PRODATIS®

The eBusiness Solution Company.

Bußgelder der Datenschutz-Aufsichtsbehörden – aktuelle Beispiele

Bußgelder der Datenschutz-Aufsichtsbehörden – aktuelle Beispiele

An einem Tätigkeitsbericht sind aus Sicht der Datenschutz-Praxis häufig die verhängten Bußgelder und die entsprechenden Sachverhalte am spannendsten. Lesen Sie, was sich dazu aus dem aktuellen Brandenburgischen Tätigkeitsbericht ziehen lässt. Fast 70.000 Euro verhängte die Datenschutz-Aufsicht in Brandenburg an Bußgeldern

Erst kürzlich hat die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg (LDA) ihren Tätigkeitsbericht für 2019 vorgelegt. Er enthält einige wichtige Hinweise, nicht nur zur Bußgeld-Praxis, sondern auch zu besonders kritischen Punkten, die bei Unternehmen mehr Aufmerksamkeit verdienen.

Nachfolgend finden Sie eine Darstellung ausgewählter Aspekte des Berichts.

Im Berichtszeitraum verhängte Bußgelder

Das Resultat der Sanktionen kann sich sehen lassen: 24 abgeschlossene Bußgeldverfahren, davon endeten immerhin 11 mit einer Geldbuße (Gesamtbußgeld 69.150 EUR).

Wichtig ist zu wissen, dass die Datenschutz-Aufsicht den überwiegenden Teil der Bußgeldverfahren noch nach altem Recht und Sanktionshöhe abgeschlossen hat (welche genau das sind, verrät die Landesbeauftragte allerdings nicht).

Anlässe waren hier etwa Videoüberwachungen, fehlende / fehlerhafte Verträge zur Auftragsverarbeitung und der mangelhafte Umgang mit Patienten- und Mitarbeiterdaten.

Von besonderer Bedeutung sind drei Bußgeldfälle, die die Beauftragte ausführlich darstellt (S. 28 ff.):

Bußgeld-Fall 1: Videoüberwachung im Schwimmbad

Der Schwimmbadbetreiber filmte munter Gäste und Mitarbeiter sowohl beim Betreten des Grundstücks als auch bei den Aktivitäten bzw. bei der Arbeit und speicherte die Aufnahmen „dauerhaft“ (wie lange, verrät der Bericht nicht).

Die Beauftragte betont, dass es wesentlich – ungeachtet der Rechtsgrundlage – auf die Erforderlichkeit im Hinblick

auf die vom Betreiber aufgeführten Zwecke ankomme, die schon offensichtlich nicht gegeben sei.

Dass er sich bei der Installation der Videokameras keinen rechtlichen Rat einholte, bewertet der Bericht als fahrlässig. Zudem benannte der Betreiber („über mehrere Jahre") keinen Datenschutzbeauftragten (trotz Benennungspflicht) und schloss keinen AV-Vertrag mit einem Dienstleister, der die Videoüberwachungsanlage wartet.

Bußgeld: 12.000 EUR

Bußgeld-Fall 2: Erteilung von Auskünften unter fremdem Logo

Ein Unternehmen beauftragte einen Dienstleister damit, Auskunftsanfragen nach Art. 15 Datenschutz-Grundverordnung (DSGVO) zu bearbeiten.

Es schloss jedoch kein AV-Vertrag, obwohl er dem Dienstleister einen umfassenden Zugriff auf alle Daten und Systeme, die zur Auskunftserteilung relevant sind, gewährte.

Überdies lag ein Verstoß gegen den Transparenzgrundsatz (Art. 12 DSGVO) vor. Der Dienstleister – über dessen Einsatz der Verantwortliche nicht gemäß Art. 13 Abs. 1 Buchst. e DSGVO informierte – erteilte die Auskunft quasi in eigenem Namen mit eigenem Logo, sodass der Betroffene nicht erkennen konnte, wer nun eigentlich der Verantwortliche war.

Zudem erfolgte die Auskunftserteilung (zunächst) nur in englischer Sprache (Verstoß gegen Grundsatz der Verständlichkeit in Art. 12 DSGVO). Problem: Richtet sich ein Unternehmen mit seinem Angebot an den deutschsprachigen Markt, muss die Auskunft zumindest auch auf Deutsch erfolgen.

Ob man einem Dienstleister – je nach Sachverhalt – einen derart umfassenden Zugriff geben möchte, muss jeder – unabhängig von der grundsätzlichen rechtlichen Zulässigkeit – selbst beurteilen.

Bußgeld: 50.000 EUR (Die Kooperation mit der Aufsichtsbehörde hat die Landesbeauftragte mildernd berücksichtigt)

Bußgeld-Fall 3: Sicherung von Patientendaten als Freundschaftsdienst

Der nächste Fall verwunderte sicherlich auch die Landesbeauftragte. Hier beauftragte ein Mediziner einen Bekannten damit, seine Patienten- und Mitarbeiterdaten zu sichern.

„Leider" speicherte der Bekannte die zu sichernden Daten auf dem Computer an seinem Arbeitsplatz. Dort entdeckte sie der Arbeitgeber wohl aufgrund der Dateigröße– schon war die unbefugte Offenlegung geschehen.

Der Fall zeigt deutlich, dass der Verantwortliche stets „verantwortlich" auch für solche Verarbeitungen bleibt, die er im Rahmen eines Auftragsverarbeitungs-Verhältnisses auslagert. Hier lag also offensichtlich ein Verstoß gegen Art. 32 i.V.m. Art. 28 DSGVO vor.

Für die Praxis von besonderer Bedeutung ist, dass der Mediziner nicht einfach darauf vertrauen durfte, dass der Dienstleister angemessene technische und organisatorische Maßnahmen zum Schutz der Daten ergreift und den Auftrag weisungsgemäß ausführt. Er hätte sich vielmehr aktiv davon überzeugen müssen.

Diese Pflicht vernachlässigen Verantwortliche in der Praxis leider immer noch allzu oft. Häufig mit dem Argument „bei dem sind die Daten schon sicher"- das ist manchmal wohl ein teurer Trugschluss.

Bußgeld: genaue Höhe unbekannt („in vierstelliger Höhe")

Anlasslose Prüfungen nehmen zu

Die Landesbeauftragte berichtet auch von zahlreichen anlasslosen Prüfungen ihrer Behörde, sowohl bei öffentlichen als auch bei nicht-öffentlichen Stellen.

Themen waren neben dem Betrieb von Facebook-Fanpages insbesondere Arztpraxen und ihre Datenschutz-Information gegenüber den Patienten und – nicht notwendige – Ein-

willigungen im Rahmen des Behandlungs-Verhältnisses. Hier war nur ca. die Hälfte der Prüfungen beanstandungsfrei (S. 40).

Achtung bei Datenübermittlung an Postdienstleister
Von Bedeutung dürfte auch die Auffassung der LfDI sein, dass sich eine Übermittlung von E-Mail-Adressen durch (Online-)Versandhändler an den Postdienstleister nicht auf berechtigte Interessen (Art. 6 Abs. 1 Buchst. f DSGVO) stützen lassen, sondern nur auf eine Einwilligung des Betroffenen (S. 52).

Das Argument, dass die Übermittlung und dadurch die Information über den Sendungsstatus (auch) im Interesse der Empfänger liegt, etwa um den Erhalt der Sendung am Zustelltag zu organisieren, ließ die LDA nicht gelten.

Begründung: Die Zustellinformation kann der Onlinehandel auch unmittelbar selbst weitergeben bzw. einen Link zur Sendungsverfolgung in die Versandbestätigung einbinden.

Zurückhaltung von Städten / Gemeinden bei Veröffentlichung von Jubilarslisten
Die Landesbeauftragte weist ausdrücklich darauf hin, dass die Veröffentlichung von Geburtstags-Jubilaren (z.B. Herr Müller feiert seinen 100. Geburtstag) im jeweiligen Amts- / Mitteilungsblatt nur mit einer informierten und ausdrücklichen Einwilligung des Jubilars möglich ist (S. 74).

Nicht jeder Betroffene wolle derart im Fokus der Öffentlichkeit stehen, sodass andere Rechtsgrundlagen nicht in Betracht kommen.

Datensicherheit bei Fax-Übermittlung von sensiblen Daten nicht gewährleistet
Zu diesem bekannten und heiß diskutierten Thema positioniert sich auch die Landesbeauftragte (S. 81 ff.). Sie hält den Einsatz von Faxgeräten- und Faxdiensten bei der Übermittlung von sensiblen Daten (z.B. im Gesundheitsbereich) gemäß Art. 32 DSGVO für unzulässig.

Achtung: Hierunter kann auch schon die Übermittlung einer Arbeitsunfähigkeitsbescheinigung per Fax zählen.

Die eingesetzten Übermittlungswege für bestimmte Datenkategorien im Unternehmen sollten also insgesamt daraufhin überprüft und ggf. nachjustiert werden.

Welche Formen der Übermittlung hält die Landesdatenschutzbeauftragte für sensible Daten geeignet und angemessen?

Hierzu zählen etwa
- die persönliche Übergabe (Authentifizierung nicht vergessen),
- der Versand per Briefpost oder Kurier (verschlossen) sowie
- die leider noch nicht allzu praxis- und massentaugliche Ende-zu-Ende-Verschlüsselung bei E-Mails.

Unverschlüsselte E-Mails zu nutzen oder per Telefax in (heute standardmäßig anzutreffenden) IP-basierten Netzen zu kommunizieren, entspreche grundsätzlich nicht den datenschutzrechtlichen Anforderungen.

Weitere interessante Zahlen und Fakten
- 878 Beschwerden sind eingegangen
- über 400 schriftliche Beratungen (telefonische wurden nicht erfasst / gezählt)
- 362 Datenpannen-Meldungen (30 Fälle davon aus dem Bereich Hacking, Phishing, Erpressen; bei 10 Meldungen waren mehr als 1.000 Personen betroffen)
- 20 mal von Abhilfemaßnahmen Gebrauch gemacht, ohne Bußgeld (10 Verwarnungen, 4 Warnungen, 6 Anordnungen bzgl. eines Tuns oder Unterlassens)
- 47 bearbeitete Bußgeldverfahren (ca. die Hälfte nach neuer Rechtslage)

Fazit: Balance zwischen Aufklärung und Sanktionen
Dem Tätigkeitsbericht lassen sich einige praxisrelevante Sachverhalte und Empfehlungen entnehmen, die in der Praxis von großer Relevanz sind.

Er zeigt zugleich, worauf Verantwortliche in Unternehmen und Behörden lieber zweimal schauen und besonderen Wert legen sollten.

Die Landesbeauftragte scheint aus der Ferne auch einen guten und fairen Ausgleich zwischen „Aufklärung“ (und Warnung) und spürbarer monetärer Sanktionierung von datenschutzrechtlichem Fehlverhalten gefunden zu haben.

Dass dieser Ausgleich nicht immer gelingt, sieht man bei anderen Aufsichtsbehörden (z.B. beim aktuellen Tätigkeitsbericht des ULD).

Quelle:
www.datenschutz-praxis.de