lohnt sich, die Aktivitäten der **AG Cloud Computing** des IT PLR im Auge zu behalten
  - Aufbau einer Deutschen Verwaltungscloud
  - Mitarbeit erwünscht!

Vielen Dank für Ihre Aufmerksamkeit !

Dr. Christoph Lahmann
Die Landesbeauftragte für den Datenschutz Niedersachsen
Stellvertreter der LfD, Leiter Referat 4
Prinzenstraße 5, 30159 Hannover
Telefon: 0511 120 4562
E-Mail: christoph.lahmann@lfd.niedersachsen.de
Internet: https://www.lfd.niedersachsen.de

Bildnachweise: www.pixelio.de