CLYDE&CO

Datenschutzrechtliches Risikomanagement bei Cyber-Angriffen

Jan Spittka, Rechtsanwalt und Partner, Clyde & Co Europe LLP

Vortragsreihe: Datenschutz in der Praxis, 30. Januar 2024

Cyber-Angriffe – ein globales Risiko

Cyber – Datenschutz und IT-Sicherheit

Datenschutzverstöße als „neue“ Risiken

PRESSEMITTEILUNG Nr. 191/23

Luxemburg, den 14. Dezember 2023

Urteil des Gerichtshofs in der Rechtssache C-340/21 | Natsionalna agentsia za prihodite

Cyberkriminalität: Die Befürchtung eines möglichen Missbrauchs personenbezogener Daten kann für sich genommen einen immateriellen Schaden darstellen

„*Jede Person, der wegen eines Verstoßes gegen* [die DSGVO] *ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.*“

„*Bei Verstößen gegen die folgenden Bestimmungen* [der DSGVO] *werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist: (…)*“

ESSEMITTEILUNG Nr. 184/23

Luxemburg, den 5. Dezember 2023

Urteile des Gerichtshofs in den Rechtssachen C-683/21 | Nacionalinis visuomenės sveikatos centras und C-807/21 | Deutsche Wohnen

Nur ein schuldhafter Verstoß gegen die Datenschutz-Grundverordnung kann zur Verhängung einer Geldbuße führen

Gehört der Adressat der Geldbuße zu einem Konzern, bemisst sich die Geldbuße nach dem Jahresumsatz des Konzerns

Agenda

- Aktuelle Bedrohungslage
- Datenschutzrecht & Cyber-Angriffe
- Sanktionen & Schadenersatz
- Fazit

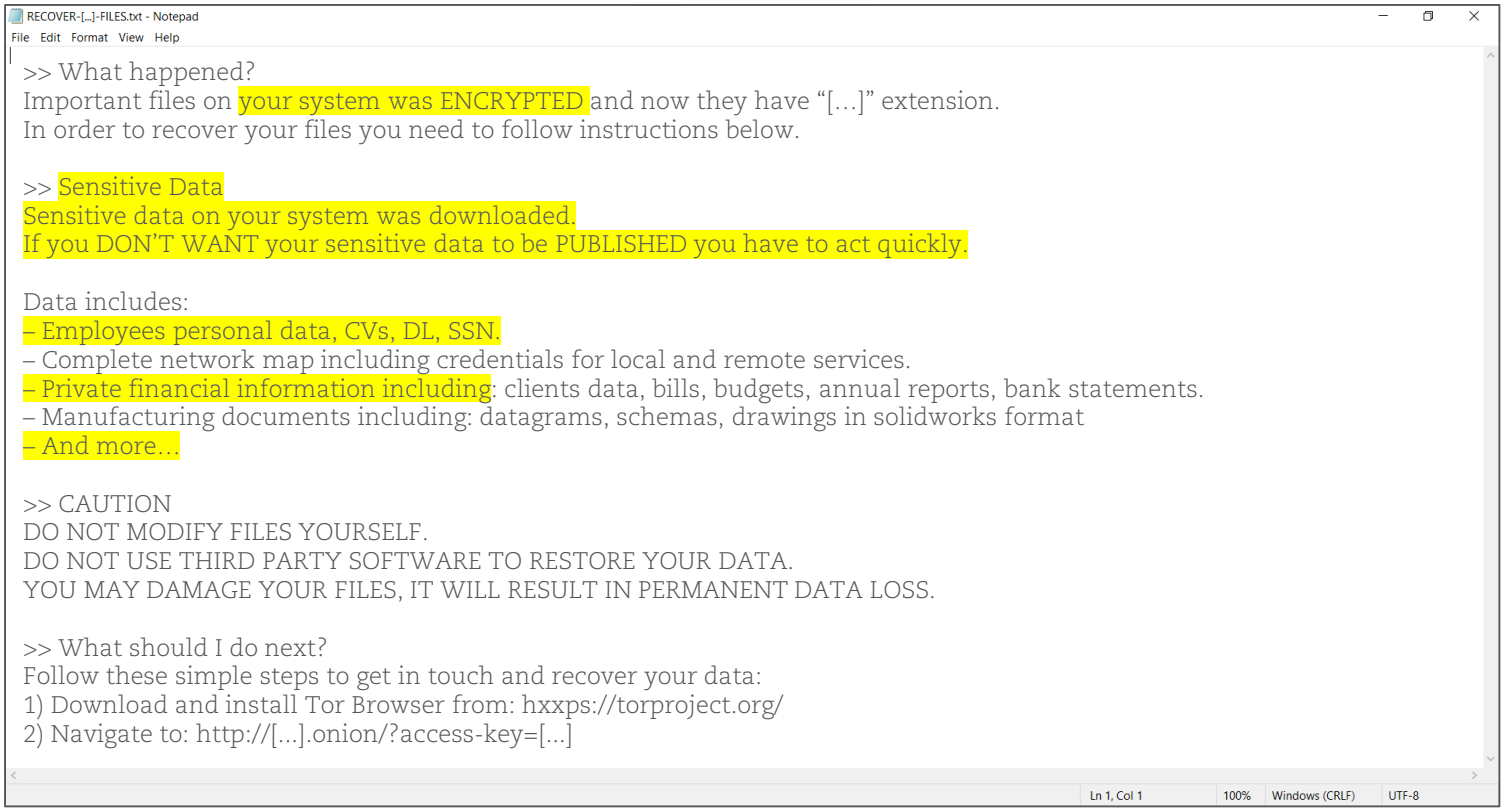
Aktuelle Bedrohungslage

Important files on your system was ENCRYPTED.

Sensitive data on your system was DOWNLOADED.

To recover your files and prevent publishing of sensitive information follow instructions in “$RECOVER-[...]-FILES" file.

Wie sieht eine **Ransom Note** aus?


RECOVER-[...]-FILES.txt - Notepad

File Edit Format View Help

>> What happened?
Important files on your system was ENCRYPTED and now they have "[...]" extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data
Sensitive data on your system was downloaded.
If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.

Data includes:
– Employees personal data, CVs, DL, SSN.
– Complete network map including credentials for local and remote services.
– Private financial information including: clients data, bills, budgets, annual reports, bank statements.
– Manufacturing documents including: datagrams, schemas, drawings in solidworks format
– And more...

>> CAUTION
DO NOT MODIFY FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

>> What should I do next?
Follow these simple steps to get in touch and recover your data:
1) Download and install Tor Browser from: hxxps://torproject.org/
2) Navigate to: http://[...].onion/?access-key=[...]

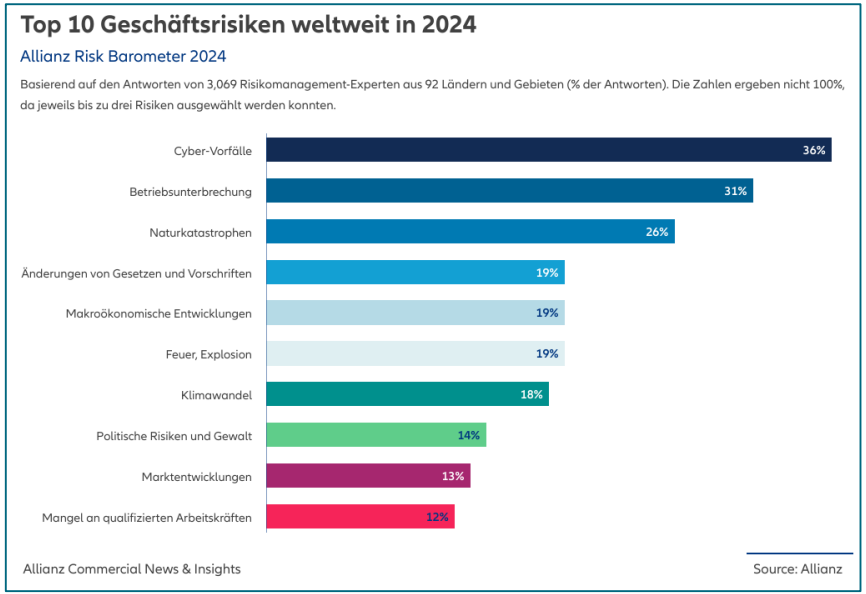
Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8

Aktuelle **Bedrohungslage**

#1

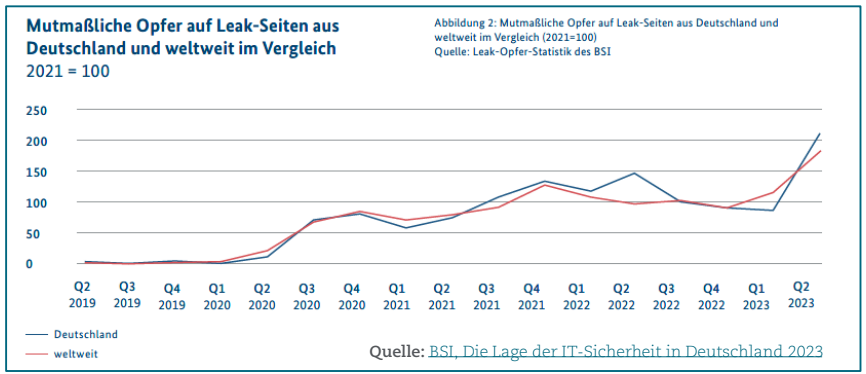
Größtes Geschäftsrisiko

Cyberangriffe bleiben im dritten Jahr in Folge das Top-Risiko für Unternehmen, erstmals mit deutlichem Abstand.



Angriffe nehmen weiter zu

Die Anzahl der Opfer auf Leak-Seiten nimmt weltweit zu, womit sich erneut ein Trend aus dem Vorjahr bestätigt.

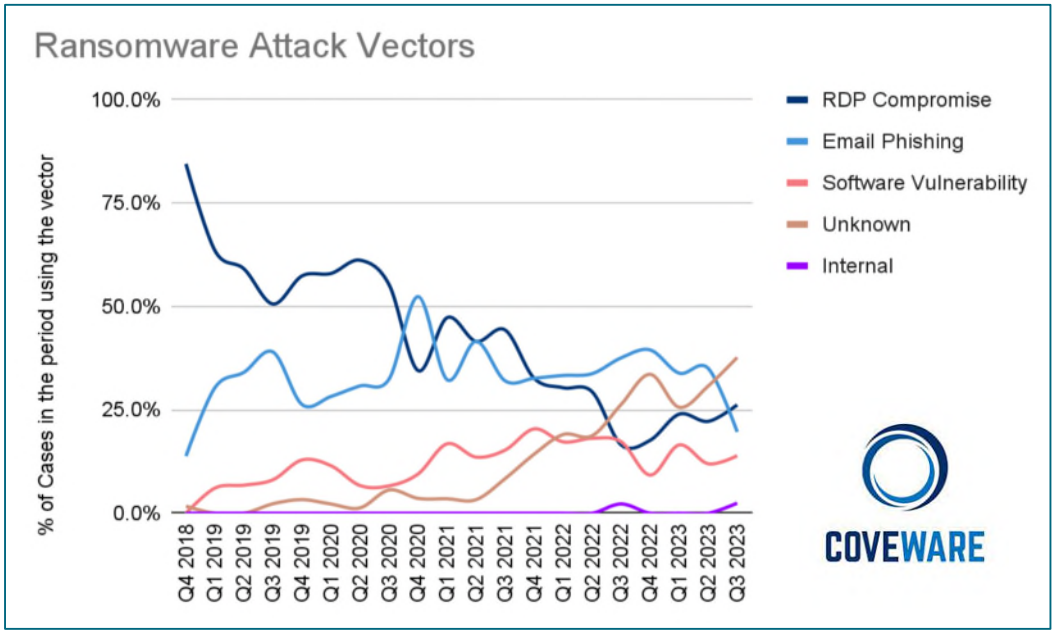


Praxistipp: Erhöhte Aufmerksamkeit bei Dienstleistern in USA & Frankreich

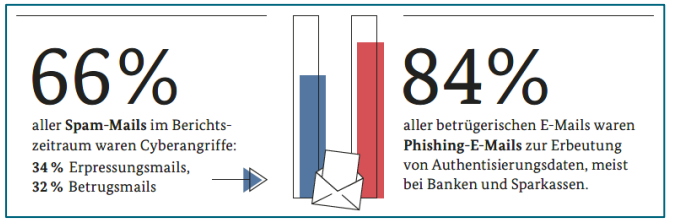
Aktuelle **Bedrohungslage**

#2 **Phishing** bleibt Dauerbrenner

Trotz neuer Angriffsmethoden bleibt Phishing auch 2024 unter den Top-Angriffsmethoden.



Quelle: Coveware, Quarterly Report 3/2023



Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland 2023

Langschläfer

Angriffsvektoren sind schwerer zu ermitteln, weil Angreifer länger in den Systemen bleiben und ihre Spuren besser verwischen.

Praxistipp: Dauer der Logfiles erhöhen

Aktuelle **Bedrohungslage**

#3

... auch **MFA** kann Phishing und den **Risikofaktor Mensch** nicht zuverlässig verhindern.

Anbieter von Phishing-as-a-Service (PhaaS) können MFA umgehen und so weiter in Systeme eindringen.

Praxistipp:
Echte Datenschutz-schulungen mit Mehrwert

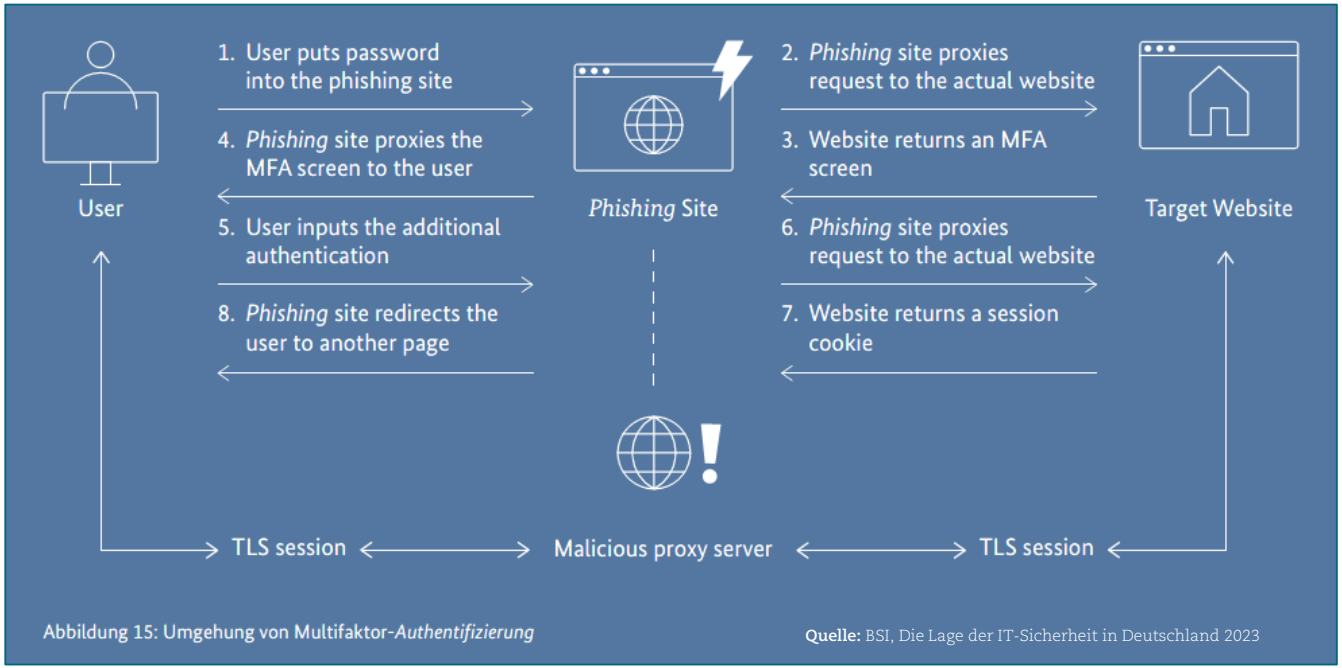


Abbildung 15: Umgehung von Multifaktor-*Authentifizierung*

Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland 2023

Aktuelle **Bedrohungslage**

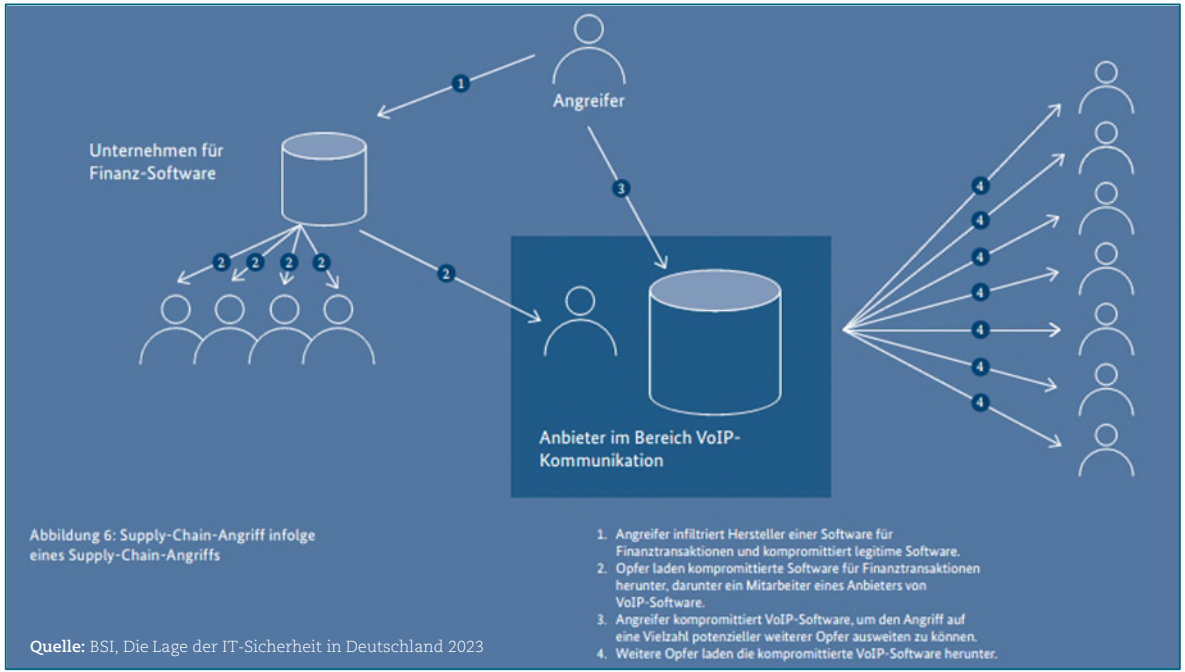


Abbildung 6: Supply-Chain-Angriff infolge eines Supply-Chain-Angriffs

1. Angreifer infiltriert Hersteller einer Software für Finanztransaktionen und kompromittiert legitime Software.
2. Opfer laden kompromittierte Software für Finanztransaktionen herunter, darunter ein Mitarbeiter eines Anbieters von VoIP-Software.
3. Angreifer kompromittiert VoIP-Software, um den Angriff auf eine Vielzahl potenzieller weiterer Opfer ausweiten zu können.
4. Weitere Opfer laden die kompromittierte VoIP-Software herunter.

Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland 2023

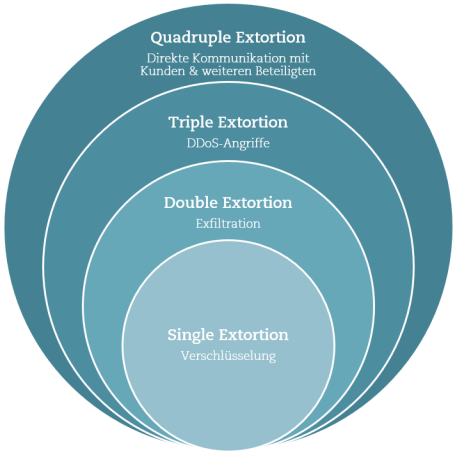
#4

Supply-Chain-Attacken werden weiter zunehmen

Auch Sicherheitsprozesse werden ausgelagert, weshalb Supply-Chain-Angriffe weiter zunehmen werden.

Praxistipp:
Dokumentation der TOMs & Löschkonzepte der Dienstleister

Aktuelle **Bedrohungslage**



#5

Angreifer werden auch in 2024 **neue Strategien** entwickeln…

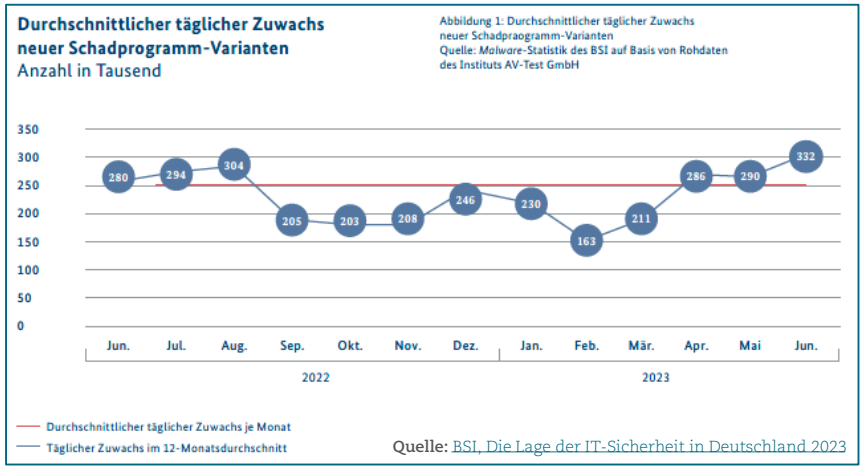
TECHNOLOGY > CYBERSECURITY | November 16, 2023

BlackCat hacks company, reports victim to SEC

The Russian ransomware gang has complained to the regulator that MeridianLink failed to disclose the cybersecurity incident in good time.

… und mit **künstlicher Intelligenz** verbessern.

Angreifer maximieren ihre Gewinne mit KI-basierten Angriffsmethoden, wie Deepfakes und Voice Cloning. Klassische Schadsoftware wird mittels KI-basierter Tools „verbessert“ werden.

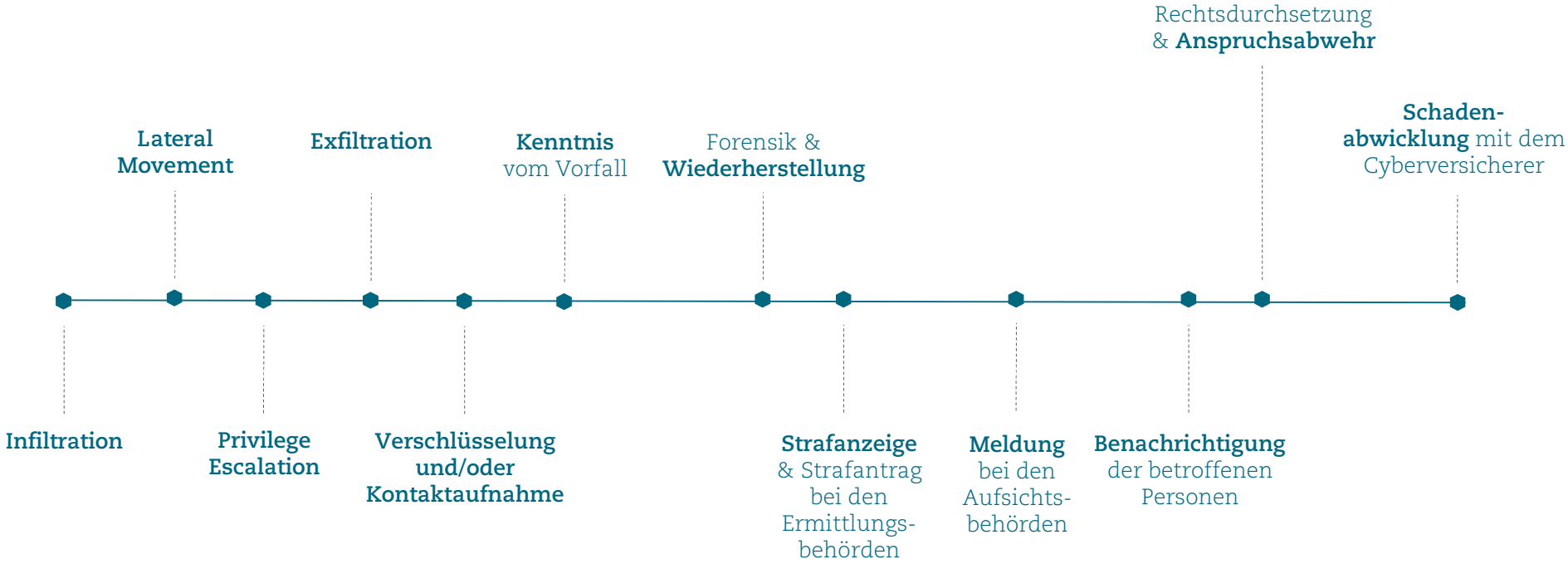


Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland 2023

Datenschutzrecht & Cyber-Angriffe

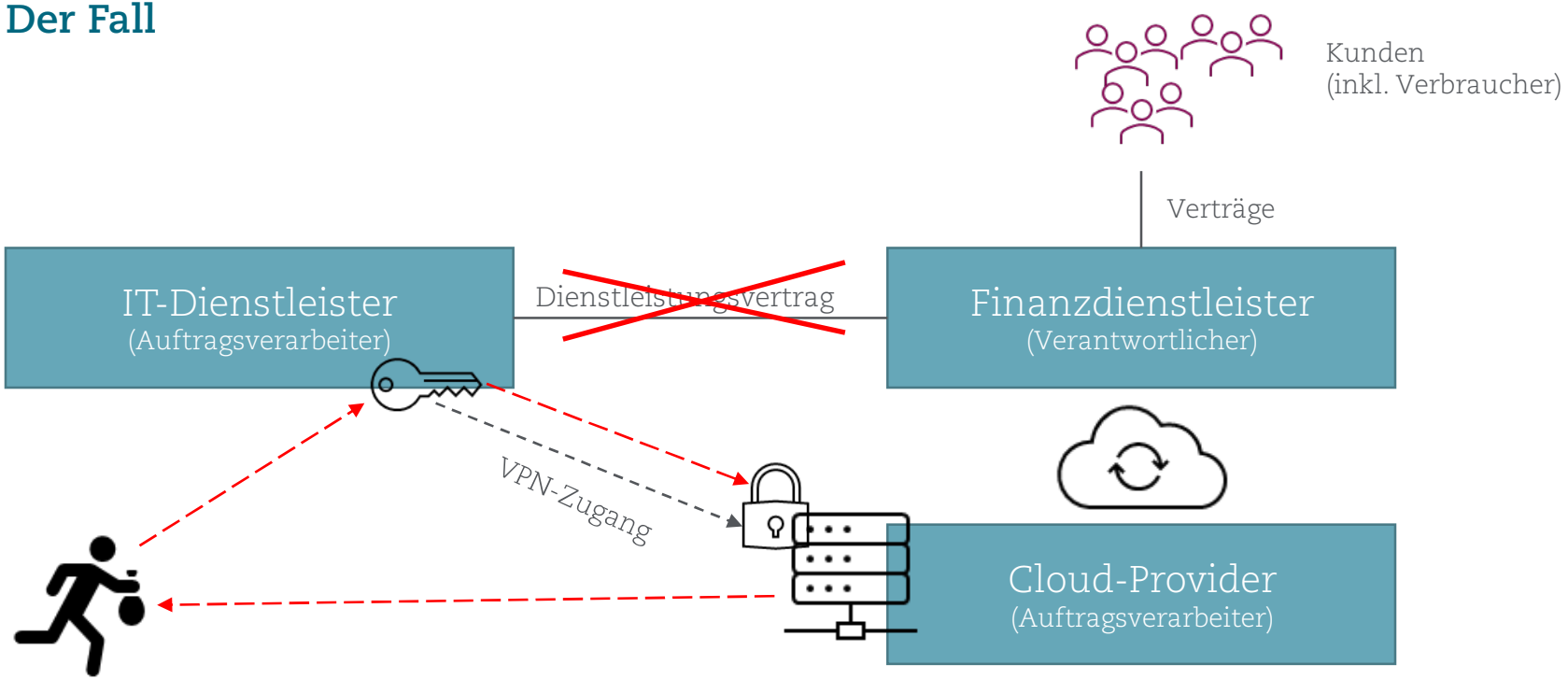
Wie läuft ein Data Breach in der Praxis ab?

Typischer Ablauf



Datenschutzrecht & Cyber-Angriffe

Der Fall



Datenschutzrecht & Cyber-Angriffe

Meldung von Datenschutzvorfällen und Störungen der Infrastruktur

§ Gesetzlich			Vertraglich & deliktisch			Sofern zweckdienlich	
Datenschutz-aufsichtsbehörden	Betroffene Personen	Bundesbehörden & weitere Rechts- bzw. Fachaufsichten	Versicherer (& Ermittlungs-behörden)	Geschäftspartner		Sonstige Beteiligte	Öffentlichkeit
Art. 33 DSGVO § 65 BDSG (§ 33 KDG)	Art. 34 DSGVO § 66 BDSG (§ 34 KDG)	§ 8b IV BSIG § 168 TKG § 83a 1 SGB X Art. 19 Abs. 2 eIDAS …	AVB der Versicherung	Datenschutz-vereinbarungen z.B. Ziff. 8.5 f. der Standardvertrags-klauseln (int.)	§ 241 Abs. 2 BGB § 242 BGB §§ 823 ff. BGB	Pressemitteilung oder sonstige Information zur Schadenminderung	

Datenschutzrecht & Cyber-Angriffe

Datenschutzrechtliche Melde- und Benachrichtigungspflichten

Verletzung **d**es **S**chutzes **p**ersonen**b**ezogener **D**aten
(*Personal Data Breach*)

„*eine* ***Verletzung der Sicherheit****, die, ob unbeabsichtigt oder unrechtmäßig, zur* ***Vernichtung****, zum* ***Verlust****, zur* ***Veränderung****, oder zur* ***unbefugten Offenlegung*** *von beziehungsweise zum* ***unbefugten Zugang*** *zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden*“

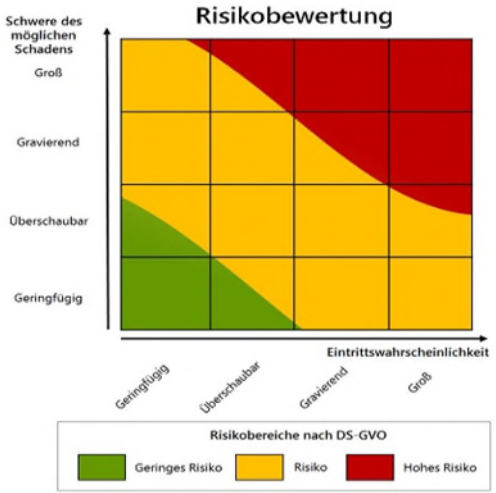
(Art. 4 Nr. 12 DSGVO)

Datenschutzrecht & Cyber-Angriffe

Datenschutzrechtliche Melde- und Benachrichtigungspflichten

Meldung an Datenschutzbehörde (Art. 33 DSGVO):

1. VdSpbD
2. Kein Ausschluss, dass voraussichtlich Risiko für die Rechte und Freiheiten natürlicher Personen
3. Frist: Unverzüglich, Begründungspflicht nach 72 Stunden
4. Möglichkeit der Nachmeldung
5. Dokumentationspflicht



https://www.lda.bayern.de/de/risiko.html

Benachrichtigung betroffener Personen (Art. 34 DSGVO):

1. VdSpbD
2. Voraussichtlich hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen
3. Kein Ausschluss nach Art. 34 Abs. 3 lit. a) oder lit. b) DSGVO
4. Ggf. öffentliche Bekanntmachung oder eine ähnliche Maßnahme nach Art. 34 Abs. 3 lit. c) DSGVO
5. Frist: Unverzüglich

Geringes Risiko

- Bei einer Datenschutzverletzung ohne Risiko (z. B. harmloser Fehlversand innerhalb einer Organisation) muss die Datenschutzaufsichtsbehörde nicht informiert werden.
- Ein Verzeichnis der Verarbeitungstätigkeiten ist (unter Berücksichtigung anderer Faktoren wie z. B. unregelmäßige Verarbeitung) bei geringem Risiko nicht zu erstellen.

Risiko ("Normal")

Bei der Verarbeitung besonderer Arten
persone
Daten, i
als hoch
„normal
werden
Religion
Katholis
eines „S

Hohes Risiko

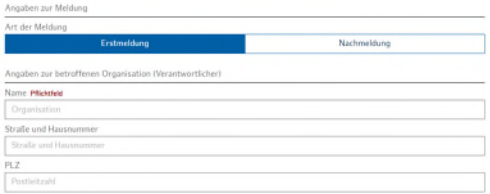
Ein hohes Risiko umfasst dagegen potentielle Schäden, deren Ausmaß für die Rechte und Freiheiten von Betroffenen gravierend und/oder ziemlich wahrscheinlich sind. Unter der DS-GVO wird dieses Risiko-Level im Verhältnis aller Verarbeitungen eher selten vorkommen. Da ein hohes Risiko aber wesentliche Rechtsfolgen für den Verantwortlichen hat, muss das mögliche Vorkommen eines hohen Risikos zwangsläufig im Blick behalten werden.

(85) Eine Verletzung des Schutzes personenbezogener Daten kann — wenn nicht rechtzeitig und angemessen reagiert wird — einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person. Deshalb sollte der Verantwortliche, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Aufsichtsbehörde von der Verletzung des Schutzes personenbezogener Daten unverzüglich und, falls möglich, binnen höchstens 72 Stunden, nachdem ihm die Verletzung bekannt wurde, unterrichten, es sei denn, der Verantwortliche kann im Einklang mit dem Grundsatz der Rechenschaftspflicht nachweisen, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt. Falls diese Benachrichtigung nicht binnen 72 Stunden erfolgen kann, sollten in ihr die Gründe für die Verzögerung angegeben werden müssen, und die Informationen können schrittweise ohne unangemessene weitere Verzögerung bereitgestellt werden.

(75) Die Risiken für die Rechte und Freiheiten natürlicher Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere — können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.

https://www.lda.bayern.de/de/risiko.html


dsb
Republik Österreich
Datenschutz behörde
КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV SLOVENSKEJ REPUBLIKY
Gegevensbeschermingsautoriteit
azop Agencija za zaštitu osobnih podataka
Úřad pro ochranu osobních údajů
ANS PDCP
Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Ανεξάρτητη εποπτική αρχή για την προστασία του ατόμου
DATATILSYNET
ANDMEKAITSE INSPEKTSIOON
CNPD
TIETOSUOJAVALTUUTETUN TOIMISTO
CNIL.
UODO
URZĄD OCHRONY DANYCH OSOBOWYCH
Nemzeti Adatvédelmi és Információszabadság Hatóság
An Coimisiún um Chosaint Sonraí Data Protection Commission
AUTORITEIT PERSOONSGEGEVENS
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
GPDP
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
Datu valsts inspekcija
VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA
CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES
idpc. INFORMATION AND DATA PROTECTION COMMISSIONER
IMY. Integritetsskydds myndigheten
aepd agencia española protección datos
INFORMACIJSKI POOBLAŠČENEC
+
Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg
Bayerisches Landesamt für Datenschutzaufsicht
Berliner Beauftragte für Datenschutz und Informationsfreiheit
TLfDI
Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD)
Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg
Landesbeauftragte für Datenschutz und Akteneinsicht
SACHSEN-ANHALT
Landesbeauftragter für den Datenschutz
Hamburg
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Freie Hansestadt Bremen
DIE LANDESBEAUFTRAGTE FÜR DATENSCHUTZ
Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern
BfDI
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Die Landesbeauftragte für den Datenschutz Niedersachsen
Datenschutzkonferenz
Der Hessische Beauftragte für Datenschutz und Informationsfreiheit
LDI NRW
UNABHÄNGIGES DATENSCHUTZZENTRUM SAARLAND
Der Landesbeauftragte für den DATENSCHUTZ und die INFORMATIONSFREIHEIT Rheinland-Pfalz
Sächsische Datenschutz- und Transparenzbeauftragte
ULD


Angaben zur Meldung

Art der Meldung

Erstmeldung | Nachmeldung

Angaben zur betroffenen Organisation (Verantwortlicher)

Name Pflichtfeld

Organisation

Straße und Hausnummer

Straße und Hausnummer

PLZ

Postleitzahl


Benachrichtigung (* = Pflichtangaben)

Art der Meldung *

Vollständige Neumeldung

Vorläufige Neumeldung (es erfolgt noch eine spätere ergänzende Meldung)

Ergänzende Meldung

1. Über den Meldenden

1.1 Kontaktdaten (* = Pflichtangaben)

Registerangaben: Registernummer (z.B. Handelsregister), Angabe des Gerichts

Ihre Registernummer, Ihr Registergericht

Umsatzsteuer-ID

Ihre Umsatzsteuer-ID

Name Ihrer Organisation (z.B. Firma, Verein) *

Name

Straße und Hausnummer *

Straße und Hausnummer der Organisation


1. Datenschutzverletzung melden (Schritt 1 von 2) →

2. Zusammenfassung (Schritt 2 von 2)

Datenschutzverletzung melden (für Verantwortliche) Angaben zu/zum Verantwortlichen

(Artikel 4 Nr. 7 DSGVO):

Name der/des Verantwortlichen

Anschrift

Telefon

E-Mail-Adresse


Meldung einer Verletzung des Schutzes personenbezogener Daten (Art. 33 DS-GVO)

Hinweise

1. Art der Meldung (Art. 33 Abs. 4)

Neumeldung

Ergänzende Meldung

Es stehen derzeit nicht alle Informationen zur Verfügung, eine ergänzende Meldung erfolgt voraussichtlich bis zum:

2. Verantwortlicher (Art. 4 Nr. 7)

Name

Straße

PLZ

Ort

Telefon

E-Mail

Art der Stelle

Bereich

Keine Angabe

Keine Angabe


MELDEFORMULAR

Angaben zum Verantwortlichen

Angaben zum Verantwortlichen

Nahmeschaftsbeauftragter

Zeitpunkt

Beschreibung

Folgen

Ergriffene Maßnahmen

Benachrichtigung der betroffenen Personen

Sonstiges

Organisation (Verantwortlicher nach DSGVO)

Kontakt

Straße Nr.

PLZ Stadt

An

Landesbeauftragte für Datenschutz Schleswig-Holstein

Holstenstraße 98

24103 Kiel

Ort, Datum

Meldung von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DSGVO oder § 41 LDSG

Sehr geehrte Damen und Herren,

hiermit melde ich Ihnen als Verantwortlicher nach DSGVO eine Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 Datenschutz-Grundverordnung (DSGVO)* / § 41 Landesdatenschutzgesetz (LDSG)*.

Angaben zur Meldung

Die Verletzung ist mir bekannt geworden am: <Datum und Uhrzeit>

Diese Meldung erfolgt binnen 72 Stunden nach Bekanntwerden: <ja / nein>

Falls nein:

<Begründung für die Verzögerung>

Name und Kontaktdaten der/des Datenschutzbeauftragten, ersatzweise einer sonstigen Anlaufstelle für weitere Informationen:

<Name und Kontaktdaten>


DER HESSISCHE BEAUFTRAGTE FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT

Meldung von Verletzungen des Schutzes personenbezogener Daten (Art. 33 DS-GVO/ § 65 BDSG i.V.m. § 500 StPO/ § 60 HDSIG)

1. Verantwortlicher (Art. 33 Abs. 1, Abs. 3 Buchst. b DS-GVO i. V. m. Art. 4 Nr. 7 DS-GVO/ § 65 Abs. 1, Abs. 3 Nr. 2 BDSG i.V.m. § 46 Nr. 7 BDSG/ § 60 Abs. 1, Abs. 3 Nr. 2 HDSIG i. V. m. § 41 Nr. 9 HDSIG)

Kontaktdaten

Bezeichnung bzw. Name der verantwortlichen Stelle:

Straße & Hausnummer:

Postleitzahl und Ort:

Allgemeine E-Mail-Adresse der verantwortlichen Stelle:

Klicken oder tippen Sie hier, um Text einzugeben.



Wo ist die Datenpanne passiert?

Name der verantwortlichen Stelle*

z.B. des Unternehmens, der Praxis, der Behörde, des Vereins

Straße und Hausnummer*

Postleitzahl*

Meldung einer Datenpanne

Allgemeine Informationen zur Verarbeitung personenbezogener Daten im Rahmen unseres Internetangebots entnehmen Sie bitte unserer Datenschutzerklärung.

Näheres zur Verarbeitung Ihrer personenbezogenen Daten entnehmen Sie bitte den Informationen nach Artikel 13 DS-GVO.

Sofern Sie nicht von dem mitgeteilten Sachverhalt betroffen sind, erhalten Sie i.d.R. keine Nachricht über das weitere Verfahren.

Angaben zur Organisation

Name/Institution*

Straße, Nr.*

Ort*

PLZ*

Website


Meldung einer Datenpanne durch Verantwortliche nach Artikel 33 DSGVO

Schritt 1 von 3

Schritt 1

Schritt 2

Schritt 3

Angaben zum Verantwortlichen

Name/Bezeichnung des Verantwortlichen*

Straße*

Hausnummer*

Postleitzahl*

Ort*

Name der Kontaktperson*


Hintergrund der Meldung

1. Art der Meldung (Pflichtfeld)

Vollständig | Vorläufig | Ergänzung

2. Bei Ergänzung: Datum der vorläufigen Meldung

(bitte auswählen)

Angaben zur verantwortlichen Organisation

3. Name der meldepflichtigen Stelle (Pflichtfeld)

(bitte ausfüllen)

4. Straße und Hausnummer der meldepflichtigen Stelle (Pflichtfeld)

(bitte ausfüllen)

5. Postleitzahl und Ort der meldepflichtigen Stelle (Pflichtfeld)

(bitte ausfüllen)

Mitteilende Behörde / öffentliche Stelle

Behörde / öffentliche Stelle

Behördenbezeichnung bzw. Name der öffentlichen Stelle

Vollständiger Name (bitte ohne Abkürzungen)

Straße & Hausnummer

Straße und Hausnr.

Postleitzahl und Ort

PLZ | Ort

Online-Service zur Meldung einer Datenschutzverletzung nach Art. 33 DS-GVO

Erläuterung zum Formular

Art der Meldung

Neumeldung

Folgemeldung

Um welchen Vorfall handelt es sich? *

Bitte wählen Sie eine Kategorie

MELDUNG EINER DATENPANNE

DURCH DEN VERANTWORTLICHEN

…H ART. 33 EU-DS-GVO (§ 51 BlnDSG)

I. WO IST DIE DATENPANNE PASSIERT?

	Feld	Text
1.	Name des Verantwortlichen	
2.	Straße und Hausnummer	
3.	PLZ	
4.	Ort	

Kontaktdaten des Meldenden

Name

Ihr Name

Straße und Hausnummer

Straße und Hausnummer

Postleitzahl

Postleitzahl

Ort

Ort

E-Mail-Adresse (Freiwillige Angabe)

E-Mail-Adresse

Bei welcher Organisation ist die Datenpanne passiert?

TLfDI Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit

Meldung von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 Datenschutz-Grundverordnung

1. Schritt: Angaben zum Verantwortlichen

Organisationsname

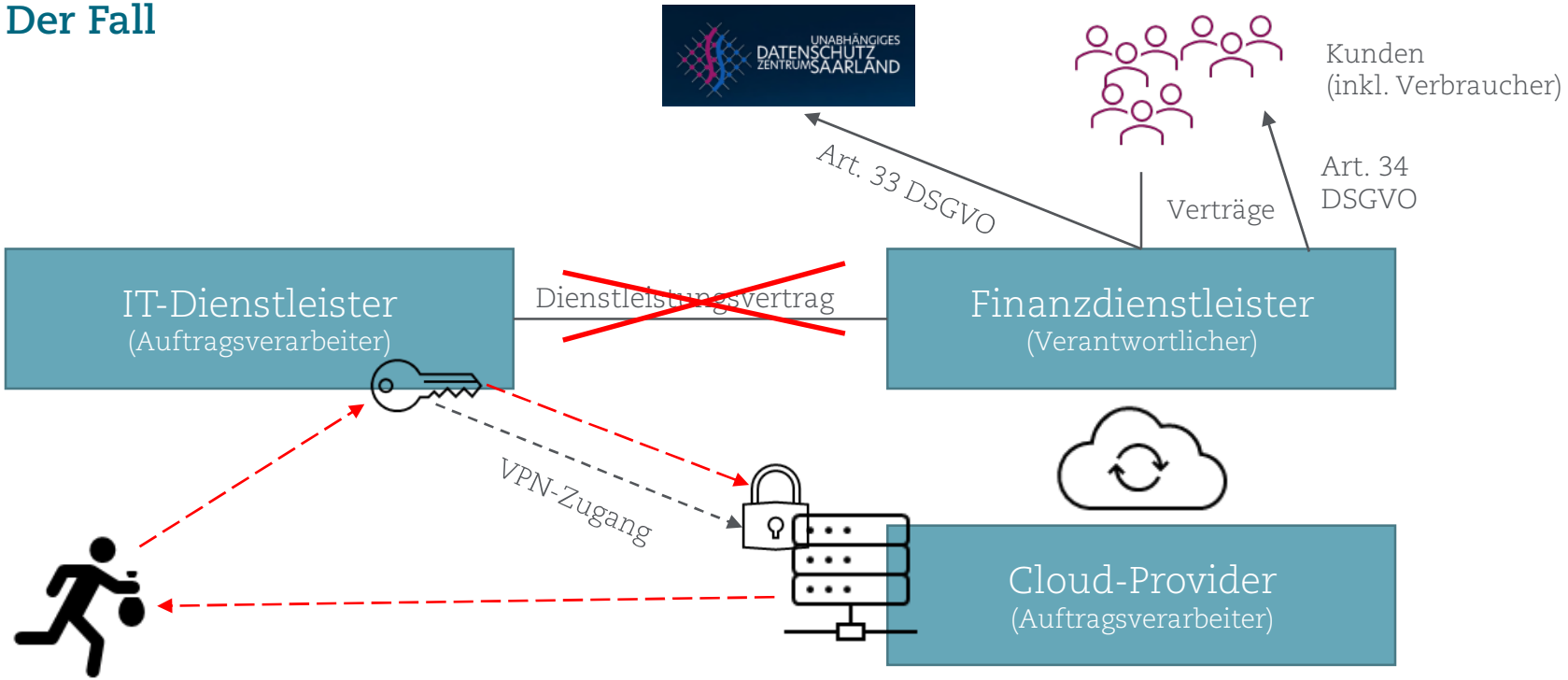
Vertretungsberechtigte

Straße und Hausnummer

PLZ/Ort

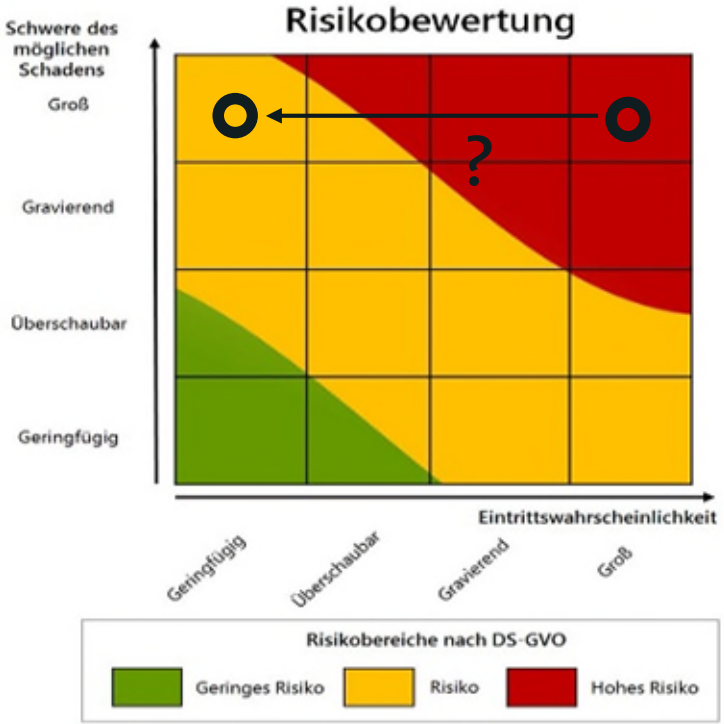
Datenschutzrecht & Cyber-Angriffe

Der Fall



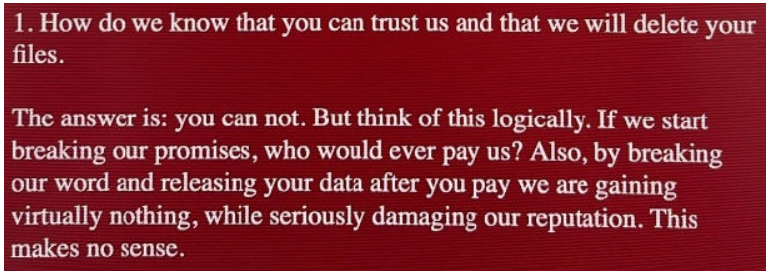
Datenschutzrecht & Cyber-Angriffe

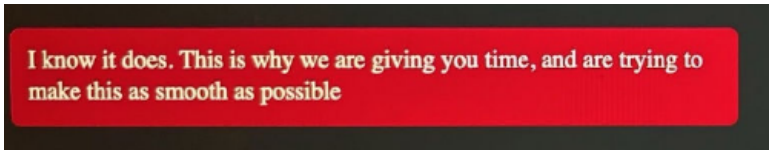
Lässt Lösegeldzahlung hohes Risiko entfallen?



Exkurs: Verhandlungen mit den Angreifern

How it started…

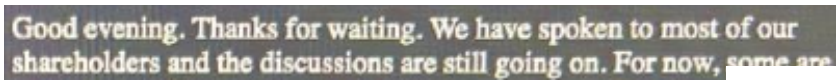




How it ended…

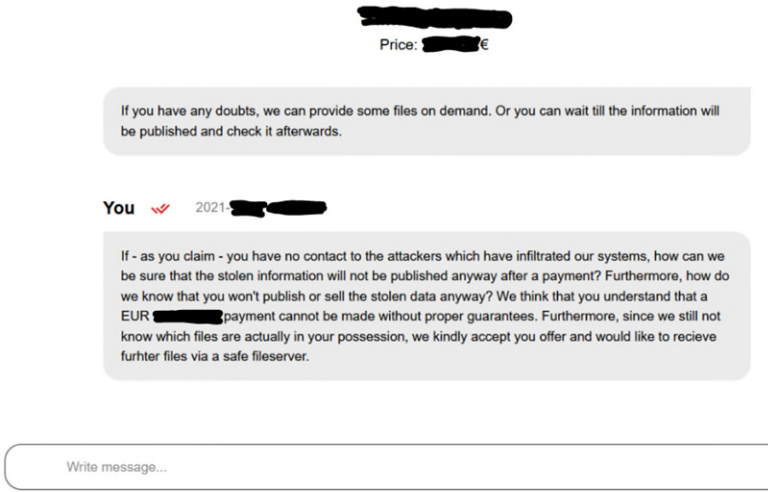
[Bitte um Zeit wg. interner Prozesse]

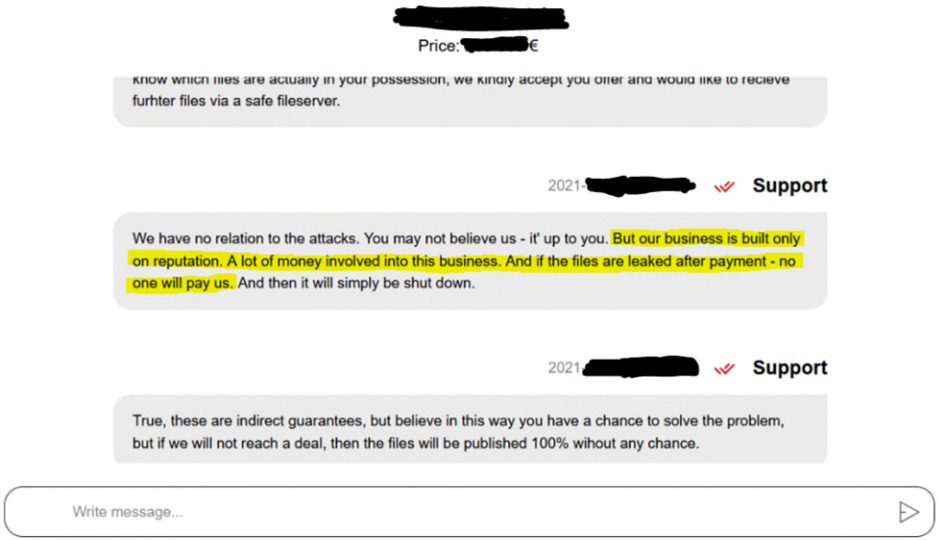
[Bitte um Zeit wg. Vorstandssitzung]



Datenschutzrecht & Cyber-Angriffe

Lässt Lösegeldzahlung hohes Risiko entfallen?





Herausforderungen und Strategien im Datenschutz- und Cybersecurity-Recht

Lässt Lösegeldzahlung hohes Risiko entfallen?

dsb
Republik Österreich
Datenschutzbehörde

Barichgasse 40-42
A-1030 Wien
Tel.: +43-1-52152 0

E-Mail: dsb@dsb.gv.at

GZ: [redacted]

Sachbearbeiterin: Mag. [redacted]

[redacted]
zH Mag. [redacted]

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde
(Art. 33 DSGVO, „Data-Breach-Verfahren")
[redacted]

Per E-Mail [redacted]

Betreff: Einstellung des Verfahrens

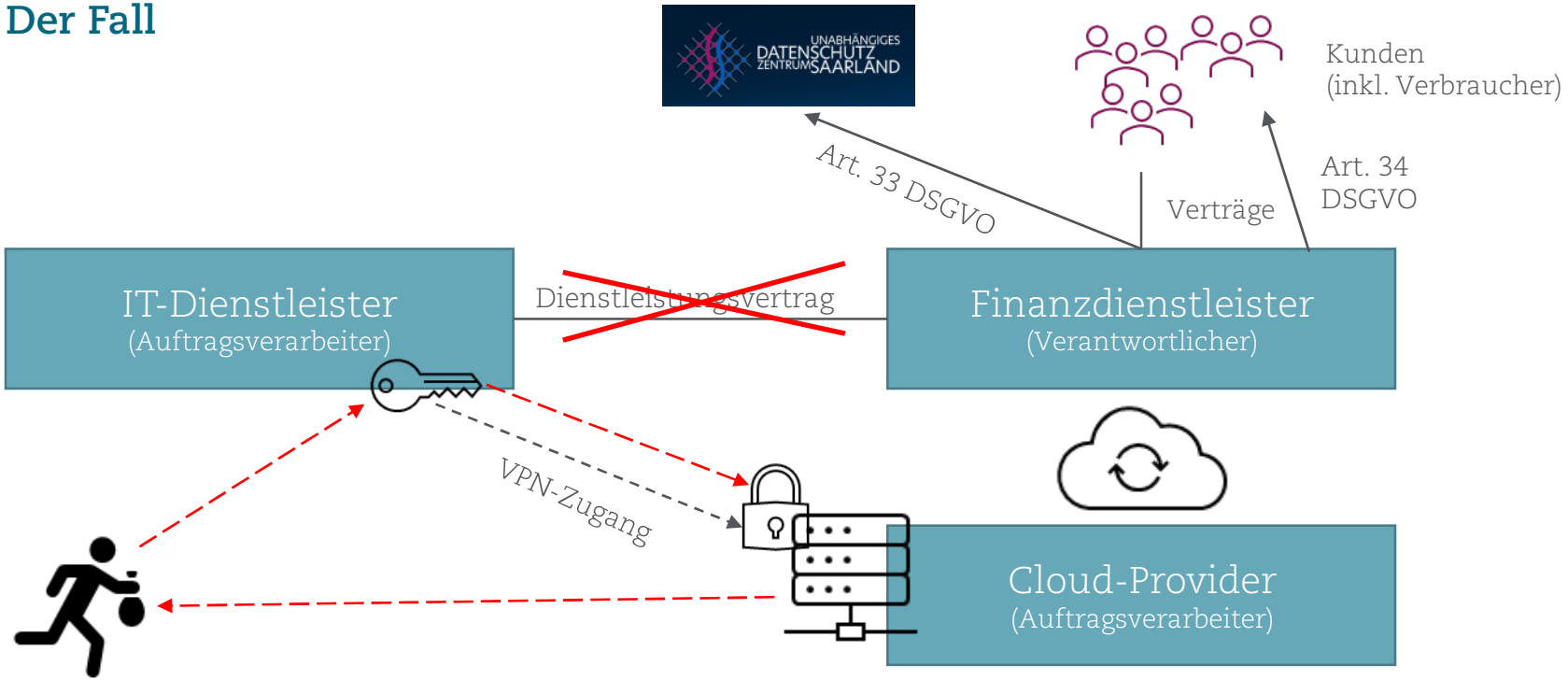
Die Verantwortliche hat geeignete Schritte unternommen, um das Risiko zu minimieren und um die nachteiligen Folgen der Sicherheitsverletzung, soweit möglich, zu beseitigen. Weitere Maßnahmen der Datenschutzbehörde iSd. Art 58 Abs. 2 lit. e DSGVO (Anweisung bzgl. Benachrichtigung der betroffenen Personen) bzw. § 22 Abs. 4 DSG (Mandatsbescheid bei Gefahr im Verzug) sind nicht geboten. Da die Angreifer ein Löschprotokoll übermittelten und somit die Betroffenen keinen Schaden erlitten, sind diese nicht zu benachrichtigen gewesen.

Das Verfahren wird daher beendet und dies der Verantwortlichen abschließend zur Kenntnis gebracht.

Sanktionen & Schadenersatz

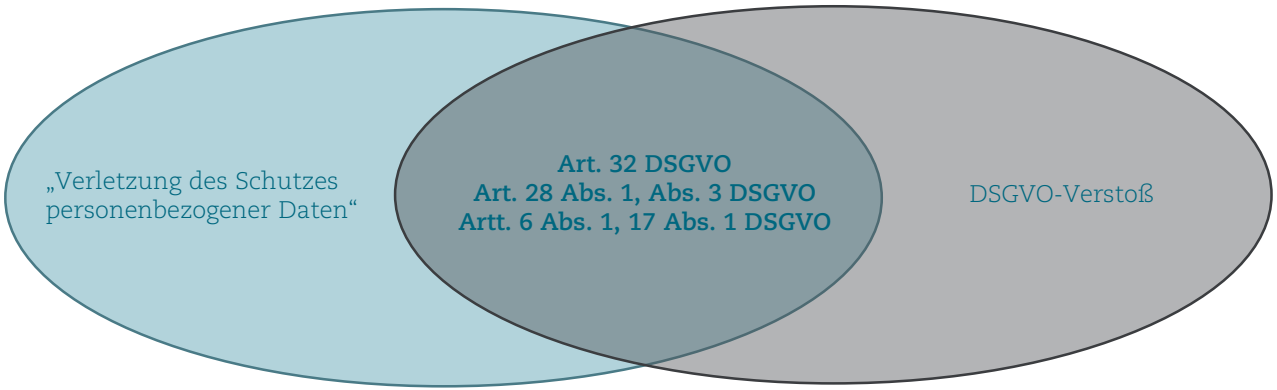
Sanktionen & Schadenersatz

Der Fall



Sanktionen & Schadenersatz

Cyber-Angriff = Datenschutzverstoß?



Sanktionen & Schadenersatz

Geldbußen

„*Bei Verstößen gegen die folgenden Bestimmungen* [der DSGVO] *werden im Einklang mit Absatz 2 Geldbußen von bis zu* **[10 000 000 EUR / 20 000 000 EUR]** *oder im Fall eines Unternehmens von bis zu* **[2 % / 4 %]** *seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist: (…)*“

PRESSEMITTEILUNG Nr. 184/23

Luxemburg, den 5. Dezember 2023

Urteile des Gerichtshofs in den Rechtssachen C-683/21 | Nacionalinis visuomenės sveikatos centras und C-807/21 | Deutsche Wohnen

Nur ein schuldhafter Verstoß gegen die Datenschutz-Grundverordnung kann zur Verhängung einer Geldbuße führen

Gehört der Adressat der Geldbuße zu einem Konzern, bemisst sich die Geldbuße nach dem Jahresumsatz des Konzerns

Sanktionen & Schadenersatz

Geldbußen – EuGH-Entscheidung Deutsche Wohnen (C-807/21)

- DSGVO-Geldbußen können direkt gegen juristische Personen verhängt werden; keine Zurechnung des Verstoßes über eine identifizierte natürliche Person notwendig;
- Verschulden erforderlich, aber:
  - Maßstab: keine Unklarheit über die Rechtswidrigkeit des Verhaltens;
  - Keine Handlung oder Kenntnis seitens des Leitungsorgans
- Konzernumsatz für Obergrenze

Sanktionen & Schadenersatz

Geldbußen – EuGH-Entscheidung Nacionalinis visuomenės sveikatos centras (C-683/21)

- DSGVO-Geldbußen können gegen den Verantwortlichen dann verhängt werden, wenn die rechtswidrige Verarbeitung durch einen Auftragsverarbeiter durchgeführt wird;
- Ausnahmen: Auftragsverarbeiter hat
  - personenbezogene Daten für eigene Zwecke verarbeitet;
  - diese Daten auf eine Weise verarbeitet hat, die nicht mit dem Rahmen oder den Modalitäten der Verarbeitung, wie sie vom Verantwortlichen festgelegt wurden, vereinbar ist;
  - Daten auf eine Weise verarbeitet, bei der vernünftigerweise nicht davon ausgegangen werden kann, dass der Verantwortliche ihr zugestimmt hätte

Sanktionen & Schadenersatz

Datenschutzverstöße bei Cyber-Angriff

„Art. 5 DSGVO

Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

(…)

(f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, ***einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung*** *und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“)“*

„Art. 32 DSGVO

Sicherheit der Verarbeitung

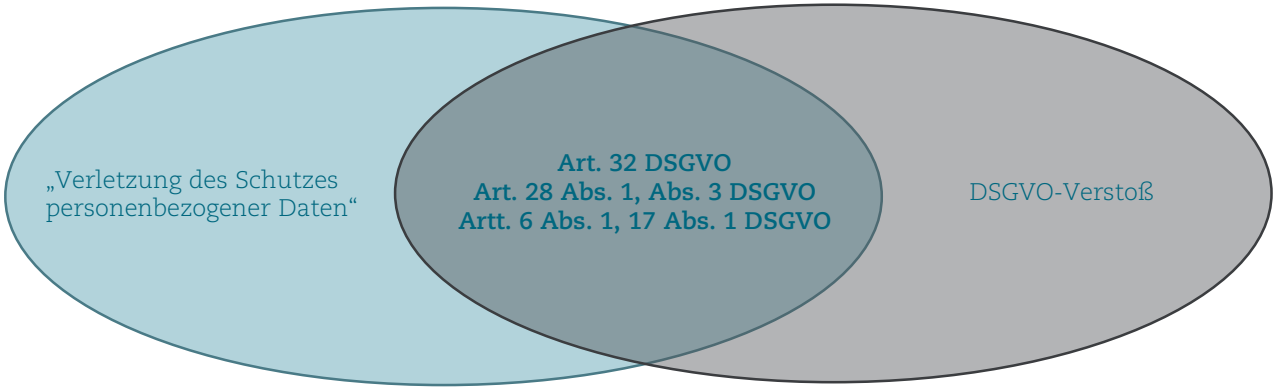
(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

(…)

(b) die Fähigkeit, die ***Vertraulichkeit****, Integrität, Verfügbarkeit und Belastbarkeit* ***der Systeme und Dienste*** *im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen“*

Sanktionen & Schadenersatz

Gelbuße nach Data Breach?



Bundesdatenschutzgesetz (BDSG)
§ 43 Bußgeldvorschriften

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

Bundesdatenschutzgesetz (BDSG)
§ 40 Aufsichtsbehörden der Länder

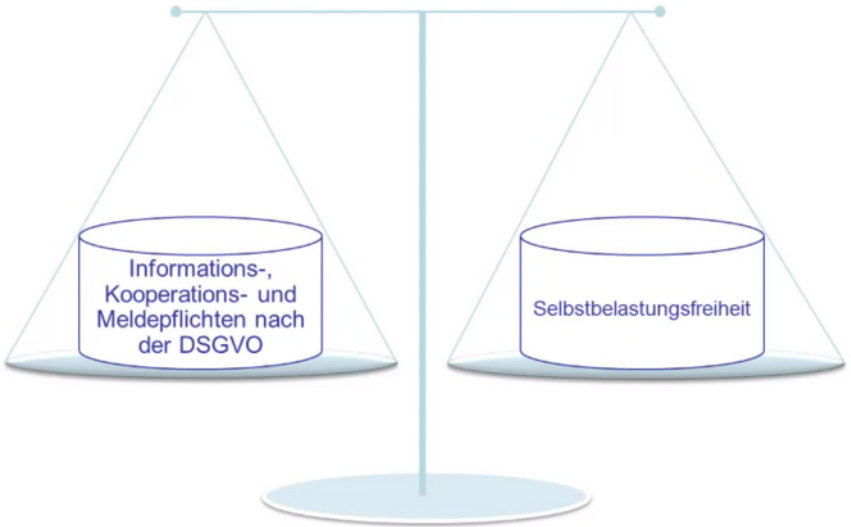
(4) Die der Aufsicht unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben einer Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Absatz 1 Nummer 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der Auskunftspflichtige ist darauf hinzuweisen.

Sanktionen & Schadenersatz

Gelbuße nach Data Breach?

„Inwieweit sich vor dem Hintergrund der genannten (bisherigen) verfassungsrechtlichen Herleitung auch juristische Personen wie die Antragstellerin auf den „nemo tenetur“ – Grundsatz berufen können, ist fraglich (bislang abgelehnt vom BVerfG, vgl. Beschluss vom 26.2.1997 – 1 BVR 2172/96, LS 2, Rn. 80 ff.). ***Nicht gänzlich ausgeschlossen scheint jedenfalls, den Grundsatz der Selbstbelastungsfreiheit (auch) aus dem Rechtsstaatsprinzip des Art. 20 Abs. 3 GG oder aus Art. 6 Abs. 1 EMRK bzw. Art. 47 Abs. 2 Satz 1 GRCh herzuleiten und auch juristischen Personen das Recht zur Auskunftsverweigerung in Fällen möglicher Selbstbelastung zuzubilligen*** *(vgl. Spittka, Si tacuisses … – nemo tenetur und die DSGVO, in: Traeger* [sic!]*, Die Macht der Daten und der Algorithmen, S. 141 (144 ff.)).“*

(OVG Schleswig, Beschl. v. 28.5.2021 – 4 MB 14/21)



Sanktionen & Schadenersatz

Datenschutzbehörden werden kreativ!

ULD

Ihre Mandantin [redacted]
Hinweis nach Art. 58 Abs. 1 Buchst. d Datenschutz-Grundverordnung - DSGVO
Meldung einer Verletzung des Schutzes personenbezogener Daten gem. Art. 33 Abs. 1 DSGVO
vom [redacted] 2022 / Ihr Zeichen [redacted]

Aus der vorliegenden Informationen ergibt sich jedoch, dass zuvor bei der Einführung neuer technischer und organisatorischer Maßnahmen zum Schutz der personenbezogenen Daten (hier: [redacted]) nicht alle Systeme einbezogen wurden. Es bestehen somit Anhaltspunkte dafür, dass geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, durch Ihre Mandantin nicht getroffen waren (Art. 32 Abs. 1 DSGVO).

Es ergeht somit folgender **Hinweis gem. Art. 58 Abs. 1 Buchst. b DSGVO**:

Die von dem Verantwortlichen [redacted] verarbeiteten personenbezogenen Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (Art. 5 Abs. 1 Buchst. f DSGVO).

Diese Maßnahmen schließen gem. Art. 32 Abs. 1 Buchst. f DSGVO gegebenenfalls unter anderem ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung ein.

Darüber hinaus wird das aufsichtsbehördliche Verfahren eingestellt.

Sanktionen & Schadenersatz

Schadenersatz

PRESSEMITTEILUNG Nr. 191/23

Luxemburg, den 14. Dezember 2023

Urteil des Gerichtshofs in der Rechtssache C-340/21 | Natsionalna agentsia za prihodite

Cyberkriminalität: Die Befürchtung eines möglichen Missbrauchs personenbezogener Daten kann für sich genommen einen immateriellen Schaden darstellen

„*Jede Person, der wegen eines Verstoßes gegen* [die DSGVO] *ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.*“

Sanktionen & Schadenersatz

DSGVO-Schadenersatzklagen als Cyberrisiko

€ 2.500

x

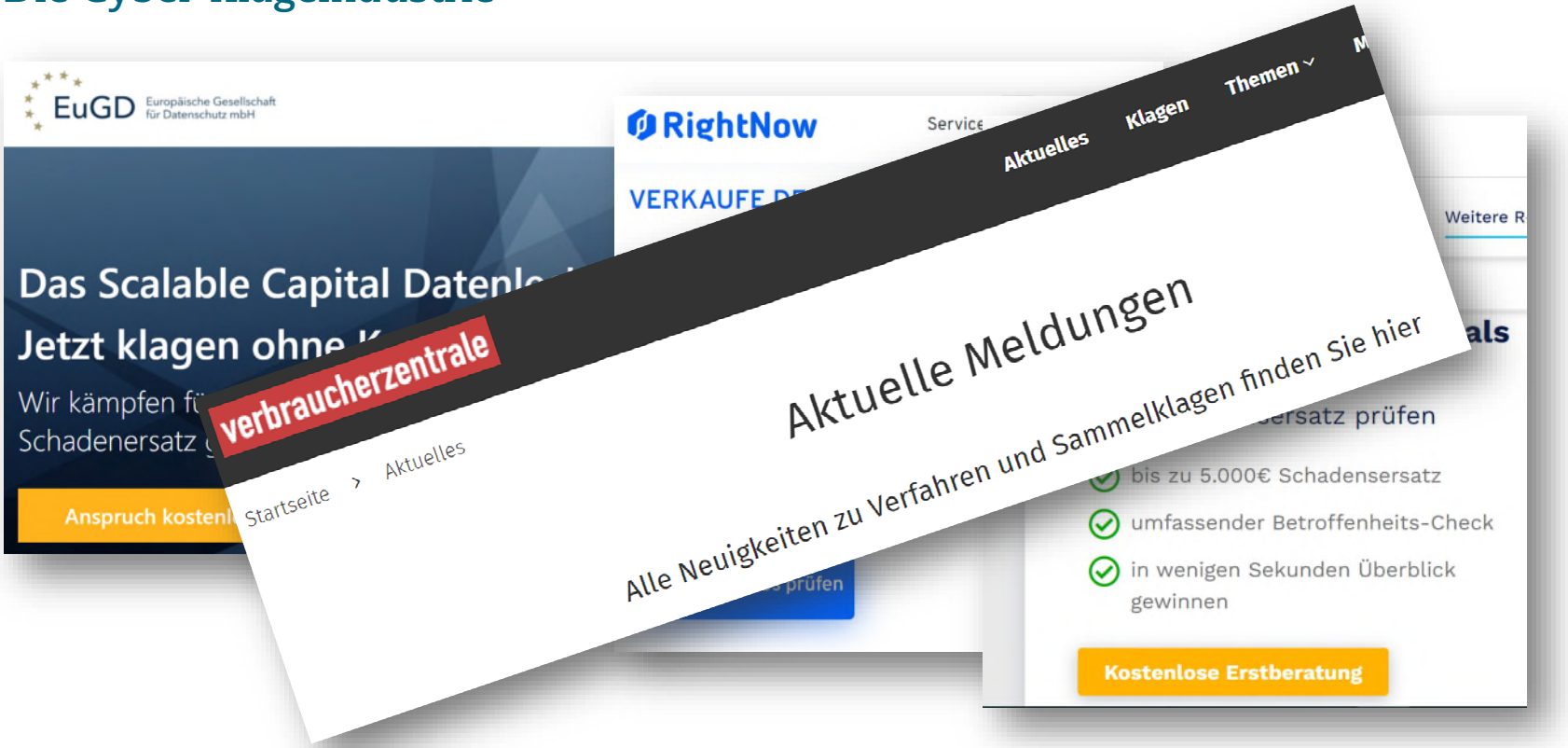
33.200

€ 83.000.000

(Schadensszenario aus LG München I, Urteil vom 9.12.2021, Az. 31 O 16606/20 [rechtskräftig])

Sanktionen & Schadenersatz

Die Cyber-Klageindustrie



Sanktionen & Schadenersatz

Urteile zu Data Scraping- Facebook (insg. wohl über 400)

Datum	Gericht (Az.)	Schadenersatz
07.12.2023	LG Lübeck (15 O 73/23)	EUR 500
20.10.2023	LG Nürnberg-Fürth (10 O 1510/22)	EUR 250
15.09.2023	LG Freiburg (Breisgau) (8 O 21/23)	EUR 0
15.08.2023	OLG Hamm (7 U 19/23)	EUR 0
14.08.2023	LG Hannover (18 O 89/22)	EUR 500
20.06.2023	LG Saarbrücken (4 O 168/22)	EUR 0
13.06.2023	LG Ravensburg (2 O 228/22)	EUR 1.000
07.06.2023	LG Bonn(13 O 126/22)	EUR 250
05.06.2023	LG München I (15 O 4501/22)	EUR 0

Sanktionen & Schadenersatz

Anspruch auf Schadenersatz aus Art. 82 DSGVO

Anspruchsvoraussetzungen:

1) DSGVO-Verstoß

   Beweislast: Kläger; Beklagter aber für Angemessenheit der Sicherheitsmaßnahmen (ähnl. Sekundäre Darlegungslast)

2) Materieller oder immaterieller Schaden

   Beweislast: Kläger

3) Kausalität zwischen DSGVO-Verstoß und Schaden

   Beweislast: Beklagter

4) Verschulden

   Beweislast: Beklagter

Schadenhöhe: Nationales Recht

EuGH-Rechtsprechung:

- *Österreichische Post* (Urt. v. 4.5.2023, Rs. C-300/21)
- *Natsionalna agentsia za prihodite* (Urt. v. 14.12.2023, Rs. C-340/21)
- *Gemeinde Ummendorf* (Urt. v. 14.12.2023, Rs. C-456/22)
- *Krankenversicherung Nordrhein* (Urt. v. 21.12.2023, Rs. C-667/21)
- *MediaMarktSaturn* (Urt. v. 25.1.2024, Rs. C-687/21)

Entscheidung	Pro Unternehmen	Pro Anspruchsteller
Österreichische Post (EuGH, Urt. v. 04.05.2023 – C-300/21)	• Bloßer Verstoß gegen DSGVO reicht für Haftung nicht aus • Materieller oder immaterieller Schaden erforderlich • Nicht jede negative Folge eines DSGVO-Verstoßes stellt immateriellen Schaden dar • Kausalität zwischen Verstoß und Schaden erforderlich • Kein Strafschadenersatz	• Keine Erheblichkeitsschwelle für Vorliegen eines immateriellen Schadens, d.h. auch Bagatellschäden erfasst
Natsionalna agentsia za prihodite (EuGH, Urt. v. 14.12.2023 – C-340/21)	• Offenlegung personenbezogener Daten oder unbefugter Zugang zu diesen stellt noch keinen DSGVO-Verstoß dar • Beweislast für das Vorliegen eines immateriellen Schadens liegt bei der betroffenen Person	• Unternehmen muss darlegen und beweisen, dass Sicherheitsmaßnahmen risikoangemessene waren • Beweislast für fehlende Kausalität zwischen DSGVO-Verstoß und Schaden beim Unternehmen • Furcht vor Missbrauch entwendeter Daten kann im Einzelfall einen immateriellen Schaden darstellen
Gemeinde Ummendorf (EuGH, Urt. v. 14.12.2023 – C-456/22)	• Anspruchsteller muss nachweisen, dass Folgen des DSGVO-Verstoßes für Schaden ursächlich waren	• Auch kurzzeitigee Verlust der Hoheit über diese Daten kann einen immateriellen Schaden darstellen
KV Nordrhein (EuGH, Urt. v. 21.12.2023 – C-667/21)	• Art. 82 DSGVO erfordert Verschulden des Unternehmens	• Unternehmen muss sich aber exkulpieren, d.h. Beweislast für fehlendes Verschulden liegt beim Unternehmen
MediaMarkt Saturn (EuGH, Urt. V. 25.01.2024 – C 687/21)	• Beweislast für DSGVO-Verstoß liegt beim Kläger • Unternehmen „haften“ nicht für Versehen der Mitarbeiter, sondern nur für eigenes technisches und organisatorische Versäumnisse • „Immaterieller Schaden“ bedarf der begründeten Befürchtung, dass Daten missbräuchlich verwendet werden könnten - rein hypothetische	• „Immaterieller Schaden“ ist unionsrechtlich und weit auszulegen – auch ausgelöste Befürchtung der betroffenen Person kann ausreichen.

Entscheidung	Pro Unternehmen	Pro Anspruchsteller
Österreichische Post (EuGH, Urt. v. 04.05.2023 – C-300/21)	• Bloßer Verstoß gegen DSGVO reicht für Haftung nicht aus • Materieller oder immaterieller Schaden erforderlich • **Nicht jede negative Folge eines DSGVO-Verstoßes stellt immateriellen Schaden dar** • Kausalität zwischen Verstoß und Schaden erforderlich • Kein Strafschadenersatz	• **Keine Erheblichkeitsschwelle für Vorliegen eines immateriellen Schadens, d.h. auch Bagatellschäden erfasst**
Natsionalna agentsia za prihodite (EuGH, Urt. v. 14.12.2023 – C-340/21)	• Offenlegung personenbezogener Daten oder unbefugter Zugang zu diesen stellt noch keinen DSGVO-Verstoß dar • **Beweislast für das Vorliegen eines immateriellen Schadens liegt bei der betroffenen Person**	• Unternehmen muss darlegen und beweisen, dass Sicherheitsmaßnahmen risikoangemessene waren • Beweislast für fehlende Kausalität zwischen DSGVO-Verstoß und Schaden beim Unternehmen • **Furcht vor Missbrauch entwendeter Daten kann im Einzelfall einen immateriellen Schaden darstellen**
Gemeinde Ummendorf (EuGH, Urt. v. 14.12.2023 – C-456/22)	• Anspruchsteller muss nachweisen, dass Folgen des DSGVO-Verstoßes für Schaden ursächlich waren	• **Auch kurzzeitigee Verlust der Hoheit über diese Daten kann einen immateriellen Schaden darstellen**
KV Nordrhein (EuGH, Urt. v. 21.12.2023 – C-667/21)	• Art. 82 DSGVO erfordert Verschulden des Unternehmens	• Unternehmen muss sich aber exkulpieren, d.h. Beweislast für fehlendes Verschulden liegt beim Unternehmen
MediaMarkt Saturn (EuGH, Urt. V. 25.01.2024 – C 687/21)	• Beweislast für DSGVO-Verstoß liegt beim Kläger • **Unternehmen „haften“ nicht für Versehen der Mitarbeiter, sondern nur für eigenes technisches und organisatorische Versäumnisse** • **„Immaterieller Schaden“ bedarf der begründeten Befürchtung, dass Daten missbräuchlich verwendet werden könnten -**	• **„Immaterieller Schaden“ ist unionsrechtlich und weit auszulegen – auch ausgelöste Befürchtung der betroffenen Person kann ausreichen.**

Sanktionen & Schadenersatz

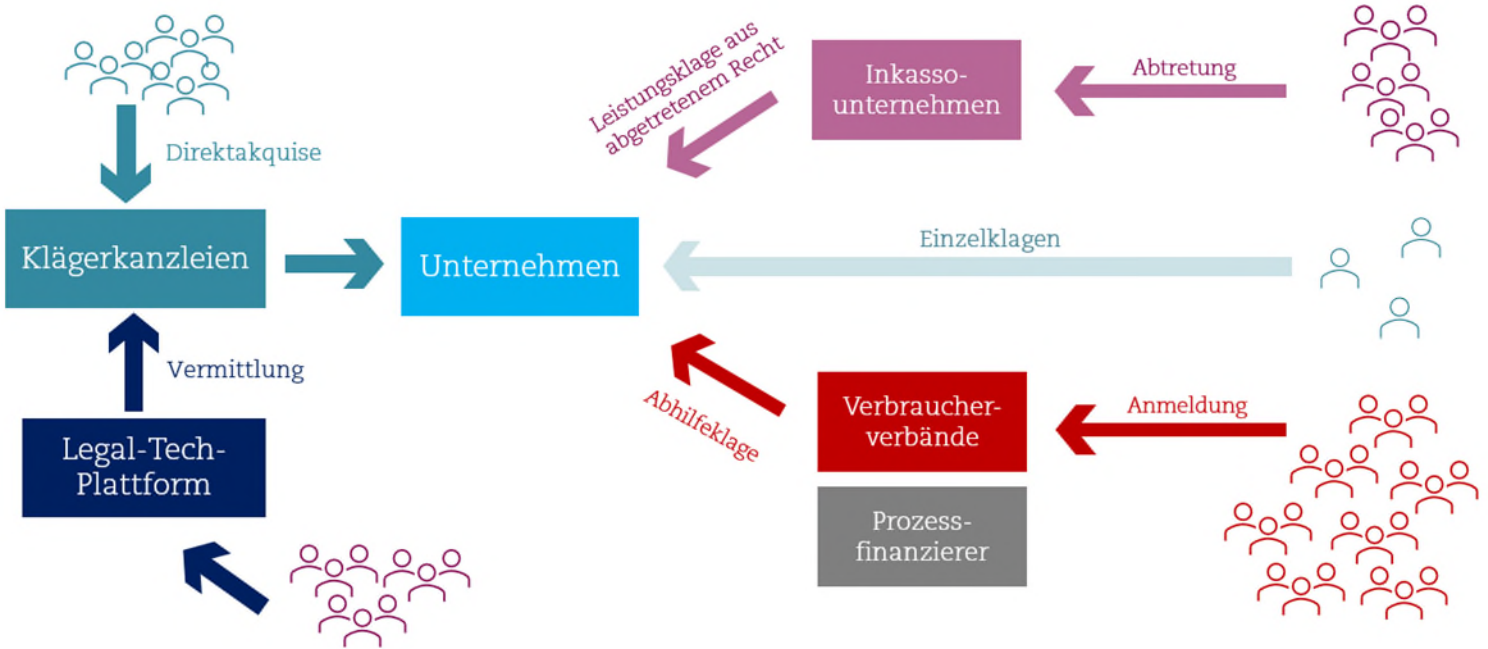
BGH fragt EuGH

- **BGH, Beschl. v. 26.09.2023, Az. VI ZR 97/22, u.a. folgende Fragen:**

  - *„Ist Art. 82 Abs. 1 DSGVO dahingehend auszulegen, dass für die Annahme eines immateriellen Schadens im Sinne dieser Bestimmung bloße negative Gefühle wie z.B. Ärger, Unmut, Unzufriedenheit, Sorge und Angst, die an sich Teil des allgemeinen Lebensrisikos und oft des täglichen Erlebens sind, genügen? Oder ist für die Annahme eines Schadens ein über diese Gefühle hinausgehender Nachteil für die betroffene natürliche Person erforderlich?“*

Sanktionen & Schadenersatz

Massenklageszenarien nach Cyberangriffen



Sanktionen & Schadenersatz

Abhilfeklage: Gleichartigkeit der Ansprüche?

Einzelfallabhängige Eignung

- Ansprüche aus Art. 82 DSGVO als Gegenstand der Abhilfeklage, falls
  - Ansprüche aus demselben oder vergleichbaren Sachverhalten, und
  - gleiche entscheidungserhebliche Tatsachen und Rechtsfragen

- U. U. mangelnde Eignung von Ansprüchen aus Art. 82 DSGVO bei Vorliegen unterschiedlicher Tatsachen, z. B.:
  - Datenvorfall betrifft für verschiedene Personen jeweils unterschiedliche Daten;
  - Datenschutzverstoß führt für verschiedene Personen zu unterschiedlichen negativen Folgen, etwa unterschiedliches unzulässiges Profiling
  - EuGH, *NAP*: „(…) *prüfen, ob diese Befürchtung* ***unter den gegebenen besonderen Umständen*** *und* ***im Hinblick auf die betroffene Person*** *als begründet angesehen werden kann.*“

Sanktionen & Schadenersatz

Abtretungsmodell: Höchstpersönlichkeit & immaterieller Schadenersatz?

AG Hannover, Urt. v. 9.3.2020, Az. 531 C 10952/19:

"Der Kläger ist nicht befugt, etwaige Ansprüche seiner Ehefrau gemäß § 82 Abs. 1 DS-GVO aus abgetretenem Recht geltend zu machen. Sofern Ansprüche auf Ersatz des immateriellen Schadens im Wege der Abtretung von Dritten geltend gemacht werden, besteht - ***mangels Übertragbarkeit dieses höchstpersönlichen Anspruchs*** *- keine Aktivlegitimation, Spittka, GRUR-Prax 2019, 475, 477."*

LG Essen, Urt. v. 23.9.2021, Az. 6 O 190/21:

"Grds. ist jede Forderung abtretbar (vgl. Grüneberg, in: Palandt, 80. Aufl. 2021, § 398 BGB Rn. 8); insb. auch Schmerzensgeldansprüche (vgl. Grüneberg, a.a.O., § 253 BGB Rn. 22). ***Ein Abtretungsverbot nach §§ 399, 400 BGB besteht nicht.*** *Die vermeintliche Forderung der Ehefrau des Kl. gegen die Bekl. unterliegt weder der Pfändung (§ 400 BGB), noch wurde die Abtretung durch Vereinbarung ausgeschlossen oder erfordert die Abtretung eine Inhaltsänderung der Leistung (§ 399 BGB)."*

Sanktionen & Schadenersatz

Standardisierte Geltendmachung: Datenschutz = Fluggastrechte?

OLG Hamm, Urt. v. 15.8.2023, Az. 7 U 19/23:

"Dieser nicht näher konkretisierte Klagevortrag in erster und zweiter Instanz dazu, die jeweilige (bezeichnender Weise nur pauschal bezeichnete) „Klägerpartei" habe Gefühle eines Kontrollverlustes, eines Beobachtetwerdens und einer Hilflosigkeit, insgesamt also das Gefühl der Angst entwickelt und Aufwand an Zeit und Mühe gehabt, reicht zur Darlegung persönlich belastender Folgen der Datenschutzverletzung nicht aus, weil hiermit ***nicht genug Beweisanzeichen objektiver Art vorgetragen sind****, in denen sich solche Gefühle bzw. der Aufwand widerspiegeln, und zwar bezogen auf den konkreten Einzelfall."*

LG Lübeck, Urt. v. 23.9.2021, Az. 15 O 73/23:

"Anders liegt es hingegen zur Überzeugung der Kammer hier, da hier eben ein von der DSGVO-Verletzung selbst zu trennender ***Datenabfluss ins Darknet samt dortiger Weiterverarbeitung und Veröffentlichung*** *durch illegal handelnde Dritte tatsächlich passiert ist und es damit zu einer konkreten und individuell benennbaren Verletzung des Rechts der Klägerseite auf informationelle Selbstbestimmung gekommen ist – eines Rechts im Übrigen, dessen Verletzung zu prüfen das Oberlandesgericht Hamm vollständig unterlassen hat. "*

Fazit

Fazit

Ende gut, alles gut?

Sehr geehrter Herr Spittka,

ich nehme Bezug auf Ihre Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO vom [redacted] für die [redacted] sowie auf die Nachmeldung vom [redacted] Für die Darstellung des Sachverhaltes danke ich Ihnen.

Nach derzeitigem Sachstand erachte ich die von Ihrer Mandantin eingeleiteten Maßnahmen für angemessen und hinreichend, um den Vorfall zu beenden und eine Wiederholung dieses Sachverhaltes zu verhindern.

Da alle betroffenen Personen von Ihrer Mandantin über den Vorfall informiert wurden, schließe ich den Vorgang mit diesem Schreiben ab.

Mit freundlichen Grüßen
Im Auftrag

1. Die Klage wird abgewiesen

2. Der Kläger hat die Kosten des Rechtsstreits zu tragen.

3. Das Urteil ist für die Beklagte gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrags vorläufig vollstreckbar.

Datenschutzrechtliches Risikomanagement bei Cyber-Angriffen

Fragen?

CLYDE&CO

Jan Spittka
Rechtsanwalt | Partner
E: jan.spittka@clydeco.com
D: +49 211 8822 8863

Office numbers
T: +49 211 8822 8800
F: +49 211 8822 8898

Clyde & Co
Dreischeibenhaus 1
40211 Düsseldorf
Germany