Baker McKenzie.

EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR

18. September 2020

Agenda

1. Einführung
2. Bisherige Abgrenzung
3. Verantwortlicher
4. Gemeinsame Verantwortlichkeit
5. Auftragsverarbeiter
6. Auftragsverarbeitungsvertrag

EDPB Guidelines 07/2020

1 Einführung

- Zur Bedeutung der Unterscheidung Verantwortlicher und Auftragsverarbeiter
- Beide werden nach der DS-GVO nicht identisch behandelt (Art. 5, 6, 9, 12 – 22 gelten bspw. nur für den Verantwortlichen, Art. 28, 29, 32-33, 44 ff. DS-GVO gelten auch für den Auftragsverarbeiter)
- Die Faustformel für die Abgrenzung, dass Verantwortlicher ist, wer über die Zwecke und Mittel der Verarbeitung entscheidet, lässt Fragen offen, bspw. wenn der Anbieter
  - einen Dienst technisch und inhaltlich beherrscht,
  - eine eigene Vertragsbeziehung zu den Betroffenen hat,
  - aufgrund einer vertraglichen Freigabe (Art. 29 DS-GVO) eigene Zwecke verfolgt.
- Es gibt nach wie vor Fragen, für die es keine klare Antwort gibt, wie bspw. ob
  - es zulässig ist, „prophylaktisch“ einen Vertrag gemäß Art. 26 DS-GVO abzuschließen,
  - Art. 44 ff. DS-GVO uneingeschränkt auf den Auftragsverarbeiter anzuwenden sind,
  - jeder Eigenzweck das „Verantwortlichen-Regime“ aktiviert (z.B. eigene Unterrichtungspflichten auslöst und den Abschluss eines parallelen c2c-Standardvertrags erforderlich macht).

EDPB Guidelines 07/2020

2 Bisherige Abgrenzung

- Working Paper 169 der Artikel 29 Datenschutzgruppe
- Die Aufsichtsbehörden veröffentlichten zahlreiche Handreichungen und Abgenzungshilfen
- **Faustformel:**
  - Verantwortlicher ist, wer Zwecke und Mittel der Verarbeitung personenbezogener Daten determiniert;
  - Auftragsverarbeiter ist, wer eine bestimmte Verarbeitung personenbezogener Daten weisungsgebunden durchführt, wobei die (insbesondere im Cloud-Umfeld absolut übliche) Beherrschung der technischen Verarbeitungsmodalitäten durch den Anbieter dem typischerweise nicht entgegensteht.
- **Streitfälle:**
  - Reisebüro;
  - Laborarzt;
  - Genomsequenzierung;
  - Signatur-Dienste;
  - Cloud-Anbieter nutzt (personenbezogene) Daten für
    - Produktverbesserung,
    - Fehlerbehebung,
    - Erfüllung eigner Rechtspflichten.

EDPB Guidelines 07/2020

3 Definition des Verantwortlichen

- Verordnungsautonome Auslegung für die Abgrenzung
- ***„die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle“***
  - Die Verantwortlichkeit verbleibt bei der juristischen Person, selbst wenn innerhalb der Organisation eine natürliche Person als „Verantwortliche“ benannt ist.
- ***„die allein oder gemeinsam mit anderen“***
- ***„über die Zwecke und Mittel der Verarbeitung“***
  - bezieht sich auf den Gegenstand der Einflussnahme des Verantwortlichen
  - In Bezug auf eine bestimmte Datenverarbeitung ist Verantwortlicher, wer bestimmt
    - warum die Verarbeitung erfolgt (d.h. "zu welchem Zweck"; oder "wozu") und
    - wie dieses Ziel erreicht werden soll (d.h. welche Mittel zur Erreichung des Ziels eingesetzt werden sollen).
  - Problemstellung: inwieweit darf der Auftragsverarbeiter Einfluss auf das "Warum" und "Wie" der Verarbeitung nehmen:
    - Der Zweck der Verarbeitung ist immer vom Verantwortlichen zu bestimmen
    - Mit Blick auf die Mittel ist zu unterscheiden zwischen: **Wesentlichen und unwesentlichen Mittel**
    - Die "wesentlichen Mittel" stehen in engem Zusammenhang mit dem Zweck und dem Umfang der Verarbeitung und sind traditionell und von Natur aus der Entscheidung des Verantwortlichen vorbehalten.
    - Die "nicht wesentlichen Mittel" betreffen eher praktische Aspekte der Implementierung, wie die Wahl einer bestimmten Art von Hard- oder Software oder die detaillierten Sicherheitsmaßnahmen, deren Entscheidung dem Auftragsverarbeiter überlassen werden kann.

EDPB Guidelines 07/2020

3 Definition des Verantwortlichen

- *„**von personenbezogenen Daten**“*
  - Verantwortlichkeit ist auch dann anzunehmen, wenn nicht absichtlich personenbezogene Daten verarbeitet werden oder fälschlicherweise davon ausgegangen wird, dass solche Daten nicht verarbeitet werden.
  - Tatsächlicher Zugang zu den Daten ist nicht erforderlich, sofern eine Einflussnahme auf Zweck und Mittel der Verarbeitung vorliegt.
- *„**entscheidet**“*
  - *Dies Beschreibt die Einflussnahme des Verantwortlichen auf Schlüsselelemente der Verarbeitung aufgrund der Ausübung bestehender Entscheidungsbefugnisse.*
  - *Maßgebliche Kriterien:*
    - *Warum findet diese Verarbeitung statt?*
    - *Wer hat entschieden, dass die Verarbeitung für einen bestimmten Zweck erfolgen soll?*
  - Die Einordnung als Verantwortlicher resultiert aus
    - einer gesetzlichen Bestimmung (unmittelbar: das Gesetz identifiziert den Verantwortlichen; indirekt: Auferlegung einer Pflicht zur Datenerhebung und –verarbeitung)
    - der faktischen Möglichkeit der Einflussnahme

      Bestimmte Verarbeitungsaktivitäten können als natürlich mit der Rolle oder den Aktivitäten einer Stelle verbunden angesehen werden, die letztlich Verantwortlichkeiten aus Sicht des Datenschutzes mit sich bringen: bspw. Arbeitgeber, Verleger, Verband
  - Auch bei vorab durch den Auftragsverarbeiter festgelegten Verarbeitungstätigkeiten verbleibt die endgültige Entscheidung in Form einer aktiven Genehmigung beim Verantwortlichen.

EDPB Guidelines 07/2020

4 Definition der gemeinsamen Verantwortlichkeit

Bestehen einer gemeinsamen Verantwortlichkeit

- *Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche.*
- Prüfung: erfolgt die Festlegung von Zweck und Mitteln von mehr als einem Beteiligten
- Die Beurteilung sollte statt auf einer formalen, auf einer faktischen Analyse der tatsächlichen Einflussnahme beruhen
  - Gründe: es könnte an einer formalen Ernennung fehlen oder die formale Ernennung spiegelt nicht die Realität wider

Bewertung der gemeinsamen Mitwirkung

- Mehr als ein Beteiligter muss einen entscheidenden Einfluss auf das „ob“ und „wie“ der Verarbeitung haben
- Erscheinungsformen:
  - eine gemeinsame Entscheidung der Beteiligten (beinhaltet eine gemeinsame Absicht)
  - konvergierende Entscheidungen:
    - die Entscheidungen ergänzen sich und sind jeweils notwendig, damit die Verarbeitung in dieser Form erfolgen kann
    - die Verarbeitung wäre ohne Beteiligung der jeweiligen Partei nicht möglich, d.h. sie sind untrennbar miteinander verbunden (*inextricably linked*)
- Der Zugang zu den Daten ist nicht entscheidend
- Eine gleichberechtigte Verantwortung der Beteiligten ist nicht notwendig, die Beteiligten können in unterschiedlichen Phasen und unterschiedlichem Maße beteiligt sein

EDPB Guidelines 07/2020

4 Definition der gemeinsamen Verantwortlichkeit

Gemeinsame Festlegung der Zwecke

- Die Verarbeitung erfolgt für die gleichen oder gemeinsame Zwecke
- Nach Rechtsprechung des EuGH auch eng miteinander verbundene oder sich ergänzende Zwecke:
  - bspw. ein sich aus der Verarbeitung ergebender gegenseitiger Nutzen
  - ein gegenseitiger Nutzen (z.B. kommerzieller Art) ohne Verfolgung eigener Zwecke durch eine Partei begründet keine gemeinsame Verantwortung (dann Auftragsverarbeitung)

Gemeinsame Festlegung der Mittel

- Es muss nicht jeder Verantwortliche in jeder Phase der Verarbeitung über alle Mittel bestimmen.
- Das Ausmaß der Einflussnahme kann unterschiedlich sein
  - bei der Nutzung einer von einem Beteiligten bereitgestellten IT-Infrastruktur/Software/etc. liegt dennoch eine gemeinsame Festlegung der Mittel vor, wenn der andere Beteiligte entscheidet diese für die Datenverarbeitung zu nutzen

Keine gemeinsame Verantwortlichkeit

- Der bloße Austausch derselben Daten zwischen zwei Stellen ohne gemeinsame Festlegung von Zweck und Mitteln stellt nur eine Datenübertragung zwischen zwei getrennten Verantwortlichen dar.
- Die Nutzung einer gemeinsamen Datenbank oder Infrastruktur ohne Festlegung gemeinsamer Zwecke
- Datenverarbeitungskette: dieselben Daten werden nacheinander von mehreren Verantwortlichen verarbeitet, wobei jeder eigene Zwecke verfolgt und eigene Mittel nutzt

EDPB Guidelines 07/2020

4 Folgen der gemeinsamen Verantwortlichkeit

Festlegung der jeweiligen Verantwortlichkeiten

- Bestimmung von „wer macht was“ durch die Festlegung der Aufgabenverteilung
- Dies soll zu einer klaren Verteilung der Verantwortung für die Einhaltung der Datenschutzbestimmungen auch in komplexen Sachverhalten führen.
- Die gemeinsamen Verantwortlichen sollten neben den in Art. 26 Abs. 1 DS-GVO ausdrücklich benannten die folgenden Pflichten und Maßnahmen regeln:
  - Implementierung allgemeiner Datenschutzprinzipien (Art. 5 DS-GVO)
  - Rechtsgrundlage für die Verarbeitung (Art. 6 DS-GVO)
    - Das EDPB empfiehlt, wo möglich, die Verarbeitung auf dieselbe Rechtsgrundlage zu stützen.
  - Sicherheitsmaßnahmen nach Art. 32 DS-GVO
  - Meldung eines Datenschutzvorfalls an die Behörde und die Betroffenen (Art. 33, 34 DS-GVO)
  - Datenschutz-Folgenabschätzung (Art. 35, 36 DS-GVO)
  - Die Einbindung eines Auftragsverarbeiters
  - Übertragung von personenbezogenen Daten in Drittländer
  - Organisation der Kommunikation mit Behörden und betroffenen Personen
- Bei der Weitergabe von Daten zwischen den Verantwortlichen, obliegt es jedem Verantwortlichen sicherzustellen, dass die Daten nicht in einer mit dem ursprünglichen Zweck der Datenerhabung unvereinbaren Art und Weise weiterverarbeitet werden.

EDPB Guidelines 07/2020

4 Folgen der gemeinsamen Verantwortlichkeit

- Die Verantwortlichkeiten müssen nicht gleich verteilt werden
- Die Verantwortlichen können einen gemeinsamen Kontakt für die Kommunikation mit Betroffenen und Behörden festlegen, woran diese jedoch nicht gebunden sind.
- Das Wesen der Vereinbarung soll der betroffenen Person zugänglich gemacht werden
  - dies sollte zumindest alle Elemente der in den Artikeln 13 und 14 genannten Informationen umfassen, sowie die jeweilige Verteilung der Verantwortlichkeiten hierfür
  - falls ein gemeinsamer Kontakt festgelegt wurde, sollte diese angegeben werden
  - die Form der Zugänglichmachung ist nicht festgelegt

EDPB Guidelines 07/2020

5 Definition des Auftragsverarbeiters

Grundvoraussetzungen:

- **eine Einheit, die getrennt vom Verantwortlichen besteht**
  - es handelt sich um eine externe Einheit
  - der Einsatz von Mitarbeitern und Ressourcen innerhalb einer Stelle begründet keine Auftragsverarbeitung
- **Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen**
  - Handeln "im Auftrag von" bedeutet, dem Interesse eines anderen zu dienen, und verweist auf das Rechtskonzept der "Delegation„
- Die Instruktionen des Verantwortlichen können dem Auftragsverarbeiter einen gewissen Ermessensspielraum belassen.
- Die Verarbeitung darf nicht für eigene Zwecke durchgeführt werden; die Überschreitung der Instruktionen des Verantwortlichen stellt einen Verstoß gegen die DS-GVO dar.
- Nach der DS-GVO werden dem Auftragsverarbeiter unmittelbar Verpflichtungen auferlegt, z.B.:
  - Verpflichtung zur Vertraulichkeit der zur Verarbeitung befugten Personen, Art. 28 Abs. 3 DS-GVO
  - Erstellung eines Verzeichnisses nach Art. 30 Abs. 2 DS-GVO
  - Ergreifen geeigneter technischer und organisatorischer Maßnahmen, Art. 32 DS-GVO
  - Benennung eines Datenschutzbeauftragten unter bestimmten Voraussetzungen, Art. 37 DS-GVO
  - Die Vorschriften über die Übermittlung von Daten in Drittländer (Kapitel V des DS-GVO) gilt auch für Auftragsverarbeiter

EDPB Guidelines 07/2020

5 Verhältnis von Verantwortlichem und Auftragsverarbeiter

Wahl des Auftragsverarbeiters

- *„Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.“*
- Elemente, die bei der Beurteilung der Angemessenheit der Garantien zu berücksichtigen sind:
  - das Fachwissen des Auftragsverarbeiters (z.B. technisches Fachwissen in Bezug auf Sicherheitsmaßnahmen und Datenverletzungen);
  - die Zuverlässigkeit des Auftragsverarbeiters;
  - die Ressourcen des Auftragsverarbeiters.
  - der Ruf des Auftragsverarbeiters auf dem Markt
  - Einhaltung eines genehmigten Verhaltenskodex oder Zertifizierungsmechanismus

Form des Vertrages oder anderen Rechtsinstruments

- muss für den Auftragsverarbeiter verbindliche Verpflichtungen festlegen
- Wenn das Rechtsinstrument nicht alle erforderlichen Mindestinhalte enthält, muss er durch einen Vertrag oder einen anderen Rechtsakt ergänzt werden.
- Das Fehlen eines Vertrages/Rechtsinstruments stellt einen ahndungsfähigen Verstoß gegen die DS-GVO dar.
- Alt-Verträge müssen auf die neue Rechtslage angepasst werden.

EDPB Guidelines 07/2020

5 Verhältnis von Verantwortlichem und Auftragsverarbeiter

Form des Vertrages oder anderen Rechtsinstruments

- Das Bestehen eines Vertrages/Rechtsinstruments ist nicht konstitutiv für das Verantwortlicher-Auftragsverarbeiter-Verhältnis.
- Fällt nur der Auftragsverarbeiter in den räumlichen Geltungsbereich der DS-GVO, so gilt die Verpflichtung aus Art. 28 Abs. 3 DS-GVO nur für diesen unmittelbar.
- Es ist nicht entscheidend, wer den Vertrag entwirft und ob dieser vom Auftragsverarbeiter einseitig gestellt wird (abhängig von Marktstellung und –macht, technischem Fachwissen).
  - Der Verantwortliche muss die Geschäftsbedingungen prüfen und akzeptieren, damit übernimmt er die volle Verantwortung.
  - Änderungen der Geschäftsbedingungen müssen dem Verantwortlichen mitgeteilt und von diesem genehmigt werden, die Veröffentlichung von Änderungen auf der Website genügt nicht.

EDPB Guidelines 07/2020

6 Inhalt des Auftragsverarbeitungsvertrages

Inhalt des Vertrages/Rechtsinstruments nach Art. 28 Abs.3 DS-GVO:

- **Gegenstand der Verarbeitung**
  - der Hauptzweck der Verarbeitung muss ausreichend spezifisch festgelegt werden
- **Dauer der Verarbeitung**
  - der genaue Zeitraum oder die Kriterien für dessen Bestimmung sind anzugeben
- **Art und Zweck der Verarbeitung**
  - Diese Beschreibung sollte je nach der spezifischen Verarbeitungstätigkeit so umfassend wie möglich sein, damit externe Parteien (z.B. Aufsichtsbehörden) den Inhalt und die Risiken der dem Auftragsverarbeiter anvertrauten Verarbeitung verstehen können.
- **Art der personenbezogenen Daten**
  - Dies sollte so detailliert wie möglich angegeben werden, der Verweis auf personenbezogene Daten entsprechend Art. 4 Abs. 1 DS-GVO ist unzureichend.
- **Kategorien der betroffenen Personen**
- **Rechte und Pflichten des Verantwortlichen**
  - Hierunter fällt die Pflicht der Bereitstellung der zu verarbeitenden Daten oder die Erteilung der Weisungen.

EDPB Guidelines 07/2020

6 Inhalt des Auftragsverarbeitungsvertrages

Inhalt des Vertrages/Rechtsinstruments nach Art. 28 Abs.3 DS-GVO:

- **Verarbeitung nur auf dokumentierte Weisung des Verantwortlichen**
  - Eine Verarbeitung ohne Weisung darf nur auf Grundlage eines Rechts der EU oder eines Mitgliedstaates erfolgen.
  - Der Verantwortliche ist hierüber zu informieren, soweit keine wichtigen Gründe des öffentlichen Interesses entgegenstehen.
- **Verpflichtung zur Vertraulichkeit der mit der Verarbeitung beauftragten Personen**
- **Verpflichtung zur Ergreifung aller nach Art. 32 DS-GVO erforderlichen Maßnahmen**
  - Der Vertrag soll nicht bloß die Bestimmungen der DS-GVO widergeben.
  - Der Vertrag muss Informationen über die zu ergreifenden Sicherheitsmaßnahmen, die Verpflichtung zur Einholung der Zustimmung des Verantwortlichen bei Änderungen und eine regelmäßige Überprüfung der Sicherheitsmaßnahmen enthalten oder darauf verweisen.
  - Die Informationen müssen so detailliert sein, dass der Verantwortliche die Angemessenheit der Maßnahmen prüfen kann.
- **Verpflichtung die in Art. 28 Abs. 2 und 4 DS-GVO benannten Bedingungen für die Einschaltung von Unterauftragsverarbeitern einzuhalten**
  - Zwei Formen der Authorisierung:
    - Erteilung einer allgemeinen Genehmigung zu Beginn, dann müssen Änderungen rechtzeitig angezeigt werden, um dem Verantwortlichen eine Widerspruchsmöglichkeit zu geben – Schweigen des Verantwortlichen kann als Zustimmung gewertet werden

EDPB Guidelines 07/2020

Inhalt des Auftragsverarbeitungsvertrages

Inhalt des Vertrages/Rechtsinstruments nach Art. 28 Abs.3 DS-GVO:

- Erteilung spezifischer Genehmigungen für einzelne Unterauftragsverarbeiter – Schweigen des Verantwortlichen ist als Ablehnung zu werten
- Der Unterauftragsverarbeiter muss denselben Verpflichtungen unterstellt werden (durch Vertrag oder Rechtsinstrument)

- **Verpflichtung zur Unterstützung des Verantwortlichen bei der Erfüllung von Betroffenenrechten**
  - Die Prüfung der Zulässigkeit von Betroffenenanfragen sollte beim Verantwortlichen verbleiben
- **Verpflichtung zur Unterstützung der Einhaltung der Art. 32 bis 36 DS-GVO**
  - Umfasst die Unterstützung bei der Implementierung von technischen und organisatorischen Sicherheitsmaßnahmen auf Seiten des Verantwortlichen
  - Unterstützung bei einer Meldung eines Datenschutzvorfalls, sowie bei der Durchführung von Datenschutz-Folgeabschätzungen
  - Diese Beistandspflichten führen nicht zu einer Verlagerung der Verantwortlichkeit
- **Verpflichtung zur Rückgabe oder Löschung der Daten nach Beendigung der Verarbeitung**
  - Falls die Wahl zu Beginn der Verarbeitung getroffen wird, sollte dem Verantwortlichen die Möglichkeit verbleiben, diese Wahl zu ändern
- **Verpflichtung zur Bereitstellung der notwendigen Informationen zum Nachweis der Einhaltung aller Verpflichtungen**

Baker McKenzie.

bakermckenzie.com