INFOLAW
WWW.INFOLAW.AT

DORDA

Cybersecurity-Vorfall – und jetzt?

Folgen, Risiken und Tipps aus der Praxis

8.5.2025

Nino Tlapak

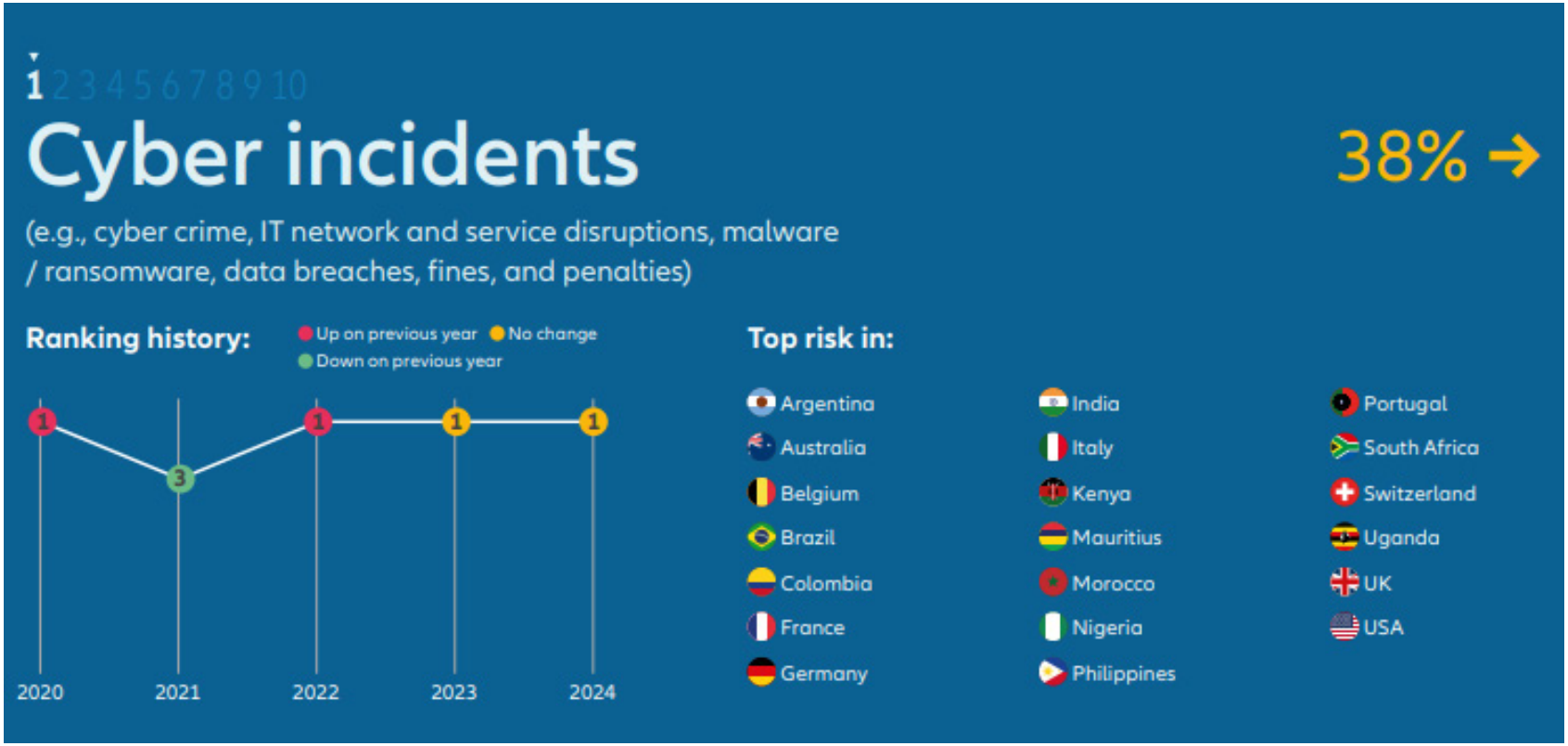
Partner and Co-Head des Datenschutz-Teams

- Universität Wien, Mag iur 2012
- Universität Wien, Universitätslehrgang Medien- und Informationsrecht, LL.M. (IT-Law) 2013
- Fachliche Schwerpunkte: Datenschutz, Cybersecurity, IT-Verträge mit Schwerpunkt auf Outsourcing und Cloud-Verträge
- ILO Clients Choice Award für Blockchain 2022-2025
- Empfohlen als Next Generation Partner im Bereich TMT und Data Privacy im renommierten internationalen Handbuch "Legal 500" sowie in Band 2 bzw 3 in "Chambers Europe"
- PrivacyConnect Co-Chair Vienna
- Vortragender für Datenschutz bei Master-Lehrgängen an der Universität Wien, Wirtschaftsuniversität, FH Technikum Wien und FH Campus Wien sowie Donau Universität Krems
- Regelmäßiger Vortragender bei einschlägigen Konferenzen und Tagungen (ITechLaw; Privacy Symposium etc)
- Mitglied der Interessensgemeinschaften "www.it-law.at" und "Privacyofficers.at"

Nino Tlapak

nino.tlapak@dorda.at

Dauerbrenner Cybersecurity



Quelle: Allianz Risk Barometer 2025
https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2025.pdf

Dauerbrenner Cybersecurity

Top 10 risks for Large-size companies*

*>US$500mn annual revenue

Source: Allianz Commercial

Figures represent how often a risk was selected as a percentage of all responses for that company size

Respondents: 1,747

Figures don't add up to 100% as up to three risks could be selected

NEW New entry in the top 10 risks

1 Macroeconomic developments ranks higher than new technologies based on the actual number of responses.

2 New technologies ranks higher than market developments based on the actual number of responses.

Rank		Percent	2024 rank	Trend
1	Cyber incidents *(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)*	43%	*1 (41%)*	→
2	Business interruption *(incl. supply chain disruption)*	36%	*2 (36%)*	→
3	Natural catastrophes *(e.g., storm, flood, earthquake, wildfire, extreme weather events)*	32%	*3 (26%)*	→
4	Changes in legislation and regulation *(e.g., new directives, protectionism, environmental, social, and governance, and sustainability requirements)*	23%	*5 (20%)*	↑
5	Climate change *(e.g., physical, operational and financial risks as a result of global warming)*	19%	*4 (23%)*	↓
6	Fire, explosion	17%	*7 (17%)*	↑
7	Political risks and violence *(e.g., political i terrorism, coup d'état, civil unrest, strikes,*			
8	Macroeconomic developments *(e.g., infla monetary policies, austerity programs)*[1]			
9	New technologies *(e.g., risk impact of arti connected / autonomous machines)*[2]			
10	Market developments *(e.g., intensified co entrants, M&A, market stagnation, marke*			

Top 10 risks for Smaller companies*

*<US$100mn annual revenue

Source: Allianz Commercial

Figures represent how often a risk was selected as a percentage of all responses for that company size

Respondents: 1,095

Figures don't add up to 100% as up to three risks could be selected

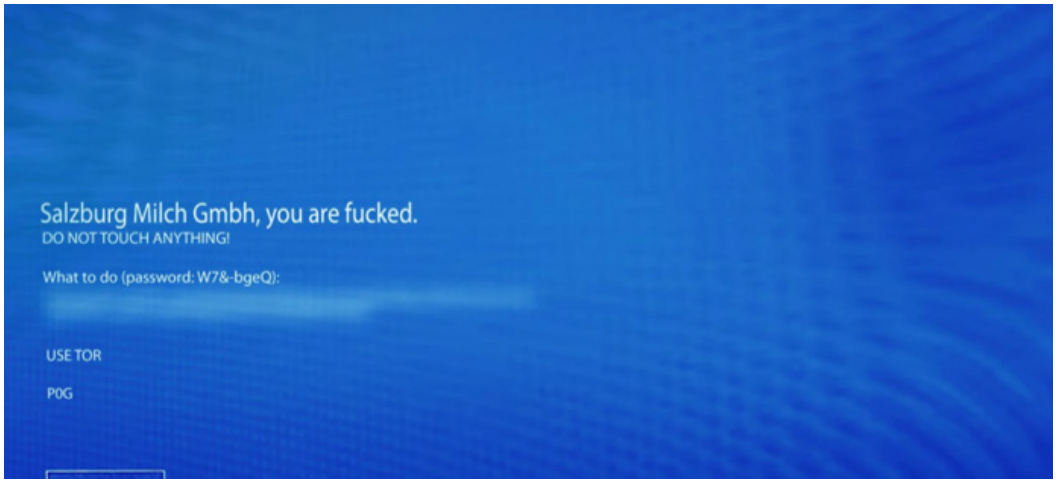
1 Macroeconomic developments ranks higher than climate change based on the actual number of responses.

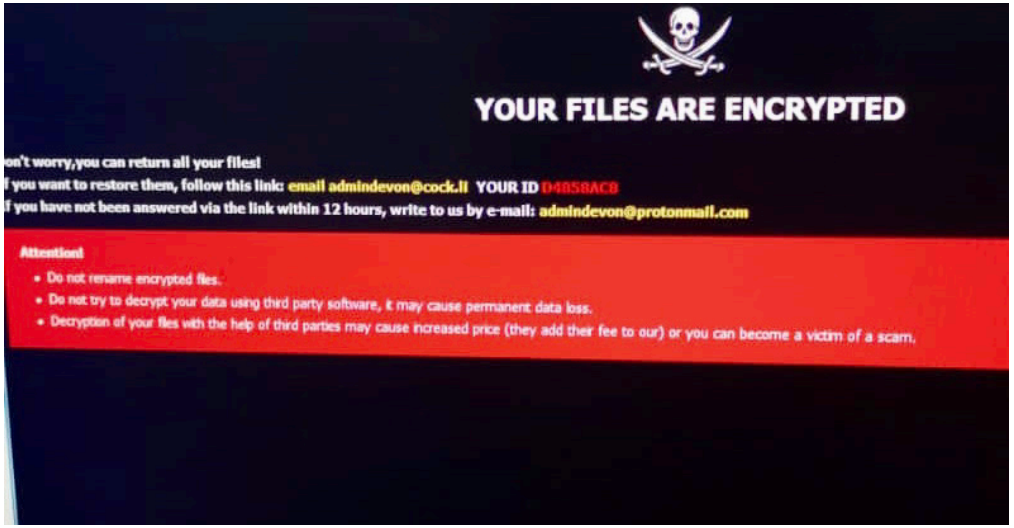
Rank		Percent	2024 rank	Trend
1	Cyber incidents *(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)*	35%	*1 (32%)*	→
2	Changes in legislation and regulation *(e.g., new directives, protectionism, environmental, social, and governance, and sustainability requirements)*	28%	*5 (21%)*	↑
3	Business interruption *(incl. supply chain disruption)*	26%	*3 (23%)*	→
4	Natural catastrophes *(e.g., storm, flood, earthquake, wildfire, extreme weather events)*	25%	*2 (24%)*	↓
5	Macroeconomic developments *(e.g., inflation, deflation, monetary policies, austerity programs)*[1]	18%	*4 (23%)*	↓
6	Climate change *(e.g., physical, operational and financial risks as a result of global warming)*	18%	*9 (13%)*	↑
7	Market developments *(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation)*	17%	*7 (16%)*	→
8	Fire, explosion	15%	*6 (20%)*	↓
9	Shortage of skilled workforce	13%	*8 (16%)*	↓
10	Political risks and violence *(e.g., political instability, war, terrorism, coup d'état, civil unrest, strikes, riots, looting)*	11%	NEW	↑

Quelle: Allianz Risk Barometer 2025
https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2025.pdf

1. Der Anlassfall ist eingetreten…

Der Anlassfall ist eingetreten: **Ransomware-Attacke**





Richtiges Verhalten

1. Erstmoment

- Erpressernachricht vorhanden?
- Ultimatum definiert?
- Reaktionszeit/Restzeit

2. Status erheben

- Welche Systeme sind betroffen bzw globaler Ausfall?
- Auswirkungen auf das Business?
- Definierte Verfahrensabläufe (Krisenstab/Ablauf-dokumentation) abrufen

3. Externe Transparenz?

- Website betroffen?
- E-Mailverkehr betroffen?
- Schnittstellensysteme betroffen (Bestellsysteme/Serviceportale/ etc)?
- VOIP Telefonie betroffen?

Richtiges Verhalten

4. Decisions

- Wird externe Unterstützung benötigt (Krisenmanagement, Recht, IT)?
- Können in den Fristen erste Schritte eingeleitet werden (Datenverlust, Loganalyse, etc)?
- Wer übernimmt eventuelle Verhandlungen mit dem Erpresser (extern/intern und wie)?
- Kryptowährungskonto bzw Erfahrungen im Umgang vorhanden?

5. Meldungen / ext Kommunikation

- Meldung innerhalb der Frist, aber mit ausreichend Info an Behörden
- Anzeigen bei Behörden (LKA, BKA, FMA, etc)
- Externe Kommunikation an Partner, Lieferanten, Kunden, etc
- Versicherungsmeldung

6. Krisenstab / Recoveryteam

- Definition Krisenstab inkl kommerzieller Entscheidungsträger
- Definition Projektteam inkl eventueller externer Ressourcen/Partner
- Review und Finalisierung Recoveryplan inkl Priorisierung und Timeline

Richtiges Verhalten

7. Dokumentation

- Dokumentationen festhalten
- Vier Augen Kontrolle bei kritischen Systemen

8. Abnahme/ Betriebsübergabe

- IT übergibt jedes finale System wie sonst an Businessowner

9. Lessons Learned

- Nacharbeiten Ablaufpläne/erweitern
- Erweiterung der Lieferantenkreise
- Verträge für Businesspartner im Standby

Lessons Learned aus der Praxis

Vorbereitende Maßnahmen

- Krisenplan erstellen & testen
- Klare Zuständigkeiten & Berichtswege
- Schulungen & Sensibilisierungsmaßnahmen
- Handordner mit Kontakten und Plänen

Ad-hoc-Maßnahmen

- rasche Faktenerhebung
- schnelle Umsetzung der Notfall-Maßnahmen
- laufende Dokumentation
- fundierte, aber schnelle Entscheidungen

2. Meldepflichten

Achtung:
ggfs mehrere Meldepflichten parallel zu erfüllen!

NIS2: Erheblicher Cybersicherheitsvorfall	DSGVO: Data Breach	DORA: Schwerwiegende IKT-bezogene Vorfälle bei Dienstleistern für Finanzunternehmen	Kursverfall wg Cybervorfall
an CSIRT/Cyber-sicherheits-behörde	an DSB	an Finanz-UN, welches wiederum an FMA zu melden hat	ggfs Meldung gem AktG

DSGVO: **Berichtspflichten** bei Data Breach

- Data Breach birgt Risiken für die Betroffenen ➔ **Frist 72h**

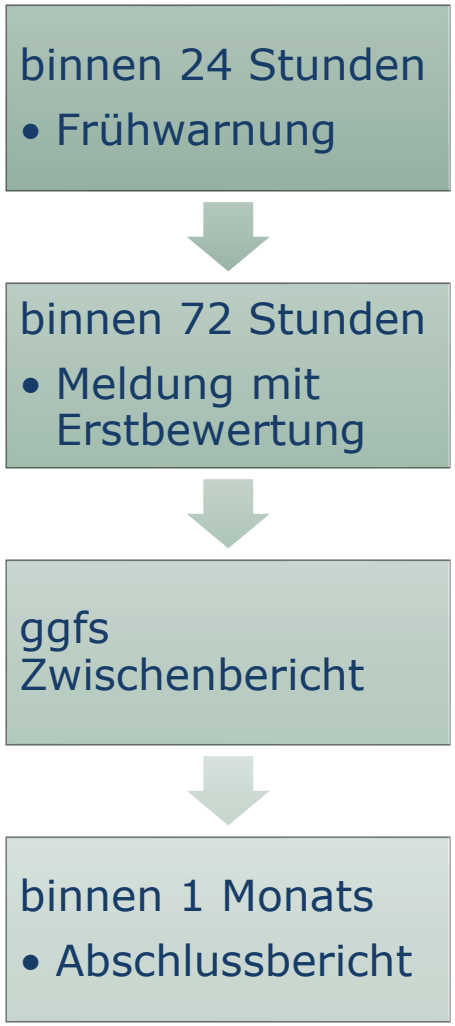
- **Kritieren**:
  - Art der Verletzung (zB unbefugte Offenlegung, Verlust)
  - Art, Sensibilität und Umfang der Daten
  - Möglichkeit, die Betroffenen zu identifizieren
  - Schwere und Wahrscheinlichkeit der drohenden Konsequenzen
  - Besonders schutzwürdige Betroffene?
  - Anzahl der Betroffenen

- Für alle Data Breaches: **interne Dokumentation**

- **on-top Benachrichtigung der Betroffenen** bei hohem Risiko
  - jedenfalls bei drohenden Schäden oder wenn Betroffene selbst Maßnahmen setzen müssen

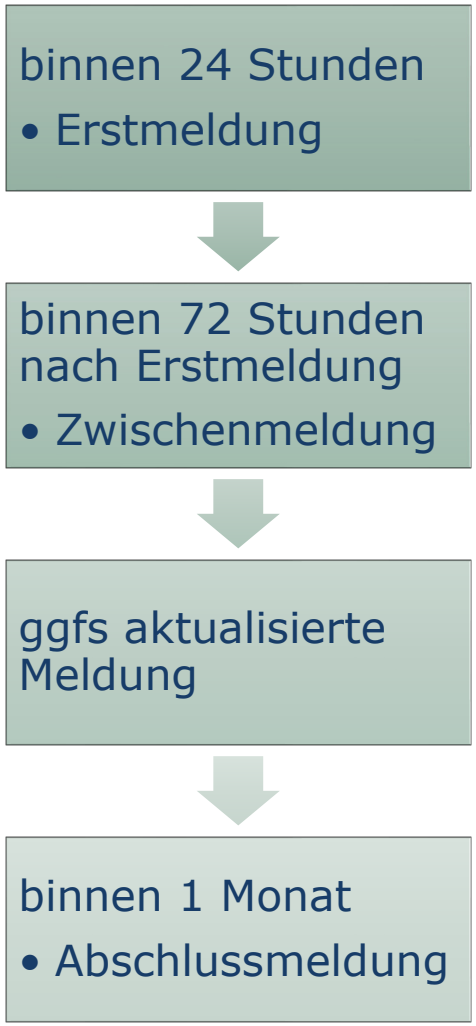
NIS 2-RL / NISG 2024: **Berichtspflichten** für erhebliche Cybersicherheitsvorfälle

- (drohende) schwerwiegende Betriebsstörung oder finanzielle Verluste oder erhebliche materielle/immaterielle Schäden
- **Kritieren**:
  - Ausmaß der Abhängigkeit
  - mögliche Auswirkungen auf Umwelt, öffentliche Ordnung/Sicherheit/Gesundheit
  - Marktanteil
  - betroffenes geografisches Gebiet
- **auch des Diensteempfängers** bei erheblicher Beeinträchtigung



DORA: **Berichtspflichten** für schwerwiegende IKT-bezogene Vorfälle

- Detaillierte Regelung, wann ein Vorfall schwerwiegend ist
- **Kriterien**:
  - Anzahl und/oder Relevanz der Kunden
  - Dauer
  - geografische Ausbreitung
  - die mit dem Vorfall verbundenen Verfügbarkeits-, Authentizitäts-, Integritäts- oder Vertraulichkeitsverluste von Daten
  - Kritikalität der betroffenen Dienste
  - wirtschaftliche Auswirkungen
- **auch der Kunden** bei Auswirkungen auf deren finanziellen Interessen



Ausblick: Cyber Resilience Act (CRA)

Cybersicherheitsanforderungen für Produkte mit digitalen Elementen

grds anwendbar ab dem 11.12.2027

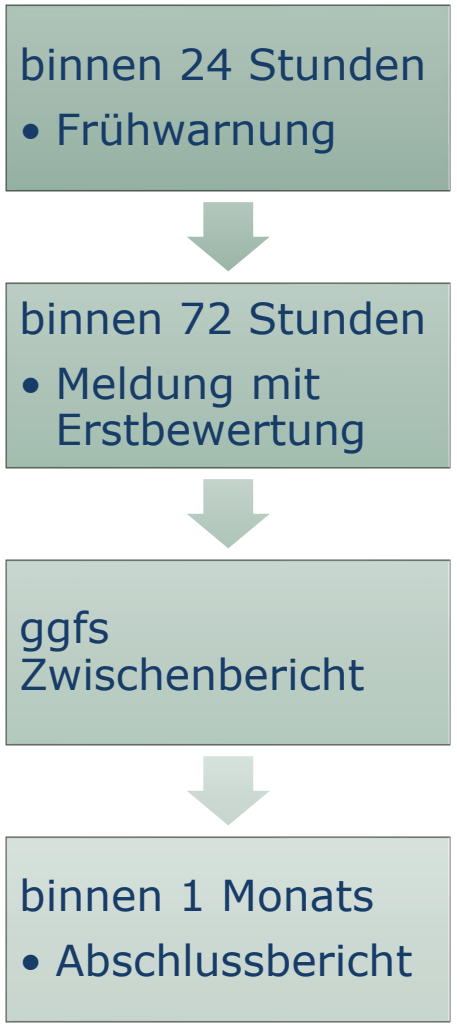
ABER: Art 14 CRA (Meldepflichten) bereits ab dem **11.9.2026**

CRA: **Berichtspflichten** für schwerwiegende Sicherheitsvorfälle

- schwerwiegende Sicherheitsvorfälle, die sich auf die Sicherheit von Produkten mit digitalen Elementen auswirken

- **Kriterien**:
  - Negative Auswirkung auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von sensiblen oder wichtigen Daten oder Funktionen; oder
  - Möglichkeit der Ausführung von böswilligem Code

- **auch die Nutzer des Produkts**



3. Geldbußen / Schadenersatz ?

Geldbußen: DSGVO, NIS2 und DORA

Verhängung von **Geldbußen grds direkt gg jP**

DSGVO	NIS2	DORA
• bis zu EUR 20 Mio / 4% des weltweiten Jahresumsatzes	• je nach Unternehmensgröße bis EUR 10 Mio oder EUR 7 Mio bzw 2% oder 1,4% des weltweiten Jahresumsatzes	• bis zu EUR 500.000 bzw 1% des Jahresumsatzes
gem **Deutsche Wohnen-Rsp** des EuGH C-807/21 genügt Verstoß durch irgendeinen Mitarbeiter; Zurechnung zu Leitungsorgan nicht mehr erforderlich	subsidiär zu Strafen nach der DSGVO, wenn dem Verstoß dasselbe Verhalten zu Grunde liegt	Strafen auch gegen Verantwortliche (§ 9 VStG) möglich

DSGVO Strafen bei Cyberattacken

British Airways

- Vorfall: über 425.000 Kundendaten wurden gestohlen
- Höhe: GBP 20 Mio
- Grund: angemessene Sicherheitsmaßnahmen hätten den Vorfall verhindert

Marriott Hotels

- Vorfall: 339 Mio Gästedaten wurden aufgrund lange bestehender Sicherheitslücken gestohlen
- Höhe: GBP 18.4 Mio
- Grund: keine angemessene Analyse möglicher Sicherheitslücken beim Erwerb der Starwood-Kette

Ö: Soweit öffentlich bekannt noch keine Strafen bei Cyberattacken

Schadenersatz bei DSGVO-Verstoß:
Voraussetzungen

bloßer DSGVO Verstoß reicht **nicht** aus

EuGH 4.10.2024, C-200/23: **bloßer Kontrollverlust**, zusätzliche negative spürbare Auswirkung (konkreter Missbrauch) nicht nötig

EuGH 20.6.2024, C-590/22**:** **Befürchtung der Datenweitergabe** samt **negativen Folgen**, Beweis der tatsächlichen Weitergabe nicht erforderlich

Beweislastverteilung

EuGH 25.1.2024, C-687/21: **Verstoß + Schaden + Kausalität** müssen vom Betroffenen bewiesen werden

EuGH 11.4.2024, C-741/21: **Fehler eines Mitarbeiters** führt nicht zum Entfall der Haftung

Schadenersatz bei DSGVO-Verstoß:
Umfang

nur **ausgleichende, keine strafende Funktion**

EuGH 4.11.2024, C-507/23: Schwere des Verstoßes + etwaiger Vorsatz (dh Haltung/Beweggründe) bei Bestimmung der Höhe **nicht relevant**

EuGH 25.1.2024, C-687/21: nur vollständiger Ausgleich des Schadens steht zu, **aber nicht mehr**

Immaterielle Schäden

EuGH 20.6.2024, C-182/22 und C-189/22: Ersatz immaterieller Schäden nicht auf Fälle **nicht** auf Fälle von **Identitätsdiebstahl oder –betrug beschränkt**

EuGH 4.11.2024, C-507/23: **Entschuldigung** kann als Ersatz ausreichend sein

Immaterieller Schadenersatz bei Hackerangriff
(EuGH 14.12.2023, C-340/21)

- **Cyberangriff** auf IT-Systeme einer bulgarischen Behörde: Offenlegung der Daten von Millionen Bürgern online
- Voraussetzungen für **immateriellen Schadenersatz**:

1. Schaden

- Angst/Befürchtung einer zukünftigen missbräuchlichen Verwendung personenbezogener Daten grds ausreichend

2. DSGVO-Verstoß

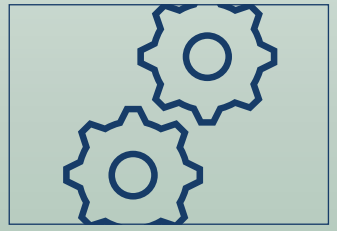
- Rechenschaftspflicht **Verantwortlicher** (auch EuGH C-687/21)
  - für Geeignetheit der Sicherheitsmaßnahmen
  - bloße Tatsache eines Cyberangriffs aber noch keine ausreichende Begründung für ungeeignete Sicherheitsmaßnahmen (nur Indiz)

3. Kausalzusammenhang zwischen Schaden und Verstoß

- Rechenschaftspflicht **Verantwortlicher**
  - keine Zurechenbarkeit des schadensverursachenden DSGVO-Verstoßes (auch EuGH C-667/21)

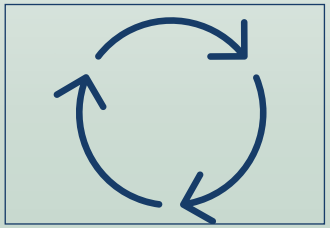
Fazit und To do's

- Verantwortlicher kann sich freibeweisen, aber nur mit **hohen Hürden**

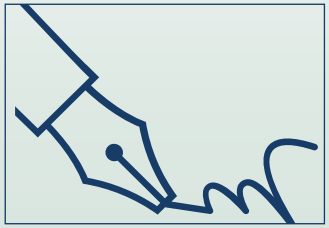


risikoangemessene geeignete technische und organisatorische Sicherheitsmaßnahmen

- Kriterien: Stand der Technik; Implementierungskosten; Art, Umfang und Zwecke der Verarbeitung; Höhe und Eintrittswahrscheinlichkeit des Risikos



Regelmäßige Evaluierung und ggfs Ergänzung/Anpassung



Dokumentation!

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

Mag Nino Tlapak, LLM

T: +43 1 533 47 95 – 23

nino.tlapak@dorda.at

Client Choice Award Lexology 2022-2025: Blockchain
TIER 1 Legal500 2007-2025: TMT
TIER 1 Legal500 2020-2025: Data Privacy & Data Protection
TIER 1 Legal500 2021-2025: Intellectual Property
BAND 1 Chambers Europe 2008-2025: TMT:IT
BAND 1 Chambers Europe 2025: TMT:Data Protection

DORDA Rechtsanwälte GmbH · Universitätsring 10 · 1010 Wien · www.dorda.at

The Legal 500 (2025)
Axel Anderl (TMT)
Hall of Fame

The Legal 500 (2025)
TMT
Tier 1

The Legal 500 (2025)
Data Privacy & Data Protection
Tier 1

Trend Anwaltsranking (2025)
Axel Anderl
Data Protection , IP and Media
Top 2 overall ranking

DORDA

Managing IP (2024)
Austrian Copyright & Design Firm of the Year

Austria Firm of the Year

Talent Management – Firm of the Year

Women in Business Law Awards Europe 2023

Client Choice winner
IT & Internet
Client Choice Awards 2025

Who's Who Legal (2025)
Axel Anderl (Data Privacy & Protection)
Thought Leader Global Elite

Chambers Europe (2025)
TMT:IT & TMT: Data Protection
Band 1

DORDA Rechtsanwälte GmbH · Universitätsring 10 · 1010 Wien · www.dorda.at