

Bußgelder nach der DSGVO

RA Malgorzata (Margo)
Steiner, MPP (Harvard)



MITTEL DER RECHTSDURCHSETZUNG – WAS AUSSER BUßGELD?

Verwarnung

Anordnung

Bußgeld



„PRIVATE“ RECHTSDURCHSETZUNG?

ART. 82 DSGVO **JEDE PERSON**, DER WEGEN EINES VERSTOßES GEGEN DIESE VERORDNUNG EIN MATERIELLER ODER IMMATERIELLER SCHADEN ENTSTANDEN IST, HAT ANSPRUCH AUF SCHADENERSATZ GEGEN DEN VERANTWORTLICHEN ODER GEGEN DEN AUFTRAGSVERARBEITER.

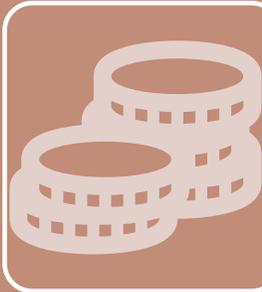
SCHADENERSATZ-
FORDERUNGEN



**WAS SAGT DIE DSGVO
UND DIE
AUF SICHTSBEHÖRDEN
ZU DEN BUßGELDERN?**

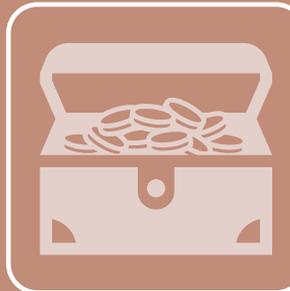


BUßGELDER NACH DER DSGVO



„Kleiner“ Bußgeldrahmen

- Bis 10 Mio EUR oder 2 % des weltweiten Jahresumsatzes des Vorjahres
- Art. 83 (4) DSGVO



„Großer“ Bußgeldrahmen

- Bis 20 Mio EUR oder 4% des weltweiten Jahresumsatzes des Vorjahres
- Art. 83 (5) DSGVO

WELCHE KRITERIEN SPIELEN BEI DER ZUMESSUNG EINE ROLLE? ART. 83 DSGVO

- „TAT-BEZOGENE-KRITERIEN“
 - Art, Schwere, Dauer des Verstoßes
 - Kategorien der Daten, die vom Verstoß getroffen sind
 - Maßnahmen zur Schadensbegrenzung
- „TÄTER-BEZOGENE“ KRITERIEN
 - Vorsätzliches oder fahrlässiges Handeln?
 - Wie gut waren die technischen und organisatorischen Maßnahmen?
 - Frühere einschlägige Verstöße des Verantwortlichen oder Auftragsverarbeiters
 - Wie gut war die Zusammenarbeit mit der Behörde?
 - Umsatz des Unternehmens

NATIONALE BUßGELD-BERECHNUNGSMODELLE

- Unterschiedliche Aufsichtsbehörden der EU-MS haben Bußgeldberechnungsmodelle veröffentlicht, die zu sehr unterschiedlichen Ergebnissen kommen

<u>DSK</u>	Niederlande
<ul style="list-style-type: none">- Bußgeldberechnung basiert primär auf “Tagessätzen”, die auf der Grundlage vom Umsatz des Vorjahres berechnet werden	<ul style="list-style-type: none">- Stärkerer Bezug zu tat- und täterbezogenen Merkmalen des Art. 84 DSGVO- Umsatz als Korrektur, wenn nach der Anwendung der tatbezogenen Kriterien ein unangemessenes Ergebnis droht

SANKTIONEN: EIN VERSTOß - ZWEI PREISSCHILDER (2020)

- Twitter: verspätete Meldung einer Datenpanne gem. Art. 33 (1) und (5) DSGVO
- Entwurf der Entscheidung von DPC Irland an andere betroffene Aufsichtsbehörden gem. Art. 60 DSGVO übermittelt
- Da kein Konsensus erzielt: Uraufführung vom Streitbeilegungsverfahren nach Art. 65 DSGVO

Vorschlag für die Bußgeldhöhe, Irland, DPC:	Bußgeldhöhe nach dem DSK-Berechnungsmodell	Kompromiss nach Streitbeilegung gem. Art. 65 DSGVO, Irland, DPC:
150-300 000 EUR	7-22 Mio EUR	450 000 EUR

EDSA-BUßGELD-BERECHNUNGSMODEL (04/2022 ENTWURF)

1

- Welche Verstöße und welche Datenverarbeitung liegen der Geldbuße zugrunde?

2

- Ermittlung der Ausgangsbasis für weitere Berechnung auf Grundlage: der Einstufung in Art. 83 Abs. 4-6, der Schwere des Verstoßes gem. Art. 83 Abs. 2 a,b,g, Umsatzes des Unternehmens

3

- Verschärfende oder mildernde Umstände im Zusammenhang mit früherem und aktuellem Verhalten des Verantwortlichen.

4

- Ermittlung des gesetzlichen Höchstbeiträge für die Verarbeitungsvorgänge

5

- Erfüllt die Geldbuße den Anforderungen der Wirksamkeit, Abschreckung und Verhältnismäßigkeit?

HÖCHSTE BUßGELDER

Statistics: Highest individual fines (Top 10)

The following statistics shows the highest individual fines imposed to date per data controller

	Controller	Sector	Country	Fine [€]
1	Amazon Europe Core S.à.r.l.	Industry and Commerce	LUXEMBOURG	746000000
2	Meta Platforms, Inc.	Media, Telecoms and Broadcasting	IRELAND	405000000
3	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	390000000
4	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	265000000
5	WhatsApp Ireland Ltd.	Media, Telecoms and Broadcasting	IRELAND	225000000
6	Google LLC	Media, Telecoms and Broadcasting	FRANCE	90000000
7	Facebook Ireland Ltd.	Media, Telecoms and Broadcasting	FRANCE	60000000
8	Google Ireland Ltd.	Media, Telecoms and Broadcasting	FRANCE	60000000
9	Google LLC	Media, Telecoms and Broadcasting	FRANCE	50000000
10	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	Employment	GERMANY	35258708

Quelle: Enforcementtracker. Com by CMS Law.Tax, 24.4.2023

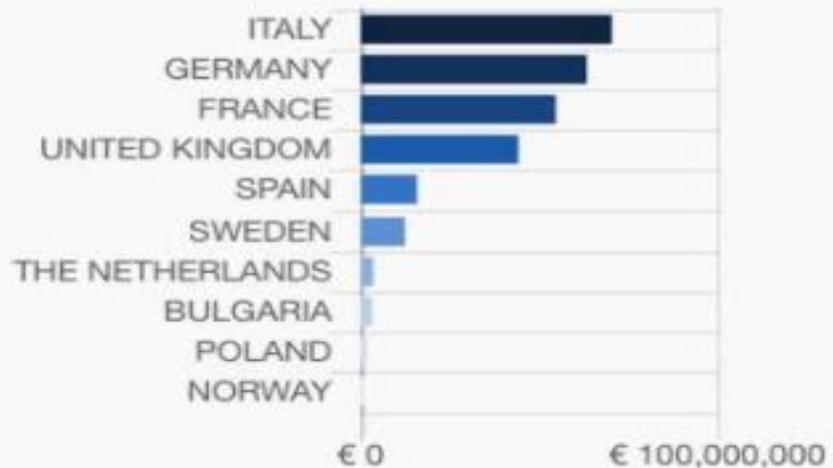
SANKTIONEN: BUßGELDER IN EU/EWR-MS 2/2021

Statistics: Countries with highest fines (Top 10)

The following statistics show how many fines and what sum of fines have been imposed per country to date (only top 10 countries).

Note: Only fines with valid information on the amount of the fine are taken into account.

1. By total sum of fines:



Country	Sum of Fines
ITALY	€ 70,393,601 (at 44 fines)
GERMANY	€ 63,386,633 (at 28 fines)
FRANCE	€ 54,661,300 (at 14 fines)
UNITED KINGDOM	€ 44,221,000 (at 4 fines)
SPAIN	€ 15,793,010 (at 183 fines)
SWEDEN	€ 12,332,430 (at 17 fines)
THE NETHERLANDS	€ 3,490,000 (at 6 fines)
BULGARIA	€ 3,210,690 (at 20 fines)
POLAND	€ 1,745,298 (at 19 fines)
NORWAY	€ 1,276,450 (at 19 fines)

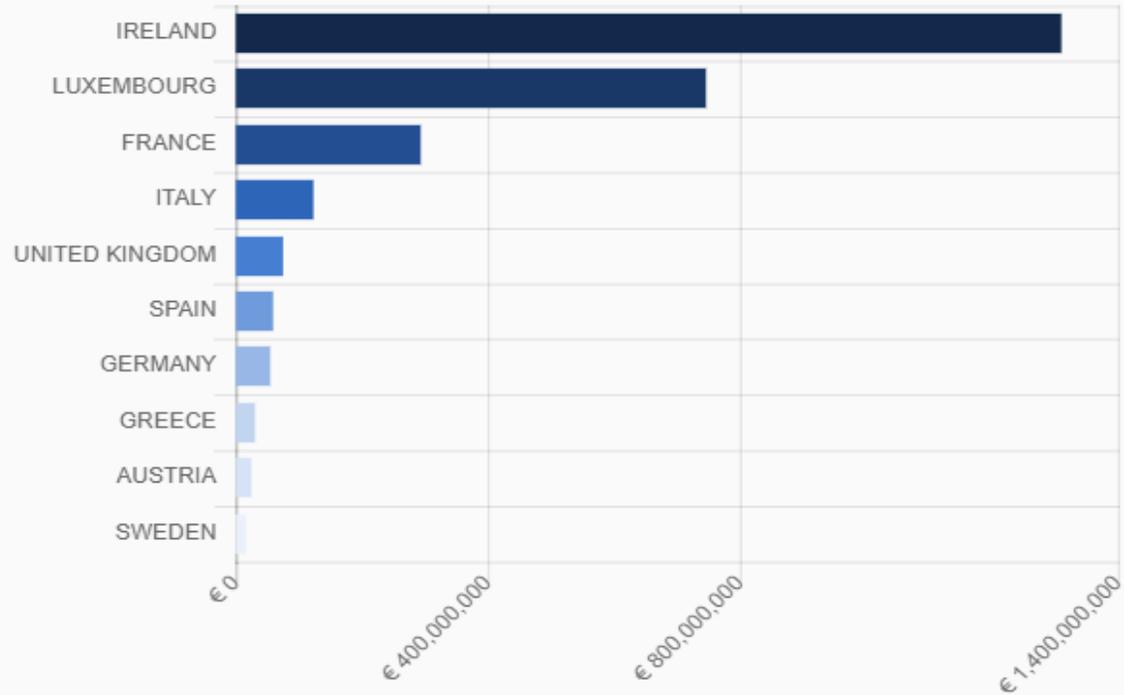
SANKTIONEN: BUßGELDER IN EU/EWR-MS 4/2023

Statistics: Countries with highest fines (Top 10)

The following statistics show how many fines and what sum of fines have been imposed per country to date (only top 10 countries).

Note: Only fines with valid information on the amount of the fine are taken into account.

1. By total sum of fines:



Country	Sum of Fines
IRELAND	€ 1,310,340,900 (at 24 fines)
LUXEMBOURG	€ 746,311,500 (at 31 fines)
FRANCE	€ 293,544,300 (at 34 fines)
ITALY	€ 123,321,596 (at 260 fines)
UNITED KINGDOM	€ 75,132,800 (at 13 fines)
SPAIN	€ 59,349,670 (at 640 fines)
GERMANY	€ 54,810,633 (at 148 fines)
GREECE	€ 30,601,000 (at 57 fines)
AUSTRIA	€ 24,775,150 (at 20 fines)
SWEDEN	€ 16,267,730 (at 29 fines)

HÄUFIGE URSACHEN FÜR BUßGELDER

Unzureichende technische und organisatorische Maßnahmen des Datenschutzes

Datenschutzverletzungen

Verstoß gegen Datenschutzprinzipien des Art. 5 DSGVO

**ANFORDERUNGEN
AN DIE
VERHÄNGUNG VON
BUßGELDERN**

RECHTSPRECHUNG

EXKURS: HAFTUNG VON UNTERNEHMEN NACH OWIG

§ 130 OWiG: HAFTUNG BEI AUFSICHTSPFLICHTVERLETZUNG: (1) Wer als **Inhaber eines Betriebes** oder Unternehmens vorsätzlich oder fahrlässig **die Aufsichtsmaßnahmen unterlässt**, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist, handelt ordnungswidrig, wenn eine solche Zuwiderhandlung begangen wird, die durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre. (...)

§ 30 OWiG: GELDBUßE FÜR JUR. PERSON BEIM HANDELN EINES ORGANS / GESELLSCHAFTERS:

(1) Hat jemand

1. als **vertretungsberechtigtes Organ** einer juristischen Person oder als Mitglied eines solchen Organs,
3. als vertretungsberechtigter Gesellschafter einer rechtsfähigen Personengesellschaft,
5. als sonstige Person, die für die Leitung des Betriebs oder Unternehmens einer juristischen Person oder einer in Nummer 2 oder 3 genannten Personenvereinigung verantwortlich handelt (...),

eine Straftat oder Ordnungswidrigkeit begangen, durch die Pflichten, welche die juristische Person oder die Personenvereinigung treffen, verletzt worden sind oder die juristische Person oder die Personenvereinigung bereichert worden ist oder werden sollte, **so kann gegen diese eine Geldbuße festgesetzt werden.**

GILT DAS AUCH FÜR DSGVO?

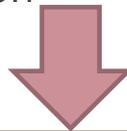
- Oder kann ich gegen ein Unternehmen ein Bußgeld verhängen, wenn einfach objektiv ein Verstoß gegen DSGVO begangen wurde?



FUNKTIONSTRÄGERPRINZIP ODER RECHTSTRÄGERPRINZIP?

LG Bonn (1&1), November 2020

- DSGVO Bußgelder können direkt gegen Unternehmen verhängt werden
- Funktionsträgerprinzip (unmittelbare Verbandshaftung) ist anwendbar
- §§ 130, 30 OWiG finden keine Anwendung, d.h. wir brauchen keine nachgewiesene schuldhaft Tat einer Leitungsperson



Geringe Anforderungen an Verhängung von Bußgeldern

LG Berlin (Deutsche Wohnen), Februar 2021

- Bußgeld gegen ein Unternehmen, in dem keine schuldhaft Tat einer Leitungsperson bewiesen wurde, wurde für unwirksam erklärt
- Rechtsträgerprinzip ist anwendbar (Haftung muss an eine Handlung einer natürlichen Person angeknüpft sein)
- §§ 130, 30 OWiG bei DSGVO-Bußgeldern anwendbar



Hohe Anforderungen an Verhängung von Bußgeldern

VORABENTSCHEIDUNGERSUCHEN DES KAMMERGERICHTS BERLIN VOR DEM EUGH

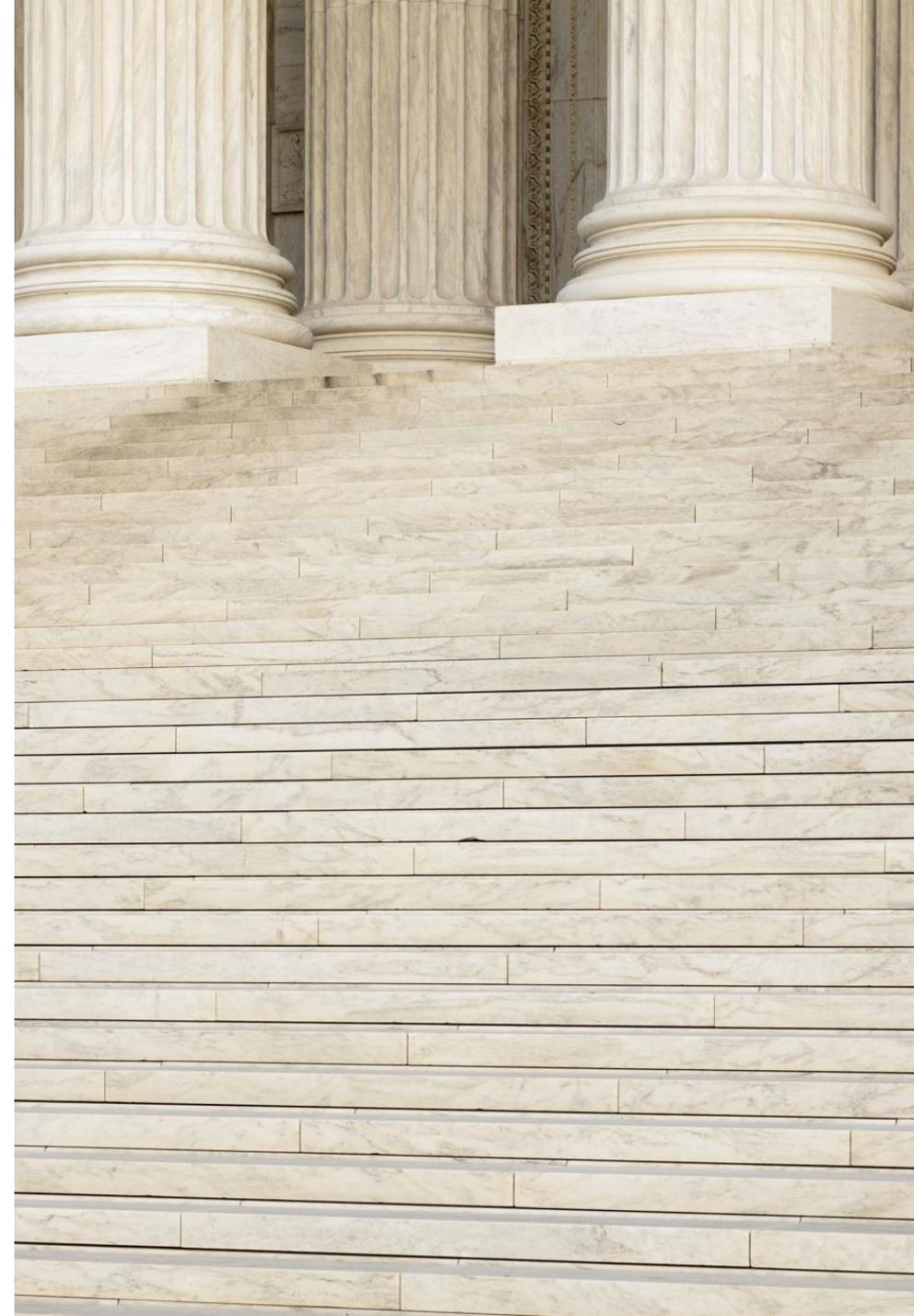
VORLAGEFRAGEN:

- kann gegen eine juristische Person eine Sanktion verhängt werden kann, ohne dass zuvor die Verantwortlichkeit einer natürlichen Person festgestellt wurde? (#Rechtsträgerprinzip);
- muss der geahndete Verstoß in jedem Fall vorsätzlich oder fahrlässig begangen worden sein? Oder reicht ein rein objektiver Verstoß gegen eine Verpflichtung aus?



SCHLUSSANTRÄGE DES GENERALANWALTS VOM 27.4.2023

- Juristische Personen als Adressaten einer Sanktion nach der DSGVO?:
 - Wegen eines Verstoßes gegen die DSGVO können Sanktionen unmittelbar gegen eine juristische Person als Täterin verhängt werden
- Erforderlichkeit, den Verstoß einer natürlichen Person zuzurechnen?
 - „Verhängung einer Geldbuße gegen Verantwortlichen ist nicht von der vorherigen Feststellung eines Verstoßes durch eine natürliche Person, die im Dienst des Verantwortlichen steht, abhängig“



SCHLUSSANTRÄGE (1) KANN JURISTISCHE PERSON ADRESSAT EINER SANKTION NACH DSGVO SEIN?

- „obviously!“

SCHLUSSANTRÄGE (2): MUSS EIN VERSTOß VON EINER LEITUNGSPERSON BEGANGEN WORDEN SEIN?

- Nein, auch wenn die Verstöße von natürlichen Personen begangen wurden, die im Rahmen der unternehmerischen Tätigkeit des Unternehmens unter Aufsicht der Leitungspersonen gehandelt haben
- Es ist auch nicht erforderlich, dass vor der Verhängung einer Sanktion gegen eine juristische Person ein Verfahren gegen eine natürliche Person durchgeführt wird.

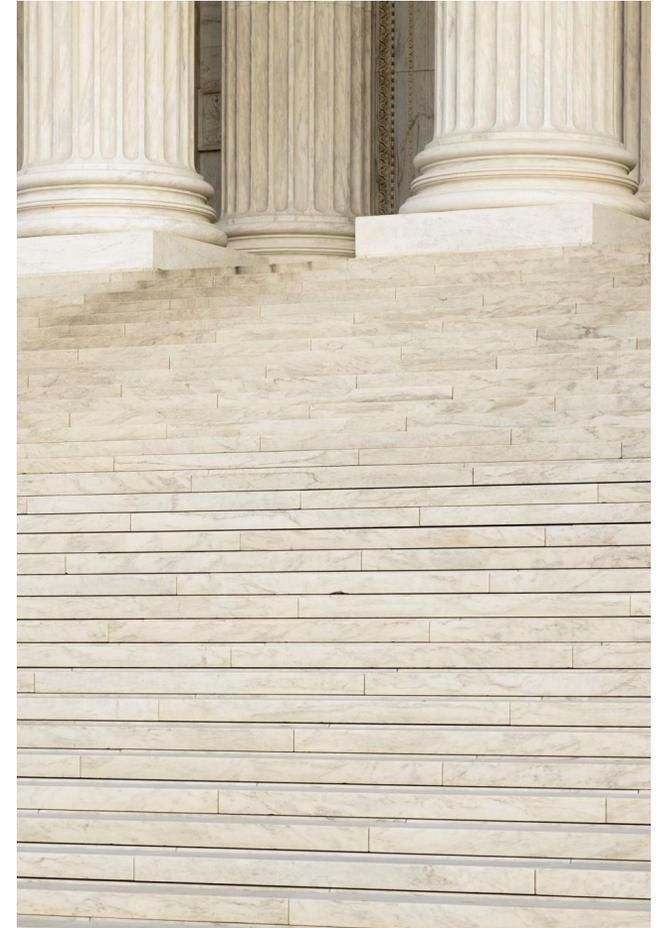


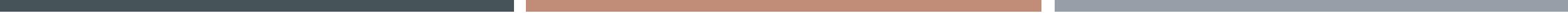
SCHLUSSANTRÄGE (3): SCHULDHAFTER VERSTOß ODER „STRICT LIABILITY“?

- Muss das Unternehmen nach Art. 83 Abs. 4 bis 6 DSGVO den durch einen Mitarbeiter vermittelten Verstoß schuldhaft begangen haben? Oder reicht für eine Bebußung des Unternehmens im Grundsatz bereits ein ihm zuzuordnender objektiver Pflichtenverstoß aus (,strict liability‘)“?
- Art. 83 DSGVO spricht **gegen ein System der objektiven (verschuldensunabhängigen) Verantwortlichkeit im Bereich von Sanktionen, d. h., er setzt Vorsatz oder Fahrlässigkeit bei der strafbaren Handlung voraus.** Aber wie sind die Anforderungen an „Fahrlässigkeit“ und Vorsatz“?



DIE ENTSCHEIDUNG DES EUGH?





**WAS IST AUS PRAKTISCHER SICHT NOCH ZU
BEDENKEN?**



BUßGELD KOMMT SELTEN ALLEIN...

Bußgeld

Presseerklärung,
Reputationsschäden

Anordnung, Daten zu löschen oder
eine Verarbeitung zu stoppen

Erhöhtes Risiko für
Schadensersatzklagen

EUGH, ÖSTERREICHISCHE POST C-300/21, 4.5.2023: SCHADENSERSATZ WEGEN EINER DATENSCHUTZVERLETZUNG

Ein bloßer Verstoß gegen die DSGVO begründet nicht schon allein einen Schadensersatzanspruch

- Ein Schaden muss tatsächlich entstanden sind (eine bestimmte „Erheblichkeit“ muss aber nicht erreicht werden (?))
- Es muss einen Kausalzusammenhang zwischen dem Schaden und dem Verstoß geben.
- Höhe des Schadensersatzanspruchs → dürfte sich nach den nationalen Vorschriften der EU Staaten richten

WAS MACHE ICH, WENN BUßGELD DROHT?



1. Ruhe bewahren



2. Anwaltsteam-Aufstellen (mit Strafrechtlern)



3. Umfassend bewerten:

die Rechtslage
und drohende Konsequenzen (Bußgeld? Presseerklärung?)



4. Verteidigungslinie definieren (Strategie & Taktik)

Kommt ein Deal in Frage?



5. Aus dem Vorfall lernen

Vielen Dank!



Margo Steiner
Group Chief Data Privacy Officer,
CompuGroup Medical

margo.steiner@cgm.com