Fehlende Einwilligung? Daten im Hausmüll? Das wird teuer!

Neue Datenschutz-Bußgelder zielen auf gesetzeskonformes Verhalten – nicht auf Existenzvernichtung

▸▸ Medical-Tribune-Recherche

Fachtagung „Datenschutz in der Medizin – Update 2018“

WIESBADEN. Ab dem 25. Mai 2018 gilt die neue EU-Datenschutzgrundverordnung auch in Deutschland. Sie soll europaweit gleichwertigen Datenschutz gewährleisten. Um das durchzusetzen, bringt sie einen knackigen Sanktionenkatalog mit sich. Was heißt das für die Praxis?

Bislang sind die Sanktionsmöglichkeiten gegen Datenschutzverstöße in den europäischen Ländern sehr unterschiedlich: In Spanien müssen sich die Behörden z.B. über die Bußgelder selbst finanzieren, berichtet Sonja Wirtz, Referentin der Datenschutzaufsichtsbehörde Rheinland-Pfalz, auf der Fachtagung „Datenschutz in der Medizin – Update 2018“. In Belgien dagegen wirken die Zuständigen ausschließlich als Mediatoren und können gar keine Bußgelder verhängen.

Und selbst innerhalb von keine Möglichkeit, Bußgelder zu verhängen, während die Behörde in Rheinland-Pfalz im Jahr 2014 ein Bußgeld gegen die Debeka Krankenversicherung in Höhe von insgesamt 1,3 Mio. Euro verhängt hat, um nur eines der Beispiele zu nennen.

Höhe der neuen Bußgelder klingt erst mal absurd

Aktuell liegen die Obergrenzen für Bußgelder bei Datenschutzverstößen noch bei 50 000 bzw. 300 000 Euro, abhängig von der Schwere des Verstoßes. Mit dem Wirksamwerden der Datenschutzgrundver-

Berechnung des Bußgeldes an einem fiktiven Fall

Bei der Entscheidung über den Betrag einer Geldbuße werden in jedem Einzelfall Zumessungskriterien (siehe Kasten unten) berücksichtigt. Beispiele zur Bußgeld-Festsetzung können deswegen nicht verbindlich sein. Der folgende **fiktive Fall** macht das Prinzip anschaulich:

Eine Arztpraxis hat über einen Zeitraum hinweg Patientendaten über den Hausmüll entsorgt und damit einen sehr schweren Datenschutzverstoß begangen. Es wurde entschieden, ein Bußgeldverfahren einzuleiten.

1) Es geht um einen Verstoß, der nach Art. 83 Abs. 5 lit. a DSGVO geahndet wird, damit liegt der Höchstbetrag der Geldbuße bei 20 Mio. €.
2) Der Jahresumsatz der Arztpraxis liegt bei angenommenen 500 000 €. Orientiert sich die Behörde an einem der BaFin-Tabelle ensprechenden System, könnte der Nominalwert bei 100 000 € (bis etwa 200 000 €) liegen.
3) Der Bußgeldbetrag wird den Zumessungskriterien der DSGVO folgend angepasst:

Dauer: über gewissen Zeitraum	+ 30 % ↑
Vorsatz: fahrlässig	– 50 % ↓
Maßnahmen zur Minderung: regulär	± 0 % →
Grad der Verantwortlichkeit: regulär	± 0 % →
Frühere Verstöße: keine	± 0 % →
Zusammenarbeit mit Behörde: regulär	± 0 % →
Kategorie der Daten	+ 25 % ↑
Verstoß wurde über Anzeige bekannt	+ 25 % ↑
Früher angeordnete Maßnahmen: keine	± 0 % →
Einhaltung von Verhaltensregeln: regulär	± 0 % →
Summe:	**+ 30 % ↑**
100 000 € + 30 %	**= 130 000 €**

4) Berücksichtigung der wirtschaftlichen Verhältnisse (§ 17 OWiG): Keine Anhaltspunkte für Verringerung

geld kommt. Das entscheidet sich anhand von Kriterien, die die DS-GVO mitliefert (§ 83 Abs. 2, siehe Kasten). Dazu gehören zum Beispiel die Art und Schwere des Verstoßes, der Grad der Verantwortung, etwai-

sung ggf. mit Zwangsgeldandrohung das Mittel der Wahl ist. Außerdem hat die Behörde in Zukunft die Möglichkeit, eine Zertifizierung zu widerrufen. Und dann kann sie eben auch noch Bußgelder verhängen.

anzuwendenden Höchstrahmen des Bußgeldes auf einen nominalen Grundwert geschlossen werden. Um ein europaweit einheitliches Vorgehen zu erarbeiten, könnten in Zukunft etwa Einteilungsmatrixen wie

Deutschland gibt es Unterschiede. Die Behörde in Baden-Württemberg hatte z.B. bisher selbst gar

„Diese Bußgeldhöhen sind natürlich nicht für die Hausarztpraxis im Mainzer Vorort erdacht"

ordnung (DSGVO) im Mai werden diese Grenzen bei 10 Millionen bzw. 20 Millionen liegen, erklärt Wirtz. Das klingt absurd hoch.

Diese Bußgeldhöhen sind natürlich nicht für die Hausarztpraxis im Mainzer Vorort erdacht worden, relativiert die Referentin. Wird ein Datenschutzverstoß festgestellt, muss zunächst geprüft werden, ob es überhaupt zu einem Bußge frühere Verstöße und die Kooperationsbereitschaft.

Denn eine Datenschutzaufsichtsbehörde hat verschiedene Sanktionsmittel zur Auswahl. Nach den Vorgaben der neuen Grundverordnung (§ 58 Abs. 2) kann sie z.B. zur Abwehr zukünftiger Verstöße eine Warnung aussprechen, während bei andauernden Verstößen eine Verwarnung und irgendwann auch eine Anwei-

Noch fehlt die einheitliche Auslegung der Kriterien

Nach einem Bußgeldkatalog sucht man allerdings noch vergebens. Zwar ist das Ziel der DSGVO nicht nur die europaweite Abstimmung der Normen, sondern auch der Bußgelder, doch noch fehlt die einheitliche Auslegung der Vorgaben. So muss in jedem konkreten Fall zunächst vom

die der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zur Anwendung kommen, über die die Unternehmen anhand der Kriterien Umsatz und Tatumstände in Gruppen eingeteilt werden, denen ein nominaler Grundwert zugeordnet wird. Im nächsten Schritt würden sich dann individuelle Umstände (§ 83 Abs. 2, siehe Kasten), gemessen an den Zumessungskriterien, positiv oder negativ auf die Höhe des Bußgeldes auswirken.

„Rechtsprechung wird nach und nach den Weg weisen"

Oder es wird irgendwann vielleicht doch einen Bußgeldkatalog geben, der – etwa wie die ADAC-Schmerzensgeldtabelle – aus der laufenden Rechtsprechung entstanden sein wird, kann sich Wirtz vorstellen. Doch bis dahin werden erst noch einige richterliche Entscheidungen gefällt werden müssen.

Anouschka Wasner

Zumessungskriterien für Geldbußen (Auszug Art. 83 DSGVO)

Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

- Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
- Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
- jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
- Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;
- etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;
- Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;
- Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
- Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;
- Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;
- Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und
- jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.