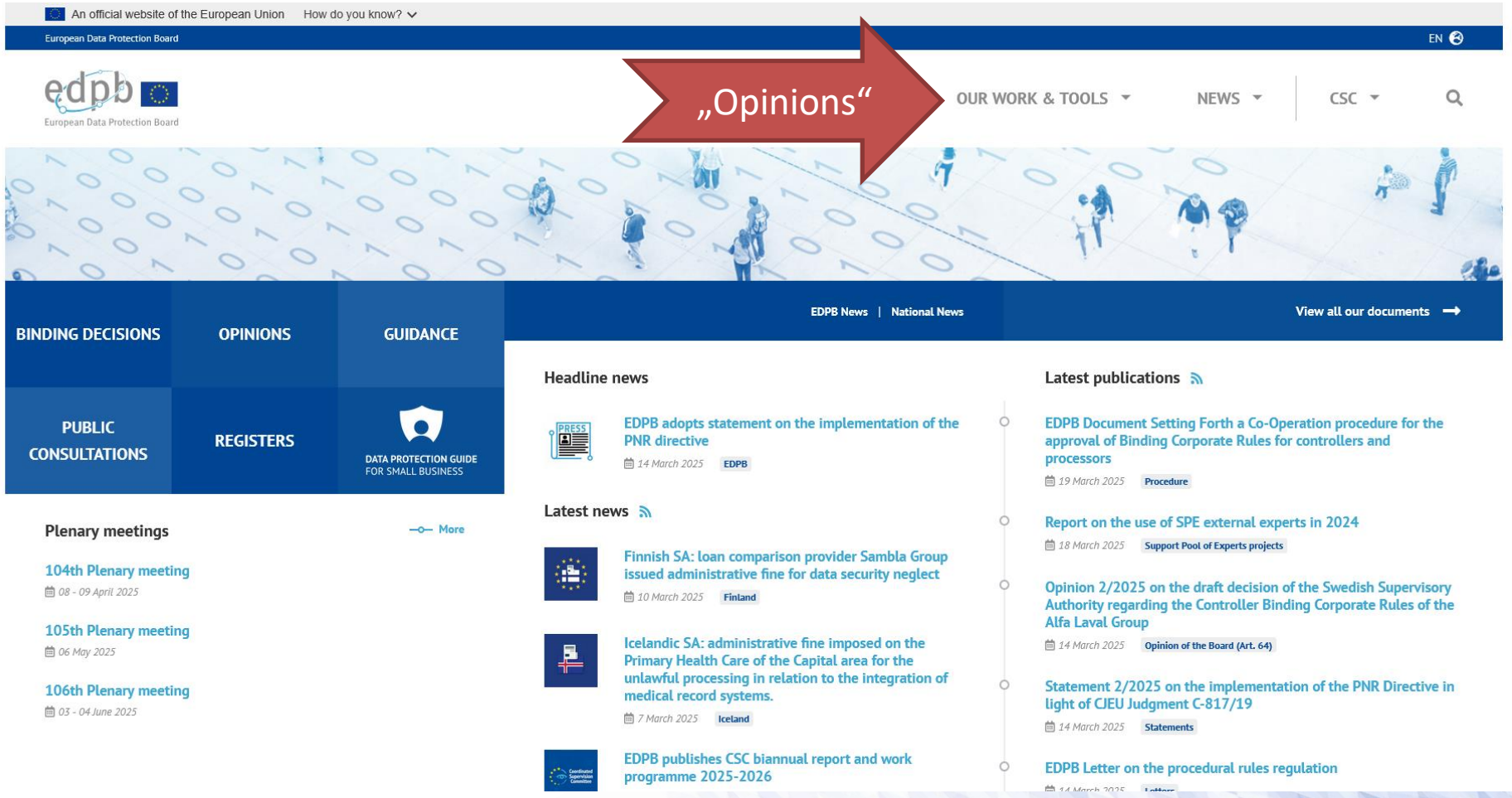
Datenschutz bei der Einbindung von Dienstleistern / Stellungnahme 22/2024 des EDSA vom 07.10.24 zu den Pflichten bei Auftragsverarbeitung

Alexander Filip, Geschäftsleiter
und Bereichsleiter beim
Bayer. Landesamt für
Datenschutzaufsicht

IHK Regensburg, 24.03.2025
(online)

EDSA was? -> Europäischer Datenschutzausschuss

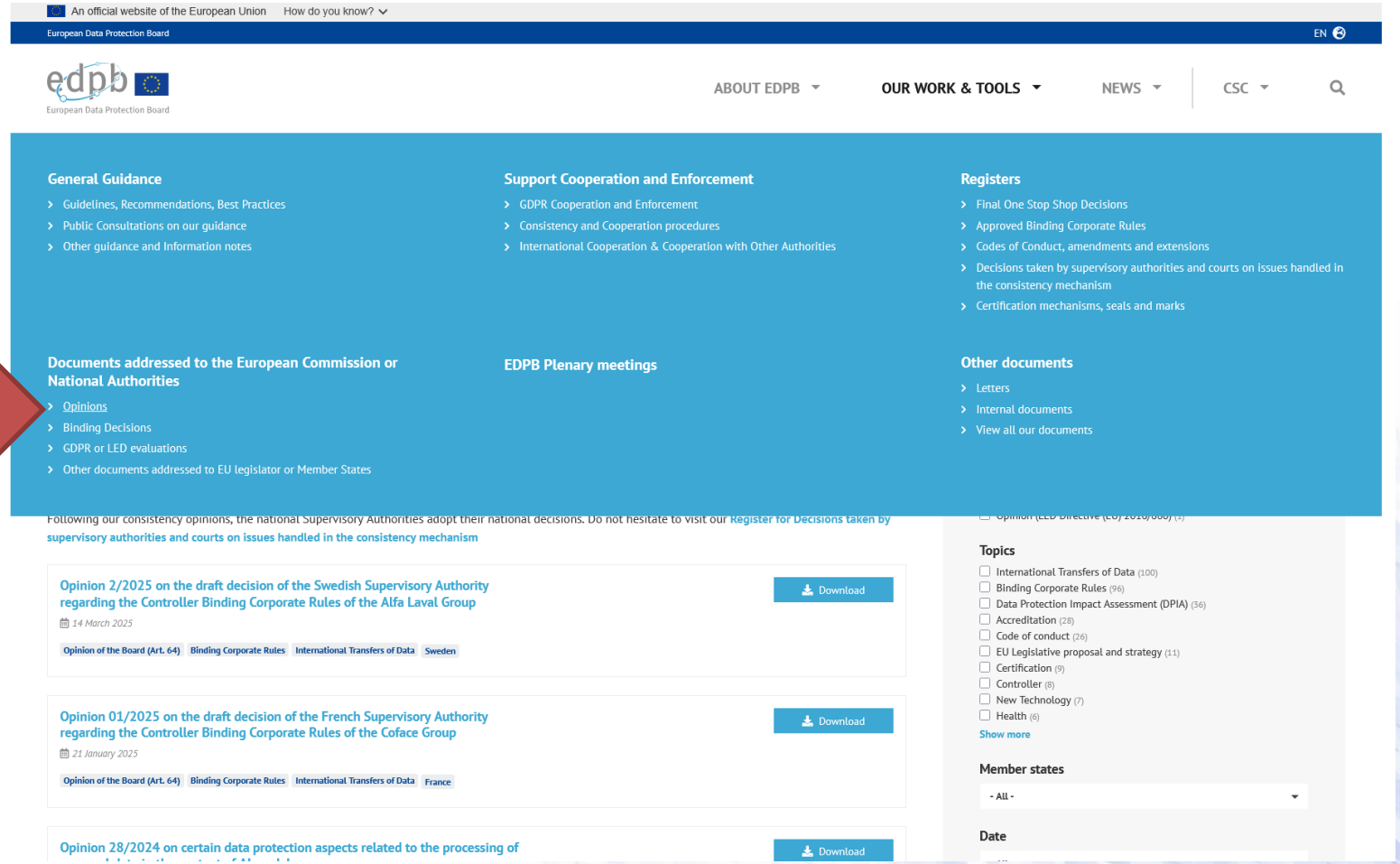
- https://www.edpb.europa.eu/edpb_en



EDSA was? -> Europäischer Datenschutzausschuss

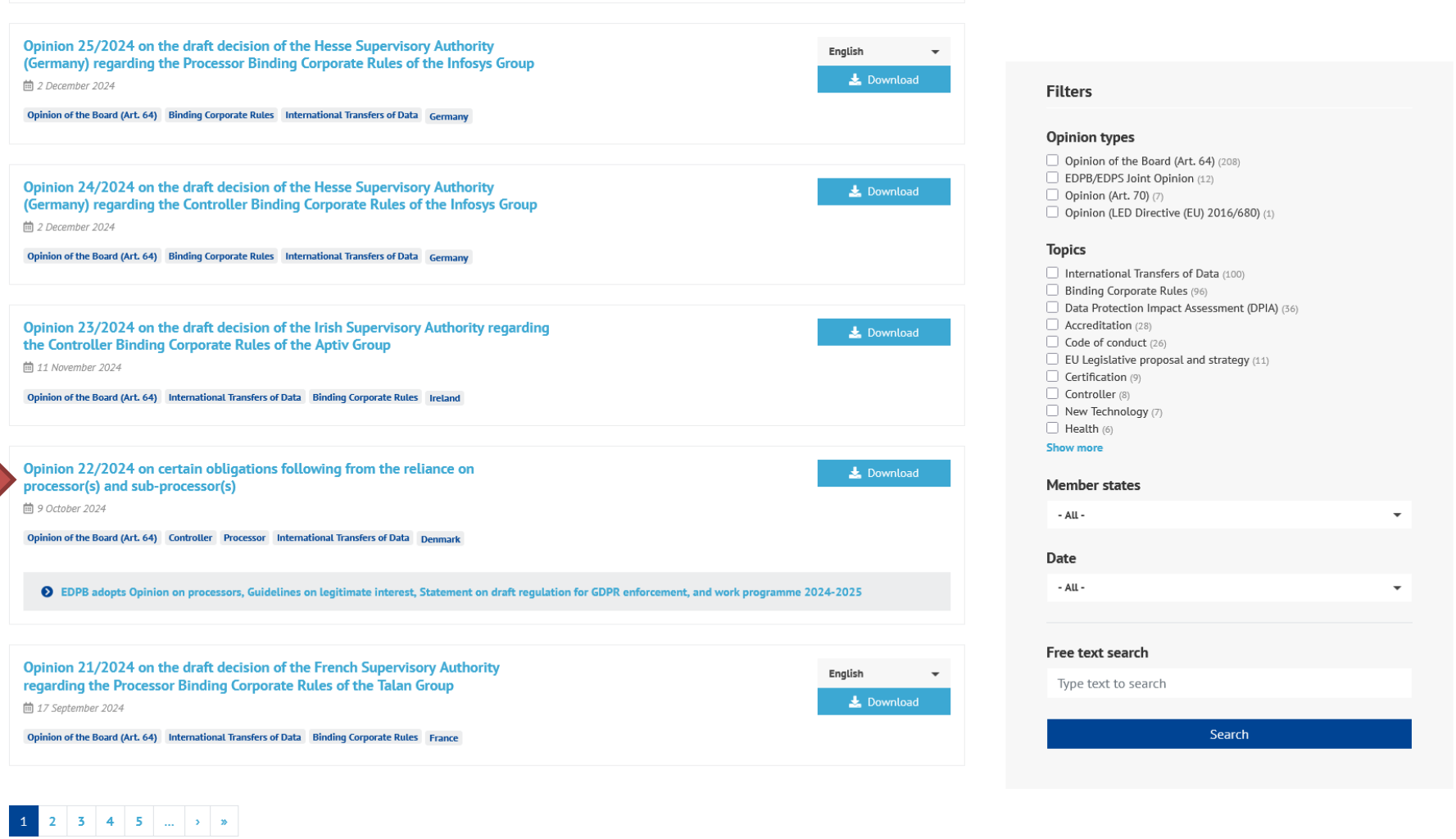
- https://www.edpb.europa.eu/edpb_en

„Opinions“



EDSA was? -> Europäischer Datenschutzausschuss

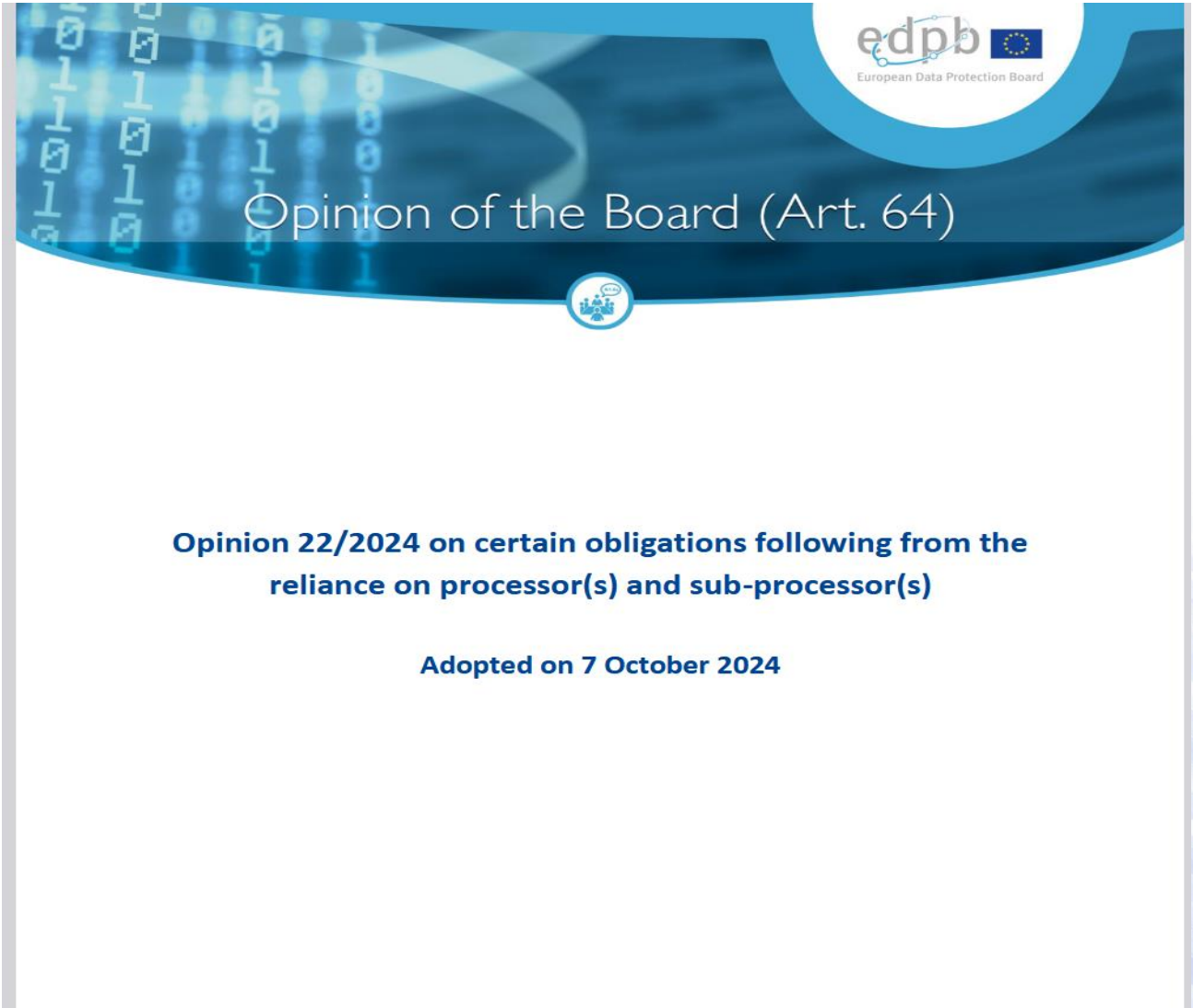
- https://www.edpb.europa.eu/edpb_en



Die ist es!

EDSA was? -> Europäischer Datenschutzausschuss

- https://www.edpb.europa.eu/edpb_en



Gestellte Fragen

Hintergrund: Klärungsersuchen der dänischen Aufsichtsbehörde nach Art. 64(2) DSGVO

Gestellte Fragen:

Q 1.1.a - Muss der Verantwortliche bei Einsatz von Auftragsverarbeitern, um die Einhaltung von Art. 28(1) und (2) DSGVO nachzuweisen, alle Auftragsverarbeiter und Unterauftragsverarbeiter sowie ggf. deren Unter-Auftragsverarbeiter etc. identifizieren/kennen, oder lediglich die erste Gruppe von Unter-Auftragsverarbeiter (die der „erste“ Auftragsverarbeiter“ einsetzt)?

Gestellte Fragen

Q. 1.1.b - In welchem Umfang und Detailgrad muss der Verantwortliche folgendes prüfen und dokumentieren:

i. ob die Auftragsverarbeiter / Unterauftragsverarbeiter „hinreichende Garantien“ mit Blick auf technische und organisatorische Maßnahmen i.S.v. Art. 28(1) bieten?

ii. den Inhalt der (AV-)Verträge zwischen dem „ersten“ AV‘er und weiteren AV‘ern dahingehend, ob den weiteren AV‘ern darin gemäß Art. 28(4) dieselben Pflichten auferlegt wurden, die im „ersten“ AVV gemäß Art. 28(3) festgelegt sind?

iii. ob die AV‘er, UnterAV‘er etc. die Anforderungen des Verantwortlichen nach Art. 28(1) erfüllen?

Gestellte Fragen

Q1.2 **-** Bei **Transfers** in ein Drittland durch einen AV‘er an einen Unter-AV‘er bzw. durch einen Unter-AV‘er an einen weiteren Unter-AV‘er: inwieweit muss der Verantwortliche aufgrund seiner Pflichten nach Art. 28(1) und Art. 44 (selbst) prüfen und nachweisen können bzw. dokumentieren, dass das DSGVO-Schutzniveau auch beim Transfer oder Weiter-Transfer an/von (Unter-)AV‘er weiterhin gewährleistet ist?

Q1.3 – Variiert der Umfang der Pflichten des Verantwortlichen aus Art. 28(1) und (2) in Verbindung mit Art. 5(2) und 24 (wie sie Q1.1 und Q1.2 festgestellt wurden) vom Risiko der jeweiligen Verarbeitung?

Falls ja, welchen Umfang haben diese Pflichten bei Verarbeitungen mit niedrigem sowie solchen mit hohem Risiko?

Gestellte Fragen

Q2 – Muss in einem AVV wörtlich oder zumindest durch einen gleichwertigen Wortlaut die in Art. 28(3)(a) vorgesehene Ausnahme

> *(„sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist“)*

enthalten sein?

Q2a – **Wenn** die Antwort zu Q2 „**nein**“ ist: Ist ein AVV, dessen Wortlaut die o.g. in Art. 28(3)(a) vorgesehene Ausnahme in einer Weise erweitert, dass damit (jedenfalls nach dem Vertragswortlaut) auch das **Recht eines Drittlands** abgedeckt sein soll

> *(z.B. „Sofern er nicht durch eine Rechtsvorschrift hierzu verpflichtet ist“),*

per se ein Verstoß gegen die DSGVO?

Q2b – **Wenn** die Antwort zu Q2 „**nein**“ ist: Kann man sagen, dass ein dergestalt erweiterter AVV-Wortlaut eine „dokumentierte Weisung des Verantwortlichen“ im Sinne von Art. 28(3)(a) darstellt?

Was steht im Gesetz?

Artikel 28 DSGVO. Auftragsverarbeiter

(1) 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.

Was steht im Gesetz?

Artikel 44 DSGVO. Allgemeine Grundsätze der Datenübermittlung

Jedwede **Übermittlung** personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung **an ein Drittland** oder eine internationale Organisation verarbeitet werden sollen, ist **nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten** und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; **dies gilt auch für die etwaige Weiterübermittlung** personenbezogener Daten aus dem betreffenden Drittland oder der betreffenden internationalen Organisation **an ein anderes Drittland** oder eine andere internationale Organisation. Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

Q1.1.a

Q 1.1 – Muss der Verantwortliche bei Einsatz von Auftragsverarbeitern, um die Einhaltung von Art. 28(1) und (2) nachzuweisen

a. alle Auftragsverarbeiter und Unterauftragsverarbeiter sowie ggf. deren Unter-Auftragsverarbeiter etc. identifizieren/kennen, oder lediglich die erste Gruppe von Unter-Auftragsverarbeiter (d.h. nur diejenigen Unter-AV'er, die der „erste" Auftragsverarbeiter" einsetzt)?

EDSA: Ja, Verantwortlicher muss die Identität (Name, Adresse, Kontaktperson) aller AV'er, UnterAV'er etc. jederzeit kennen.

- und zwar abhängig vom Grad des Risikos der Verarbeitung
- schon deshalb, weil Unter-AV'er gemäß Art. 28(2) immer nur mit vorheriger Genehmigung des Verantwortlichen eingeschaltet werden dürfen
- zudem auch wegen der Informationspflichten, Art. 13(1)(e) bzw. Art. 14(1)(e) sowie der Auskunftspflicht nach Art. 15(1)(c) – Nennung aller konkreten Datenempfänger erforderlich, außer wenn unmöglich (EuGH, C-154/21, Rn. 51)

Q1.1.a

- Wegen Art. 28(1) und (2) muss der Verantwortliche die Information zur Identität aller AV‘er, Unter-AV‘er etc. **jederzeit zur Verfügung haben** („readily available at all times“)
- AV‘er sollte dem Verantwortlichen proaktiv alle Informationen zur Identität der UnterAV‘er etc. zur Verfügung stellen
- zu empfehlen, hierzu Details im AVV ausdrücklich zu regeln (z.B. wie und in welcher Form der Auftragsverarbeiter dem Verantwortlichen die Informationen liefern soll)

Q1.1.b.i und b.iii

Q1.1.b - In welchem Detailgrad muss der Verantwortliche (selbst) folgendes prüfen und dokumentieren:

i. dass die Auftragsverarbeiter / Unterauftragsverarbeiter „hinreichende Garantien“ mit Blick auf technische und organisatorische Maßnahmen i.S.v. Art. 28(1) bieten?

iii. ob die AV‘er, UnterAV‘er etc. die Anforderungen des Verantwortlichen nach Art. 28(1) erfüllen?

Antwort EDSA:

- Ausgangspunkt ist die Rechenschaftspflicht, Art. 5(2) und Art. 24.
- Die Einschaltung von AV‘er darf nicht zu einer Senkung des Schutzniveaus führen
- Der Verantwortliche hat wegen Art. 24(1) und Art. 28(1) die Verantwortung, dass die Auftragskette nur aus AV‘ern/Unter-AV‘ern besteht, die hinreichende Garantien liefern, dass Verarbeitung im Einklang mit der DSGVO

Q1.1.b.i und b.iii

- Hinsichtlich des **ersten AV'ers** muss der Verantwortliche die Eignung der Garantien „**on a case by case basis**" prüfen, in Abhängigkeit von der Art etc. der Verarbeitung und vom **Risiko.**
- „Oft wird es für den Verantwortlichen notwendig sein", Dokumentation des AV'ers zu prüfen (z.B. VVT, Information Security Policy, Audit-Reports etc.)
- Es gibt nicht „den einen, einzigen Weg", sondern **verschiedene Möglichkeiten**:
  - "Neither Article 28(1) GDPR itself nor previous EDPB documents provide an exhaustive list of the documents or actions that the processor should show or demonstrate"
  - dem Auftragsverarbeiter Fragen stellen
  - Anforderung von Dokumentation/Unterlagen
  - Zertifizierungen, Audits von vertrauenswürdigen Dritten
  - eigene Vor-Ort-Prüfungen (EDSA-Opinion 22/2024, Randnummer 41)

Entscheidend erscheint mir: EDSA gibt hier gewisse Flexibilität ("on a case by case basis") – je höher das Risiko für die Rechte/Freiheiten, desto enger muss die Prüfung sein.

Q1.1.b.i und b.iii

- EDSA: eine **Pflicht**, die Garantien zu prüfen, hat der Controller immer, aber der Umfang der Überprüfung richtet sich nach den Risiken der Verarbeitung für die betroffenen Personen („the **extent** of such verification will in practice vary depending on … the risk …“)
- Der Verantwortliche wird, **je nach Risiko**,
  - die Inhalte der AV-Verträge und Unter-AV-Verträge entweder selbst prüfen (müssen)
  - „und/oder“ dem „ersten“ AV‘er **erweiterte** Prüfungs- und Dokumentationspflichten auferlegen (müssen)
- Der Verantwortliche trägt die **Beweislast** dafür, dass insbesondere die Datensicherheit auch bei den AV‘ern und Unter-AV‘ern gewährleistet ist (dazu gibt es mehrere EuGH-Urteile, C-340/21, C-687/21)
  - EDSA: Dokumentation ist wichtig!
  - AV‘er und Unter‘AV‘er müssen den Verantwortlichen bzw. „ihren“ Auftraggeber über alle Elemente der Verarbeitung informieren, die relevant sind für die Beurteilung, ob hinreichende TOM existieren (Unterstützungspflicht aus dem AVV, Art. 28(3)(e), (f), (h))
    - empfehlenswert, die Modalitäten und Häufigkeit dieser Info-Bereitstellung im AVV zu regeln

Q1.1.b.i und b.iii

- Verantwortlicher kann sich auf Informationen des AV‘er verlassen, **aber nur, wenn die gelieferte Information tatsächlich die Einhaltung der DSGVO belegt (EDSA, Rn. 51)**
  - Das heißt ja im Ergebnis, dass der Verantwortliche die bereitgestellten Informationen auch prüfen muss.
- Die Pflicht des AV‘ers, den Unter-AV‘ern dieselben Pflichten wie im „ersten“ AVV aufzuerlegen (Art. 28(4)), mindert nicht die eigene Verantwortung des Verantwortlichen aus Art. 24(1) und Art. 28(1), DSGVO-Konformität sicherzustellen und nachzuweisen. (Rn. 57).
- Die Letztverantwortung dafür, ob ein bestimmter Unter-AV‘er eingesetzt werden soll oder nicht, verbleibt beim Verantwortlichen (Rn. 58).
- *”(…) the controller may choose to rely on the information received from its processor and if necessary build on it. For example, in case where the information received by the controller seems **incomplete, inaccurate or raises questions**, or where appropriate based on the circumstances of the case including the **risk** associated with the processing, the controller **should ask for additional information and/or verify the information and complete/correct it** if necessary.”*

Q1.1.b.ii

b. In welchem Detailgrad muss der Verantwortliche folgendes prüfen und dokumentieren:

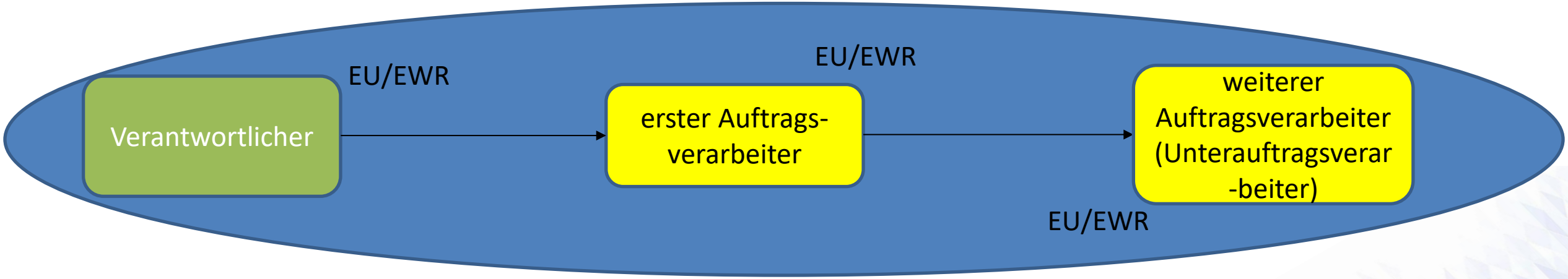
ii. *den **Inhalt** der AV-Verträge zwischen dem „ersten“ AV‘er und weiteren AV‘ern dahingehend, ob den weiteren AV‘ern darin gemäß Art. 28(4) dieselben Pflichten auferlegt wurden, die im „ersten“ AVV gem. Art. 28(3) festgelegt sind?*

EDSA*:*

- Die (AVV-)Transfer-Standardvertragsklauseln („SCC“) der KOM geben dem Verantwortlichen jedenfalls ein Recht, vom Auftragsverarbeiter jegliche Unter-AVV im Wortlaut zu verlangen (folgt auch aus Art. 28(3)(h) DSGVO (Kontroll-/Audit-Recht des Verantwortlichen)
- Weder DSGVO selbst noch die SCC enthalten aber eine ausdrückliche Pflicht des Verantwortlichen, die Unter-AVV zu verlangen.
- **keine** Pflicht des Verantwortlichen, **systematisch** (also immer) **alle** Unter-AVV zu verlangen, um zu prüfen, ob gem. Art. 28(4) alle Pflichten auf jeden Unter-AV‘er auferlegt wurden (!)
- Verantwortlicher sollte je nach Einzelfall prüfen, ob er seiner Nachweispflicht (nur) dann nachkommen kann, wenn er einen Unter-AVV selbst herausverlangt (und geprüft hat)
  - Fazit: **Frage des Einzelfalls**. Insbesondere bei Datenschutzverletzungen oder Hinweisen auf Probleme beim Unter-AVV‘er wird Vorlage des AVV aber in aller Regel erforderlich sein.

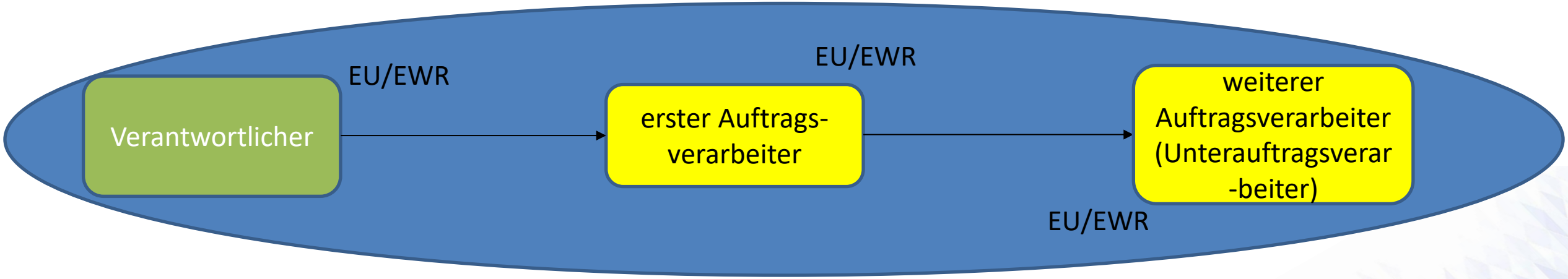
Auftragskette *ohne* Datentransfer

Q1.1.a und 1.1.b - noch einmal bildlich:



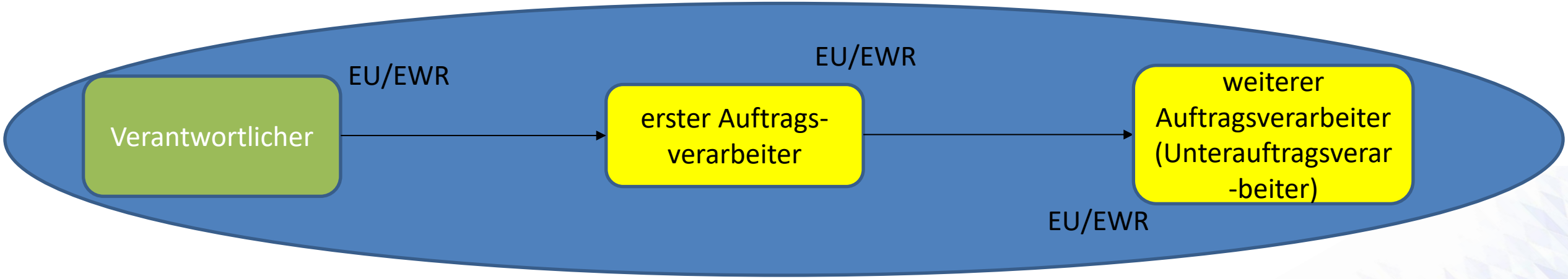
- Übergeordnete Frage: Inwieweit muss der Verantwortliche den/die Unterauftragsverarbeiter kontrollieren?
- EDSA-Opinion 22/2024, Frage 1.1.a: Muss der Verantwortliche alle Auftragsverarbeiter und Unterauftragsverarbeiter in der Kette „identifizieren“ (kennen), um die Einhaltung von Art. 28(1) und (2) nachweisen zu können?
- EDSA, Rn. 30/31: ja, schon deshalb, weil er betroffenen Personen die Information gemäß Art. 13(1)(e)/14(1)(e) über die Identität aller Datenempfänger sowie Auskunft gem. Art. 15(1)(e) über die Identität aller konkreten Datenempfänger erteilen muss

Auftragskette *ohne* Datentransfer



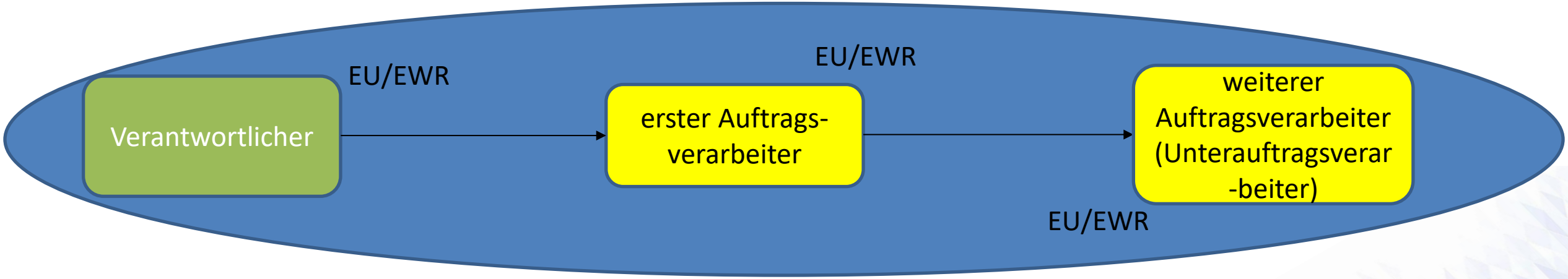
- **EDSA-Frage 1.1.b.i.: Inwieweit muss der Verantwortliche die Garantien jedes AV‘ers/Unter-AV‘ers prüfen?**
  - EDSA-Opinion 22/2024, Rn. 38 ff. argumentiert mit den Pflichten des Verantwortlichen aus Art. 24(1) und Art. 28(1) DSGVO
  - Rn. 40: *„With respect to the choice of the initial processor, the controller should verify the sufficiency of the guarantees provided **on a case-by-case basis** taking into account the nature, scope, context and purposes of processing as well as the risks for the rights and freedoms of natural persons, on the basis of the type of processing entrusted to the processor.”*
  - Rn. 41: *“For example, the controller may choose to draw a questionnaire as a means to gather information from its processor to verify the relevant guarantees, ask for the relevant documentation, rely on publicly-available information and/or certifications or audit reports from trustworthy third parties and/or perform on-site audits.”*

Auftragskette *ohne* Datentransfer



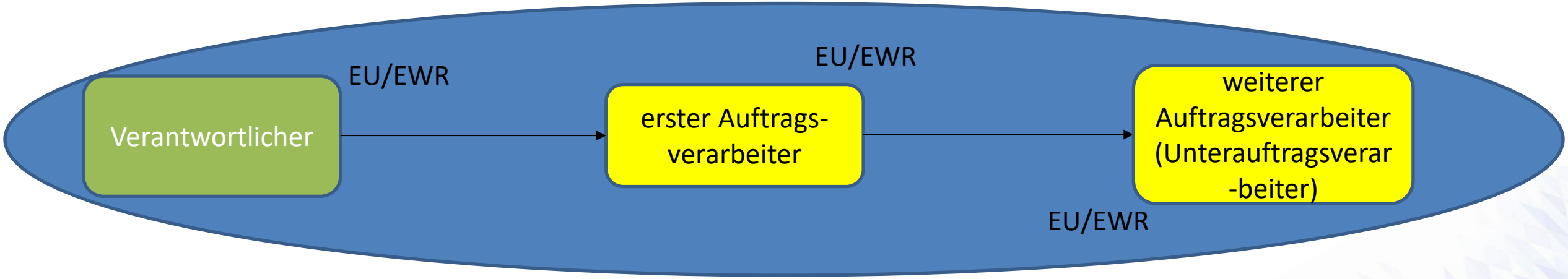
- **EDSA-Frage 1.1.b.i.: Inwieweit muss der Verantwortliche die Garantien jedes AV‘ers/Unter-AV‘ers prüfen?**
  - Rn. 48 ff.: *„the **extent** of such verification will in practice **vary** depending on the nature of these organisational and technical measures determined by the controller based on, among other criteria, **the risk associated with the processing**. For example, where the processing activities present a lower risk to the rights and freedoms of data subjects, the corresponding ‘appropriate measures’ will be less strict. Therefore, the extent of the controller’s verification may be less extensive in practice. (…) Conversely, in the event of higher risks arising from the processing (…) , the controller’s level of verification may be more important. (…)”*
  - *“In this regard, **depending** on the level of the risk associated with the processing activity, the controller **may** increase the level of its verification **by verifying the sub-processing contracts by itself** and/or also impose on the initial processor an extended verification and documentation.”*

Auftragskette *ohne* Datentransfer



- **EDSA-Frage 1.1.b.i.: Inwieweit muss der Verantwortliche die Garantien jedes AV‘ers/Unter-AV‘ers prüfen?**
  - Rn. 57: *„even if, according to Article 28(4) GDPR, it is under the direct responsibility of the processor engaging a sub-processor to ensure that the same data protection obligations as set out in the initial contract between the controller and the processor are imposed on that other processor, this does not lift the responsibility of the controller to ensure compliance with the requirements of Article 28(1), and Article 24(1) GDPR and for being able to demonstrate this compliance.”*
  - *Rn. 59: “(…) the controller may choose to rely on the information received from its processor and if necessary build on it.* ***For example, in case where the information received by the controller seems incomplete, inaccurate or raises questions,*** *or where appropriate based on the circumstances of the case including the* ***risk*** *associated with the processing, the controller should ask for additional information and/or verify the information and complete/correct it if necessary.”*

Auftragskette *ohne* Datentransfer



- **EDSA-Frage 1.1.b.*ii*.: muss der Verantwortliche den Inhalt jedes Unterauftragsvertrags (Art. 28(4)) selbst prüfen und dokumentieren?**
  - Rn. 69: *"the controller does **not** have a duty to **systematically** ask for the sub-processing contracts to check whether the data protection obligations provided for in the initial contract have been passed down the processing chain. The controller should assess, **on a case-by-case basis**, whether requesting a copy of such contracts or reviewing them at any time is necessary for it to be able to demonstrate compliance in light of the principle of accountability."*
  - *Rn. 70: "For example, **in case of doubts** as to the processor's or sub-processor's compliance with the requirements of Articles 28(1) and 28(4) or upon request by the SA, the controller should ask for the contract for its review (e.g. in the event that the additional processor is affected by a data breach, or in case of other publicly available information or other information available to the controller)"*

Q1.2

Q1.2 **-** Bei **Transfers in ein Drittland** durch einen (Unter-)AV‘er an einen (weiteren) (Unter-)AV‘er: inwieweit muss der Verantwortliche aufgrund seiner Pflichten nach Art. 28(1) und Art. 44 (selbst) prüfen und nachweisen können bzw. dokumentieren, dass das DSGVO-Schutzniveau durch den Transfer oder Weiter-Transfer an/von (Unter-)AV‘er weiterhin gewährleistet ist?

EDSA:

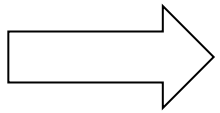
- Verweis auf die Interpretation des Transfer-Begriffs in Leitlinien 05/2021
- Transfer darf nur stattfinden, wenn der Verantwortliche ihn genehmigt hat!

Exkurs: Übermittlung an Drittland - Begriff

bildlich:

Interpretation des EDSA in den Leitlinien 05/2021: **„Übermittlung an ein Drittland“ (Transfer):**

Verantwortlicher oder Auftragsverarbeiter (Datenexporteur)

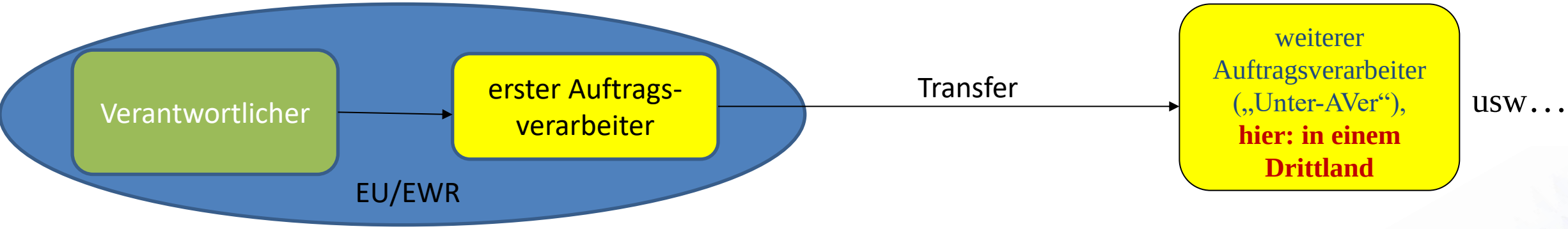


Offenlegung personenbezogener Daten

anderer Verantwortlicher oder Auftragsverarbeiter, der **„sich in einem Drittland befindet“** (Datenimporteur)

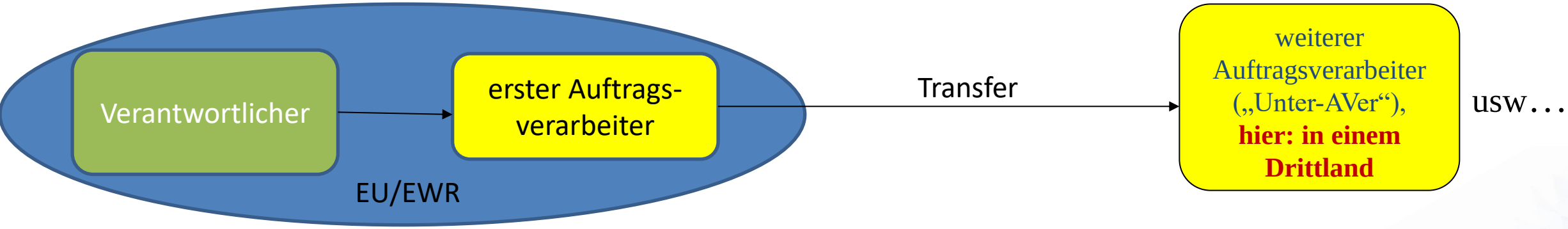
Das Element **„befindet sich in einem Drittland“** ist sehr schillernd (aber heute nicht Thema)

Q1.2 - Auftragskette *mit* Datentransfer



- Wo liegt hier der Transfer vor? Antwort: Beim Datenfluss vom ersten Auftragsverarbeiter an den Unterauftragsverarbeiter
- D.h. für diesen Datenfluss müssen die Anforderungen aus Kapitel V DSGVO eingehalten werden
- z.B. möglich durch Standardvertrags-Modul 3, den der erste Auftragsverarbeiter (= Datenexporteur) mit dem Unterauftragsverarbeiter (=Datenimporteur) abschließt, **plus Transfer Impact Assessment** (siehe Schrems-II-Urteil des EuGH)
- **EDSA-Opinion 22/2024, Frage 1.2, Rn. 72 ff.: Inwieweit muss der Verantwortliche prüfen und sicherstellen, ob/dass in diesem Szenario die Anforderungen an Transfers aus Kap. V DSGVO eingehalten werden?**

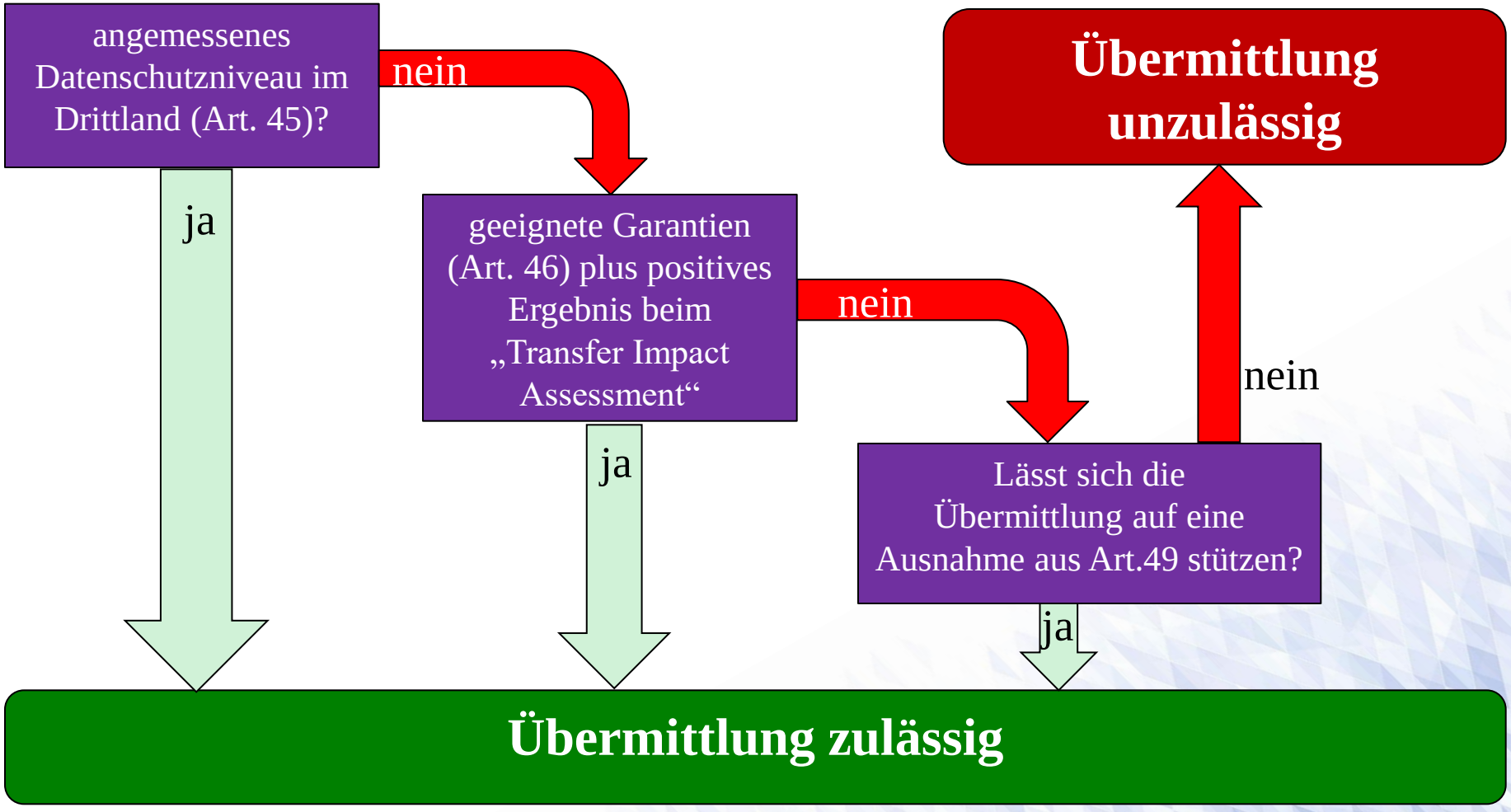
Q1.2 - Auftragskette *mit* Datentransfer



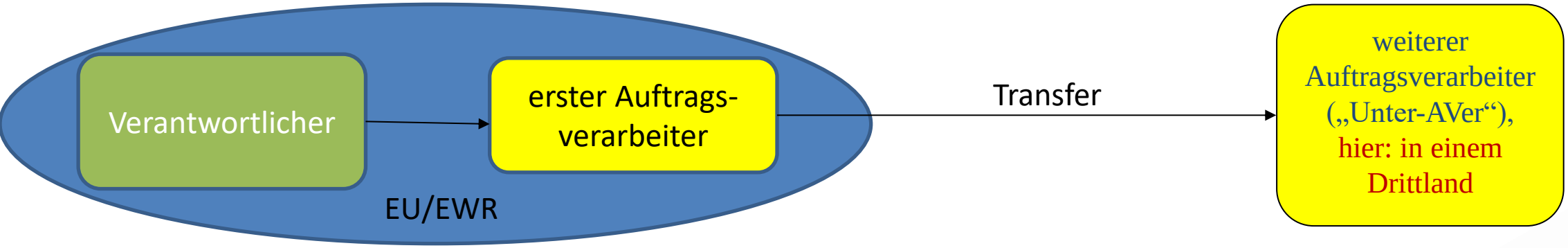
- EDSA-Opinion 22/2024, Rn. 76: In diesem Fall ist der Verantwortliche zwar nicht „Datenexporteur“, dies ist vielmehr der erste Auftragsverarbeiter …
- aber Rn. 79: *„Considering that the transfer is a processing activity carried out on behalf of the controller, the **controller** is also responsible and **could** be liable under **Chapter V**, **and also** has to ensure that the processor provides for sufficient guarantees under **Article 28**.”*
- *Rh. 86: “(…) practical difficulties invoked by controllers concerning control over the engagement of subprocessors by their processor – which may make it difficult for them to verify the ‘sufficient guarantees’, especially regarding transfers to third countries – do **not** exonerate the controller from its responsibilities in the processing.”*

Exkurs: mögliche Transfer-Grundlagen

Die laut Kapitel V DSGVO zur Verfügung stehenden Grundlagen für Übermittlungen in Drittländer:

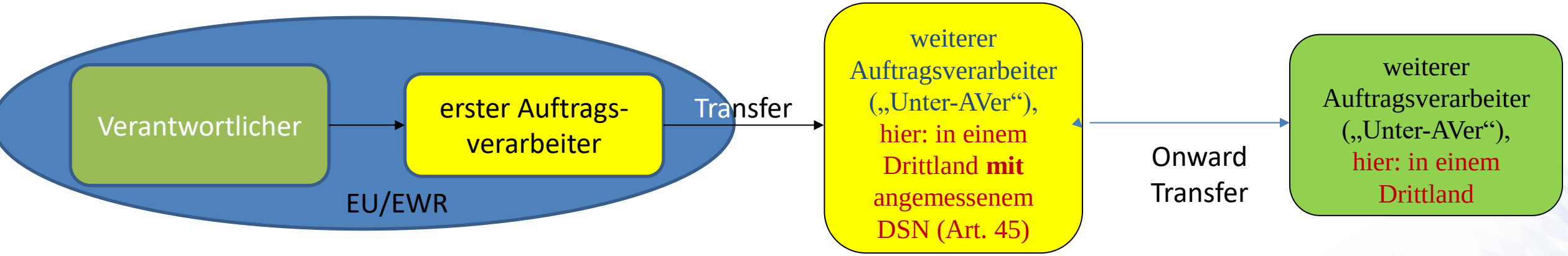


Q1.2 - Auftragskette *mit* Datentransfer



- Rn. 88: *„(…) the controller should know where the sub-processors are located and where transfers – including remote access – take place”*
- Rn. 91: *“As regards the extent of the controller’s duty to assess this documentation, it depends on the type of ground used for the initial or onward transfer by the (sub-)processors (as data exporter)”*
- *Rn. 93:* Wenn Transfer-Grundlage **Art. 45** (Drittland mit angemessenem Datenschutzniveau) ist, muss der Verantwortliche **nur** prüfen, ob der Angemessenheitsbeschluss in Kraft ist und der konkrete Transfer davon umfasst ist.

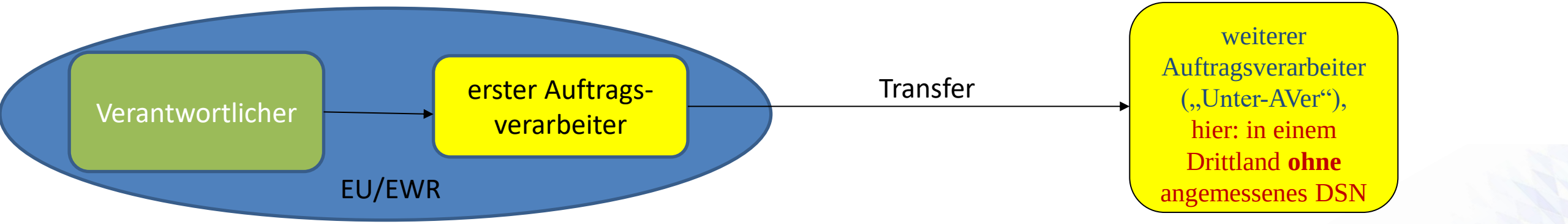
Q1.2 - Auftragskette *mit* Datentransfer



Wenn Transfer-Grundlage **Art. 45** (Drittland mit angemessenem Datenschutzniveau) ist:

- Rn. 94 (Thema **Onward Transfer**/Weitertransfer durch den Artikel-45-Importeur in ein anderes Drittland): Wenn der Transfer-Empfänger, der die Daten unter Art. 45 erhalten hat, diese in ein weiteres Drittland übermittelt, muss der Verantwortliche **nicht** per se prüfen, ob dabei die in der Rechtsordnung des (Artikel-45-) Drittlands geregelten Voraussetzungen für einen Weitertransfer im konkreten Fall eingehalten werden.

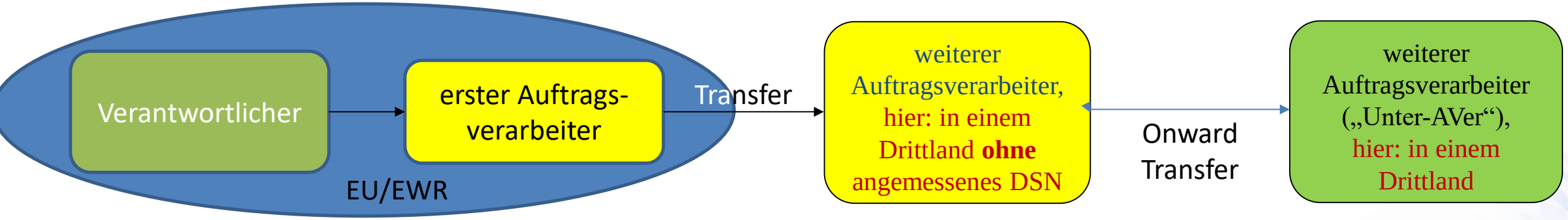
Q 1.2 - Auftragskette *mit* Datentransfer



Wenn Grundlage des Transfers **Art. 46** (z.B. Standardvertragsklauseln) ist:

- Rn. 96: *„(…) the controller should assess the appropriate safeguards put in place and be attentive about any problematic legislation that could prevent the sub-processor from complying with the obligations established in its contract with the initial processor. More specifically, the controller should ensure that such a* ***transfer impact assessment*** *is carried out”*
- *“(…) where the assessment received by the controller seems incomplete, inaccurate or raises questions, the controller should ask for additional information, verify the information and complete/correct it if needed (…). (T)he controller should pay particular attention particularly (…) to the* ***legislation and practices governing access to the transferred personal data by the third country’s public authorities****”*

Q1.2 - Auftragskette *mit* Datentransfer



Wenn Grundlage des Transfers **Art. 46** (z.B. Standardvertragsklauseln) ist:

- Rn. 97 zu **Onward Transfers** (= Weitertransfer durch Drittlands-Importeur aus seinem Drittland in dasselbe oder ein weiteres Drittland): *"Appropriate safeguards under Article 46 GDPR usually include provisions laying down rules that will govern any onward transfers. This means that controllers do not have to verify whether those rules as such are in line with the requirements of Chapter V GDPR. However, **controllers should be able to show documentation relating to such onward transfers**. This means that the controller should receive this information from the (sub-)processors/exporters, showing that the importers **actually** comply with the requirements for onward transfers as laid down in the appropriate safeguards instrument."*
- Zu Onward Transfers sind also die **Prüf-/Dokumentationsanforderungen** für den Verantwortlichen bei Art. 46-Tools laut EDSA **höher** als zu Onwards Transfers, die einem Transfer nachfolgen, der auf Art. 45 DSGVO (Angemessenheitsbeschluss) beruht.

Q2

*Q2 – **Muss** ein AVV gem. Art. 28(3) ausdrücklich oder jedenfalls in einem gleichwertigen Wortlaut die in Art. 28(3)(a) vorgesehene Ausnahme („**sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist**“) enthalten, um im Einklang mit der DSGVO zu stehen?*

EDSA:

- Verträge können nicht das Gesetz aushebeln
- Jeder AVV muss den Fall regeln, bei dem der Auftragsverarbeiter gesetzlich verpflichtet ist, die Daten abweichend von den Weisungen des Verantwortlichen zu verarbeiten (Rn. 105)

Q2

- Der AV‘er ist nach Art. 28(3)(a) verpflichtet, den Verantwortlichen in einem solchen Fall zu informieren (sofern ihm das nicht gesetzlich untersagt ist)
  - EDSA: … und diese Informationspflicht sollte auch im AVV explizit geregelt werden.
- Bei Auftragsvergabe in Drittland: Transfer-SCCs sehen vor, dass der AV‘er den Verantwortlichen informieren muss, sobald er **außerstande** ist, die **Daten nur nach Weisung zu verarbeiten** (Kl. 8.1)
- **Schlussfolgerung EDSA: nicht zwingend erforderlich, im AVV den Wortlaut *„sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist“* aufzunehmen**, jedoch sehr empfehlenswert
  - Achtung: Für **Transfer-AVV** wird dies aber kaum sinnvoll sein (und wäre aufgrund des dadurch dann aufgeworfenen - und bitte möglichst zu vermeidenden - Themas „Veränderungen am SCC-Wortlaut“ ohnehin problematisch), da der Auftragsverarbeiter dort eben nicht dem Recht „der Union oder eines EU-Mitgliedstaats“, sondern eben eines Drittlands unterliegt…

Q2a

Q2a – Wenn die Antwort zu Q2 „nein“ ist: Ist ein AVV, dessen Wortlaut die o.g. in Art. 28(3)(a) vorgesehene Ausnahme so erweitert, dass damit (jedenfalls nach Wortlaut) ***auch das Recht eines Drittlands*** *abgedeckt ist (z.B. „Sofern er nicht durch eine Rechtsvorschrift hierzu verpflichtet ist“),* ***per se ein Verstoß*** *gegen die DSGVO?*

EDSA:

Von diesem Wortlaut können zwei unterschiedliche Fälle umfasst sein: rechtliche Anforderungen

- (1) des EU-Rechts / des Rechts eines Mitgliedstaats
- (2) aus der Rechtsordnung eines Drittlands

Q2a

- Wenn die Parteien nachweisen können, dass nur Fall (1) gemeint ist, dann ist es kein Problem
- Fall (2) ist aber ein Problem
- Wenn der AV‘er in einem Drittland sitzt, liegt es in der Natur der Sache, dass der AV‘er u.U. einer rechtlichen Anforderung des **Rechts eines Drittlands** folgen muss…
- Rn. 116 (EDSA springt über seinen Schatten, **für die Praxis sehr wichtig, beseitigt Rechtsunsicherheit**): *„The EDPB takes the view that, with respect to personal data processed outside of the EEA, Article 28(3)(a) GDPR **does not prevent - on principle -** the inclusion, in the contract, of provisions that address third country law requirements to process transferred personal data.”*
- Die Transfer-SCCs enthalten
  - eine Pflicht, die Rechtsordnung des Drittlands (vor Transferbeginn!) zu prüfen (“Transfer Impact Assessment”, Klausel 14 Transfer-SCCs)
  - Und eine Pflicht, den Exporteur im Falle von Datenzugang durch Drittlands-Behörden zu informieren (Kl. 15)

Q2a

- Bei Transfers in ein Drittland (mit Angemessenheitsbeschluss oder mit sog. geeigneten Garantien, z.B. SCCs) gilt: Rechtsvorschriften des Drittlands, die
  - den **Wesensgehalt der EU-Grundrechte** nicht verletzen
  - und die Grundsätze von **Erforderlichkeit** und **Verhältnismäßigkeit** wahren,

  stehen mit dem DSGVO-Schutzniveau im Einklang.
- Das ist der Standard, der nach DSGVO immer zu waren ist, auch im Transferfall.
- Antwort zu Q2a: Die Einfügung des Wortlauts *„Sofern er nicht durch eine Rechtsvorschrift hierzu verpflichtet ist“* (d.h. ohne Beschränkung auf das EU-Recht bzw. Recht eines Mitgliedstaats) ist **nicht per se ein Verstoß gegen die DSGVO**. Jedoch entbindet dies die Beteiligten nicht von der Einhaltung der DSGVO.

Q2b

Q2b – Wenn die Antwort zu Q2 „nein“ ist: Kann ein dergestalt erweiterter AVV-Wortlaut als „dokumentierte Weisung des Verantwortlichen“ im Sinne von Art. 28(3)(a) angesehen werden?

- Folge wäre ja: Dann dürfte der Auftragsverarbeiter Daten an eine Drittlands-Behörde herausgeben und würde damit nicht gegen die DSGVO verstoßen

Antwort EDSA: Nein!

- „Weisung“ impliziert, dass der Verantwortliche es ist, der die Verarbeitung steuert.
- Vorgänge, die nicht den Willen des Verantwortlichen bzw. eine Vorgabe des Verantwortlichen darstellen, können nicht als „Weisung“ angesehen werden.
- „Weisungen“ müssen zudem spezifisch und widerrufbar sein

Vielen Dank!

Alexander Filip

Bayer. Landesamt für Datenschutzaufsicht