LATHAM & WATKINS LLP

NIEDERER KRAFT FREY

Cyber Security Incidents – Wie vermeidet man rechtliche Risiken in Deutschland und der Schweiz?

Donnerstag, 10. Juni 2021 | 16:30 – 18:00 Uhr (CEST)

Agenda

I. Einführung

- Vorstellung von Cyber-Angriffs-Fällen
- Grundlagen zu Cyber Security Incidents

II. Cyber Security Incidents: Risiken & Strategien

- Überblick über rechtliche Rahmenbedingungen sowie Herausforderungen
- Risiken und Handhabung von Datenschutzvorfällen
- Haftung des Managements bei Cyber Security Incidents

III. Folgen von Cyber Security Incidents: Verteidigung gegen Bußgelder & Schadensersatz

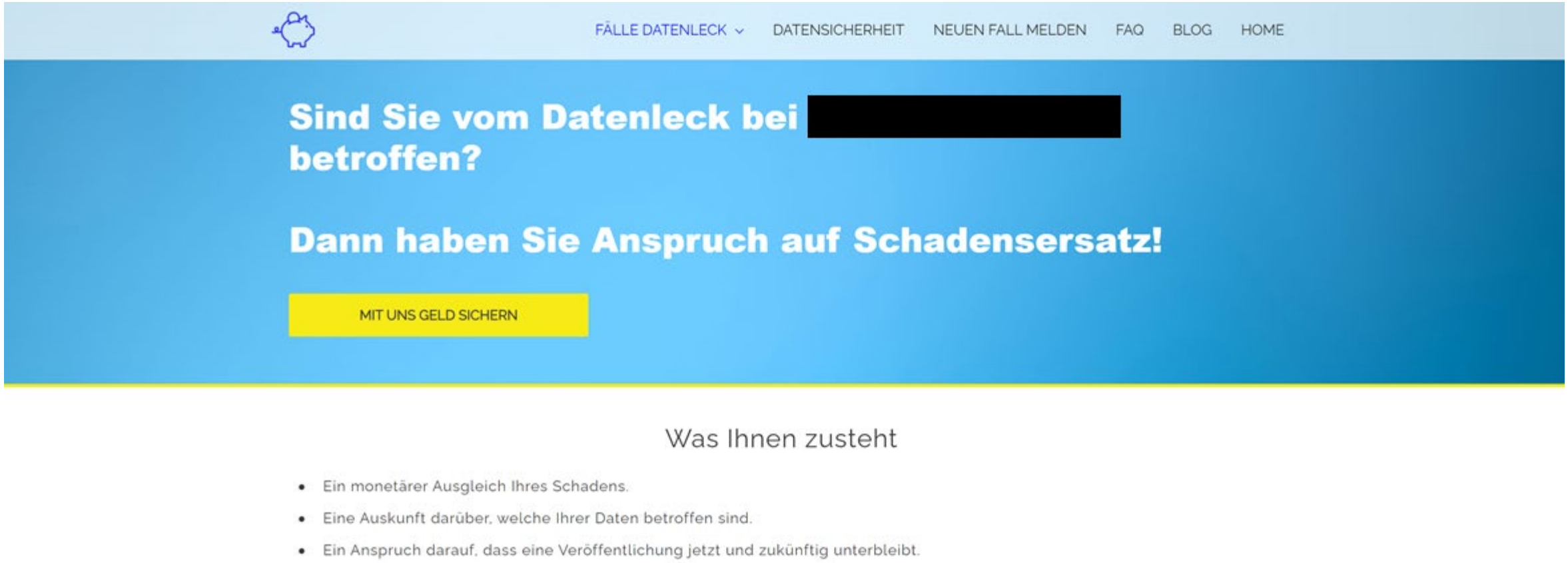
- Übersicht über verhängte DSGVO-Bußgelder im In- und Ausland
- Aktuelle Entwicklungen in der Rechtsprechung sowie Fallbeispiele
- Grundlagen von DSGVO-Schadensersatz sowie DSGVO-Schadensersatz als Geschäftsmodell

LATHAM & WATKINS LLP

NIEDERER KRAFT FREY

Einführung

Beispiel: Werbung um Kläger wegen Cyber Incidents



Welle von Ransomware Attacken in der Schweiz

- Daten auf dem Computer sind nicht mehr verfügbar respektive sind verschlüsselt
- Schadensbegrenzung
- Identifikation der infizierten Systeme
- Detektion
- Strafanzeige
- Zahlung von Lösegeldern?
- Forensische Untersuchungen?
- Sicherung der verschlüsselten Daten
- Neuinstallation der betroffenen Systeme

Quelle: www.entec.ch und https://www.ncsc.admin.ch

Mögliche Erklärungen für Ransomware Attacken

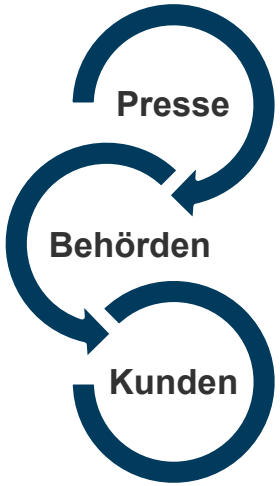
- Änderung des Fokus der Cyberkriminellen von B2C zu B2B (=deep pockets)
- Schweiz beliebter Standort für Rechenzentren
- Die Schweiz hat viele EMEA-Headquarters
- Schweizer Unternehmen unterschätzen den Umgang mit Cyber-Attacken massiv und sind nicht vorbereitet
- «Employee Awareness» ist ungenügend – Attacken sind zu 99% Spear-Phishing-E-Mails, die Mitarbeiter versehentlich öffnen
- Kein Interesse an der Implementierung von IT-Standards (z.B. ISO)
- Mangelnde Strafverfolgung

Cyber Security Incidents - Fallbeispiel

- **Fallkonstellation**
  Bank B verspricht ihren Kunden im Rahmen eines Gewinnspiels verschiedene Sachgewinne. Um an dem Gewinnspiel teilnehmen zu können müssen sich die Kunden unter Angabe ihrer personenbezogenen Daten online registrieren

- **Datenleck**
  In Folge dessen tauchen Anschrift, Kontonummer, Telefonnummern und Mailadressen von **20.000 Kunden**, die sich für die Verlosung registriert haben, im Internet frei zugänglich auf

- **Folgen**



- ➢ Datenpanne wird öffentlich
- ➢ Datenschutzbehörden nehmen Ermittlungen auf
- ➢ Erste Kunden klagen auf Schadensersatz

Cyber Security Incidents – Rechtlicher Rahmen (EU)

- **Art. 32 DSGVO**
  Verantwortliche (Art. 4 Nr. 7 DSGVO) und Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO) sind zur Implementierung von geeigneten technischen und organisatorischen Maßnahmen verpflichtet und müssen insoweit ein angemessenes Schutzniveau gewährleisten

- **Art. 4 Nr. 12 DSGVO: „Verletzung des Schutzes personenbezogener Daten“**
  „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. 5 Abs. 1 lit. f DSGVO**
  „Personenbezogene 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 ("**Integrität und Vertraulichkeit**")“

Cyber Security Incidents – Rechtlicher Rahmen (CH)

- **Art. 8 Abs. 1 und 2 rev. DSG**
  (1) Der Verantwortliche (Art. 5 lit. j rev. DSG) und Auftragsbearbeiter (Art. 5 lit. k rev. DSG) gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit. (2) Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden.

- **Art. 5 lit. h rev. DSG: „Verletzung der Datensicherheit“**
  "Eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden".

Folgen & Risiken von Datenschutzverletzungen (EU)

- **Meldepflichten**
  - Art. 33 DSGVO: Meldepflicht des Verantwortlichen gegenüber der zuständigen Behörde – binnen 72 Stunden, maßgeblich etwa Risiken i. S. d. Erwgr. 85 S. 1 DSGVO
  - Art. 34 DSGVO: Meldepflicht des Verantwortlichen gegenüber der betroffenen Person im Falle eines hohen Risikos für die persönlichen Rechte und Freiheiten – unverzüglich

- **Risiken bzgl. Bußgeldern**
  - Bußgelder bei Verletzung der Meldepflichten aus Artt. 33, 34 DSGVO, bis zu EUR 10 Mio o. 2 % des Vorjahresumsatzes, Art. 83 Abs. 4 lit. a DSGVO
  - Bußgelder wegen unzureichender Datensicherheit
  - Bußgelder wegen Fehlern beim Einsatz von Auftragsverarbeitern
  - Bußgelder wegen Verstößen gegen weitere Vorgaben der DSGVO

- **Reputationsrisiken sowie Risiken für bestehende Geschäftsbeziehungen**

- **Massenhafte Schadensersatzforderungen durch betroffene Personen**

Folgen & Risiken von Datenschutzverletzungen (CH)

- **Meldepflichten**
  - Art. 24 Abs. 1 rev. DSG: Meldepflicht des Verantwortlichen gegenüber der zuständigen Behörde – so rasch als möglich
  - Art. 24 Abs. 3 rev. DSG: Meldepflicht des Auftragsbearbeiters gegenüber dem Verantwortlichen - so rasch als möglich
  - Art. 24 Abs. 4 rev. DSG: Meldepflicht des Verantwortlichen gegenüber der betroffenen Person, wenn es zu ihrem Schutz erforderlich ist oder die zuständige Behörde dies verlangt

- **Risiken bzgl. Bußgeldern**
  - Busse bis CHF 250'000 – ad personam (!)
  - Keine Bußgelder bei Verletzung der Meldepflichten aus Art. 24 rev. DSG
  - Bußgelder wegen unzureichender Datensicherheit: Art. 61 Bst. c rev. DSG
  - Bußgelder wegen Fehlern beim Einsatz von Auftragsbearbeitern: Art. 61 Bst. b rev. DSG
  - Bußgelder wegen Verstößen gegen weitere Vorgaben der rev. DSG

- **Reputationsrisiken sowie Risiken für bestehende Geschäftsbeziehungen**
- **Klagen / Schadenersatzforderungen von betroffenen Personen eher selten**

Haftung des Managements (DE)

- **Organhaftung:**
  Nach deutschem Recht grundsätzlich denkbar
  - § 93 AktG: Haftung der Vorstandsmitglieder von Aktiengesellschaften
  - § 43 GmbHG: Haftung von GmbH-Geschäftsführern

- **Zentrale Voraussetzung für Schadensersatzansprüche:**
  Pflichtverletzung in Form einer Verletzung der Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters

- **Überwachungspflicht des Aufsichtsrats**

- **Unzureichende IT-Security als Verstoß?**
  Nach Auffassung von vielen Stimmen in der Fachliteratur denkbar, dementsprechend auch Schadensersatzansprüche im Verhältnis Gesellschaft → Vorstandsmitglied bzw. Geschäftsführer vorstellbar

- **Bisherige praktische Relevanz**

Haftung der Vorstandsmitglieder (CH)

- **Das Vorstandsmitglied haftet, wenn folgende Voraussetzungen erfüllt sind:**
  - Position und Tätigkeit als Vorstandsmitglied
  - Pflichtverletzung
  - Fahrlässiges oder vorsätzliches Verhalten
  - Schäden
  - Keine Exkulpation und Kausalität
  - Recht zur Geltendmachung von Haftungsansprüchen
  - Beweislast

- **Wer kann klagen (wann)**
  - Gesellschafter (Unternehmensfortführung)
  - Gläubiger (in Konkurs)
  - Unternehmen (Going Concern)

Vorbereitende Maßnahmen

- **Ausstattung**
  Unternehmen müssen über eine effektive und hinreichend finanziell sowie personell ausgestattete Datenschutzorganisation verfügen

- **Unabdingbar:**
  - Unternehmensspezifische Risikoanalyse
  - Sorgfältige Auswahl, Instruktion und Kontrolle der Mitarbeiter
  - Den Vorgaben von Art. 24 Abs. 1 und 5 Abs. 2 DSGVO entsprechende Organisation des betrieblichen Datenschutzes sowie tatsächliche Durchsetzung dieser Vorgaben

- **Dokumentation**
  Umfassende und gerichtsfeste Dokumentation entsprechender Strukturen und Prozesse

- **IT-Sicherheit**
  Dokumentation der mit IT-Dienstleistern (im Vorfeld) abgeschlossenen Verträge und vereinbarten technischen und organisatorischen Maßnahmen zur Gewährleistung einer angemessenen Datensicherheit

Strategie zur Abwehr von Cyber Security Incidents

- Regelmässige Installation von Sicherheitsupdates des Betriebssystems sowie installierter Programme
- Aktualisierung des genutzten Virenschutzprogrammes
- Einrichtung einer Firewall
- Kritischer Umgang mit persönlichen Daten
- Gebrauch von sicheren Passwörtern (mind. 8 Zeichen, bestehend aus Zahlen, Gross-und Kleinbuchstagen und Sonderzeichen wie «@»; regelmässige Erneuerung)
- Erstellung von Backups (Sicherheitskopien, die z.B. Daten oder Fotos im Fall eines Datenverlustes wiederherstellen)
- Sicherheitsstatus des Computers überprüfen

Cyber Security Incident Response Plan

- **Cyber Security Incident Response Plan (CIRP)**
  Vorbereitung eines CIRP ist besonders wichtig, um das Risiko von Schadensersatzforderungen zu verringern

- **Aufgaben- und Maßnahmenverteilung**
  Projektplanung, Projektsteuerung sowie Bestimmung einer Task-Force: Geschäftsleitung, IT-Security, Risikomanagement, Datenschutzbeauftragter, Rechtsabteilung, Kommunikationsabteilung und weitere

- **Sachverhaltsaufklärung**

- **Kommunikation**
  Information der Mitarbeiter, gesetzliche Informations- und Mitbestimmungsrechte des Betriebsrats, Kommunikation mit den Behörden

- **Dokumentation des Vorfalls und der ergriffenen Maßnahmen**
  Ursachen des Vorfalls, Maßnahmen zur Sachverhaltsaufklärung, ermittelte Indizien, Schritte zur Schadensbegrenzung

LATHAM & WATKINS LLP

NIEDERER KRAFT FREY

Verteidigung gegen DSGVO-Bußgelder

Bitte stimmen Sie jetzt ab

Wie hoch war das bis dato höchste von einer Aufsichtsbehörde in Deutschland verhängte DSGVO-Bußgeld?

DSGVO-Bußgelder – Allgemeiner Überblick (DE)

€ 0,3 Mio.	▪ Süddeutscher Fußballverein (LfDI Baden-Württemberg) (10.03.2021) ▪ Fahrlässige Verletzung der datenschutzrechtlichen Rechenschaftspflicht
€ 10,4 Mio. **nicht rechtskräftig**	▪ Hardware-Lieferant (LfD Niedersachsen) (08.01.2021) ▪ Unrechtmäßige Videoüberwachung von Mitarbeitern und Kunden über einen Zeitraum von mindestens zwei Jahren
€ 35,2 Mio.	▪ Modeunternehmen (HmbBfDI) (01.10.2020) ▪ Nach Auffassung der Behörde Durchführung unverhältnismäßiger Kontrollmaßnahmen, die hunderte Mitarbeiter des Service Centers Nürnberg betrafen
€ 1,2 Mio.	▪ Krankenkasse (LfDI Baden-Württemberg) (30.06.2020) ▪ Verwendung der Daten von 500 Gewinnspielteilnehmern für Werbezwecke
€ 9,5 Mio. / **€ 0,9 Mio**	▪ Telekommunikationsunternehmen (BfDI) (09.12.2019) ▪ Unberechtigte konnten durch mangelnde Authentifizierung bei der Kundenbetreuung andere Kundendaten erhalten
€ 14,5 Mio. / **Einstellung**	▪ Immobilienunternehmen (BlnBDI) (05.11.2019) ▪ Speicherung von Daten ehemaliger Mieter in einem Archivsystem ohne Rechtsgrundlage und ohne Löschmöglichkeit

DSG-/ und DSGVO-Bussgelder (CH) I

- **Unter dem geltenden DSG maximale Busse "nur" CHF 10'000**
  Praktisch keine Bussen und Rechtsprechung. Praktisch keine Statistiken

- **Revidiertes DSG führt Bussen bis maximal CHF 250'000 ein**
  Es werden Bussen für die folgenden Verstösse auferlegt:
  - bei vorsätzlich falscher, unvollständiger oder unterlassener Information über die Datenbearbeitung (Art. 60 Abs. 1 rev. DSG)
  - bei mangelhafter Kooperation mit dem EDÖB (Art. 60 Abs. 2 rev. DSG)
  - bei Verletzung der Informationspflicht über automatisierte Einzelentscheide (Art. 60 Abs. 1 Bst. a rev. DSG)
  - bei Nichtbefolgung einer Verfügung des EDÖB (Art. 63 rev. DSG)
  - bei Verletzung der Datensicherheit und Exportrestriktionen (Art. 61 Bst. a und c rev. DSG)
  - bei mangelhafter Bestellung des Auftragsbearbeiters (Art. 61 Bst. b rev. DSG)
  - bei Verletzung der beruflichen Schweigepflicht (Art. 62 rev. DSG)

DSG-/ und DSGVO-Bussgelder (CH) II

- **Ad Personam (!)**
  - Gemäss Botschaft und Aussagen im Gesetzgebungsverfahren zielen Bussen auf Leitungspersonen ab. Es kann jedoch nicht ausgeschlossen werden, dass Bussen auf ausführenden Mitarbeitern ohne Leitungsfunktion auferlegt werden
  - Busse wird nur dann dem Unternehmen auferlegt, wenn Aufwand zur Ermittlung der strafbaren Person unverhältnismässig ist. In einem solchen Fall ist die Busse maximal CHF 50'000
  - Aber: nur bei Vorsatz oder Eventualvorsatz

- **Notifikationspflicht in der Schweiz?**
  - Unter dem geltenden DSG keine Notifikationspflicht bei Cyber Security Incidents
  - Es gibt jedoch sektorspezifische Notifikationspflichten (z.B. im Finanz- und Energiesektor)

- **DSGVO direkt anwendbar – aber noch keine direkte Vollstreckung der Bussen in der Schweiz möglich. Bundesrat kann Staatsverträge abschliessen**

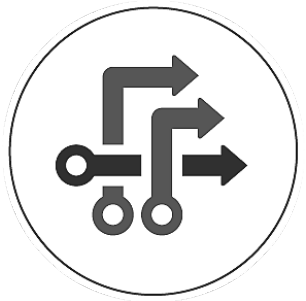
- **Je nach Konstellation nicht alle DSGVO Bestimmungen direkt auf Schweizer Unternehmen anwendbar: z.B. Art. 56 (federführende Aufsichtsbehörde)**

DSGVO-Bußgelder – Cyber Security Incidents (EU)

€ 28 Mio.	▪ Telekommunikationsanbieter (Garante - Italien) (15.01.2021) ▪ Mehrere Millionen Werbeanrufe ohne Einwilligung, Informationsmängel in Apps und unzureichende TOMs
€ 22 Mio.	▪ Airline (ICO - UK) (16.10.2020) ▪ Cyberangriff führte zum Diebstahl von Kreditkartennummern
€ 20 Mio.	▪ Hotelunternehmen (ICO - UK) (30.10.2020) ▪ Unbekannte Hacker erbeuteten über mehrere Jahre hinweg Daten von 339 Mio. Hotelgästen
€ 450.000,00	▪ Kommunikationsplattform (Data Protection Commision - Irland) (09.12.2020) ▪ Verstoß gegen Meldepflichten nach einer Datenpanne
€ 475.000,00	▪ Online-Buchungsplattform (Autoriteit Persoonsgegevens - Niederlande) (10.12.2020) ▪ Verstoß gegen Meldepflichten nach einer Datenpanne

Rechtlicher Rahmen von DSGVO-Bußgeldern (DE)

§§ 130, 30 OWiG bilden die Rahmenbedingungen für Bußgelder gegen Unternehmen



Grundsatz

Nach dt. Bußgeldrecht keine unmittelbare Haftung von Unternehmen

Zurechnung

Setzt eine sog. “Anknüpfungstat” voraus

Anknüpfungstat

Rechtswidrig & schuldhaft / vorwerfbar begangene Pflichtverletzung einer Leitungsperson

Sonderbußgeldrecht

Die Anwendbarkeit der §§ 130, 30 OWiG auf die Verhängung von DSGVO-Bußgeldern ist umstritten

Bitte stimmen Sie jetzt ab

Gehen die deutschen Datenschutzbehörden davon aus, dass ein Verstoß einer Leitungsperson für die Zurechnung und mithin direkte Bebußung eines Unternehmens erforderlich ist?

Rechtlicher Rahmen von DSGVO-Bußgeldern

Die DSK hält §§ 130, 30 OWiG bzgl. DSGVO-Bußgeldern für unanwendbar – mit erheblichen Folgen für die Praxis

§§ 130, 30 OWiG

Finden keine Anwendung

Leitungsperson

Eine Verantwortlichkeit für die Verletzungshandlung seitens einer Leitungsperson oder eines gesetzlichen Verteters ist nicht erforderlich

Mitarbeiter

Unternehmen haften für das Fehlverhalten sämtlicher ihrer Beschäftigter

Rechtsprechung

LG Bonn: Urt. v. 11.11.2020, Az. 29 OWi 1/20 [rechtskräftig]

Der Fall:

- **Anlass**:
  Anruferin gelang es im Call-Center durch Angabe des Namens und Geburtsdatums eines Kunden, Kenntnis von dessen Mobiltelefonnummer zu erlangen
- **Bußgeldbescheid**:
  BfDI verhängt Bußgeld i.H.v. EUR 9,55 Mio. gegen Telekommunikationsunternehmen
- **Argumentation**:
  Unternehmen hat mangels geeigneter Schutzmaßnahmen gegen Vorgaben des Art. 32 DSGVO verstoßen

Wertung des Gerichts:

- **Funktionsträgerprinzip**:
  DSGVO-Bußgelder können direkt gegen Unternehmen verhängt werden. §§ 130, 30 OWiG finden keine Anwendung –vielmehr Haftungsmechanismen des EU-Kartellrechts
- **Höhe Bußgeld**: Verhängtes Bußgeld ist unangemessen hoch und auf EUR 900.000 zu kürzen

Rechtsprechung

LG Berlin: Beschl. v. 18.02.2021, Az. (526 OWi LG) 212 Js-OWi 1/20 (1/20) [nicht rechtskräftig]

Der Fall:

- **Bußgeldbescheid**: Berliner Datenschutzbehörde verhängt gegen ein Unternehmen ein (hohes) Bußgeld
- **Argumentation Behörde**: Unternehmen hat Vorgaben zum technisch-organisatorischen Datenschutz bei der Einführung und Anwendung von Löschroutinen verletzt
- **Adressat**: Behörde hat Bußgeld direkt gegen das Unternehmen verhängt

Wertung des Gerichts:

- **Unwirksamkeit Bescheid**: Bescheid ist aufgrund Verstoßes gegen Gesetzlichkeits- und Schuldprinzip unwirksam. Unternehmen können nicht taugliche Täter von DSGVO-Verstößen sein
- **Rechtsträgerprinzip**: §§ 130, 30 OWiG finden auf die Verhängung von DSGVO-Bußgeldern Anwendung – damit ist nachgewiesene Pflichtverletzung einer Leitungsperson erforderlich

Aktueller Stand: Staatsanwaltschaft hat sofortige Beschwerde eingelegt

LATHAM & WATKINS LLP

NIEDERER KRAFT FREY

Verteidigung gegen DSGVO-Schadensersatzforderungen

Bitte stimmen Sie jetzt ab

Wie hoch war die bis dato höchste von einem deutschen Gericht zugesprochene Schadenssumme aufgrund einer Verletzung der DSGVO?

Rechtsprechung (DE): zusprechende Urteile

Entscheidung	Schadensersatz	Kernaussage des Gerichts
AG Hildesheim, Urt. v. 05.10.2020 (43 C 145/19)	EUR 800	▪ Der Begriff des immateriellen Schadens ist weit auszulegen (Abschreckungswirkung)
LAG Köln, Urt. v. 14.09.2020 (2 Sa 358/20)	EUR 300	▪ Schadensersatz nach der DSGVO soll einen erzieherischen Effekt haben
ArbG Dresden, Urt. v. 26.08.2020 (13 Ca 1046/20)	EUR 1.500	▪ Schadensersatz soll eine abschreckende Wirkung haben
ArbG Neumünster, Urt. v. 11.08.2020 (1 Ca 247 c/20)	EUR 1.500	▪ Schadensersatz soll eine abschreckende Wirkung haben
LG Darmstadt, Urt. v. 26.05.2020 (13 O 244/19)	EUR 1.000	▪ Der Kontrollverlust über Daten begründet einen Schaden
ArbG Düsseldorf, Urt. v. 05.03.2020 (9 Ca 6557/18)	EUR 5.000	▪ Die effektive Sanktionierung von DSGVO-Verstößen ist nur durch eine „abschreckende Wirkung“ des Schadensersatzes zu erreichen

Rechtsprechung (DE): ablehnende Entscheidungen

Entscheidung	Kernaussage des Gerichts
OLG Stuttgart, Urt. v. 31.03.2021 (9 U 34/21)	▪ Keine Beweislastumkehr oder Beweiserleichterung – Beweisregeln der ZPO gelten
LG Frankfurt a.M., Urt. v. 18.01.2021 (2-30 O 147/20)	▪ Der Kläger muss darlegen, dass ein Schaden entstanden ist
OLG Dresden, Urt. v. 12.01.2021 (4 U 1600/20)	▪ Für einen Entschädigungsanspruch bedarf es entweder eines schwerwiegenden Persönlichkeitseingriffs oder einer sonstigen erheblichen Beeinträchtigung
OLG München, Urt. v. 08.12.2020 (18 U 5493/19)	▪ Eine weniger schwerwiegende Verletzung des Persönlichkeitsrechts kann unter Umständen einen immateriellen Schaden darstellen (Sperrung eines Nutzerprofils nicht ausreichend)
LG Landshut, Urt. v. 06.11.2020 (51 O 513/20)	▪ Schmerzensgeld nach der DSGVO ist nicht für einen Bagatellverstoß ohne ernsthafte Beeinträchtigung zu gewähren

Learn more: Die Latham & Watkins Schadensersatztabelle

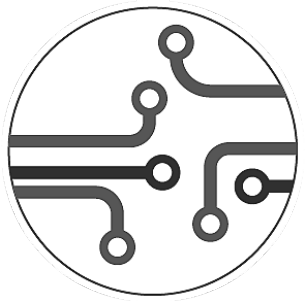
Übersicht über relevante Urteile bzgl. DSGVO-Schadensersatz: https://de.lw.com/thoughtLeadership/Latham-DSGVO-Schadensersatztabelle

Haftungsvoraussetzungen, Art. 82 DSGVO

„Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz […]“

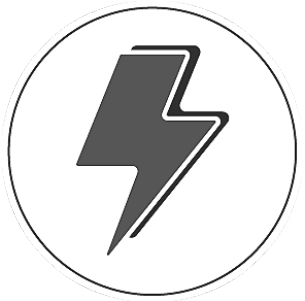
Anspruchsgegner

Verantwortlicher oder Auftragsverarbeiter



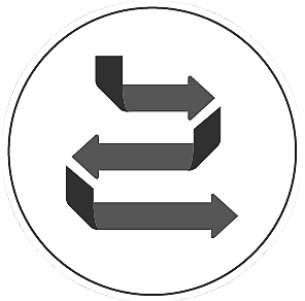
DSGVO-Verstoß

Oftmals unzureichende Datensicherheit oder gegen Auskunftsverfahren



Schaden

Materieller Vermögensschaden oder immaterielle Beeinträchtigung



Kausalität

Eingetretener Schaden muss auf Verstoß beruhen

Der Schadensbegriff des Art. 82 DSGVO

Der Schadensbegriff des Art. 82 DSGVO umfasst sowohl materielle Schäden als auch immaterielle Beeinträchtigungen. Die Reichweite des Anspruchs in der Rechtsprechung ist jedoch nach wie vor umstrittne.

Weiter Schadensbegriff

Schadensersatz auch bei geringfügigen Beeinträchtigungen

Enger Schadensbegriff

Datenschutzverstoß muss zu einer konkreten, nicht nur unbedeutenden oder empfundenen Verletzung von Persönlichkeitsrechten geführt haben

Missbrauchsrisiko

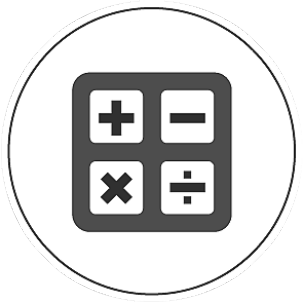
Ausdehnung auf bloße Unannehmlichkeiten?

DSGVO-Schadensersatz als Geschäftsmodell

Bekannt gewordene Bußgeldverfahren oder Datenpannen rufen vermehrt kommerzielle Prozessfinanzierer auf den Plan

Werbung

Aktives und gezieltes Marketing



Vergleich

Geschäftsmodell in anderen Rechtsgebieten bereits etabliert – etwa Entschädigungsansprüche gegen Fluggesellschaften

Beispiele

Kleinfee, EuGD, RightNow

Verteidigung gegen Schadenersatzforderungen (CH)

- **Generell: Klagen auf Schadenersatzforderungen in der Schweiz eher selten**
- **Art. 82 DSGVO: keine analoge Bestimmung in der Schweiz**
- **Art. 32 rev. DSG verweist auf Klagen zum Schutz der Persönlichkeit richten sich nach den Artikeln 28, 28a sowie 28 g–28l des Zivilgesetzbuchs:**
  - Vorliegen einer widerrechtlichen Persönlichkeitsverletzung
  - Schadenersatz, Anspruch auf Gewinnherausgabe, Genugtuung, Unterlassungsansprüche etc.
- **Kosten und Kostenrisiko für betroffene Personen in der Regel zu hoch**
- **Schadensbeweis sehr schwierig zu erbringen**
- **Das zivilrechtliche Instrument der "Massenklagen" ist als solches nicht im Schweizer Datenschutzrecht bekannt**
- **Daher DSG Schadenersatzklagen (noch) kein Geschäftsmodell in der Schweiz**

Rechtsprechung

OLG Stuttgart, Urt. v. 31.03.2021, Az. 9 U34/21

Der Fall:

- **Hintergrund**:
  Hackerangriff gegen Finanzdienstleister
  - ➢ Hacker verschafften sich widerrechtlich Zugriff auf personenbezogene Daten von Kunden
  - ➢ Daten wurden anschließend im Internet veröffentlicht (einschließlich Kreditkartennummern)
- **Klage**:
  Betroffene Klägerin macht Schadensersatz geltend – wegen angeblicher Verstöße gegen Vorgaben zur Datensicherheit und zur Beantwortung von Auskunftsersuchen (Art. 15 DSGVO)

Wertung des Gerichts:

- **Haftungsvoraussetzungen**:
  Kein Schadensersatz mangels DSGVO-Verstoßes und Kausalität
  - ➢ **Auskunftsersuchen**: Schon kein Verstoß gegen Art. 15 DSGVO ersichtlich
  - ➢ **Datensicherheit**: Keine Verletzung der Vorgaben zur Datensicherheit wegen unrechtmäßiger Veröffentlichung von Daten

Rechtsprechung

OLG Stuttgart, Urt. v. 31.03.2021, Az. 9 U34/21

Zur Darlegungs- und Beweislast:

- **Keine Beweislastumkehr**:
  Rechenschaftspflicht nach Art. 5 Abs. 2 und Art. 24 Abs. 1 DSGVO begründet keine Beweislastumkehr oder Beweiserleichterung – Beweisregeln der ZPO gelten

- **Folge**:
  Klägerin trägt grundsätzlich Darlegungs- und Beweislast

- **Einschränkung**:
  Sekundäre Darlegungslast der Beklagten
  - **Beweisnot**: Klägerin hat keine nähere Kenntnis der maßgeblichen Umstände und auch keine Möglichkeit zur weiteren Sachaufklärung (hier verneint)
  - **Zumutbarkeit**: Beklagte hat Kenntnis von wesentlichen Tatsachen und kann Auskunft unschwer erteilen

Vorlagebeschluss des OGH zum EuGH

OGH, Beschl. v. 15.04.2021, Geschäftszahl: 6Ob35/21x

Vorlagebeschluss zum EuGH:

- **Verletzung gleich Verstoß (?)**: Reicht bereits die Verletzung von Bestimmungen der DSGVO als solche für die Zuerkennung von Schadenersatz aus?

- **Zusätzliche EU-rechtliche Anforderungen:** Gibt es neben den Grundsätzen der Effektivität und Äquivalenz weitere Vorgaben des Unionsrechts, die nationale Gerichte bei der Bemessung des Schadenersatzes nach Art. 82 DSGVO beachten müssen?

- **Erheblichkeitsschwelle**: Setzt ein immateriellen Schaden voraus, dass eine Konsequenz oder Folge der Rechtsverletzung von zumindest einigem Gewicht vorliegt, die über den durch die Rechtsverletzung hervorgerufenen Ärger hinausgeht?

Vorlagebeschluss des OGH zum EuGH

OGH, Beschl. v. 15.04.2021, Geschäftszahl: 6Ob35/21x

Folgen des Vorlagebeschlusses zum EuGH für die Praxis (1/2):

Die Entscheidung hat voraussichtlich erhebliche Auswirkungen für laufende und künftige Verfahren um Schadensersatzforderungen nach Art. 82 DSGVO.

- **Entscheidung des EuGH:** Betrifft zentrale Fragen zu den Voraussetzungen von Schadensersatz, durchschnittliche Verfahrensdauer: 1,5 Jahre.
- **Prognose:** Die Richtung der Entscheidung ist erfahrungsgemäß schwer vorherzusehen. In den letzten Jahren jedoch eher verbraucherfreundliche Entscheidungen
- **Umsetzbarkeit:** Die Richter lassen sich auch von etwaigen Umsetzbarkeitsfragen nicht von sehr „datenschutzfreundlichen“ Entscheidungen abhalten, vgl. „Schrems II“-Urteil.

Vorlagebeschluss des OGH zum EuGH

OGH, Beschl. v. 15.04.2021, Geschäftszahl: 6Ob35/21x

Weitere Folgen des Vorlagebeschluss zum EuGH für die Praxis (2/2):

- **Klagehäufigkeit:** Die Anzahl von Schmerzensgeldforderungen und Gerichtsverfahren um Schadensersatz nach Art. 82 DSGVO hat in den letzten Jahren stark zugenommen.
- **Tendenz**: Kläger, Verbraucheranwälte, Rechtsdienstleister wie *EugD, RightNow, Kleinfee* & Co. sowie Prozessfinanzierer könnten weiter ermutigt werden Ansprüche geltend zu machen bzw. durchzusetzen
- **Folgen für laufende Verfahren:** Grundsätzlich sind Aussetzungen denkbar, etwa deutsche Gerichte sind zu solchen Aussetzungen jedoch nicht verpflichtet
- **Darlegungs- und Beweislast:** Zudem können Gerichte Klagen auch nach den Entscheidungen des BVerfG und des OGH abweisen, wenn ein Verstoß oder ein Schaden nicht hinreichend nachgewiesen sind.

LATHAM & WATKINS LLP

NIEDERER KRAFT FREY

Ihre Fragen

Clara-Ann Gordon

Technology (M&A und Litigation),
Datenschutz, Dispute Resolution,
Partnerin, Datenschutzbeauftragte
Zürich

T +41.58.800.8426
E clara-ann.gordon@nkf.ch

Tim Wybitul

Datenschutz (Litigation & Trial),
Partner, Datenschutzbeauftragter,
Frankfurt am Main

T +49.69.6062.6550
E tim.wybitul@lw.com

Disclaimer

Diese Präsentation wurde als Informationsangebot für Latham-Mandanten und Freunde der Kanzlei erstellt. Sie soll und wird kein Mandatsverhältnis zwischen dem Betrachter und Latham & Watkins LLP begründen und sollte auch nicht als Ersatz für die Konsultation eines qualifizierten Rechtsanwalts angesehen werden. Wenn Sie eine rechtliche Beratung zu diesem oder einem anderen Thema benötigen, verlassen Sie sich nicht auf diese Präsentation, sondern wenden Sie sich bitte an Ihren Latham & Watkins LLP-Anwalt, der Ihnen helfen kann, eine auf Ihre spezielle Situation zugeschnittene rechtliche Beratung zu erhalten.

Die Präsentation wurde nicht erstellt oder entworfen, um die einzigartigen Sachverhalte oder Umstände anzusprechen, die in einem bestimmten Fall auftreten können, und Sie sollten sich nicht und sind nicht befugt, sich auf diesen Inhalt als Quelle für eine Rechtsberatung zu verlassen, ebenso begründet dieses Seminarmaterial kein Mandatsverhältnis zwischen Ihnen und Latham & Watkins.