Sanktionsmöglichkeiten bei Datenschutzverstößen

Dr. Bernd Schütze

Seminar Datenschutz-Grundverordnung (DS-GVO)

HEALTHCARE SOLUTIONS

Agenda

Datenschutzrechtliche Sanktionsmöglichkeiten

- Befugnisse Aufsichtsbehörden
- Bußgelder
- Strafvorschriften

Befugnisse Aufsichtsbehörden

Befugnisse Datenschutz Aufsichtsbehörden

Art. 58 Abs. 1 DS-GVO: Untersuchungsbefugnisse

Befugnisse,

- Verantwortlichen bzw. ggf. dessen Vertreter, Auftragsverarbeiter **anzuweisen, alle Informationen bereitzustellen**, die für die Erfüllung ihrer Aufgaben erforderlich sind
- **Untersuchungen** in Form von Datenschutzüberprüfungen **durchzuführen**
- eine Überprüfung der nach Artikel 42 Absatz 7 erteilten Zertifizierungen durchzuführen
- den Verantwortlichen oder den Auftragsverarbeiter auf einen vermeintlichen Verstoß gegen diese Verordnung hinzuweisen
- vom Verantwortlichen und Auftragsverarbeiter **Zugang zu allen personenbezogenen Daten und Informationen**, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten
- **Zugang** zu den **Geschäftsräumen**, einschließlich **aller Datenverarbeitungsanlagen und -geräte**, des Verantwortlichen und des Auftragsverarbeiters zu erhalten

Befugnisse Datenschutz Aufsichtsbehörden

Art. 58 Abs. 2 DS-GVO: Abhilfebefugnisse

Befugnisse,

- einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen
- einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen diese Verordnung verstoßen hat
- den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach dieser Verordnung zustehenden Rechte zu entsprechen
- den Verantwortlichen oder den Auftragsverarbeiter **anzuweisen**, Verarbeitungsvorgänge gegebenenfalls **auf bestimmte Weise** und **innerhalb eines bestimmten Zeitraums** in **Einklang mit der DS-GVO** zu bringen

Befugnisse Datenschutz Aufsichtsbehörden

Art. 58 Abs. 2 DS-GVO: Abhilfebefugnisse

Befugnisse,

- den Verantwortlichen **anzuweisen**, die von einer Verletzung des Schutzes personenbezogener Daten **betroffenen Person entsprechend zu benachrichtigen**
- eine **vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots**, zu verhängen
- die **Berichtigung oder Löschung** von personenbezogenen Daten oder **die Einschränkung der Verarbeitung** und die **Unterrichtung der Empfänger** der Daten über die angeordneten Maßnahmen anzuordnen

Befugnisse Datenschutz Aufsichtsbehörden

Art. 58 Abs. 2 DS-GVO: Abhilfebefugnisse

Befugnisse,

- eine Zertifizierung zu widerrufen oder die Zertifizierungsstelle anzuweisen, eine gemäß den Artikel 42 und 43 erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden
- eine **Geldbuße gemäß Artikel 83** zu verhängen**, zusätzlich zu oder anstelle** von in diesem Absatz genannten Maßnahmen, je nach den Umständen des Einzelfalls
- die **Aussetzung der Übermittlung von Daten** an einen Empfänger in einem **Drittland** oder an eine internationale Organisation anzuordnen.

Befugnisse Datenschutz Aufsichtsbehörden

Art. 58 Abs. 3 DS-GVO: Genehmigungs- und Beratungsbefugnisse

Befugnisse,

- **Verantwortlichen** im Rahmen der der vorherigen **Konsultation nach Art. 36** (DSFA) zu **beraten**
- Von sich aus oder auf Anfrage: **Stellungnahmen zu allen Fragen**, die im Zusammenhang mit dem **Schutz personenbezogener Daten stehen**, an das nationale Parlament, die Regierung des Mitgliedstaats oder an sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit zu richten
- **Verhaltensregeln** nach Art. 40: Stellungnahme abzugeben und **Entwürfe billigen**
- Zertifizierungsstellen gemäß Artikel 43 zu akkreditieren
- **Drittstaatenverarbeitung**
  - **Standarddatenschutzklauseln** nach Art. 28 Abs. 8 und Art. 46 Abs. 2 lit. d **festzulegen**
  - **Vertragsklauseln** gemäß Art. 46 Abs. 3 lit. a zu **genehmigen**,
  - **Verwaltungsvereinbarungen** gemäß Art. 46 Abs. 3 lit. b zu **genehmigen**
  - **Verbindliche interne Vorschriften** gemäß Art. 47 zu **genehmigen**

Bußgelder

Bußgelder

Art. 83. Abs. 5,6 DS-GVO: Geldbußen bis zu 20 Mill Euro (bzw. 4% Umsatz)

- Verstöße bzgl.
  - Artt. 5, 6, 7, 9 (fehlende oder fehlerhaft eingeholte Einwilligung)
  - Artt. 12-22 (Verstoß gegen die Rechte der/des Betroffenen)
  - Artt. 44 bis 49 (Unrechtmäßige Übermittlung in ein Drittland oder int. Organisation)
  - Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde

  beseitigen.
- D.h.
  - Einwilligungsformulare sowie Prozess Einholung Einwilligung wie auch Widerspruch Einwilligung anpassen
  - Prozesse zur Wahrung Betroffenenrechte etablieren (z.B. Archivierungs- und Löschkonzept)
  - Prüfen, ob und wie Daten in ein Drittland übermittelt werden (z.B. Wartung)

Bußgelder

Art. 83. Abs. 4 DS-GVO: Geldbußen bis zu 10 Mill Euro (bzw. 2% Umsatz)

- Verstöße bzgl.
  - Art. 25 (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen)
  - Art. 28 (Auftragsverarbeiter)
  - Art. 29 (Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters)
  - Art. 30 (Verzeichnis von Verarbeitungstätigkeiten)
  - Art. 31 (Zusammenarbeit mit der Aufsichtsbehörde)
  - Art. 32 (Sicherheit der Verarbeitung)
  - Artt. 33 u. 34 (Meldung von Datenpannen an Aufsichtsbehörde und Betroffenen)
  - Art. 35 (Datenschutzfolgenabschätzung)
  - Artt. 36 bis 39 (Datenschutzbeauftragter)

Bußgelder

Art. 83. Abs. 2 DS-GVO: Bei Verhängung zu berücksichtigen

- Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, z.B.
  - Meldete der Verantwortliche bzw. der Auftragsverarbeiter selbst das Vergehen an die Aufsichtsbehörde?
  - Erfuhr die Aufsichtsbehörde vom Betroffenen davon? Ggfs. aufgrund der Tatsache, dass der Verantwortliche den Betroffenen auf diese Möglichkeit hinwies?
  - Wurde die Aufsichtsbehörde erst über Dritte (z. B. Presse) informiert?
- Art, Schwere und Dauer des Verstoßes wie beispielsweise
  - Liegt ein genereller Verstoß vor, d. h. man kann generell der gesetzlichen Pflicht nicht genügen?
  - Sind es nur die konkreten Umstände des Einzelfalles, die ein Genügen der gesetzlichen Pflicht verhindern?
  - Wie groß ist der potentielle Schaden für jeden einzelnen Betroffenen? Wie groß ist der Schaden insgesamt?
- Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes, d.h. insbesondere ist zu betrachten
  - Wurde die gesetzliche Pflicht vom Verantwortlichen im Ablauf seiner Prozesse ignoriert?
  - Wurde fahrlässig einem einzelnen Betroffenen sein Recht verweigert

Bußgelder

Art. 83. Abs. 2 DS-GVO: Bei Verhängung zu berücksichtigen

- Umfang der Zusammenarbeit mit der Aufsichtsbehörde, z.B.
  - Wurden der Aufsichtsbehörde unverzüglich alle benötigten Informationen gegeben?
  - Wurden Anstrengungen unternommen, um nachteilige Auswirkungen zu mildern?
  - Wurden Anstrengungen unternommen, damit künftig Verstöße dieser Art nicht mehr vorkommen?
- Sind etwaige einschlägige frühere Verstöße bekannt?
  - Ist es Wiederholungstatbestand?
- Die Kategorien personenbezogener Daten, d.h. insbesondere ist zu betrachten
  - Im Kontext der Gesundheitsversorgung/-forschung handelt es sich immer um besondere Kategorien von Daten, sodass ein Verstoß schwerer wiegt

Bußgelder

§ 43 BDSG (neu)

- Geldbuße bis zu 50.000 Euro, wer vorsätzlich oder fahrlässig
  - a) entgegen § 30 Abs. 1 (Bewertung Kreditwürdigkeit bzgl. Verbraucherkredite) ein Auskunftsverlangen nicht richtig behandeln oder
  - b) entgegen § 30 Abs. 2 S. 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet
- Hinweis:
  - Gegen Behörden und sonstige öffentliche Stellen werden keine Geldbußen verhängt (§ 43 Abs. 3 BDSG)
  - Eine Meldung nach Art. 33 DS-GVO darf in einem Strafverfahren nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden (§ 43 Abs. 4 BDSG)

Strafvorschriften

Strafvorschriften

§ 42 BDSG (neu)

- Freiheitsstrafe bis zu 3 Jahren oder Geldstrafe

  Nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen ohne Rechtsgrundlage

  a) einem Dritten übermitteln oder
  b) auf andere Art und Weise zugänglich machen und hierbei gewerblich handeln

- Freiheitsstrafe bis zu 2Jahren oder Geldstrafe

  Nicht allgemein zugängliche personenbezogene Daten

  a) ohne Rechtsgrundlage verarbeiten oder
  b) durch unrichtige Angaben erschleicht und
     1. hierbei gegen Entgelthandeln oder
     2. in der Absicht handeln, sich oder einen anderen zu bereichern oder einen anderen zu schädigen

Strafvorschriften

§ 42 BDSG (neu)

- Hinweis
  - Verfolgung nur auf Antrag. Antragsberechtigt sind: betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde (§ 42 Abs. 3 BDSG)
  - Eine Meldung nach Art. 33 DS-GVO darf in einem Strafverfahren nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden (§ 42 Abs. 4 BDSG)

Strafvorschriften

Management Summary

Bußgelder der DS-GVO, Freiheitsstrafe BDSG n.F.

Geldbußen bis zu 20 Mill Euro (bzw. 4% Umsatz)

Verstöße bzgl.

- Artt. 5, 6, 7, 9 (fehlende oder fehlerhaft eingeholte Einwilligung)
- Artt. 12-22 (Verstoß gegen die Rechte der/des Betroffenen)
- Artt. 44 bis 49 (Unrechtmäßige Übermittlung in ein Drittland oder int. Organisation)
- Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde

Geldbußen bis zu 10 Mill Euro (bzw. 2% Umsatz)

Verstöße bzgl.

- Art. 25 (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen)
- Art. 28 (Auftragsverarbeiter)
- Art. 29 (Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters)
- Art. 30 (Verzeichnis von Verarbeitungstätigkeiten)
- Art. 31 (Zusammenarbeit mit der Aufsichtsbehörde)
- Art. 32 (Sicherheit der Verarbeitung)
- Artt. 33 u. 34 (Meldung von Datenpannen an Aufsichtsbehörde und Betroffenen)
- Art. 35 (Datenschutzfolgenabschätzung)
- Artt. 36 bis 39 (Datenschutzbeauftragter)

§ 42 BDSG (neu)

Freiheitsstrafe bis zu 3 Jahren oder Geldstrafe

- **Nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen ohne Rechtsgrundlage**
  - a) einem Dritten übermitteln oder
  - b) auf andere Art und Weise zugänglich machen und hierbei gewerblich handeln

Freiheitsstrafe bis zu 2 Jahren oder Geldstrafe

- **Nicht allgemein zugängliche personenbezogene Daten**
  - a) ohne Rechtsgrundlage verarbeiten oder
  - b) durch unrichtige Angaben erschleicht und
    1) hierbei gegen Entgelthandeln oder
    2) in der Absicht handeln, sich oder einen anderen zu bereichern oder einen anderen zu schädigen

Vorgehen Aufsichtsbehörden

Vorgehen Aufsichtsbehörden

Vorgehen muss europäisch harmonisiert werden

- vor Feststellung Datenschutzverstoß
  - Art. 58 Abs. 2 lit. a DS-GVO = Warnung
- Datenschutzverstoß festgestellt
  - Art. 58 Abs. 2 lit. b, c DS-GVO = Verwarnen
  - Art. 58 Abs. 2 lit. d, e, f, g, h, j DS-GVO = Anweisungen bzgl. Abhilfe
  - Art. 58 Abs. 2 lit. b, i DS-GVO = Bußgelder
- Grundsatz: Verhängung von Geldbußen muss in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein (Art. 83 Abs. 1 DS-GVO)
- Beachtung ErwGr. 148
  - „Im Falle eines **geringfügigeren Verstoßes** oder falls voraussichtlich zu verhängende Geldbuße eine **unverhältnismäßige Belastung** für eine **natürliche Person** bewirken würde, **kann anstelle einer Geldbuße eine Verwarnung** erteilt werden."
  - Cave: ErwGr. 148 gilt nicht für juristische Personen!

Fazit

Unternehmen/Organisationen müssen bedenken

- Aufsichtsbehörden können
  a) unangekündigt Datenschutz-Audits durchführen, wobei eine vollumfängliche Unterstützung mit Offenlegung aller Informationen und aller IT-Verfahren zu gewähren ist
  b) anweisen, wie Verarbeitungsverfahren geändert werden müssen, damit sie iun Einklang mit der DS-GVO erfolgen
  c) Verarbeitungsverfahren einschränken oder beenden
- Freiheitsstrafen können verhängt werden, wenn nicht allgemein zugängliche personenbezogene Daten
  - einer großen Zahl von Personen ohne Rechtsgrundlage Dritten zugänglich gemacht werden
  - einer großen Zahl von Personen auf andere Art und Weise zugänglich gemacht und hierbei gewerblich gehandelt wird
  - ohne Rechtsgrundlage verarbeitet werden

Fazit

Unternehmen/Organisationen müssen bedenken

- Bußgelder werden verhängt
  - fehlende oder fehlerhaft eingeholte Einwilligung
  - Verstoß gegen die Rechte der/des Betroffenen
  - Unrechtmäßige Übermittlung in ein Drittland oder int. Organisation
  - Nichtbefolgung der Anweisung einer Aufsichtsbehörde
  - Unzureichende Zusammenarbeit mit der Aufsichtsbehörde
  - Ungenügende Gewährleistung der Sicherheit der Verarbeitung
  - Fehlerhafte Auftragsverarbeitung
  - Fehlendes oder fehlerhaftes Verzeichnis der Verarbeitungstätigkeiten
  - Fehlende oder fehlerhafte Datenschutzfolgenabschätzung
  - Fehlende oder Fehlerhafte Benennung des Datenschutzbeauftragten
  - Fehlende oder fehlerhafte Meldung von Vorfällen an Aufsichtsbehörde/Betroffenen