ANWALTSKANZLEI
DIERCKS

Schrems II, die neuen Standardvertragsklauseln & der risikobasierte Ansatz der DSGVO

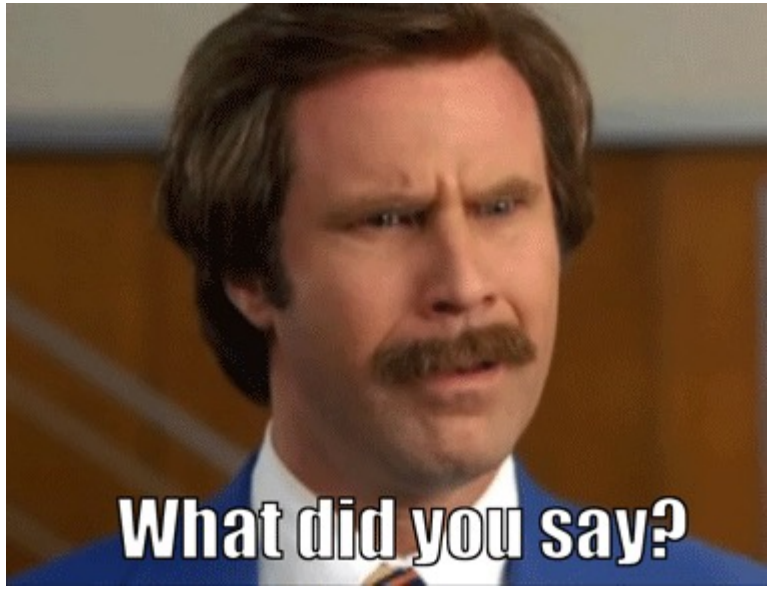
3. Hannoverscher Datenschutztag

Hannover, 12. Mai 2022

ANWALTSKANZLEI DIERCKS

Risikobasierter Ansatz bei Drittstaatentransfers

Die Aufsichtsbehörden:



Others, including me:

Der Reihe nach oder „Was diskutieren wir heute“?

ANWALTSKANZLEI DIERCKS

Risikobasierter Ansatz bei Drittstaatentransfers

1. Was hat der EuGH in Schrems II gesagt?
2. Was meint risikobasierter Ansatz?
3. Was fordert Art. 46 Abs. 2 c) DSGVO in Form von Klausel 14 der SCC der EUKom?
4. Wie ist die Haltung des EDPB?
5. Wieso trägt die Auffassung des EDPB nicht?
6. Wieso kann die Auffassung des EDPB in der Rechtspraxis nicht durchgesetzt werden?
7. Ändert das Vladeck „Gutachten“ etwas an den Ausführungen?
8. Conlusio
9. AddOn: Die sehr pragmatische Auffassung

ANWALTSKANZLEI DIERCKS

Was hat der EuGH in und mit Schrems II gesagt?

(Und vor allem: Was hat er nicht gesagt.)

Was hat der EuGH gesagt?

ANWALTSKANZLEI DIERCKS

- **Der EuGH erklärte den Angemessenheitsbeschluss „Privacy Shield“ der EU-Kommission iSd. Art. 45 DSGVO für ungültig,**
  - **da aus Sicht des EuGH kein angemessenes bzw. vergleichbares Schutzniveau bestand.**

- **Der EuGH erklärte hinsichtlich der Standardvertragsklauseln, SVK (englisch: Standard Contract Clauses, SCC), dass diese nicht mehr per se eine geeignete Garantie im Sinne von Art. 46 Abs. 2 c) DSGVO darstellen, sondern**
  - **dass der Datenexporteur in jedem Einzelfall prüfen (müsse), *ob das Recht des Drittlandes nach Maßgabe des Unionsrechts einen angemessenen Schutz der auf der Grundlage von SVK übermittelten personenbezogenen Daten gewährleistet und ob der Importeur im Drittland erforderlichenfalls mehr Garantien als die durch diese Klauseln gebotenen gewährt*.**

- **Der EuGH sagte nicht,**
  - **welche Kriterien für die Angemessenheit des Schutzes der übermittelten Daten und die Erforderlichkeit weiterer Garantien angelegt werden müssen.**
  - **welche „Garantien“ (Maßnahmen) getroffen werden müssen.**

- **Der EuGH sagt NICHT, dass keine Daten mehr in die USA übermittelt werden dürften.**

ANWALTSKANZLEI
DIERCKS

Der „risikobasierte Ansatz“ der DSGVO

Regelungskonzept des risikobasierten Ansatzes

ANWALTSKANZLEI DIERCKS

- **Prinzip des »risikobasierten Ansatzes« = Regelungskonzept, mit dem datenschutzrechtliche Pflichten der konkreten Gefährdungssituation für die Rechte und Freiheiten der betroffenen Person angepasst werden.**
- **»*Risiko*« = »e*in Szenario mit einem Ereignis und dessen Konsequenzen, das bezüglich seiner Schwere und seiner Eintrittswahrscheinlichkeit beurteilt wird*«. [EDPB, Leitlinien zur Datenschutz-Folgenabschätzung]**
- **Mit dem risikobasierten Ansatz können TOM dem tatsächlichen (erwarteten) Risiko der Verarbeitung entsprechend angepasst werden.**
- **Der Ansatz trägt dem Umstand Rechnung, dass zwar keine Verarbeitung risikolos ist, jedoch nicht jedes Risiko zu einer unvertretbaren Rechtsverletzung der betroffenen Personen führt.**

ANWALTSKANZLEI DIERCKS

Das Regelungskonzept des risikobasierten Ansatzes gilt für *jede* Datenverarbeitung

- Der risikobasierte Ansatz ist als Kernelement des Konzepts der Rechenschaftspflicht i.S.v. Art. 5 Abs. 2 DSGVO in Art. 24 Abs. 1 DSGVO verankert.
- Art. 24 Abs. 1 enthält die Verpflichtung des Verantwortlichen bei *jeder Datenverarbeitung* zur *Feststellung der Risiken* für die Rechte und Freiheiten natürlicher Personen und zur *Berücksichtigung der Eintrittswahrscheinlichkeit und Schwere* dieser Risiken, und zwar in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung.
- 32 Abs. 1 DSGVO fordert diese Abwägung noch einmal spezifisch im Hinblick auf die Sicherheit der Verarbeitung: *Unter »Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten«.*

Risikobasierter Ansatz im Rahmen von Drittstaatentransfers

ANWALTSKANZLEI DIERCKS

Der EuGH verlangt, dass der Datenexporteur in jedem Einzelfall prüfen (müsse), *ob das Recht des Drittlandes nach Maßgabe des Unionsrechts einen angemessenen Schutz der auf der Grundlage von SVK übermittelten personenbezogenen Daten gewährleistet und ob der Importeur im Drittland erforderlichenfalls mehr Garantien als die durch diese Klauseln geboten[n] gewährt*.

Wie genau soll denn die »Bestimmung« etwaiger der Angemessenheit des Schutzes und der gegebenenfalls weiteren erforderlichen Maßnahmen im Einzelfall bestimmt werden, wenn eben nicht unter anderem

- **die Eintrittswahrscheinlichkeit des Risikos eines Datenzugriffs durch einen Dritten,**
- **die Art der verarbeiteten Daten,**
- **deren Zwecke der Datenverarbeitung und**
- **die Schwere (Folgen) des möglichen Risikoeintritts**

Berücksichtigung finden?

Überraschung!

- **Eine solch transferspezifische und risikoorientierte Abwägung sehen die „neuen“ SVK (SCC) der EUKom vor.**
- **In den Klauseln 14 a), b) wird v. d. Parteien ein umfassendes Transfer Impact Assessment (TIA) gefordert.**
- **Juristisch ist das TIA kein gänzlich neues Wesen, sondern im Grunde eine Verhältnismäßigkeitsprüfung.**

ANWALTSKANZLEI DIERCKS

Standard Contract Clauses (SCC)

Standard Contract Clauses (SCC)

ANWALTSKANZLEI DIERCKS

Nach **Klausel 14 a)** SVK müssen Parteien zusichern, keinen Grund zu der Annahme zu haben, dass
- *Rechtsvorschriften* (Rechtslage, d.h. Legislatur) und
- *Gepflogenheiten* (Rechtspraxis, d.h. Anwendung durch Behörden, Gerichte)

im Land des Datenimporteurs nicht über das notwendige Schutzniveau für die übermittelten Daten verfügten.

Klausel 14 b) zählt Aspekte in drei Fallgruppen auf (nicht abschließend):

(i) *die **besonderen Umstände der Übermittlung,** einschließlich der Länge der Verarbeitungskette, der Anzahl der beteiligten Akteure und der verwendeten Übertragungskanäle, beabsichtigte Datenweiterleitungen, die Art des Empfängers, den Zweck der Verarbeitung, die Kategorien und das Format der übermittelten personenbezogenen Daten, den Wirtschaftszweig, in dem die Übertragung erfolgt, den Speicherort der übermittelten Daten,*

(ii) *die angesichts der besonderen Umstände der Übermittlung **relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes** (einschließlich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten) sowie die geltenden Beschränkungen und Garantien,*

(iii) *alle **relevanten vertraglichen, technischen oder organisatorischen Garantien**, die zur Ergänzung der Garantien gemäß diesen Klauseln eingerichtet wurden, einschließlich Maßnahmen, die während der Übermittlung und bei der Verarbeitung personenbezogener Daten im Bestimmungsland angewandt werden.*

- Wortlaut von Klausel 14 b) zeigt deutlich, dass die Legislatur (ii) nur eine Rolle, aber nicht »die« Rolle für das TIA spielt.
- Daneben müssen im konkreten Fall
  - die (praktische) Rechtsanwendung (ii),
  - die vertraglichen, technischen und organisatorischen Schutzmaßnahmen (iii)
  - die Datenkategorien, Zwecke der Verarbeitung und Empfänger der Daten (i)

berücksichtigt werden.

Die Ansicht des EDPB

Die Ansicht des EDPB

ANWALTSKANZLEI DIERCKS

Ausschließlich Prüfung von Rechtslage und Rechtspraxis eines Drittlandes.

- **Prüfumfang unklar, da widersprüchliche Angaben/Anforderungen seitens EDPB:**
  - **Einerseits soll der Verantwortliche [auch KMU] die Rechtslage prüfen (die ansonsten im Rahmen von Art. 45 Abs. 2 DSGVO durch die EUKOM (sic!) geprüft wird)**
  - **Andererseits soll der Umfang der Bewertung auf die Gesetzgebung und Praktiken beschränkt sein, die für den Schutz der spezifischen Daten, die übertragen werden, relevant sind, im Gegensatz zu den allgemeinen und weitreichenden Angemessenheitsbewertungen, die die Europäische Kommission gem. Art. 45 DSGVO durchführt.**

Die Ansicht des EDPB und dessen Folgen

ANWALTSKANZLEI DIERCKS

Ausschließlich Prüfung von Rechtslage und Rechtspraxis eines Drittlandes.

Nach dem EDPB kann dabei die Prüfung von Rechtslage wie -praxis nur zu zwei Ergebnissen führen:

I. **entweder es besteht ein angemessenes Schutzniveau und die Datenübermittlung ist möglich**

II. **oder es besteht kein angemessenes Schutzniveau.**

Im letzteren Fall muss die Datenübermittlung entweder eingestellt werden oder effektive zusätzliche (technische) Maßnahmen ergriffen werden.

- **Das EDPB beschränkt das TIA n. Ziffer 14 b) der SCC iSv Art. 46 Abs. 2c) auf Rechtslage und Rechtspraxis**
  - ➢ **verlangt damit eine inhaltliche Beschränkung eines Durchführungsbeschlusses der EUKom.**
- **Forderung an Verantwortliche (Unternehmen, auch KMU), - unabhängig von Art der Datenübermittlung - Rechtslage und Rechtspraxis in Drittländern zu prüfen.**
  - ➢ **Eine Aufgabe die sonst der EUKom obliegt und die Datenschutzbehörden – aus gutem Grund! – selbst überhaupt nicht erfüllen können.**

Die Ansicht des EDPB - Begründung

ANWALTSKANZLEI DIERCKS

Ausschließlich Prüfung von Rechtslage und Rechtspraxis eines Drittlandes.

Begründung

EuGH habe im Schrems-II-Urteil auf keinen subjektiven Faktor wie die Wahrscheinlichkeit eines Zugriffs Bezug genommen. (Der EuGH spricht aber von angemessenen Schutzmaßnahmen und geeigneten Garantien, die Angemessenheit und Geeignetheit kann nicht ohne Risikobetrachtung, also „subjektiven“ Faktoren, bestimmt werden.)

Der EuGH stellte fest, dass über Art. 44 Satz 2 DSGVO für alle Arten von Datentransfers in Kapitel 5, unabhängig vom Sicherungsinstrument (z.B. SVK), der gleiche Maßstab für das Schutzniveau gelten soll, konkret »ein Schutzniveau gewährleisten, das dem in der Union garantierten Schutzniveau der Sache nach gleichwertig ist«.

EDPB folgert daraus (scheinbar), dass, wenn der Angemessenheitsbeschluss (AB) für ein Drittland (z.B. Privacy Shield) sich nicht »der Sache nach gleichwertig« zum Unionsrecht verhält, andere Instrumente aus Kapitel 5 (z.B. SVK) für eine Übermittlung in eben dieses Drittland (z.B. USA) nur genutzt werden können, wenn jegliche Kollision zwischen den Pflichten aus den SVK und der Rechtslage im Drittland ausgeschlossen ist – und zwar unabhängig vom konkreten Einzelfall.

Tja. Das trägt nicht.

ANWALTSKANZLEI DIERCKS

Warum die Auffassung des EDPB nicht trägt

ANWALTSKANZLEI DIERCKS

Warum die Auffassung des EDPB nicht trägt

1. Es existiert keine Gleichschaltung der Instrumente des Kapitel V
2. Art. 45 und Art. 46 verfügen über andere Schutzaufträge
3. Selbstregulierung und Risikobewertung sind in der DSGVO angelegt
4. Schutz von personenbezogenen Daten ist auch nach dem EuGH nicht absolut
5. Argumente einer zwingenden „Benachrichtigungspflicht“ der Betroffenen und daraus folgender unzureichender Rechtsschutz geht fehl

Warum Ansicht des EDBP nicht trägt

ANWALTSKANZLEI DIERCKS

Es existiert keine Gleichschaltung aller Instrumente des Kapitel V durch dem EuGH

- Das »*der Sache nach gleichwertig*« ist eine Anforderung, die nur im Erwägungsgrund (EG) 104 erwähnt wird. EG 104 ist jedoch ausschließlich für die Auslegung von Art. 45, d.h. für Angemessenheitsbeschlüsse, relevant, nicht für SCC nach Art. 46 DSGVO.
- Das »*der Sache nach gleichwertig*« aus EG 104 findet seinen Ursprung wiederum in der Entscheidung des EuGH zu Schrems I und der Auslegung der DS-RL mit Blick auf den damals geltenden Angemessenheitsbeschluss »Safe Harbour«. Schon hier war die Verbindung von »*angemessenes Schutzniveau*« (Wortlaut Art. 25 DS-RL) und »*der Sache nach gleichwertig*« (Ergänzung durch EuGH) systematischer Kritik ausgesetzt.

Art. 45 und Art. 46 DSGVO verfügen über unterschiedliche Schutzaufträge

- Art. 45 DSGVO beschreibt ein zeitlich langwieriges, formalisiertes, **generisches Verfahren**, (d.h. unabhängig von Branche, Geschäftsprozess, Unternehmen, Datenarten, Zwecken) in Form einer umfassende Prüfung des Schutzniveaus eines Empfängerlandes **durch die EUKOM.**
- Bei Art. 46 Abs. 2 c) DSGVO und den SVK (SCC) handelt es sich um eine **interorganisatorische und transferbezogene** Bewertung anhand einer zu dokumentierenden TIA für den konkreten Fall **durch die Parteien** selbst.

Warum Ansicht des EDBP nicht trägt

ANWALTSKANZLEI DIERCKS

Selbstregulierung und Risikobewertung sind in DSGVO einschl. Art. 46 sowie SCC angelegt

- Selbstregulierung und Risikobewertung sind in Art. 5, 24, 32 und 35 DSGVO angelegt
- Instrumente der Art. 32 u 35 haben gemein, dass sie dem Verantwortlichen bei der Bewältigung der einhergehenden Unsicherheiten einen **Prognosespielraum** bei der Entscheidungsfindung zur **Skalierung der Schutzmaßnahmen** zugestehen.
- Art. 46 Abs. 2 DSGVO spricht von „geeignete Garantie“ -> **Eignung** kann sich nur aus **risikoorientierter** Bewertung bestimmen (Woraus sonst?)
- Folgerichtig wird nichts anderes im TIA nach Art. 14 a und b) SCC gefordert:
  - Eine **TIA** ist ihrem Umfang nach einer Art **»Mini-Adäquanzentscheidung« der Parteien des SCC**

Schutz von personenbezogenen Daten ist auch nach EuGH nicht absolut

- Auch nach dem EuGH gilt der Schutz personenbezogener Daten nicht absolut (*„Die in den Art. 7 und 8 der Charta niedergelegten Rechte können jedoch keine uneingeschränkte Geltung beanspruchen, sondern müssen im Hinblick auf ihre gesellschaftliche Funktion gesehen werden“*).
- Bei einem Vollzug der »0-Toleranz«-Interpretation des EDPB durch die Behörden wird zwangsläufig auch in Rechte und Freiheiten von Dritten eingegriffen, die durch die GRCh gewährt werden (ua Informationsfreiheit Art. 11, unternehmerische Freiheit Art. 16 und das Eigentum Art. 17).
  - Erst eine risikoorientierte Auslegung wahrt diese Verhältnismäßigkeit.
  - Daher ist es auch konsequent, dass sich der risikobasierte Ansatz ausweislich Art. 24 Abs. 1 Satz 1 DSGVO auf alle Verarbeitungen bezieht, also auch auf Übermittlungen nach Art. 44 DSGVO (siehe II.).

Warum Ansicht des EDBP nicht trägt.

ANWALTSKANZLEI DIERCKS

Argument der zwingenden Benachrichtigung von Betroffenen geht fehl

Auch der EGMR kennt und erkennt Notwendigkeit von Geheimdienstoperationen und damit auch die Notwendigkeit der Nicht-Benachrichtigung von Betroffenen:

Der Europäische Gerichtshof für Menschenrechte (EGMR) urteilte 2010, dass im Bereich eine Benachrichtigung der Betroffenen über solche Maßnahmen zwar grundsätzlich zu erfolgen habe, aber nicht wenn und soweit damit die Maßnahme selbst oder aber die Arbeit dieser Behörden als solche gefährdet werde.
(EGMR, Case of Kennedy v. The United Kingdom, no. 26839/05, 18. Mai 2010)

[Über das „vergleichbare“ und „angemessene“ Schutzniveau könnte man bei einem Blick in die EU ohnehin sehr, sehr lange sprechen. Die Zeit haben wir nur leider gerade nicht.]

ANWALTSKANZLEI
DIERCKS

Conclusio

Conclusio

ANWALTSKANZLEI DIERCKS

Die Interpretation des EDPB des Schrems II Urteil sowie die Auslegung der Ziffer 14 der SCC hinsichtlich der Negierung eines risikobasierten Ansatzes halten einer näheren Betrachtung nicht stand.

Vielmehr ist auch bei einem Transfer Impact Assessment i.S.v. Art. 46 Abs. 2 c) DSGVO und Klausel 14 b) der SVK das Prinzip des risikobasierten Ansatzes der DSGVO zu berücksichtigen und über eine Verhältnismäßigkeitsprüfung mit einzubeziehen.

Bei Beschlüssen der EU-Kommission, wie der Durchführungsbeschluss zu den SVK, handelt es sich um EU-Sekundärrecht nach Art. 288 AEUV, sie sind bindend.

Rechtsauffassungen des EDPB bzw. der Datenschutzbehörden sind dagegen eben nur dies: unverbindliche Rechtsauffassungen.

Ausführlich zu dem Vorstehenden mit mzwN:
Diercks/Roth, Datenübermittlung in unsichere Drittstaaten - ZdiW 08/2021, 313.

ANWALTSKANZLEI
DIERCKS

Rechts(durchsetzungs)praxis

Rechts(durchsetzungs)praxis

ANWALTSKANZLEI DIERCKS

Die Rechenschaftspflicht des Art. 5 Abs. 2 DSGVO führt nicht zu einer „Beweislastumkehr“!

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

- **Unter Verweis auf Art. 5 Abs. 2 DSGVO fordern Aufsichtsbehörden, dass Verantwortliche die Datenschutzkonformität von verwendeten Produkten vollumfänglich nachweisen müssten.**
  - ➢ **Dies geht soweit, dass bei der Nutzung SaaS-Produkten von einigen Aufsichtsbehörden die Ergebnisse forensischer Laboruntersuchungen bezüglich der Datenverarbeitung und Datenübermittlung gefordert werden.**

Dabei handelt es sich um eine unzulässige Überdehnung des Art. 5 Abs. 2

- Die DSGVO fordert selbstverständlich eine Prüfung und Absicherung des Verantwortlichen bei der Auswahl seiner Auftragnehmer *im Rahmen der gesetzlichen Anforderungen* (die sich in Ihren Grundsätzen aus Art. 5 Abs. 1 ergeben!)
- Im Rahmen von SaaS-Anwendungen bedeutet dies, dass insb. die Anforderungen des Art. 28 DSGVO vom Verantwortlichen zu erfüllen sind.
- Eine forensische Prüfung jeder 0 und 1 von genutzter (Saa-)Software ist an keiner Stelle der DSGVO verlangt.
- Die Forderung forensischer Labore würde die Vertragskonstrukte des Art. 28 DSGVO (und Art. 26) obsolet machen.
- Die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO entbindet die Aufsichtsbehörde nicht vom Amtsermittlungsgrundsatz!

Rechts(durchsetzungs)praxis

ANWALTSKANZLEI DIERCKS

Die Aufsichtsbehörde unterliegt dem Untersuchungsgrundsatz nach § 24 VwVfG

(1) Die Behörde ermittelt den Sachverhalt von Amts wegen. Sie bestimmt Art und Umfang der Ermittlungen; an das Vorbringen und an die Beweisanträge der Beteiligten ist sie nicht gebunden. […]

(2) Die Behörde hat alle für den Einzelfall bedeutsamen, auch die für die Beteiligten günstigen Umstände zu berücksichtigen.

(3) […]

- **Im konkreten Fall genügt der pauschale Hinweis auf das Schrems-II-Urteil des EuGH nicht.**
- **Im konkreten Fall genügt der pauschale Verweis auf mögliche Befugnisse von US-Behörden nicht.**
- **Es bedarf vielmehr der fundierten Prüfung im Einzelfall, ob und warum eine datenschutzkonforme Übermittlung derzeit ausgeschlossen ist. So ist unter anderem zu ermitteln,**
    - ob eine konkrete Gefahr für die Grundrechte der Betroffenen bereits verwirklicht ist, gerade stattfindet oder unmittelbar bevorsteht,
    - inwieweit ein Wechsel des Dienstleisters und damit eine Verlagerung der Datenverarbeitung in die EU den Verantwortlichen zumutbar ist sowie ob dies mit Blick auf die o.g. Risikoabwägung für den Datenschutz auch tatsächlich erforderlich wäre,
        - wobei im Rahmen der Zumutbarkeit ist auch der finanzielle und personelle Aufwand des Verantwortlichen in der Risikoabwägung zu berücksichtigen ist.

(Benedikt, ZdiW, 01/2021, 12, 15; Schwartmann/Burkhard, ZD 2021, 235, 239)

ANWALTSKANZLEI DIERCKS

Die Aufsichtsbehörde muss ihr (Auswahl-)Ermessen im Rahmen des § 40 VwVfG (fehlerfrei) ausüben.

Ist die Behörde ermächtigt, nach ihrem Ermessen zu handeln, hat sie ihr Ermessen entsprechend dem Zweck der Ermächtigung auszuüben und die gesetzlichen Grenzen des Ermessens einzuhalten.

Auswahlermessen und Verhältnismäßigkeit nach 40 VwVfG im Rahmen der Störerauswahl:

Die Störerauswahl richtet sich im Datenschutzrecht wie auch im Gefahrenabwehrrecht nach dem Gedanken der Effektivität „verstanden als möglichst wirksame und schnelle Gefahrenbeseitigung“, bei der die Ermessensausübung auch im Übrigen dem Grundsatz der Verhältnismäßigkeit genügen muss.
(vgl. *Schreiber, ZD 2019, 55, 59 mwN*.)

Da bei der Ermessensauswahl auch die Zumutbarkeit und die Intensität der Belastung für den in Anspruch genommenen Störer berücksichtigt werden müssen, ist der Verantwortliche im datenschutzrechtlichen Sinne nicht in jedem Fall der richtige Adressat der verwaltungsrechtlichen Maßnahme.
(*BVerfG* BeckRS 2000, 30096329, Schreiber, ZD 2019, 55, 60 mwN. Schwartmann/Burkhard, ZD 2021, 235, 238.)

ANWALTSKANZLEI
DIERCKS

Ändert daran das Vladeck „Gutachten“ etwas?

ANWALTSKANZLEI DIERCKS

Nein.

- Das Vladeck Memo zeigt die Komplexität des US-Rechtssystems auf.
  - Es zeigt insbesondere auf, dass noch sehr viele Fragen im Zusammenhang mit FISA 702, FISA 501 oder sonstigen Gesetzen des CLOUD-Act ungeklärt sind.
    - So etwa, wie weit überhaupt die Anwendungsbereiche dieser Gesetze gehen.
- Des Weiteren wird aufgezeigt, dass es selbstverständlich auch Rechtsmittel gegen Anweisungen und/oder Anfragen seitens der Unternehmen gibt.
  - Vertieft eingegangen wird auf diese jedoch nicht.
- Den Betroffenen stehen - gänzlich anders als von der DSK suggeriert – ebenfalls Maßnahmen zur Verfügung.
  - *Es heißt wörtlich im Memo: „Es (gibt) zahlreiche gesetzliche und nicht-gesetzliche Rechtsbehelfe, die Betroffenen aus der EU/dem EWR zumindest in einigen dieser Zusammenhänge theoretisch zur Verfügung stehen – einschließlich der Geltendmachung, dass die zuständigen US-Behörden ihre gesetzlichen Befugnisse überschritten haben“.*
  - Es scheitert nur praktisch zuweilen daran, dass die Betroffenen keine Kenntnis von den Datenverarbeitungen erhalten.
  - **Aber**: Das ist – wie aufgezeigt in der EU nicht anders! Vgl. das EGMR-Urteil zur Nichtbenachrichtigung in Geheimdienstangelegenheiten

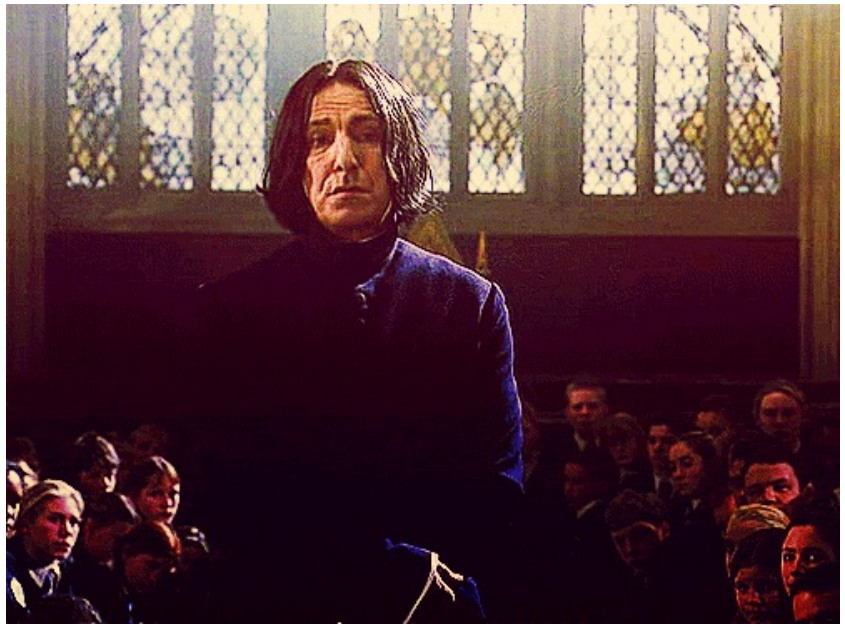
ANWALTSKANZLEI
DIERCKS

Die ganz pragmatische Ansicht.

ANWALTSKANZLEI
DIERCKS

Supersafeharbourshield is on the way.

Und meine Mandanten haben erstmal wieder Ruhe.



ANWALTSKANZLEI DIERCKS

Vielen Dank!

ANWALTSKANZLEI DIERCKS

Rechtsanwältin Nina Diercks
M.Litt., University of Aberdeen

Deepenstöcken 12
22529 Hamburg

T: + 49 (0)40 21 06 20 10
F: + 49 (0)40 21 07 05 20

diercks@anwaltskanzlei-diercks.de
https://anwaltskanzlei-diercks.de

DIERCKS DIGITAL RECHT

https://diercks-digital-recht.de
https//twitter.com/kanzleidiercks