Verantwortliche und Auftragsverarbeiter: Zu den Leitlinien des EDSA (Entwurf) zum “Controller” und “Processor”

14. September 2020 von David Vasella

Der Europäische Datenschutzausschuss (EDSA) hat den **Entwurf neuer Leitlinien zu den Begriffen von Controller und Processor** (des Verantwortlichen und des Auftragsverarbeiters) veröffentlicht (Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, 2. September 2020). Der Entwurf befindet sich bis zum 19. Oktober 2020 in der Vernehmlassung.

Die Leitlinien bauen teilweise auf den früheren Leitlinien der Artikel-29-Datenschutzgruppe (WP29) zum gleichen Thema auf, die aber noch auf der Datenschutzrichtlinie beruht haben. Verwiesen sei zudem auf den Leitfaden des EDPS zu den Begriffen des Verantwortlichen, des Auftragsverarbeiters und der gemeinsam Verantwortlichen.

Die Leitlinien umfassen 48 Seiten und gliedern sich etwa wie folgt:

- Definition des Verantwortlichen
- Definition der gemeinsam Verantwortlichen
- Definition des Auftragsverarbeiter
- Definition des “Dritten” bzw. “Empfängers” (“third party”/“recipient”)
- Beziehung zwischen dem Verantwortlichen und seinem Auftragsverarbeiter
- Beziehung zwischen gemeinsam Verantwortlichen

Die Leitlinien enthalten zu den Begriffsbestimmungen am Ende jeweils Flussdiagramme (s. dazu unten).

Die folgende Bemerkungen zu den einzelnen Punkten sind keine reine Zusammenfassung, sondern enthalten Erläuterungen, Interpretationen usw., und folgen nicht dem Aufbau des EDSA.

1. Zum Begriff des Verantwortlichen

Diese Ausführungen entsprechen in weiten Teilen der früheren Stellungnahme der WP29. Ausgangspunkt bei der Zuteilung aller Rollen – alleine oder gemeinsam Verantwortlicher und Auftragsverarbeiter – bleibt die Bestimmung über die Zwecke und Mittel der Verarbeitung;.

1.1“Zwecke und Mittel”

Es ist nicht der Ausgangspunkt der Ausführungen des EDSA, aber der logische Ausgangspunkt: die Bestimmung über der die Zwecke und Mittel der Verarbeitung:

- “**Zweck**” meint das faktische Ergebnis, das mit der Verarbeitung angestrebt wird, also das “wozu” der Verarbeitung.
- “**Mittel**” meint die Modalitäten der Verarbeitung, also das “wie” der Verarbeitung. Der Begriff ist irreführend, den Mittel klingt instrumental; gemeint sind aber nicht nur die Hilfsmittel der Verar-

beitung (eine Applikation etc.), sondern alle Umstände, die datenschutzrechtlich relevant sind, d.h. die sich auf die Risiken der Verarbeitung für die Betroffenen auswirken können.

Denn die Funktion der Rollenzuweisung ist die Zuweisung der datenschutzrechtlichen Rechte und vor allem Pflichten, und nachdem das materielle Datenschutzrecht darauf zielt, angemessen mit Risiken umzugehen, kann die Rollenzuweisung und damit die Zuweisung der Verantwortung für den Umgang mit Risiken nur an den Risikofaktoren anknüpfen.

Dies zeigt sich in der Umschreibung der Mittel der Verarbeitung ("means of processing") durch den EDSA, der **anhand der Risikogeneigtheit zwischen wesentlichen und anderen Mitteln ("essential means" und "non-essential means") unterscheidet**:

> "**Essential means**" are **closely linked to the purpose and the scope of the processing** [also: besonders risikogeneigt] […] . Examples of essential means are the type of personal data which are processed ("**which data** shall be processed?"), the duration of the processing ("**for how long** shall they be processed?"), the categories of recipients ("**who shall have access** to them?") and the categories of data subjects ("**whose personal data** are being processed?"). "**Non- essential means**" concern **more practical aspects** of implementation, such as the choice for a particular type of hard- or software or the detailed security measures which may be left to the processor to decide on.

Diese Unterscheidung ist Ausgangspunkt für die Definition des Verantwortlichen – und später der gemeinsam Verantwortlichen – und die Abgrenzung zum Auftragsverarbeiter:

> Determining the purposes and the means amounts to deciding respectively the "why" and the "how" of the processing: given a particular processing operation, **the controller is the actor who has determined why the processing is taking place (i.e., "to what end"; or "what for") and how this objective shall be reached (i.e. which means shall be employed to attain the objective).** A natural or legal person who exerts such influence over the processing of personal data, thereby participates in the determination of the purposes and means of that processing in accordance with the definition in Article 4(7) GDPR.

1.2 Begriff des Verantwortlichen

1.2.1 Zwecke und "essential means"

Verantwortlicher ist, wer die **Zwecke und Mittel** der Verarbeitung bestimmt (der Rechtsprechung des EuGH folgend mit oder ohne Zugriff auf die Personendaten). Der Verantwortliche muss aber nicht unbedingt *alle* Mittel bestimmen, sondern eben nur **die "essential means"**, denn nur diese prägen das Risiko der Verarbeitung so stark, dass sich der Verantwortliche selbst darum kümmern muss; nur die Bestimmung dieser Mittel ist also auslagerungsfeindlich. Andere Umstände, "non-essential means", können dagegen auch dem Auftragsverarbeiter überlassen werden.

Bedeutsam (und positiv) ist in diesem Zusammenhang die Feststellung des EDSA, dass nur derjenige ein Verantwortlicher sein kann, der **sowohl die Zwecke als auch die "essential means" der Verarbeitung** – und nicht nur eins davon – bestimmt:

> The controller must decide on both purpose and means of the processing as described below. As a result, **the controller cannot settle with only determining the purpose. It must**

> **also make decisions about the means of the processing**. Conversely, the party acting as processor can never determine the purpose of the processing.

Das hat zunächst zur Konsequenz, dass der Verantwortliche seine **Pflichten verletzt**, wenn er den Zweck setzt, sich aber um die **Regelung der essential means foutiert** und z.B. einem Auftragsverarbeiter überlässt. Ein Arbeitgeber, der eine HR-Software einsetzt, die Aufbewahrungsdauer der Daten aber nicht bestimmt, verletzt dadurch das Datenschutzrecht und kann sich nicht dadurch exkulpieren, dass er unbesehen Standardeinstellungen der Software übernimmt.

Es bedeutet weiter, dass ein Auftragsverarbeiter, **der ausserhalb seiner Rolle auch "essential means" aber nicht die Zwecke der Verarbeitung bestimmt, dadurch noch nicht zum Verantwortlichen wird**. Ein solcher Auftragsverarbeiter bleibt Auftragsverarbeiter und verletzt seine Pflichten, aber eben nicht die Pflichten eines Verantwortlichen (vgl. auch Art. 28 Abs. 10 DSGVO). Das bedeutet auch, dass nicht allein deshalb eine gemeinsame Verantwortung vorliegen kann, weil ein Auftragsverarbeiter seine Kompetenzen überschreitet; dazu unten.

1.2.2 Indizien zur Bestimmung

Begrifflich ist die Definition des Verantwortlichen klar, faktisch aber häufig nicht, weshalb auf Indizien und Fallgruppen zurückzugreifen ist. Interessant – wenn auch nicht neu – sind in diesem Zusammenhang die folgenden Hinweise des EDSA:

- **Die Verantwortlichkeit kann ausdrücklich oder – häufiger – mittelbar durch das Gesetz erfolgen**. I.d.R. ist diejenige Stelle verantwortlich, der das Gesetz eine Aufgabe überträgt. Häufig sind z.B. Formulierungen wie in Art. 85a BVG ("Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe […]") oder ausdückliche Aufgabenzuweisungen wie z.B. an das ASTRA in Art. 10 OV-UVEK oder an Arbeitgeber z.B. in Art. 6 ArG:

  > the purpose of the processing is often determined by the law. The controller will normally be the one designated by law for the realization of this purpose, this public task. For example, this would be the case **where an entity which is entrusted with certain public tasks (e.g., social security) which cannot be fulfilled without collecting at least some personal data**, sets up a database or register in order to fulfil those public tasks. In that case, the law, albeit indirectly, sets out who is the controller. […]

- Häufiger ist die **Verantwortlichkeit aufgrund faktischer Bestimmung von Zweck und Mitteln**: Massgebend ist hier, welche Stelle faktisch über Zwecke und Mittel entscheidet. Dabei verweist der EDSA z.B. auf "traditionelle Rollenverständnisse" (I know it when I see it…), lässt aber natürlich zu, dass die Qualifikation im Einzelfall abweicht, und weist auf die Bedeutung vertraglicher Regelungen zwischen den Datenbearbeitern als Indiz hin.
- Beispiele für Verantwortliche kraft Gewohnheit sind Arbeitgeber oder Anwaltskanzleien (die aber auch nach allgemeinen Regeln verantwortlich wären).

  > In practice, certain processing activities can be considered as **naturally attached to the role or activities** of an entity ultimately entailing responsibilities from a data protection point of view. […] existing traditional roles and professional expertise that **normally imply** a certain responsibility will help in identifying the controller, for example an employer in relation to processing personal data about his employees,

> a publisher processing personal data about its subscribers, or an association processing personal data about its members or contributors.

2. Gemeinsam Verantwortliche

2.1 Zum Begriff

Wer sich hier Klarheit erhofft hat, wird enttäuscht. Das Konzept der gemeinsamen Verantwortung, das durch die Kasuistik des EuGH geprägtes Stückwerk ist, wird nicht umfassend und grundsätzlich begründet und ausgeführt. Einige Hinweise sind aber hilfreich bzw. tragen zu Klärungen bei. **Man darf die Aussagen des EDSA m.E. wie folgt zusammenfassen**:

- Mehrere Stellen sind gemeinsam verantwortlich, wenn sie **sowohl die Zwecke als auch die wesentlichen Mittel der Verarbeitung bzw. eines Teils einer Verarbeitung gemeinsam bestimmen**. Es genügt nicht, wenn sich diese gemeinsame Bestimmung nur auf den Zweck oder nur auf die Mittel der Verarbeitung bezieht.
- Eine gemeinsame Bestimmung liegt dann vor, wenn die Verarbeitung in ihrer Form nicht möglich wäre, d.h. relevant anders ausfiele, würde man einen der Beiträge wegdenken.
- Das kann auch aus wirtschaftlichen Gründen der Fall sein, nämlich dann, wenn die Verarbeitung aufgrund von ökonomischen Gegebenheiten durch mehrere Stellen bestimmt wird. Es genügt demgegenüber nicht, dass eine Verarbeitung dem wirtschaftlichen Interesse beider Stellen dient; die **(hypothetische) Kausalität der Beiträge bleibt erforderlich**.

2.2 Gemeinsame Bestimmung von Zweck *und* Mitteln

Unklar war bisher zunächst, ob die gemeinsame Verantwortung die gemeinsame Bestimmung **sowohl von Zweck als auch Mitteln** oder **nur eines dieser Faktoren** voraussetzt. In der genannten früheren Stellungnahme ging die WP29 von letzterem aus. Der Wortlaut von Art. 4 Nr. 7 DSGVO (ebenso wie von Erwägungsgrund 79) spricht aber dafür, dass sich der massgebliche Einfluss auf “Zwecke *und* Mittel” beziehen muss; das allein klärt die Frage aber nicht. Auch liess sich der Facebook-Entscheid des EuGH (der Betreiber einer Fanpage ist gemeinsam verantwortlich, weil er durch die Parametrierung der Verarbeitung von Facebook beeinflusst) anders lesen, obwohl die Frage hier weder ausdrücklich gestellt noch beantwortet wurde; denn hier genügte das Ermöglichen der Verarbeitung durch Facebook, ohne dass der Betreiber der Website diese folgende Verarbeitung inhaltlich mitgestaltet (anders noch als beim Fanpage-Entscheid), ausser vielleicht sehr indirekt durch die Auswahl des Nutzerkreises seiner Website.

Der EDSA stellt nun wie oben erwähnt klar, dass die **gemeinsame Verantwortung voraussetzt, dass jeder der gemeinsam Verantwortlichen sowohl den Zweck als auch die wesentlichen Mittel der Verarbeitung mitbestimmt**:

> Not all processing operations involving several entities give rise to joint controllership. The overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing operation. More specifically, joint participation **needs to include the determination of purposes on the one hand and the determination of means on the other hand**. **If each of these elements are determined by all entities concerned, they should be considered as joint controllers of the processing at issue**.

Das ist eine willkommene und keineswegs selbstverständliche Klarstellung eines wesentlichen Punkts, denn bisher liess sich zumindest nicht ausschliessen, dass ein Auftragsverarbeiter, der zu grossen Einfluss auf wesentliche Mittel der Verarbeitung hat, zum gemeinsam Verantwortlichen wird (bspw. ein Auftragsverarbeiter, der konzernintern die IT nicht nur beschafft, sondern auch konfiguriert und dadurch Einfluss bspw. auf die Speicherdauer nimmt). Das dürfte nun nicht mehr zutreffen – ein solcher Auftragsverarbeiter ist, wie oben angesprochen, weder alleine noch gemeinsam verantwortlich, sondern bleibt ein Auftragsverarbeiter (auch wenn zu grosser Einfluss des Auftragsverarbeiters für beide Beteiligten risikobehaftet ist). Offen ist, ob sich der EuGH dieser Auffassung anschlösse; gesichert ist das kaum.

2.3 Was heisst "gemeinsame" Bestimmung?

Der EDSA führt bei der Gemeinschaftlichkeit bei der Bestimmung von Zweck und Mitteln eine – soweit ersichtlich – neue Terminologie ein:

- die **gemeinsame Entscheidung** *("common decision")*; hier liegt eine einzige Entscheidung über Zweck und Mittel vor, die mehrere Stellen gemeinsam fällen; und
- die **konvergierenden Entscheidungen** *("converging decisions")*; hier entscheiden die beteiligten Stellen jeweils für sich, fällen also mehrere Entscheidungen ohne gemeinsamen Entscheidungsprozess, doch "konvergieren" diese Entscheidungen.

Was heisst "konvergieren"? Der EDSA erläutert dies wie folgt, wobei er das Kriterium des "inextricably linked" bemüht, was schon bei der Google Spain-Entscheidung des EuGH nicht zur Klarheit beitragen konnte (Hervorhebungen diesmal im Original):

> […] Decisions can be considered as converging on purposes and means **if they complement each other and are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing**. As such, an important criterion to identify converging decisions in this context **is whether the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked**.

2.3.1 Gemeinsame Bestimmung des Zwecks

Der EDSA nimmt hier Bezug auf das Fashion ID-Urteil, in dem der EuGH die gemeinsame Bestimmung des Zwecks deshalb bejaht hatte, weil unterschiedliche **Interessen wirtschaftlich miteinander verknüpft** waren. Der EDSA führt weiter aus:

> […] joint controllership may also […] be established when the entities involved **pursue purposes which are closely linked or complementary**.

Was heisst nun "closely linked or complementary"? Wie soeben festgehalten, dürfte das der Fall sein, wenn beide Zwecke die Verarbeitung prägen, diese ohne einen der Zwecke also gar nicht oder in datenschutzrechtlich relevant anderer Form stattfände. Das kann seinen Grund natürlich auch in wirtschaftlichen Gegebenheiten haben, weshalb der EDSA fortfährt:

>

> Such may be the case [...] when there is a **mutual benefit arising from the same processing operation, provided that each of the entities involved participates in the determination of the purposes and means** of the relevant processing operation.

Das ist eine bedenkliche Aussage, weil der EDSA den Eindruck entstehen lässt, ein "mutual benefit" könne bereits eine gemeinsame Verantwortlichkeit bewirken. Er fügt aber an, "provided that each of the entities participates in the determination". Der "mutual benefit" kann demnach gerade nicht ausreichend, den beteiligten Stellen eine gemeinsame Zweckbestimmung zuzuschreiben. Das ist zwar positiv, doch leider bleibt der EDSA bei diesem kritischen Punkt unklar. Er fährt fort:

> In Fashion ID, for example, the CJEU clarified that a website operator participates in the determination of the purposes (and means) of the processing by embedding a social plug-in on a website in order to optimize the publicity of its goods by making them more visible on the social network. The CJEU considered that the processing operations at issue were performed **in the economic interests of both the website operator and the provider of the social plug-in**.

Diese Aussage ist in einer arbeitsteiligen Wirtschaft – bei der die ökonomischen Interessen vielfach "inextricably linked" sind – hochproblematisch. Dem EDSA gelingt es insgesamt nicht, die gemeinsame Zweckbestimmung in denjenigen Fällen zu definieren, in denen die beteiligten Stellen unterschiedliche, aber verbundene Zweckt verfolgen.

Schaut man aber nochmals auf den Entscheid i.S. Fashion ID drängt sich eine Eingrenzung auf: Die gemeinsame Verantwortung war hier auf den Vorgang der Erhebung von Personendaten über das Facebook-Plugin und auf die Übermittlung dieser Daten an Facebook beschränkt; nur dieser Verarbeitungsschritt ist insoweit relevant. Und hierzu hat der EuGH festgehalten,

> 78 Mit der Einbindung eines solchen Social Plugins in ihre Website hat Fashion ID im Übrigen entscheidend das Erheben und die Übermittlung von personenbezogenen Daten der Besucher dieser Seite zugunsten des Anbieters dieses Plugins, im vorliegenden Fall Facebook Ireland, beeinflusst, **die ohne Einbindung dieses Plugins nicht erfolgen würden**.

Das drängt den Schluss auf, dass die **Kausalität des Beitrags entscheidend** ist: Fashion ID hat die Erhebung und Übermittlung von Personendaten durch das Einbinden erst ermöglicht. Das ist der entscheidende Faktor. Die Zwecke einer Verarbeitung sind also dann gemeinsam bestimmt, wenn die Verantwortlichen einen Zweck gemeinsam bestimmen oder wenn sie zwar unterschiedliche Zwecke verfolgen, die **Verarbeitung ohne eine dieser Zweckverfolgungen aber relevant anders ausfiele**.

Das entspricht der oben ziterten Aussage des ESDA,

> *Decisions can be considered as converging on purposes and means if they complement each other **and are necessary for the processing to take place in such manner that they have a tangible impact** on the determination of the purposes and means of the processing*

Im Ergebnis darf man also wohl den Schluss ziehen, dass unterschiedliche Zwecke gemeinsam sind, **wenn sie beide kausal für die betreffende Verarbeitung bzw. den betreffenden Verarbeitungsteil sind**. Dieser Schluss ist auch vereinbar mit dem Facebook-Entscheid des EuGH, denn hier war der

Zweck des Betreibers der Fanpage – Erkenntnisse über seine "Fans" zu gewinnen – durch die entsprechende Parametrisierung mitkausal für die Verarbeitung durch Facebook, und mit dem Zeugen-Jehovas-Urteil, denn hier verfolgten die Mitglieder der Gemeinschaft der Zeugen Jehovas den Verkündungszweck und konnten selbst entscheiden, unter welchen konkreten Umständen sie Personendaten über aufgesuchte Personen erheben, welche Daten sie erheben und wie sie sie verarbeiten, und die Gemeinschaft verfolgte denselben Zweck, ermunterte zur Verkündung und führte die Listen der Personen, die keine Besuche mehr wünschten, was wohl als Mitbestimmung über die Mittel der Verarbeitung verstanden werden kann.

2.3.2 Gemeinsame Bestimmung der Mittel

Auch die Mittel müssen gemeinsam bestimmt werden. Aber wie? Der EDSA sagt dazu sinngemäss folgendes:

- Die gemeinsame Verantwortlichkeit setzt nicht voraus, dass alle beteiligten Stellen alle wesentlichen Mittel gemeinsam bestimmen; die **Beiträge an die Bestimmung der Mittel können sich nicht nur in der Intensität, sondern auch im Gegenstand unterscheiden**;
- es genügt sogar, wenn eine der Stellen die Mittel der Verarbeitung bestimmt und eine andere Stelle entscheidet, sich dieser Mittel zu bedienen (wie eben bei Fashion ID), denn diese Entscheidung ist auch eine über die Mittel. Das heisst, dass eine gemeinsame Verantwortlichkeit nicht schon dadurch ausgeschlossen ist, dass eine der Stellen die Mittel der Verarbeitung alleine bestimmt, denn **der Entscheid über den Einsatz der Mittel für eine konkrete Verarbeitung ist seinerseits eine Bestimmung dieser Mittel**. Das bedeutet auch, dass eine Stelle, die die Mittel der Verarbeitung prägt, aber nicht einer *konkreten* Verarbeitung (z.B. Bereitstellung einer Plattform oder einer Cloudinfrastruktur), dennoch die konkreten Verarbeitung mitprägt.

Dieser Punkt dürfte vor allem auch bei Shared Services im Konzern relevant sein. Denn hier wird oft ein Standardservice für die gesamte Gruppe eingekauft (Workday, SAP-Dienste, Microsoft 365 etc.). Die einzelne Konzerngesellschaft hat hier oft keine Alternative zu dieser Infrastruktur. Da aber kein Konzerndatenschutzrecht existiert, stellt der Einsatz dieser Infrastruktur eine – wenn auch etwas unfreie – Entscheidung dieser Konzerngesellschaft dar, so dass eine gemeinsame Bestimmung der Mittel im Sinne des EDSA vorliegt.

Dadurch kommt der EDSA einer gemeinsam Verantwortlichkeit bei jeder gemeinsam genutzten Infrastruktur aber nahe, weshalb er fortfährt:

> It is important to underline that the use of a common data processing system or infrastructure will not in all cases lead to qualify the parties involved as joint controllers, in particular where the **processing they carry out is separable and could be performed by one party without intervention from the other** or where the **provider is a processor in the absence of any purpose of its own** [...].

Damit unterstreicht der EDSA im Ergebnis, dass der gemeinsamen Zweckbestimmung besonders dann entscheidendes Gewicht zukommt, wenn ein Mittel der Verarbeitung in der gemeinsam genutzten Infrastruktur besteht; in solchen Fällen muss sorgfältig beurteilt werden, ob wirklich eine gemeinsame Bestimmung eines einzigen Zwecks erfolgt bzw. mehrere Zwecke so miteinander verbunden sind, dass die Verarbeitung ohne einen der Zwecke anders ausfiele.

Im Beispiel der Shared Services ist daher nicht unbesehen von einer gemeinsamen Zweckbestimmung auszugehen, gerade weil kein Konzerndatenschutzrecht existiert und folglich jede Konzerngesellschaft als datenschutzrechtlich eigenständige Stelle zu sehen ist. Zumindest dann, wenn die konzernweit ein-

gesetzte Infrastruktur **Zwecken dient, die jede Konzerngesellschaft individuell verfolgt** (HR, IT-Services, Accounting usw.), ist nicht von einer gemeinsamen Verantwortung auszugehen. Dient die Infrastruktur aber Zwecken, die mehreren Konzerngesellschaften gemein sind, und wird sie daher für eine Verarbeitung genutzt, die ohne die Zwecke aller beteiligten Stellen anders ausfiele, liegt eine gemeinsame Verantwortung nahe, z.B. bei einem konzernweiten Mitarbeiterverzeichnis oder einem CRM-System, das gemeinsam genutzt wird.

2.4 Gemeinsame Bestimmung: in Bezug worauf?

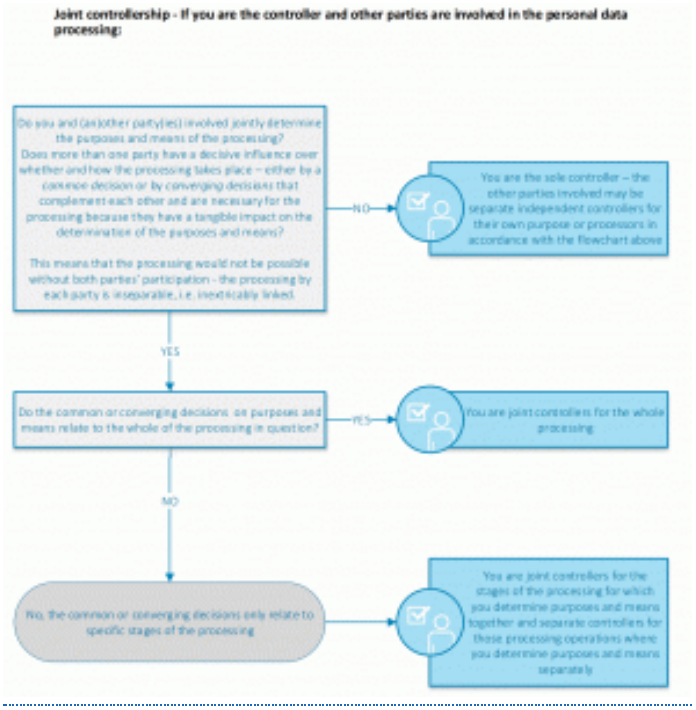
Unklarheit besteht ferner bei der Frage, worauf sich die Bestimmung der Rollen genau bezieht. Der EuGH scheint hier eine klare Linie zu verfolgen: Die Rolle kann sich je nach Verfahrensschritt unterscheiden und ist also relativ granular zu bestimmen. Dabei ist nicht nach einem rechtlichen Begriff von Verarbeitungsphasen zu suchen, sondern zu fragen, **worauf sich die Kontrolle der jeweiligen Datenbearbeiter faktisch erstreckt**. Wenn ein Bearbeiter nur für einen bestimmten Teil einer Verarbeitung Zwecke und wesentliche Mittel (mit-)bestimmt, ist er nur für diesen Teil verantwortlich und nicht für das, was vor oder nach diesem Verarbeitungsteil geschieht.

Der EuGH hat deshalb im Fashion ID-Entscheid festgehalten:

> 72 Aus dieser Definition geht hervor, dass eine Verarbeitung personenbezogener Daten **aus einem oder mehreren Vorgängen** bestehen kann, von denen jeder eine der **verschiedenen Phasen** betrifft, die eine Verarbeitung personenbezogener Daten umfassen kann.
>
> […]
>
> 74 Daraus folgt […], dass eine natürliche oder juristische Person offenbar **nur für Vorgänge der Verarbeitung personenbezogener Daten, über deren Zwecke und Mittel sie – gemeinsam mit anderen – entscheidet, […] gemeinsam mit anderen verantwortlich sein kann**. Dagegen kann […] diese natürliche oder juristische Person für vor- oder nachgelagerte Vorgänge in der Verarbeitungskette, für die sie weder die Zwecke noch die Mittel festlegt, nicht als im Sinne dieser Vorschrift verantwortlich angesehen werden.
>
> […]
>
> 76 […] ist festzustellen, dass die Vorgänge der Verarbeitung personenbezogener Daten, für die Fashion ID gemeinsam mit Facebook Ireland […] entscheiden kann, […] das Erheben der personenbezogenen Daten der Besucher ihrer Website und deren Weitergabe […] sind. Dagegen ist […] auf den ersten Blick ausgeschlossen, dass Fashion ID über die […] Verarbeitung […] entscheidet, die Facebook Ireland nach der Übermittlung dieser Daten an sie vorgenommen hat […] .

Der EDSA nimmt hierauf Bezug, aber relativ knapp und ohne weitere Hinweise. Man kann hier anmerken, dass die erforderliche Unterscheidung nach Verarbeitungsschritten in der Praxis kaum immer befolgt wird, auch nicht von den Behörden (etwa von der DSK, wenn sie Google für Google Analytics pauschal als gemeinsam Verantwortlichen einstuft).

Der EDSA fügt seiner Stellungnahme am Ende ein Flowchart zur gemeinsamen Verantwortlichkeit an:



2.5 Folgen der gemeinsamen Verantwortlichkeit

2.5.1 Vereinbarung: Gegenstand

Nach Art. 26 DSGVO müssen die gemeinsam Verantwortlichen "in einer Vereinbarung in transparenter Form fest[legen], wer von ihnen welche Verpflichtung gemäß [der DSGVO] erfüllt"; d.h. sie müssen sämtliche Compliance-Pflichten so klar aufteilen, dass keine negativen Kompetenzkonflikte bestehen. Die Vereinbarung solle **mindestens folgende Punkte regeln**:

- Sicherstellung der allgemeinen Bearbeitungsgrundsätze;
- Rechtsgrundlage;
- Datensicherheitsmassnahmen;
- Meldung von Verletzungen gegenüber Behörden und Betroffenen;
- Datenschutzfolgeabschätzungen;
- Einsatz von Auftragsverarbeitern;
- Übermittlung in Drittstaaten;
- Kommunikation mit Betroffenen; ggf. einen gemeinsam Kontakt für Betroffene – das ist nicht zwingend, aber empfohlen (z.B. der DPO oder dere EU-Vertreter eines der Verantwortlichen);
- Kommunikation mit Behörden.

Bei der Rollenzuweisung haben die gemeinsam Verantwortlichen eine gewisse Flexibilität. Es sind auch Überschneidungen möglich, z.B. muss sich jeder der Verantwortlichen – sofern er Datenzugriff hat – an die Zweckbindung halten, und **jeder gemeinsam Verantwortliche müsse sein eigenes Verfahrensverzeichnis führen** und ggf. **einen DPO bestellen**. Der EDSA empfiehlt, die Kriterien der Aufgabenzuweisung zu dokumentieren.

Der EDSA sagt fast nichts zur Frage, was gilt, **wenn einer der gemeinsamen Verantwortlichen nicht der DSGVO untersteht**. Hier sind drei Lösungen denkbar:

— Es kann **keine gemeinsame Verantwortung** vorliegen, weil der aussereuropäische Verantwortliche nicht unter die DSGVO und damit auch nicht unter die Definition der gemeinsamen Verantwortung fällt; der europäische Verantwortliche muss daher sämtliche Pflichten nach der DSGVO erfüllen, der aussereuropäische die Pflichten nach dem auf ihn anwendbaren Recht (sofern sein IPR nicht auf die DSGVO verweist);

— der aussereuropäische Verantwortliche **untersteht infolge der gemeinsamen Verantwortung der DSGVO**, auch wenn kein Tatbestand von Art. 3 DSGVO erfüllt ist;

— der aussereuropäische Verantwortliche **untersteht nicht der DSGVO, muss sich aber verpflichten**, die ihm zugewiesenen Pflichten nach dem Standard der DSGVO zu erfüllen, denn sonst würde durch diese Zuweisung die DSGVO unterlaufen. In diesem Fall kann eine Verletzung einer solchen Pflicht durch den aussereuropäischen Verantwortlichen zwar nicht nach der DSGVO behördlich sanktioniert werden, doch wird dies durch die Mitverantwortung des europäischen Verantwortlichen bis zu einem gewissen Grad kompensiert.

Gegen den ersten Fall sprechen praktische Überlegungen. Der EDSA scheint aber en passant davon auszugehen, dass aussereuropäische gemeinsam Verantwortliche im EWR einen EU-Vertreter haben, was ein Indiz dafür wäre, dass nur gemeinsam verantwortlich sein kann, wer der DSGVO untersteht. Es scheint daher nicht unvertretbar, bei Mitverantwortlichen, die Art. 3 DSGVO nicht erfüllen, nie von einer gemeinsamen Verantwortung auszugehen.

Gegen den zweiten Fall spricht, dass keine Rechtsgrundlage besteht für eine Anwendung der DSGVO in solchen Fällen.

Der dritte Weg scheint ebenfalls vertretbar, d.h. eine Vereinbarung, in der ausdrücklich darauf hingewiesen wird, welcher der gemeinsamen Verantwortlichen der DSGVO nicht untersteht und **vereinbart wird, dass dieser im Rahmen der gemeinsamen Verantwortung dennoch die DSGVO einhält**. Sofern sich die betroffenen Personen im EWR aufhalten, werden die Hauptpflichten in solchen Fällen ohnehin häufig beim europäischen Verantwortlichen liegen. Aus den Erwägungen des EDSA lässt sich ferner ableiten – eindeutig ist das allerdings nicht -, dass den betroffenen Personen immer ein Kontaktpunkt innerhalb des EWR bereitgestellt werden muss, so dass die Rolle des Ansprechpartners dem Verantwortlichen mit Sitz in der EU zuzuweisen wäre.

2.5.2 Vereinbarung: Form

Die DSGVO verlangt in Art. 26 in der deutschen Fassung eine “Vereinbarung” zwischen den gemeinsam Verantwortlichen, in der englischen Fassung aber “an arrangement”. Formelle Erfordernisse bestehen daher nicht; der EDSA empfiehlt aber aus Accountability- und Haftungsgründen eine gegenseitig verbindliche Vereinbarung (hält dies aber offenbar nicht für zwingend). Das “arrangement” müsse die Pflichtenverteilung zudem klar und deutlich festhalten. Empfohlen, aber nicht zwingend ist ferner eine Beschreibung der gemeinsamen Verantwortung, des Verarbeitungszwecks, der Kategorien der in gemeinsamer Verantwortung verarbeiteten Daten und der Kategorien betroffener Personen.

2.5.3 Vereinbarung: Mitteilung an die betroffenen Personen

Die Verantwortlichen müssen der betroffenen Person “das wesentliche der Vereinbarung” “zur Verfügung” stellen (Art. 26 Abs. 2 DSGVO). Bisher durfte man davon ausgehen, das “Wesentliche” seien die Punkte nach Art. 26 Abs. 1 DSGVO, d.h. wer für die Wahrnehmung der Betroffenenrechte zuständig ist. Der EDSA ist aber strenger: **“Das Wesentliche” umfasse für jedes Element der Informationspflicht nach Art. 13 und 14 DSGVO, welcher Verantwortliche für die Einhaltung des jeweiligen Elements zuständig ist** (also einschliesslich der Speicherdauer, der TOMs usw.), und zudem die Angabe eines Kontaktpunkts für die Betroffenen (die allerdings frei bleiben, sich an jeden der gemeinsam Verantwortlichen zu wenden, weshalb geregelt werden sollte, wie Betroffenenanfragen intern behandelt werden).

Immerhin: Diese Angaben müssen nicht unbedingt in einer DSE enthalten sein. Es ist **zulässig, sie erst auf Anfrage offenzulegen**. Es lohnt sich daher, in Vereinbarungen gemeinsam Verantwortlicher nicht nur festzulegen, wer die betroffene Person informiert, sondern auch welche Angaben mit welchem Inhalt auf spontan oder auf Anfrage zur Verfügung gestellt werden (ggf. mit einem Musterdokument).

3. Auftragsverarbeitung

3.1 Begriff des Auftragsverarbeiters

Die Definition des Auftragsverarbeiters ist einfach: Ein Auftragsverarbeiter ist eine Stelle, die nicht Teil des Verantwortlichen ist, sondern eine eigenständige Stelle (eine Abteilung eines Unternehmens ist daher nie Auftragsverarbeiterin, ebensowenig wie ein Arbeitnehmer oder Freelancer), und die Personendaten nicht für eigene Zwecke verarbeitet, sondern für jene des Verantwortlichen. Sie darf über nicht-wesentliche Mittel der Verarbeitung bestimmen, und sie kann über wesentliche Mittel mitbestimmen; letzteres darf sie nicht, wird dadurch aber nicht zum Verantwortlichen, weder zum gemeinsam noch zum alleinigen Verantwortlichen.

Der EDSA hält hierzu fest, dass **nicht jeder Dienstleister ein Auftragsverarbeiter ist**. Massgebend ist die Natur ("the nature") der Dienstleistung. Hier schliesst sich der EDSA der Schwerpunkttheorie des BayLDA an:

> In practice, **where the provided service is not specifically targeted at processing personal data** or **where such processing does not constitute a key element of the service**, the service provider may be in a position to independently determine the purposes and means of that processing which is required in order to provide the service.

Keine Auftragsverarbeiter sind daher typischerweise etwa **Taxizentralen** oder **Anwaltskanzleien**. Bei vielen Dienstleistern hängt die Einstufung von der Ausgestaltung ab – ein Dienstleister ist ein Auftragsverarbeiter, wenn der Verantwortliche ausreichende Kontrolle über die Datenverarbeitung hat bzw. wenn der Dienstleister diese nicht hat. Ein **Call Center** bspw. ist ein Auftragsverarbeiter, soweit sein Kunde über die Verarbeitung der Daten durch das Call Center bestimmt und letzteres Daten nur im Rahmen der Weisungen verarbeiten darf.

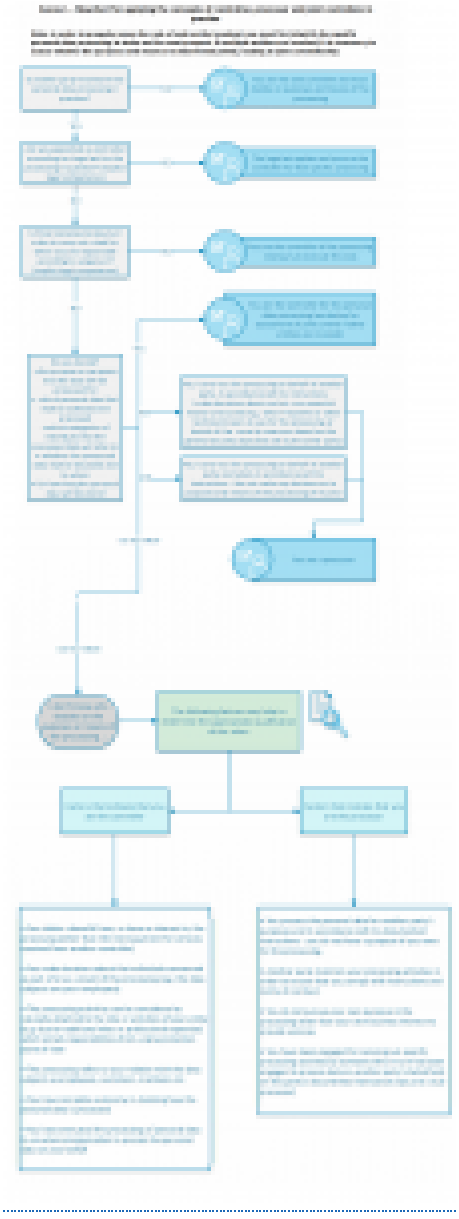
Im Fall von IT-**Supportleistungen** ist ebenfalls zu unterscheiden:

- Verlangt die Art der Support- und Maintenance-Leistungen zwingend den systematischen Zugriff auf Personendaten des Kunden, ist der Dienstleister ein Auftragsverarbeiter.
- Ermöglicht die Supportleistung dagegen nur punktuell den Zugriff auf Personendaten ("purely incidental and therefore very limited in practice"), ist der Dienstleister weder ein Auftragsverarbeiter noch ein Verantwortlicher, sondern ein Dritter, und sein Kunde ist gehalten, den Datenzugriff durch geeignete Sicherheitsmassnahmen möglichst zu beschränken.

Ein Anbieter **umfassender IT-Leistungen** (im Bsp. des EDSA eines Produkts wie z.B. M365, das Kommunikation, Videokonferenzen, Dokumentenmanagement, Kalenderfunktionen und Textverarbeitung umfasst, ist ebenfalls ein Auftragsverarbeiter – der Kunde muss hier aber die essential means bestimmen, d.h. dafür Sorge tragen, dass die Anforderungen bspw. an die Datenlöschung umgesetzt werden, und zwar seine Anforderungen und nicht einfach Standardeinstellungen.

Ein **Reinigungsinstitut** ist ebenfalls weder Auftragsverarbeiter noch Verantwortlicher, sondern Dritter, weil die Datenverarbeitung – so eine solche überhaupt erfolgt – nicht bestimmungsgemäss erfolgt, sondern wiederum nur "incidentially". Die Vereinbarung mit dem Reinigungsinstitut muss die Verarbeitung von Personendaten daher wiederum untersagen, und der Verantwortliche muss den Zugriff auf Personendaten durch angemessene Massnahmen minimieren.

Auch hierzu findet sich in der Stellungnahme des EDSA ein Flowchart:



3.2 Rechtsfolgen der Auftragsverarbeitung

Der EDSA bestätigt die unbestrittene Auffassung, dass die Auftragsverarbeitung privilegiert ist, d.h. dass Rechtsgrundlage für die Verarbeitung durch den Verantwortlichen auch Rechtsgrundlage ist für die Übermittlung an den Auftragsverarbeiter und für dessen Verarbeitung.

Wichtiger sind die weiteren Hinweise des EDSA, der insgesamt eine strenge Haltung einnimmt (die für KMU umsetzbar sein dürfte, in Teilen aber nicht für grössere Provider):

3.2.1 Auswahl des Auftragsverarbeiters; "hinreichende Garantien"

Der EDSA betont, dass der Verantwortliche verpflichtet ist, nur Auftragsverarbeiter einzusetzen, die hinreichend Garantien für geeignete technische und organisatorische (Sicherheits-)Massnahmen ("TOMs")

bieten (vgl. Art. 28 Abs. 1 DSGVO). Der Auftragsverarbeiter muss diese **TOMs dabei so benennen, dass der Verantwortliche eine eigene Entscheidung über ihre Angemessenheit treffen** und diese Entscheidung – gemäss dem Accountability-Grundsatz – dokumentieren kann.

Der Verantwortliche kann sich deshalb nicht darauf beschränken, vertraglich "angemessene Sicherheitsmassnahmen" zu verlangen. Er muss vielmehr eine den Umständen angemessene, eigene und dokumentierte **Risikoeinschätzung** treffen. Dabei hat er neben der Sensitivität der Daten insbesondere folgende Faktoren zu berücksichtigen:

- das Fachwissen des Auftragsverarbeiters;
- seine Zuverlässigkeit;
- seine Ressourcen;
- u.U. auch seine Reputation;
- die Einhaltung genehmigter Verhaltensregeln.

Diese Sicherheit muss der Auftragsverarbeiter dauerhaft bieten. Der EDSA sieht den Verantwortlichen daher in der Pflicht, sie **"in regelmässigen Abständen" zu überprüfen**, ggf. durch Audits.

3.2.2 Vereinbarung mit dem Auftragsverarbeiter

3.2.2.1 Form

Der EDSA bestätigt zunächst, dass die Vereinbarung zwischen Verantwortlichem und Auftragsverarbeiter i.S.v. Art. 28 Abs. 3 DSGVO ("Auftragsdatenverarbeitungsvereinbarung"; "ADV") **in jeder Textform** geschlossen werden kann, also auch elektronisch ohne den Einsatz qualifizierter Signaturen, nicht aber mündlich. Der EDSA empfiehlt aber Unterschriftlichkeit.

3.2.2.2 Inhalt

Der Inhalt der Vereinbarung wird in Teilen in Art. 28 Abs. 3 DSGVO vorgegeben. Der EDSA nimmt hier aber eine strenge Haltung ein, die **ADV deutlich umfangreicher** und die entsprechenden Verhandlungen schwieriger machen könnte.

Folgende Punkte müssen ADV gemäss dem EDSA enthalten (nicht abschliessend; vorbehalten bleiben die weiteren Inhalte nach Art. 28 Abs. 3 DSGVO):

- Die **Pflichten des Verantwortlichen** (was sich aus Art. 28 Abs. 3 DSGVO nicht ergibt), z.B. die Pflicht,
  - Weisungen zu geben und zu dokumentieren (was anscheinend nicht dem Auftragsverarbeiter überlassen werden darf; klar ist das aber nicht);
  - die Rechtmässigkeit der Verarbeitung sicherzustellen;
  - die Verarbeitung des Auftragsverarbeiters zu überwachen (wobei der EDSA nicht begründet, weshalb diese Pflichten auch vertraglich gegenüber dem Auftragsverarbeiter zu übernehmen sind, und in der Praxis ist das auch selten der Fall).
- generell die **Pflichten des Auftragsverarbeiters**, wobei es nicht genüge, nur den Wortlaut von Art. 28 DSGVO zu wiederholen;

— die **TOMs** – das ist nach dem EDSA **zwingender Bestandteil des Vertrags**, der die TOMs nennen oder jedenfalls auf sie verweisen muss, und die TOMs müssen so detailliert sein, dass der Verantwortliche ihre Angemessenheit beurteilen (und seiner Accountability-Pflicht nachkommen) kann;

— zudem müsse eine Pflicht vereinbart werden, bei **Änderungen der TOMs die Zustimmung des Verantwortlichen** einzuholen (was allerdings nicht gelten kann, wenn das Sicherheitsniveau dadurch nicht gesenkt wird); und eine Pflicht, die TOMs **regelmässig zu prüfen**;

— eine **Beschreibung der Verarbeitung**, die dem Auftragsverarbeiter ein Verständnis der Risiken erlaubt und so detailliert ist, dass der Gegenstand der Verarbeitung klar ist;

— die Dauer der Verarbeitung oder die Kriterien für ihre Bestimmung;

— die **Art und der Zweck** der Verarbeitung, so dass Dritte – z.B. Aufsichtsbehörden – den Gegenstand und die Risiken der Verarbeitung einschätzen können;

— die Art der **verarbeiteten Daten**, wobei "Personendaten" nicht reicht; bei besonderen Kategorien von Personendaten sollten diese spezifiziert werden ("Gesundheitsdaten" usw.);

— die **Kategorien der Betroffenen**, ebenfalls ausreichend detailliert;

— das Verbot der **Unterbeauftragung** ohne Genehmigung des Verantwortlichen, wobei diese Genehmigung wie von der DSGVO vorgesehen in allgemeiner Form mit einem Vetorecht kombiniert vereinbart werden kann. In diesem Zusammenhang genüge es nicht, wenn der Auftragsverarbeiter lediglich eine Liste der Unterauftragsverarbeiter nachführt, ohne den Verantwortlichen darauf hinzuweisen; der Auftragsverarbeiter muss **Wechsel vielmehr aktiv mitteilen** ("actively indicate or flag");

— auch muss der Auftragsverarbeiter genehmigten **Unterauftragsverarbeitern in der Sache die Pflichten aus dem ADV überbinden**. Dazu gehöre auch das Auditrecht "des Verantwortlichen" oder eines von diesem beauftragten Prüfers, was danach klingt, dass der Verantwortliche selbst – und nicht der Auftragsverarbeiter – dieses Recht haben muss, durch die ganze Kette von Auftragsverarbeitern hindurch (eindeutig ist der EDSA hier aber ebenfalls nicht);

— die Pflicht des Auftragsverarbeiters, dem Verantwortlichen **bei der Beantwortung von Betroffenenbegehren zu unterstützen**, wobei es genügen kann, wenn der Auftragsverarbeiter Anfragen weiterleitet (eine Erstreckung der Antwortfrist komme nicht in Frage, nur weil Informationen des Auftragsverarbeiters beschafft werden müssen). Jedenfalls solle der Verantwortliche selbst entscheiden, wie auf Betroffenenbegehren zu reagieren ist;

— die Pflicht, den Verantwortlichen **im Zusammenhang mit Sicherheitsmassnahmen zu unterstützen**. Hier genüge es nicht, diese Unterstützungspflichten lediglich zu wiederholen; vielmehr müsse der ADV spezifizieren, auf welche Weise zu unterstützen ist (zum Beispiel durch vereinbarte Abläufe und Vorlagen in einem Annex). Allerdings könne Art und Umfang der Unterstützung stark schwanken. Sicherheitsverletzungen seien aber jeweils unverzüglich mitzuteilen; empfohlen sei die Vereinbarung einer maximalen Mitteilungsfrist und eines Ansprechpartners;

— die Pflicht, **Daten nach dem Ende der Auftragsverarbeitung zu löschen oder zurückzugeben**. Der ADV kann das Verfahren festlegen (wobei der Verantwortliche seine Meinung in diesem Fall später ändern darf) oder eine entsprechende Anweisung des Verantwortlichen vorbehalten, wobei hier der Prozess der entsprechenden Anweisung abgebildet werden solle. Der Auftragsverarbeiter sollte die Löschung bestätigen;

— die Pflicht, beim **Nachweis der Compliance zu unterstützen**. Der ADV solle festlegen, welche Informationen dazu wie häufig übermittelt werden sollen, z.B. Angaben über die Funktion der

Systeme den Auftragsverarbeiters, Sicherheitsmassnahmen, Standort und Aufbewahrung von Daten, Zugriff auf und Übermittlungen von Daten, Unterauftragsverarbeiter usw.;

— den Umgang mit **widerrechtlichen Weisungen**, z.B. ein Abstimmungsverfahren und ein Kündigungsrecht des Auftragsverarbeiters, sollte der Verantwortliche an einer widerrechtlichen Weisung festhalten.

3.2.3 Weisungsbindung

Der Auftragsverarbeiter ist definitionsgemäss an die Weisungsgewalt des Verantwortlichen gebunden. Überschreitet er seine Kompetenzen, kann er zum Verantwortlichen werden (sofern er Zwecke und essential means (mit-)bestimmt).

Die Weisungen können sich laut EDSA z.B. auf den Umgang mit Personendaten und Sicherheitsmassnahmen beziehen. Eine abschliessende Liste findet sich hier nicht; klar ist aber, dass sich das Weisungsrecht nur auf die Verarbeitung von Personendaten bezieht, weshalb der Auftragsverarbeiter kaum zu befürchten braucht, mit dem Weisungsrecht werde der Leistungsvertrag ausgehebelt (auch wenn dies in der Praxis zu Verhandlungen führt).

Weisungen sind ferner **zu dokumentieren** (wie angesprochen wohl durch den Verantwortlichen). Der EDSA empfiehlt deshalb, in die Vereinbarung einen Prozess zur Erteilung der Weisungen aufzunehmen, z.B. durch eine Musterweisung; zwingend ist das aber nicht, es reicht, Weisungen in Textform zu übermitteln. Sie sollten laut EDSA aber zusammen mit der Verarbeitung aufbewahrt werden. Das deutet darauf hin, dass es keine "Weisung" in diesem Sinne darstellt, wenn der Verantwortliche selbst mit den Auftragsdaten interagiert, z.B. gehostete Daten löscht, obwohl diese Löschung Infrastruktur des Auftragsverarbeiters verwendet. Entsprechend müssen solche Weisungen auch nicht eigens dokumentiert werden (soweit sich eine Nachverfolgbarkeit nicht aus dem Gebot der Datensicherheit ergibt).

3.2.4 Vertraulichkeit

Der Auftragsverarbeiter muss sicherstellen – und der ADV muss dies vorschreiben -, dass die Personen unter seiner unmittelbaren Verantwortung (z.B. Arbeitnehmer) einer Vertraulichkeitspflicht unterliegen. Hier genügt aber eine gesetzliche Pflicht, z.B. aus dem Arbeits- oder Auftragsrecht; der Auftragsverarbeiter ist daher nicht verpflichtet, NDAs unterschreiben zu lassen.

3.2.5 Unterauftragsverhältnisse

Wie bereits erwähnt müsse der Auftragsverarbeiter den Verantwortlichen auch bei einer allgemeinen Genehmigung **jeweils aktiv mitteilen, welche Unterauftragsverarbeiter** er einzusetzen beabsichtigt. Dabei müsse der Auftragsverarbeiter mindestens den Standort, das Aufgabengebiet und die getroffenen Sicherheitsmassnahmen mitteilen ("proof of what safeguards have been implemented"). Diese Information sei notwendig, damit der Verantwortliche seiner Accountability-Pflicht entsprechen kann. In diesem System solle der Verantwortliche zudem angeben, nach welchen Kriterien der Auftragsverarbeiter seine Unterauftragsverarbeiter auszuwählen hat. Das dürfte in der Praxis noch zu reden geben.

4. Weitere Begriffsbestimmungen

Art. 4 Nr. 10 DSGVO definiert den "Dritten" in Abgrenzung zum den anderen Rollen und erwähnt dabei auch Stellen, die **"unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters**" tätig werden. Darauf nimmt Art. 29 DSGVO Bezug; diese Bestimmung hält fest, dass "dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte" Personen Daten nur weisungsgemäss ver-

arbeiten dürfen. Dabei handelt es sich jeweils um den gleichen Personenkreis, nämlich Arbeitnehmer und arbeitnehmerähnliche Personen:

> It is, however, generally understood asreferring to persons **that belong to the legal entity of the controller or processor** (an **employee** or a role **highly comparable to that of employees**, e.g. interim staff provided via a temporary employment agency) but only insofar as they are authorized to process personal data.

Ein "**Dritter**" ist sodann jede Stelle, die weder betroffene Person noch Verantwortlicher noch Auftragsverarbeiter ist und weder als Mitarbeiter angestellt noch in vergleichbarer Position für einen Verantwortlichen oder Auftragsverarbeiter tätig ist (Art. 4 Nr. 10 DSGVO).

Ein "**Empfänger**" schliesslich ist jede Stelle ausserhalb des Verantwortlichen, der dieser Personendaten zugänglich macht, z.B. ein anderer Verantwortlicher oder ein Auftragsverarbeiter (ausser EU-Behörden im Rahmen einer Untersuchung; Erwägungsgrund 31: "Behörden, gegenüber denen personenbezogene Daten aufgrund einer rechtlichen Verpflichtung für die Ausübung ihres offiziellen Auftrags offengelegt werden [...] sollten nicht als Empfänger gelten").