BayLDA

Bayerisches Landesamt für Datenschutzaufsicht

Online-Vorträge zu Datenschutz in der Praxis

an der

Universität des Saarlandes, Institut für Rechtsinformatik

Auftragsverarbeitung in Zeiten von KI

Dilemma oder Herausforderung ?

Michael Will, BayLDA

12. Dezember 2023

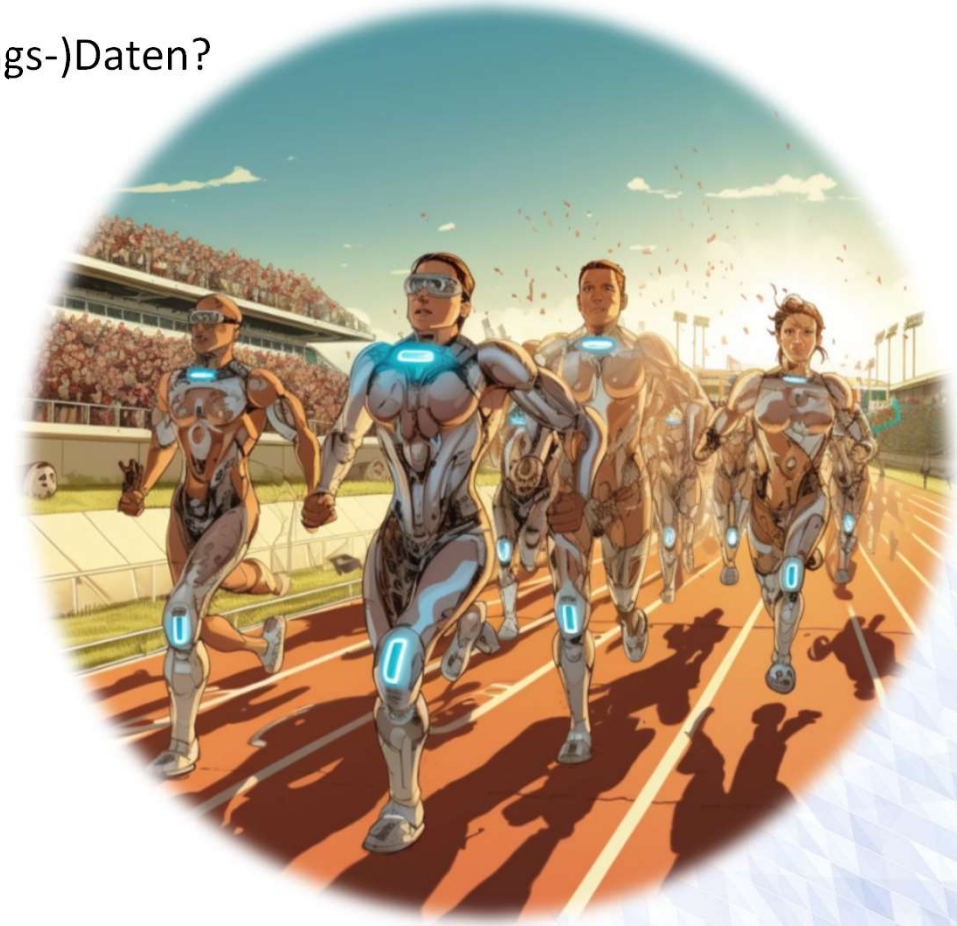
Verantwortlicher und Auftragsverarbeiter – früher?

Zauberer und Zauberlehrling?

„Hat der alte Hexenmeister
Sich doch einmal wegbegeben!
Und nun sollen seine Geister
Auch nach meinem Willen leben.
Seine Wort' und Werke
Merkt ich und den Brauch,
Und mit Geistesstärke
Tu' ich Wunder auch."

Verantwortlicher und Auftragsverarbeiter – heute?

Wettlauf um (Trainings-)Daten?



Hintergrund I

2022 Coordinated Enforcement Action

Use of cloud-based services by the public sector

Adopted on 17 January 2023

Taking into account the possible sensitive nature and large amounts of data processed by public bodies, it is however essential that the fundamental right to the protection of personal data is guaranteed by all public administrations. The EDPB therefore underlines the need for public bodies to act in full compliance with the GDPR when using cloud-based products or services. In this regard, the report also provides a list of points of attention that stakeholders should take into account when concluding agreements with CSPs:

- Carry out a DPIA;
- Ensure that the roles of the involved parties are clearly and unequivocally determined;
- Ensure the CSP acts only on behalf of and according to the documented instructions of the public body and identify any possible processing by the CSP as a controller;
- Ensure that a meaningful way to object to new sub processors is possible;
- Ensure that the personal data are determined in relation to the purposes for which they are processed;
- Promote the DPO's involvement;
- Cooperate with other public bodies in negotiating with the CSPs;
- Carry out a review to assess if processing is performed in accordance with the DPIA;
- Ensure that the procurement procedure already envisages all the necessary requirements to achieve compliance with the GDPR;

Hintergrund II
DSK-Beschluß zu Microsoft 365

„Die DSK stellt unter Bezugnahme auf die Zusammenfassung des Berichts fest, dass der Nachweis von Verantwortlichen, Microsoft 365 datenschutzrechtskonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten „Datenschutznachtrags vom 15. September 2022“ nicht geführt werden kann.“

https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf

Grenzbereiche: Kundendaten

Vertraglich festgelegte Laufzeit

"Kundendaten" bezeichnet alle Daten, einschließlich aller Text-, Audio-, Video- oder Bilddateien und Software, die Microsoft vom Kunden oder im Namen des Kunden durch die Nutzung des Onlinedienstes zur Verfügung gestellt werden.

(Nachtrag zum Datenschutz für Microsoft-Produkte und -Dienste, 1. Januar 2023)

Personenbezogene Daten sind eine Teilmenge der Kundendaten

Für die Zwecke von Cloud-Diensten sind personenbezogene Daten eine Teilmenge der Kundendaten (wie in der Vereinbarung definiert).

(Auftragsverarbeitungsvertrag für Cloud Services, SAP Support und SAP Services, 10/2023)

Daten, die in Cloud-Dienste eingegeben werden

"Kundendaten" sind alle Inhalte, Materialien, Daten und personenbezogenen Daten, die autorisierte Benutzer in das Produktionssystem eines Cloud-Dienstes eingeben oder aus seiner Nutzung und Speicherung im Cloud-Dienst ableiten (z. B. kundenspezifische Berichte).

(SAP-Allgemeine Geschäftsbedingungen für Cloud Services, 2/2023)

Grenzbereiche: Kundendaten

Vertraglich festgelegte Laufzeit

"Kundendaten" bezeichnet alle Daten, einschließlich aller Text-, Audio-, Video- oder Bilddateien und Software, die Microsoft vom Kunden oder im Namen des Kunden durch die Nutzung des Onlinedienstes zur Verfügung gestellt werden.

(Nachtrag zum Datenschutz für Microsoft-Produkte und -Dienste, 1. Januar 2023)

Personenbezogene Daten sind eine Teilmenge der Kundendaten

Für die Zwecke von Cloud-Diensten sind personenbezogene Daten eine Teilmenge der Kundendaten (wie in der Vereinbarung definiert).

(Auftragsverarbeitungsvertrag für Cloud Services, SAP Support und SAP Services, 10/2023)

Daten, die in Cloud-Dienste eingegeben werden

"Kundendaten" sind alle Inhalte, Materialien, Daten und personenbezogenen Daten, die autorisierte Benutzer in das Produktionssystem eines Cloud-Dienstes eingeben oder aus seiner Nutzung und Speicherung im Cloud-Dienst ableiten (z. B. kundenspezifische Berichte).

(SAP-Allgemeine Geschäftsbedingungen für Cloud Services, 2/2023)

Grenzbereiche: Zwecke

Verarbeitung dient der Gewährleistung/Verbesserung

… der IT-Sicherheit

… unseres Services

… unserer Produkte

meint: Big Data-Analysen, maschinelles Lernen, Produktverbesserung **und** -entwicklung

=> Wertschöpfung durch Daten, Grundbedingungen von KI u.v.m.?

Eigene Zwecksetzungen des Processors - Modelle -

Microsoft-DPA 12/2020 (überholt)

Microsoft wird Kundendaten und personenbezogene Daten **nur in Übereinstimmung mit den dokumentierten Anweisungen des Kunden** und wie nachstehend beschrieben und eingeschränkt nutzen und anderweitig verarbeiten, (a) um dem Kunden die Onlinedienste zur Verfügung zu stellen, **und** (b) für die **rechtmäßigen Geschäftsvorgänge** von Microsoft, die mit der Bereitstellung der Onlinedienste an den Kunden verbunden sind

Verarbeitung für legitime Geschäftstätigkeiten von Microsoft

Für die Zwecke dieses DPA umfassen „legitime Geschäftstätigkeiten von Microsoft“ die folgenden **Aktivitäten**, jeweils mit der Bereitstellung der Onlinedienste für den Kunden verbunden:
(1) Abrechnungs- und Kontoverwaltung;
(2) Vergütung (z. B. Berechnung von Mitarbeiterprovisionen und Partner-Incentives);
(3) interne Berichterstattung und Geschäftsmodellierung (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 (vorbehaltlich der im Folgenden beschriebenen Beschränkungen für die Offenlegung verarbeiteter Daten).

Bei der Verarbeitung für legitime Geschäftstätigkeiten von Microsoft wird Microsoft Kundendaten oder personenbezogene Daten nicht für folgende Zwecke verwenden oder anderweitig verarbeiten: (a) Benutzerprofilerstellung, (b) Werbung oder ähnliche kommerzielle Zwecke oder (c) alle anderen Zwecke, mit Ausnahme der in diesem Abschnitt genannten Zwecke.

Eigene Zwecksetzungen des Processors - Modelle -

Microsoft-DPA 1/2023

Microsoft wird Kundendaten, Professional Services-Daten und personenbezogene Daten nur wie nachstehend beschrieben und eingeschränkt nutzen und anderweitig verarbeiten, (a) um dem Kunden die Produkte und Services **in Übereinstimmung mit den dokumentierten Anweisungen** des Kunden zur Verfügung zu stellen

und (b) für die Geschäftstätigkeiten, die durch die Bereitstellung der Produkte und Services an den Kunden veranlasst sind

Verarbeitung für Geschäftstätigkeiten, die durch die Bereitstellung der Produkte und Services an den Kunden veranlasst sind

Für die Zwecke dieser DPA bezeichnet „Geschäftstätigkeit" die vom Kunden in diesem Abschnitt **autorisierten Verarbeitungsvorgänge**.

Der Kunde **autorisiert** Microsoft:

(i) zur Erstellung aggregierter statistischer, nicht personenbezogener Daten aus Daten, die pseudonymisierte Identifikatoren enthalten (wie etwa Nutzungsprotokolle, die eindeutige, pseudonymisierte Identifikatoren enthalten) und

(ii) zur Berechnung von Statistiken bezogen auf Kundendaten oder Professional Services-Daten

in jedem Fall ohne auf den Inhalt von Kundendaten oder Professional Services-Daten zuzugreifen oder diese zu analysieren und beschränkt auf die Erreichung der folgenden Zwecke, jeweils soweit durch die Bereitstellung der Produkte und Services für den Kunden veranlasst.

Diese Zwecke sind:

- Abrechnungs- und Kontoverwaltung;
- Vergütung wie etwa Berechnung von Mitarbeiterprovisionen und Partner-Incentives;
- Interne Berichterstattung und Geschäftsmodellierung wie etwa Prognose, Umsatz, Kapazitätsplanung und Produktstrategie; und
- Finanzberichterstattung.

Bei der Verarbeitung für diese Geschäftstätigkeiten wendet Microsoft die Grundsätze der Datenminimierung an …

Eigene Zwecksetzungen des Processors – Einordnungsversuche

Noch Processor oder schon (Joint-)Controller?

Umfasst ausschließlich Handeln auf Weisung trotzdem auch eigenständige Verarbeitungstätigkeiten, insbesondere im Bereich der IT-Sicherheit?

Da

- „der Auftragsverarbeiter … alle gemäß Art. 32 erforderlichen Maßnahmen ergreift“ (Art. 28 Abs. 3 Buchst. c) DS-GVO)
- „… der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen trifft, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“ (Art. 32 Abs. 1 DS-GVO)

Genügt das Art. 6 Abs. 3 DS-GVO?

Eigene Zwecksetzungen des Processors – Einordnungsversuche

Weisung, Rechtsgrundlage, Zweckänderung

Wem gehören „die“ Daten? :Abschichtungen: Infrastruktur, Telemetrie, „Systemdaten“?

Weisung – „Ersatz“ für Rechtsgrundlage

Schnittstelle Controller – Processor:

Übermittlung oder nur Zweckänderung i.S.v. Art. 6 Abs. 4 DSGVO?

Einzelheiten: DSK-AG M 365, Abschlussbericht, Z. 425 - 771

Eigene Zwecksetzungen des Processors – Einordnungsversuche

Rechtsgrundlagen der Datenzugriffe?

für Controller 1:

ursprüngliche Verarbeitungsbefugnis (z.B. Art. 6 Abs. 1 Buchst. b) DS-GVO)?

Art. 6 Abs. 1 Buchst. f) DS-GVO?
Art. 9 DS-GVO?

für Processor/Controller 2:

soweit pbD (wohl) nur Art. 6 Abs. 1 Buchst. f) DS-GVO?

Sonderfragen

Verarbeitung von besonders geschützten Daten ?

„Infektionstheorie“ des EuGH
i.S. Meta ./. Bundeskartellamt (Rn. 89)

„Wenn ein Datensatz, der sowohl sensible als auch nicht sensible Daten enthält, Gegenstand solcher Vorgänge ist **und insbesondere als Ganzes erhoben wird, ohne dass die Daten zum Zeitpunkt dieser Erhebung voneinander getrennt werden können**, ist die Verarbeitung dieses Datensatzes aber als im Sinne von Art. 9 Abs. 1 DSGVO untersagt anzusehen, sofern sie **mindestens ein sensibles Datum** umfasst und keine der in Art. 9 Abs. 2 DSGVO genannten Ausnahmen greift.“

Sonderfragen

„Cybersicherheit“ bzw. „Netzsicherheit“ als berechtigte Interessen?

EuGH i.S. Meta./. Bundeskartellamt: **„Ja, aber…?“** (Rn. 119 ff.)

„Zweitens stellt das Ziel der **Gewährleistung der Netzsicherheit**, wie aus dem 49. Erwägungsgrund der DSGVO hervorgeht, ein berechtigtes Interesse von Meta Platforms Ireland dar, das geeignet ist, die im Ausgangsverfahren in Rede stehende Verarbeitung zu **rechtfertigen**.

Hinsichtlich der Erforderlichkeit der Verarbeitung zur Verwirklichung dieses berechtigten Interesses wird das vorlegende Gericht jedoch zu prüfen haben, ob und inwieweit sich die Verarbeitung personenbezogener Daten, die aus Quellen außerhalb des sozialen Netzwerks Facebook erhoben wurden, **tatsächlich als erforderlich erweist, um zu gewährleisten, dass die innere Sicherheit dieses Netzwerks nicht beeinträchtigt wird**.

In diesem Zusammenhang wird es, wie in den Rn. 108 und 109 des vorliegenden Urteils ausgeführt, auch zu prüfen haben, ob zum einen das berechtigte Interesse an der Verarbeitung der Daten nicht in zumutbarer Weise **ebenso wirksam mit anderen Mitteln** erreicht werden kann, die weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen, insbesondere die durch die Art. 7 und 8 der Charta garantierten Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingreifen, und zum anderen, ob der in Art. 5 Abs. 1 Buchst. c DSGVO verankerte **Grundsatz der „Datenminimierung“** gewahrt wird.“

KI-Verordnung als Lösung?

- **Grundsätze der DSGVO** in Bezug auf personenbezogene Daten: **gelten weiterhin**!
- Unterschiedliche Pflichten je nach Risikostufe
- KI-Systeme mit hohem Risiko:
  - Registrierung in einer EU-Datenbank
  - Umfassende Prüf- und Transparenzpflichten
- KI-Systeme mit begrenztem Risiko:
  - Mindestanforderungen an Transparenz für fundierte Nutzerentscheidungen
- grds. **keine KI-spezifischen** DV-Regelungen

Eigene Zwecksetzungen des Processors – Ausblick

Folgepflichten des Processors/Controllers 2

- Als Empfänger bei Betroffenenauskunft konkret zu benennen
  (EuGH, Urt. V. 13.01.2023, C- 154/21)
- Adressat sonstiger Betroffenenrechte
- Gewährleistung des Widerspruchsrecht
  gem. Art. 21 Abs. 4 DSGVO
- ggf. Transfertatbestand
  gem. Kap. 5

Eigene Zwecksetzungen des Processors – Ausblick

Gestaltungsaufgaben:

- genaue Eingrenzung der für Processor-Zwecke zur Verfügung stehenden Datenarten
- genaue, aber auch hinreichend umfassende Beschreibung der Processor-Zwecksetzungen
- Transparenz **für Betroffene** durch Controller **und** Processor
- Gewährleistung von Betroffenenrechten
- Datenminimierung!

BayLDA

Bayerisches Landesamt für
Datenschutzaufsicht

Danke für Ihre Aufmerksamkeit !
Auf ein frohes Datenschutzjahr 2024 !