Datenschutz im Gesundheitswesen

Rechtsfolgen/ Sanktionen bei Verstößen

05. und 06. November 2024 Online-Seminar

Rechtsanwalt Dietmar Corts
Zertifizierter Berater für Steuerstrafrecht (DAA)

CP Corts & Partner
Rechtsanwälte
Elisenstraße. 4-10, 50667 Köln
Tel.: 0221 / 277947-0
Fax: 0221 / 277947-21
E-Mail: dietmar.corts@corts-partner.com

www.corts-partner.com

Übersicht

I. Aktuelle Bußgeldverfahren

II. Rechtsfragen im Bußgeldverfahren

III. Behördliches Vorgehen

IV. Schadensersatzansprüche

V. Guidelines EDSA

VI. Zusammenfassung

I. Aktuelle Bußgeldverfahren

Spektakuläre Bußgeldverfahren

Facebook: 1 Mio. €
- persönliche Daten von Nutzern und Freunden ohne Einwilligung gesammelt

Amazon: 35 Mio. €
- Tracking Cookies ohne Einwilligung und ohne Datenschutzhinweis

Google: 60 Mio. €
- Tracking Cookies zu Werbezwecken ohne Einwilligung und ohne Datenschutzhinweis

Vodafone: 12 Mio. €
- Werbeanschriften, -anrufe und DSGVO-Verstöße

H&M: 35 Mio. €
- mehrere Mitarbeiter des Service-Centers bespitzelt

I. Aktuelle Bußgeldverfahren

CEGEDIM SANTÉ Unternehmen

Bescheid: 05.09.2024

Bußgeld: 800.000 EUR

Verletztes Recht: Art. 5 Abs. 1 lit. a DSGVO, Art. 66 Abs. 2 DSGVO, Art. 66 Abs. 3 DSGVO

Vorgang:

- Management-Software an Arztpraxen verkauft
- personenbezogene Daten verarbeitet, an seine Kunden weitergeleitet
- die Informationen zur Erstellung von Studien nutzen konnten
- Daten nicht anonymisiert, sondern nur pseudonymisiert
- Betroffene konnten identifiziert werden
- keine Genehmigung für Datenverarbeitung

I. Aktuelle Bußgeldverfahren

Patient einer Arztpraxis

Bescheid: 31.12.2023

Bußgeld: 5.000 €

Verletztes Recht: Art. 5 DSGVO, Art. 6 DSGVO, Art. 9 DSGVO

Vorgang:

- Patient: Bewertungsportal im Internet kritisch geäußert
- Arzt reagierte, wobei er personenbezogene Daten des Patienten - wie Diagnosen und Behandlungsergebnisse -veröffentlichte

I. Aktuelle Bußgeldverfahren

Mitarbeiter

Bescheid: 2024

Bußgeld: 75.000 EUR

Verletztes Recht: Art. 9 DSGVO, Art. 32 DSGVO

Vorgang:

- Mitarbeiter musste krankheitsbedingte Ausfälle per E-Mail in einem E-Mail-Verteiler mit 25 Kollegen und Vorgesetzten melden

I. Aktuelle Bußgeldverfahren

Bußgeld gegen kleines Unternehmen

Bescheid: 2024

Bußgeld: 9.600 EUR

Verletztes Recht: Art. 9 Abs. 2 DSGVO

Vorgang:

- ehemalige Mitarbeitende nach Ausscheiden aggressiv versucht, frühere Kollegen abzuwerben
- ehemaliger Arbeitgeber erfuhr davon
- informierte aktuelle Arbeitsstelle über Verhalten ihrer Angestellten
- Information beinhaltete Daten zu Krankschreibungen und Krankenhausaufenthalten

I. Aktuelle Bußgeldverfahren

Immobilienunternehmen

Bescheid: 2024

Bußgeld: 16.600 EUR

Verletztes Recht: Art. 5 Abs. 1 lit. a, b, c DSGVO, Art. 6 DSGVO

Vorgang:

- keine Vereinbarungen über gemeinsame Datenverantwortlichkeit mehrerer Unternehmen
- Daten erhoben und verarbeitet, ohne rechtliche Grundlage
- Löschungsanfragen von drei Betroffenen wurde nicht rechtzeitig nachgekommen

I. Aktuelle Bußgeldverfahren

Bußgeld gegen Unternehmen Immobilienbranche

Bescheid: 2024

Bußgeld 9.600 EUR

Verletztes Recht: Art. 5 Abs. 1 lit. a DSGVO, Art. 6 DSGVO, Art. 30 DSGVO

Vorgang:

- Bußgeld gegen Unternehmen Immobilienbranche
- unvollständiges Verzeichnis über Verarbeitungstätigkeiten
- fehlten notwendige Pflichtinformationen
- gespeicherte Daten verspätet gelöscht

I. Aktuelle Bußgeldverfahren

Unternehmen

Bescheid: 2024

Bußgeld: 3.000 EUR

Verletztes Recht: Art. 17 DSGVO

Vorgang:

- erhobene personenbezogene Daten nicht rechtzeitig gelöscht

I. Aktuelle Bußgeldverfahren

Online-Händler

Bescheid: 2024

Bußgeld: 6.000 EUR

Verletztes Recht: Art. 33 Abs. 1 DSGVO

Vorgang:

- Behörde mit deutlicher Verspätung über Datenpanne informiert

I. Aktuelle Bußgeldverfahren

Logistikunternehmen

Bescheid: 2024

Bußgeld: 32.000 EUR

Verletztes Recht: Art. 32 Abs. 1 DSGVO

Vorgang:

- Zustellerlisten nicht ordnungsgemäß entsorgt

I. Aktuelle Bußgeldverfahren

Hotel

Bescheid: 2024

Bußgeld: 16.000 EUR

Verletztes Recht: Art. 6 DSGVO

Vorgang:

- Personalausweiskopien gespeichert

I. Aktuelle Bußgeldverfahren

Dedalus, Anbieter von Software für medizinische Analyselabore

Bescheid: 2022

Bußgeld: 1.500.000 EUR

Verletztes Recht: Art. 28 DSGVO, Art. 29 DSGVO, Art. 32 DSGVO

Vorgang:

- Gesundheitsdaten von 500.000 Personen offengelegt
- Namen, Sozialversicherungsnummern, medizinische Informationen zu Erkrankungen, Behandlungen, genetische Daten
- Daten ohne Verschlüsselung und ausreichende Authentifizierung auf Server mit öffentlichem Zugriff über Internet
- gravierender Verstoß Art. 32 DSGVO
- mehr Daten erhoben, als für Zweck notwendig
- Verstoß gegen Art. 29 DSGVO
- nach französischen Vorschriften Höchstbetrag

I. Aktuelle Bußgeldverfahren

Doctissimo

Bescheid: 2023

Bußgeld: 380.000 EUR

Verletztes Recht: Art. 5 Abs. 1 lit. e DSGVO, Art. 9 DSGVO, Art. 26 DSGVO, Art. 32 DSGVO

Vorgang:

- betreibt Website für Artikel, Tests, Quizze und Diskussionsforen für Gesundheit und Wohlbefinden
- Daten von durchgeführten Tests 24 Monate lang
- Daten über drei Jahren inaktiven Accounts ohne Anonymisierung
- keine Warnung oder Mechanismus zur Einholung der Einwilligung
- „http“-Kommunikationsprotokoll ohne SSL-Verschlüsselung verwendet
- Risiko Datenlecks
- Website automatisch Werbecookies auf Endgerät des Nutzers
- nach Ablehnen zwei Werbecookies gesetzt blieben
- 280.000 EUR Verstöße DSGVO
- 100.000 EUR Verwendung von Cookies.

I. Aktuelle Bußgeldverfahren

Unternehmen

Bußgeld: 20.000 EUR

Verstoß gegen: Art. 9 Abs. 1 DSGVO, Art. 6 Abs. 1 DSGVO

Vorgang:

- Corona-Pandemie: unsachgemäßer Umgang mit Gesundheitsdaten der Beschäftigten
- Daten über Impfstatus der Arbeitnehmer in Belegplan
- Kenntlich, in welchem Raum der Impfschutz höher oder niedriger ist

I. Aktuelle Bußgeldverfahren

Apotheke

Bußgeld: 6.500 EUR

Verstoß gegen: Art. 5 Abs. 1 lit. f DSGVO

Vorgang:

- nach Hinweis: Unterlagen und Dokumente gefunden
- personenbezogene Daten in Müllraum
- Vielzahl unberechtigter Personen hatte Zugang
- Videoüberwachung: auch die Bedienplätze der Arbeitnehmer*innen im Blickfeld
- Hinweisschild fehlte
- Teileinstellung, wegen Videoüberwachung

I. Aktuelle Bußgeldverfahren

Unternehmer

Bußgeld: 200 EUR

Verstoß gegen: § 26 BDSG

Vorgang:

- Unternehmen hatte personenbezogene Daten seiner Beschäftigten im Internet veröffentlicht: Urlaubsdaten

I. Aktuelle Bußgeldverfahren

Ärztin

Bußgeld: 500 EUR

Verstoß gegen: Art. 15 DSGVO

Vorgang:

- Ärztin hatte verspätet Auskunft über gespeicherte Daten erteilt

I. Aktuelle Bußgeldverfahren

Universitätsklinikum Magdeburg

Bußgeld: 9.000 EUR

Verstoß gegen: Art. 33 DSGVO

Vorgang:

- Datendiebstahl durch ehemalige Mitarbeiterin
- Mitarbeiterin Zugehörigkeit zur linksextremen Szene
- Meldeangaben von Personen, mit Bezug zur Rechten-Szene und zur AfD
- aufgefallen am 15. Mai 2021
- Meldung an Behörde erst Oktober 2021

I. Aktuelle Bußgeldverfahren

Arzt

Bußgeld: 50 EUR

Verstoß gegen: Art. 83 Abs. 4 lit. a DSGVO, Art. 32 DSGVO

Vorgang:

- Patientenakten im Altpapiercontainer entsorgt

I. Aktuelle Bußgeldverfahren

Unternehmen aus der Gesundheitsbranche

Bußgeld: 37.500 EUR

Verstoß gegen: Art. 6 Abs. 1 DSGVO, Art. 9 Abs. 1 DSGVO, Art. 38 Abs. 6 DSGVO

Vorgang:

- Mitarbeiter und Patienten mit Videokameras überwacht
- Datenschutzbeauftragter keine unabhängige Person, gehörte zur Unternehmensleitung
- Interessenkonflikt mit seiner Rolle als Datenschutzbeauftragter

II. Rechtsfragen im Bußgeldverfahren

EuGH C 807/21 - Deutsche Wohnen

- Deutschen Wohnen Bußgeldbescheid 14 Millionen Euro
- personenbezogene Daten nicht ordnungsgemäß gelöscht
- Unternehmen muss sich Verhalten jeder Person zurechnen lassen, die für das Unternehmen handelt

1. Bußgeld setzt zwingend vorsätzliche oder fahrlässige Verletzung voraus
2. nicht Pflichtverletzung über vertretungsberechtigte Person (Leitungsorgan)
3. ausschließlich DSGVO, nicht §§ 30, 130 OWiG
4. Unternehmensbegriff: wirtschaftliche Einheit, auch mit mehreren juristischen Personen
   Konzernumsatz maßgeblich

II. Rechtsfragen im Bußgeldverfahren

Sanktionen nach BDSG sind:

- Strafverfahren § 42 BDSG Freiheitsstrafe bis 3 Jahre oder Geldstrafe

- Geldbußen § 43 BDSG bis 50.000 €

Hinsichtlich Sanktionen gilt nemo tenetur-Grundsatz, d.h. man muss sich nicht selbst belasten und nicht nach dem Verantwortlichen suchen, nur den Fehler beseitigen und Schaden begrenzen

II. Rechtsfragen im Bußgeldverfahren

Verstöße gegen Art. 83 V, VI DSGVO:

- Bußgelder bis 20 Mio. Euro oder bis 4 % des gesamten weltweit erzielten Jahresumsatzes des Unternehmens im vorangegangenen Geschäftsjahr (je nachdem, was höher ist)

Verstöße gegen Art. 83 IV DSGVO:

- Bußgeld bis zu 10 Mio. Euro oder bis zu 2 % des Jahresumsatzes

II. Rechtsfragen im Bußgeldverfahren

Ursachen für Einleitung von Bußgeldverfahren:

- Beschwerde von Dritten bei Aufsichtsbehörde nach Art. 77 DSGVO
- eigene Datenpannenmeldung nach Art. 33 DSGVO bei der Aufsichtsbehörde
- Beschwerden von Verbraucherschutzorganisationen
- Presseberichte
- Whistleblower
- Betriebsrat

II. Rechtsfragen im Bußgeldverfahren

1. Einfache Fälle:

- E-Mail wird versehentlich im cc statt im bcc versendet

2. Mittelschwere Fälle:

- Komplizierte technische Gestaltung

3. Schwerwiegende Vorfälle:

- Datenschutzverstoß ist Teil einer unzureichenden Datenschutzorganisation
- ein vom Verantwortlichen zu vertretender Fehler des Datenschutzsystems
- Hacking/ IT-Sicherheit
- Microsoft Exchange
- Schadprogramme für Windows-Systeme in Form von Microviren: Emotet

III. Behördliches Vorgehen

Untersuchungsbefugnisse der Aufsichtsbehörde laut Art. 58 I DSGVO:

- Informationsanforderung
- Datenschutzüberprüfung durch Behörde
- Zertifizierungsüberprüfung
- Hinweis an Verantwortlichen auf vermeintlichen Verstoß
- Verlangen auf Zugang zu Daten und Infos
- Zugang zu Räumlichkeiten und Datenverarbeitungsanlagen

III. Behördliches Vorgehen

Abhilfebefugnisse der Behörde gemäß Art. 58 II DSGVO:

- Warnung vor voraussichtlichen Verstößen
- Verwarnung, wenn verstoßen wurde
- Anordnung: Verarbeitungsvorgänge in Ordnung zu bringen
- Anweisung: betroffene Personen zu benachrichtigen
- Vorübergehende oder endgültige Verarbeitungsbeschränkung bzw. Verbot
- Anordnung der Berichtigung

III. Behördliches Vorgehen

Abhilfebefugnisse der Behörde gemäß Art. 58 II DSGVO:

- Löschungsanordnung
- vorübergehende/ endgültige Einschränkung der Verarbeitung
- Unterrichtung von Empfängern
- Widerruf einer Zertifizierung
- Anordnung der Übermittlungsaussetzung an Drittland oder internationale Organisationen
- verschiedene Maßnahmen sind parallel zulässig

III. Behördliches Vorgehen

Aktuelle Behörden-Praxis:

- Androhung von Zwangsgeldern: häufig
- Zwangsgeldfestsetzung: selten
- Anweisungen: selten
- Verwarnungen: häufig
- Beanstandungen: häufig
- Verhängung von Bußgeld: häufig
- Klagen gegen Maßnahmen: selten

IV. Schadensersatz aus DSGVO

Rechtsgrundlage § 82 DSVGO

LG Bonn, 24.05.2022:

Bei Auskunft nach Art. 15 DSGVO muss über alle Daten, die über die betroffene Person vorliegen, Auskunft erteilt werden.

- „Die Abrechnung betreffenden personenbezogenen Daten der Klägerin (Krankenversicherungsdaten, Rechnungen, Zahlungen und Zahlungsdaten) sind Daten im Sinne der DSGVO."
- „Schreiben der Klägerin an die Beklagten und umgekehrt sind grundsätzlich ihrem gesamten Inhalt nach als personenbezogene Daten gemäß Art. 4 Nr. 1 DSGVO anzusehen. Dass die Schreiben und Rechnungen der Klägerin bereits bekannt sind, schließt für sich genommen den datenschutzrechtlichen Auskunftsanspruch nicht aus."

IV. Schadensersatz aus DSGVO

LG Bonn, Beschluss vom 24.05.2022 - 9 O 158/21,

openJur 2022, 1613

Tenor

wird der Verkündungstermin vom 27.05.2022 aufgehoben und die mündliche Verhandlung gemäß § 156 ZPO wiedereröffnet.

Gründe

Die Beklagten haben mit nachgelassenem Schriftsatz vom 14.04.2022 neue Tatsachen vorgetragen, auf die die Klägerin mit Schriftsatz vom 12.05.2022 in relevanter Weise erwidert hat, sodass die mündliche Verhandlung wiederzueröffnen ist.

Die Kammer weist gemäß § 139 ZPO auf Folgendes hin:

So ist für die Kammer nicht nachvollziehbar, dass die Beklagte zu 1) die die Abrechnung betreffenden personenbezogenen Daten der Klägerin (Krankenversicherungsdaten, Rechnungen, Zahlungen und Zahlungsdaten) im Sinne der DSGVO beauskunftet haben. Schreiben der Klägerin an die Beklagten und umgekehrt sind grundsätzlich ihrem gesamten Inhalt nach als personenbezogene Daten gemäß Art. 4 Nr. 1 DS-GVO anzusehen. Dass die Schreiben und Rechnungen der Klägerin bereits bekannt sind, schließt für sich genommen den datenschutzrechtlichen Auskunftsanspruch nicht aus. Sofern die Beklagten die erteilte Auskunft beschränkt auf die Behandlungsunterlagen als vollständig bezeichnen, sind, wie klägerseits zu Recht beanstandet, die Abrechnungsdaten nicht erfasst, gleichwohl jedoch zu beauskunften. Vor dem Hintergrund dieses Fehlverständnisses kommt es nicht darauf an, dass die Beklagte zu 1) die Auskunft als vollständig bezeichnet (vgl. BGH, Urteil vom 15.06.2021 - VI ZR 576/19 -).

Des Weiteren kommt in Betracht, dass auch interne Vermerke oder interne Kommunikation bei der Beklagten zu 1) Informationen über die Klägerin enthalten können; die auf der Grundlage dieser personenbezogenen Daten vorgenommene Beurteilung der Rechtslage seitens der Beklagten zu 1) oder Dritter selbst stellt aber keine Information über den Betroffenen und damit kein personenbezogenes Datum dar (vgl. BGH, Urteil vom 15.06.2021 - VI ZR 576/19 -).

Den bisherigen, prozessual zuzulassenden Auskünften der Beklagten zu 1) ist nicht hinreichend deutlich zu entnehmen, dass sich interne Vermerke, interne Kommunikation oder auch die Kommunikation sowohl mit dem Versicherer, der ebenfalls zu beauskunften ist, als auch den Prozessbevollmächtigten der Beklagten hinsichtlich der personenbezogenen Daten auf die erteilte Auskunft beschränkt, auch wenn der - nicht nachgelassene - Schriftsatz der Beklagten vom 23.05.2022 hierauf hindeutet.

Es besteht Gelegenheit zur Stellungnahme für die Beklagte zu 1) zum Hinweis der Kammer bis zum ...2022.

IV. Schadensersatz aus DSGVO

Rechtsgrundlage § 82 DSVGO

OLG Düsseldorf, Urteil 28.10.2021:

Vorwurf:

- Gesundheitsakte von GKV an falsche E-Mail-Adresse gesandt
- Löschung des E-Mail-Postfaches erfolgte mehrere Monate später
- Betroffene wusste das 9 Monate lang nicht

Vorschrift: Art. 6 DSGVO

Schadensbetrag: 2.000 €

IV. Schadensersatz aus DSGVO

Rechtsgrundlage § 82 DSVGO

LG Köln, Urteil 18.05.2022:

Vorwurf:

- Datenleck mit Konto-, Ausweisdaten bei Finanzdienstleister
- fehlende organisatorische Maßnahmen

Vorschrift: Art. 32 DSGVO

Schadensbetrag: 1.200 €

IV. Schadensersatz aus DSGVO

EUGH-Urteil vom 04. Mai 2023 (C-300/21) zu § 82 DSGVO

- Schadensnachweis erforderlich, es gibt keine Erheblichkeitsschwelle, Schadenshöhe nach nationalen Gesetzen

IV. Schadensersatz aus DSGVO

Rechtsgrundlage § 82 DSVGO

OLG Köln, Urteil 14.07.2022:

Vorwurf:

- Verspätete Auskunft von Anwalt an früheren Mandanten

Vorschrift: Art. 15 DSGVO

Schadensbetrag: 500 €

V. Guidelines EDSA

Guidelines zur Bußgeldberechnung:

- 24.05.2023 (Version 2.1): Veröffentlichung der Guidelines 04/2022 des Europäischen Datenschutzausschusses (EDSA)
- Sollen die von der Art. – 29 – Datenschutzgruppe in 2017 erlassenen Guidelines WP253 ergänzen
- Neues Konzept für einheitliche Basis für Berechnung von Bußgeldern schaffen
- Ziel: einheitliche Ausgangslage und Methode der Berechnung
- Bußgeldberechnung soll einzelfallbezogen bleiben und umfassende Abwägung aller jeweiligen Umstände erfordern, Ermessen der nationalen Behörden bleibt nach wie vor erheblich
- Bußgelder mit deutlich abschreckenderem Charakter
- Umsatz und Unternehmensgröße sollen nicht mehr zentral im Vordergrund
- anders als beim bisher deutschen Bußgeldkonzept

V. Guidelines EDSA

Berechnungskonzept mit 5 Schritten:

1. Ermittlung des Verarbeitungsprozesses als Grundlage der Bußgeldentscheidung

2. Ausgangspunkt der Berechnung anhand der jeweiligen Verstoßkategorie (Artikel 83 Abs. 4 bis 6 und Schwere und Dauer des Verstoßes Artikel 83 Abs. 2 sowie weltweit erzielter Jahresumsatz eines Unternehmens Artikel 83 Abs. 4 und 5)

3. 4. und 5. Schritt Sicherstellen, dass Gesamtsumme dem Erfordernis eines wirksamen verhältnismäßigen und abschreckenden Bußgeldes genügt und nicht die gesetzlichen Maximalsummen nach Art. 83 Abs. 4 bis 6 überschritten werden

…gewährt Aufsichtsbehörden Ermessen zur weiteren Anpassung der Bußgeldsumme

V. Guidelines EDSA

- Anders als nach bisherigem deutschen Bußgeldmodell:

- Unternehmensumsatz nicht mehr grundlegender Berechnungsausgangspunkt nur noch eines von mehreren Kriterien

- Guidelines sollen kleine Unternehmen entlasten

- Datenschutzaufsichtsbehörden sollen unmittelbar Bußgelder gegen Muttergesellschaften für Datenschutzverstößen von Tochtergesellschaften verhängen

VI. Zusammenfassung

I. gute Meldeorganisation

II. gute Dokumentation und detaillierte Begründung von Vorfallbearbeitung

III. sofortige Reaktion auf Behördenaktion

IV. sofortige Kontaktaufnahme mit Behörde

V. möglichst sofortige Anpassungsmaßnahmen

VI. sofortige Kommunikation von Anpassungsmaßnahmen mit Behörde

VII. ständige aktive Kommunikation mit Behörde

VIII. keine Hilfestellung für Ermittlungen gegen verantwortliche Personen

Vielen Dank

für Ihre Aufmerksamkeit!