deutsches forschungsnetz

Haftungsrisiken bei Datenschutzverstößen

82. Betriebstagung des DFN | 25.03.2025

Marc-Philipp Geiselmann

Agenda

- Durchsetzungsregime
- Haftung und Recht auf Schadensersatz
- Datenleck

Duales Durchsetzungsregime

- Behördliche Durchsetzung durch Bußgelder, Art. 83 DSGVO
- Ausgestaltung ist den Mitgliedstaaten überlassen, Art. 83 Abs. 7 DSGVO

> (7) Unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 2 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.

Duales Durchsetzungsregime

- Behördliche Durchsetzung durch Bußgelder, Art. 83 DSGVO
- Ausgestaltung ist den Mitgliedstaaten überlassen, Art. 83 Abs. 7 DSGVO
- Keine Verhängung von Geldbußen gegen Behörden, § 43 Abs. 3 BDSG

> (3) Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 werden keine Geldbußen verhängt.

Duales Durchsetzungsregime

- Private Durchsetzung durch Schadensersatzansprüche, Art. 82 DSGVO

Art. 82
Haftung und Recht auf Schadenersatz

(1) 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.

Duales Durchsetzungsregime

- Private Durchsetzung durch Schadensersatzansprüche, Art. 82 DSGVO

Art. 82
Haftung und Recht auf Schadenersatz

(1) 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.

Haftung und Recht auf Schadensersatz

- Voraussetzungen
  - Verstoß gegen die DSGVO
  - Schaden
  - Kausalität des Verstoßes für den Schaden
- Rechtsfolge
  - Schadensersatz

Haftung und Recht auf Schadensersatz

- Voraussetzungen
  - Verstoß gegen die DSGVO
  - Schaden
  - Kausalität des Verstoßes für den Schaden

  } Bestreiten

- Rechtsfolge
  - Schadensersatz
- Einwendung: keine Verantwortlichkeit, Art. 82 Abs. 3 DSGVO

> (3) Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

Haftung und Recht auf Schadensersatz

- Verstoß gegen „diese Verordnung“ DSGVO
  - Jeder Verstoß gegen die Verordnung
  - Vorbereitungshandlungen
  - Verstöße gegen delegierte Rechtsakte, ErwG. 146 S. 5 DSGVO

„Zu einer Verarbeitung, die mit der vorliegenden Verordnung nicht im Einklang steht, zählt auch eine Verarbeitung, die nicht mit den nach Maßgabe der vorliegenden Verordnung erlassenen delegierten Rechtsakten und Durchführungsrechtsakten und Rechtsvorschriften der Mitgliedstaaten zur Präzisierung von Bestimmungen der vorliegenden Verordnung im Einklang steht.“

Haftung und Recht auf Schadensersatz

- Schaden

Art. 82
Haftung und Recht auf Schadenersatz

(1) 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.

Haftung und Recht auf Schadensersatz

- Schaden

Materieller Schaden	Immaterieller Schaden
Differenzhypothese	Körperliche & seelische Schäden
Kosten für eine Heilbehandlung	Schmerzensgeld
Reparaturkosten	
Kosten für Ersatz	
Nutzungsausfall	
	Nicht: Affektionsinteresse
	Nicht: Lebenszeit

Haftung und Recht auf Schadensersatz

- Schaden
  - Materieller und immaterieller Schaden umfasst
  - Weite Auslegung, ErwG. 146 S. 3 DSGVO
  - Keine Erheblichkeitsschwelle oder Bagatellgrenze
  - Datenverlust an sich, Kontrollverlust, ungutes Gefühl?
  - Verstoß gegen die DSGVO ≠ Schaden

„Der Begriff des Schadens sollte im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden, die den Zielen dieser Verordnung in vollem Umfang entspricht.“

Haftung und Recht auf Schadensersatz

- Schaden: Grenzen des immateriellen Schadens
  - EuGH, Urteil vom 4. Mai 2023, Österreichische Post, C-300/21, ECLI:EU:C:2023:370
  - Urteil vom 14. Dezember 2023, Gemeinde Ummendorf, C-456/22, EU:C:2023:988
  - EuGH, Urteil vom 14. Dezember 2023, Natsionalna agentsia za prihodite, C-340/21, ECLI:EUC:2023:986
  - EuGH, Urteil vom 25. Januar 2024, MediaMarktSaturn, C-687/21, EU:C:2024:72
  - EuGH, Urteil vom 11. April 2024, juris, C-741/21, EU:C:2024:288
  - EuGH, Urteil vom 20. Juni 2024, Scalable Capital, C-182/22 und C-189/22, EU:C:2024:531
  - EuGH, Urteil vom 4. Oktober 2024, Agentsia po vpisvaniyata, C-200/23, ECLI:EU:C:2024:827

Haftung und Recht auf Schadensersatz

- Schaden: Beispiele
  - Diskriminierung
  - Identitätsdiebstahl, -betrug
  - Rufschädigung
  - Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten
  - Unbefugte Aufhebung der Pseudonymisierung
  - Andere gesellschaftliche Nachteile

Haftung und Recht auf Schadensersatz

- Kausalität
  - Begrenzung auf Vorhersehbarkeit, Ausschluss ganz außergewöhnlicher Folgen

Haftung und Recht auf Schadensersatz

- Einwendung: keine Verantwortlichkeit, Art. 82 Abs. 3 DSGVO
  - Verschulden wird vermutet
  - Weder vorsätzliches noch fahrlässiges Handeln
  - Betrachtung des Einzelfalls
  - Bei Datenleck: übliche Sorgfalt zum Schutz der Daten
  - Umfassende Dokumentation der Maßnahmen über Art. 5 Abs. 2 DSGVO (allgemeine Rechenschaftspflicht) hinaus
  - Zertifizierungen allein sind nicht ausreichend

Haftung und Recht auf Schadensersatz

- Rechtsfolge: Schadensersatz
  - Bemessung nach §§ 287 ZPO
  - Dauer, Art, Umfang der betroffenen personenbezogenen Daten
  - Höhe muss mehr als symbolisch sein

Haftung und Recht auf Schadensersatz

- Beispiel: Rechtswidriger Schufa-Eintrag
  - 5.000 EUR, wenn eine Einmeldung zur Schufa nach dem Erlass eines Vollstreckungsbescheids und vor dessen Zustellung an den Betroffenen erfolgt, LG Mainz, Urteil vom 12.11.2021 – 3 O 12/20
  - 1.500 EUR für die Herbeiführung einer rechtswidrigen Schufa-Eintragung, OLG Dresden, Beschluss vom 29.08.2023 – 4 U 1078/23
  - 1.000 EUR bei rechtswidrigem SCHUFA-Eintrag, LG Lüneburg, Urteil vom 14.07.2020 – 9 O 145/19
  - 500 EUR für unberechtigten Negativeintrag bei der SCHUFA, OLG Koblenz, Urteil vom 18.05.2022 – 5 U 2141/21
  - 500 EUR DSGVO-Schaden für unberechtigten SCHUFA-Eintrag, BGH, Urteil vom 28.01.2025 - VI ZR 183/22

Haftung und Recht auf Schadensersatz

- Beispiel: Auskunftsanspruch, Art. 15 DSGVO
  - 1.000 EUR bei unzureichender Auskunft, so LAG Hamm, Urteil vom 11.5.2021 – 6 Sa 1260/20
  - 1.000 EUR je unvollständig beantwortetem Auskunftsverlangen, LAG Berlin-Brandenburg, Urteil vom 18.11.2021 – 10 Sa 443/21
  - 500 EUR bei verspäteter Auskunft OLG Köln, Urt. v. 14.7.2022 – 15 U 137/21
  - Zuvor: 0,00 EUR LG Bonn, Urteil vom 1.7.2021 – 15 O 356/20; Verzögerte Auskunft stellt selbst keinen Schaden dar.

Datenleck

Im Zeitraum von Januar 2018 bis September 2019 ordneten unbekannte Dritte durch die Eingabe randomisierter Ziffernfolgen über die Kontakt-Import-Funktion des Netzwerks Telefonnummern zu Nutzerkonten zu und griffen die zu diesen Nutzern vorhandenen Daten ab (sog. Scraping). Die auf diese Weise erlangten und nunmehr mit einer Telefonnummer verknüpften Daten von ca. 533 Millionen Nutzern wurden im April 2021 im Internet öffentlich verbreitet. Hiervon waren auch persönliche Daten des Klägers (Telefonnummer in Verknüpfung mit den Daten seines Nutzerkontos, d.h. Nutzer-ID, Vorname, Nachname, Geschlecht und Arbeitsstätte) betroffen. Nach dem Vortrag des Klägers informierte die Beklagte weder die zuständige Datenschutzbehörde noch ihn selbst über den Vorfall.

Quelle: BGH, Urteil vom 18. November 2024, VI ZR 10/24 Rn. 5.

Datenleck

- Voraussetzungen
  - Verstoß gegen die DSGVO – Art. 5, 25, 32 DSGVO

Art. 32

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 gegebenenfalls unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

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

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Datenleck

- Voraussetzungen
  - Verstoß gegen die DSGVO – Art. 32 DSGVO
  - Schaden – Kontrollverlust, ungutes Gefühl
  - Kausalität des Verstoßes für den Schaden (+)
- Einwendung: keine Verantwortlichkeit (-)
- Rechtsfolge: Schadensersatz

1.000 EUR!!!

Datenleck

Achtung: Verliere nicht deinen Anspruch

Zum 31.12.2024 droht die **Verjährung der Ansprüche** Betroffener des Datenlecks bei Facebook. Zögere nicht deine Schadensersatzansprüche geltend zu machen, **bevor die Zeit abgelaufen ist**!

Verliere nicht deine Chance Schadensersatz – Facebook / Meta hat deine Daten auf dem Gewissen!

Jetzt Handynummer eingeben und sofort zeigt der Checker Dir an, ob du betroffen bist:

Ihre Mobilnummer

+49160123456789

Bitte geben Sie Ihre Mobilnummer im Internationalen Format an, beginnend mit +49, ohne Bindestriche und ohne Leerzeichen.

Jetzt checken

https://www.wbs.legal/i/dl-facebook/ (zuletzt abgerufen am 15.03.2025).

Datenleck

- BGH, Urteil vom 18. November 2024, VI ZR 10/24
  - Kurzzeitiger Verlust der Kontrolle über personenbezogene Daten stellt einen immateriellen Schaden dar – Rn. 30
  - Nachweis des Kontrollverlusts nötig, sich daraus entwickelnde Befürchtungen oder Ängste müssen nicht nachgewiesen werden – Rn. 31
  - Ohne Kontrollverlust: Begründete Befürchtung der missbräuchlichen Verwendung – Rn. 32
  - Bloße Behauptung der Befürchtung oder rein hypothetisches Risiko der missbräuchlichen Verwendung nicht ausreichend – Rn. 32

Datenleck

Zu den weitergehenden Folgen hat der Kläger vorgetragen, wegen des Scraping-Vorfalls in einem Zustand großen Unwohlseins und großer Sorge über möglichen Missbrauch der ihn betreffenden Daten verblieben zu sein. Dies manifestiere sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen. Seit dem Vorfall erhalte er unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail. Diese enthielten Nachrichten mit offensichtlichen Betrugsversuchen und Phishing-Attacken. Das habe dazu geführt, dass er nur noch mit äußerster Vorsicht auf jegliche E-Mails und Nachrichten reagieren könne und jedes Mal einen Betrug fürchte und Unsicherheit verspüre. Zur aufgewendeten Zeit und Mühe trug der Kläger vor, er habe sich mit dem "Datenleak" auseinandersetzen, den Sachverhalt ermitteln, sich um eine Auskunft der Beklagten kümmern und selbst weitere Maßnahmen ergreifen müssen.

Quelle: BGH, Urteil vom 18. November 2024, VI ZR 10/24 Rn. 40.

Datenleck

bb) Äußerst zweifelhaft erscheint daher, ob hier eine Festsetzung in "gegebenenfalls nur einstelliger Höhe" mit dem Effektivitätsgrundsatz zu vereinbaren wäre (so aber obiter OLG Celle, Urteil vom 4. April 2024 - 5 U 31/23, juris Rn. 102). Dagegen hätte der Senat von Rechts wegen keine Bedenken, den notwendigen Ausgleich für den eingetretenen Kontrollverlust als solchem in einem Fall wie dem streitgegenständlichen in einer Größenordnung von 100 € (so obiter OLG Hamm, GRUR-RS 2024, 16856 Rn. 40) zu bemessen.

Quelle: BGH, Urteil vom 18. November 2024, VI ZR 10/24 Rn. 100.

Fazit

- Investitionen in die Datensicherheit
- Investitionen in die Datensicherheit
- Investitionen in die Datensicherheit

Fazit

Art. 32

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 gegebenenfalls unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

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

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Haben Sie Fragen?