Die Bußgeldregelungen nach der DS-GVO

Sonja Wirtz

Referentin beim Landesbeauftragen für den Datenschutz
und die Informationsfreiheit Rheinland-Pfalz

Wie üben deutsche Aufsichtsbehörden Ihre Befugnisse aus?

1. **Wie** erfährt die Aufsichtsbehörde von einem Verstoß?
2. **Amtsermittlungsgrundsatz**
3. Auskunftsersuchen an den Verantwortlichen
4. Verantwortliche **muss** Auskunft geben ohne sich dabei selbst zu belasten
5. Auskunft kann durch Zwangsmittelverfahren erzwungen werden
6. Und/oder die fehlende Auskunftserteilung kann mit einem Bußgeld geahndet werden

→ **Erst nachdem der Verantwortliche ausreichend Möglichkeiten zur Äußerung hatte entscheidet die Aufsichtsbehörde über ein Bußgeld**

Quelle: http://www.campushunter.de/wer-wie-was-warum

Welche Mittel haben die deutschen Aufsichtsbehörden bereits heute?

Quelle: https://www.bdsg-externer-datenschutzbeauftragter.de

Zulässige Maßnahmen bei Verstößen gegen das BDSG vor dem 25. Mai 2018

- **Untersuchungsbefugnisse:** § 38 Abs. 1 BDSG
- **Abhilfebefugnisse:**
  - Erlass einer **Anordnung** zur Beseitigung festgestellter Verstöße
    (§ 38 Abs. 5 Satz 1 BDSG)
  - **Untersagung**, wenn der Verstoß entgegen der Anordnung trotz der Verhängung eines Zwangsgeldes nicht beseitigt wird
    (§ 38 Abs. 5 Satz 2 BDSG)
  - Verlangen den **Datenschutzbeauftragten abzuberufen**
    (§ 38 Abs. 5 Satz 3 BDSG)
  - Verhängen von **Bußgeldern** (§ 43 Abs. 1 und 2 BDSG)

Und haben die Aufsichtsbehörden Ihre Befugnisse genutzt?

Quelle: https://www.bahn.de

2009: Bußgeld gegenüber der Deutschen Bahn i.H.v. **1,12 Mio. Euro**

Und haben die Aufsichtsbehörden Ihre Befugnisse genutzt?

Quelle: https://www.lidl.de/

2010: Bußgeld gegenüber 35 LIDL-Vertriebsgesellschaften i.H.v. **1,5 Mio. Euro**

Und haben die Aufsichtsbehörden Ihre Befugnisse genutzt?

Quelle: http://www.handelsblatt.com

2014: Bußgeld gegenüber der Debeka Krankenversicherung i.H.v. **1,3 Mio. Euro + 600.000 € für eine Stiftungsprofessur zum Datenschutz**

Zulässige Maßnahmen bei Verstößen gegen die DS-GVO gegen Unternehmen ab dem 25. Mai 2018

- **Untersuchungsbefugnisse:** Art. 58 Abs. 1 DS-GVO
- **Abhilfebefugnisse:**
  - **Warnung** (Art. 58 Abs. 2 lit a) DS-GVO)
  - **Verwarnung** (Art. 58 Abs. 2 lit b) DS-GVO)
  - **Anweisung** (Art. 58 Abs. 2 lit c) bis e) DS-GVO)
  - **Anordnung** von Beschränkung oder Löschung p.b. Daten (Art. 58 Abs. 2 lit g) DS-GVO)
  - **Widerruf der Zertifizierung** bzw. Anweisung zum Widerruf (Art. 58 Abs. 2 lit h) DS-GVO)
  - Verhängen von **Bußgeldern** (Art. 58 Abs. 2 lit i) DS-GVO)
  - **Anordnung** der Aussetzung der Übermittlung in Drittländer (Art. 58 Abs. 2 lit j) DS-GVO)

Ziel der Abhilfemaßnahmen nach der DS-GVO

Schutz in allen Mitgliedsstaaten soll gleichwertig sein, daher sollen auch die Sanktionen gleichwertig sein (Mittel: Kohärenzverfahren) (Erw. 10, 11).

Abhilfemaßnahmen sollen daher

- **wirksam**,
- **verhältnismäßig** und
- **abschreckend**

sein (Art. 83 Abs. 1 DS-GVO).

Welche Abhilfemaßnahmen greifen bei welchen Fällen?

- **Warnung:** Maßnahme zur Abwehr zukünftiger Verstöße
- **Verwarnung:** Maßnahme bei andauernden oder in der Vergangenheit liegenden Verstößen (VA)
- **Anweisung:** Maßnahme bei andauernden Verstoß → Ziel: Beendigung des Verstoßes (VA mit Zwangsgeldandrohung)
- **Anordnung** von Beschränkung oder Löschung p.b. Daten: Wie Anweisung
- **Widerruf der Zertifizierung** bzw. Anweisung zum Widerruf
- Verhängen von **Bußgeldern:** Kann neben Anweisung und Anordnung oder bei Verstößen in der Vergangenheit oder andauernden anstatt ausgesprochen werden (Art. 83 Abs. 2 Satz 1 DS-GVO)
- **Anordnung** der Aussetzung der Übermittlung in Drittländer: s.o.

Verwarnung oder Geldbuße?

- **Art. 29 WP** (WP 253)**:** Geldbußen sind wichtiges Instrument der DS-GVO und nicht automatisch das letzte Mittel → bei Streit zwischen Aufsichtsbehörden über Geldbußen entscheidet der eur. Datenschutzausschuss.

- **Verwarnung:** Statt einem Bußgeld kann eine Verwarnung ausgesprochen werden, wenn es sich um einen **geringfügigen Verstoß** handelt oder um eine **nat. Person**, wenn ein Bußgeld für diese nat. Person eine **unverhältnismäßige Belastung** darstellen würde (Erw. 148).

Drei Schritte zur Geldbuße

1. Entscheidung über das **„ob“** eine Geldbuße festgelegt wird anhand der Kriterien des Art. 83 Abs. 2 DS-GVO → Kommt man zu dem Ergebnis, dass keine Geldbuße sinnvoll ist, wird eine **Verwarnung** ausgesprochen
2. Festlegung des **Höchstbetrages** Art. 83 Abs. 4 bis 6 DS-GVO
   - → Ein Verstoß gegen Art. 83 Abs. 4 kann in den höheren Bußgeldrahmen des Art. 83 Abs. 6 fallen, wenn der Verstoß bereits Gegenstand einer Anweisung war
   - → Bei Verstößen gegen mehrere Bußgeldtatbestände gilt der Höchstbetrag des schwerwiegendsten Verstoßes
3. Das **„wie“** des Bußgeldes: Festsetzen eines konkreten Betrages

   → Die Kriterien des Art. 83 Abs. 2 DS-GvO dürfen bei der Berechnung des konkreten Bußgeldes erneut verwendet werden (WP 253 S. 9)

Schritt 1: Entscheidung über das „ob“ der Geldbuße
Kriterien des Art. 83 Abs. 2 DS-GVO

Lit:

a) **Art, Schwere und Dauer**: Zweck, Zahl und erlittener Schaden bei den Betroffen als Kombination für die Entscheidung über die Schwere und Art des Verstoßes: Zwischen dem Verstoß und dem Schaden muss kein kausaler Zusammenhang bestehen (Erw. 75).

b) **Vorsatz oder Fahrlässigkeit**: Vorsatz = mit Wissen und Wollen; bei Handlungen durch die oberste Führungsebene oder von dieser genehmigt, handelt es sich immer um Vorsatz. Ebenfalls wenn entgegen des Rats des Datenschutzbeauftragten oder unter Missachtung vorhandener Richtlinien gehandelt wird. Mangelnde Ressourcen sind kein Grund von Bußgeld abzusehen.

Schritt 1: Entscheidung über das „ob“ der Geldbuße
Kriterien des Art. 83 Abs. 2 DS-GVO

Lit:

c) **Maßnahmen zur Minderung:** Verantwortungsvolles Verhalten = Tut der Verantwortliche alles erdenkliche, um die Folgen des Verstoßes für die betroffenen Personen gering zu halten.

d) **Grad der Verantwortung:** Wurden technisch und organisatorische Maßnahmen sowie Arbeitsabläufe etabliert, die Datenschutzverstöße verhindern sollen?

e) **Frühere Verstöße:** Wie hat sich der Verantwortliche bei früheren Verstößen verhalten? Gab es gleiche Verstöße bereits? Gab es Verstöße, die in gleicher Weise begangen wurden?

Schritt 1: Entscheidung über das „ob“ der Geldbuße
Kriterien des Art. 83 Abs. 2 DS-GVO

Lit:

f) **Zusammenarbeit mit der Aufsichtsbehörde:** Erfüllung von Auskunfts- und Zutrittspflichten kann nicht berücksichtig werden. Aber hat die Zusammenarbeit z.B. zu einer Vermeidung von Beeinträchtigung für betroffene Personen geführt?

g) **Kategorien p.b. Daten:** Art. 9 und 10 DS-GVO

h) **Art und Weise wie der Verstoß der AB bekannt wurde:** Fahrlässige oder vorsätzliche Nichtmeldung von Datenschutzverstößen kann Schwere der Sanktion beeinflussen

i) **Einhaltung früher angeordneter Maßnahmen**

j) **Einhaltung von genehmigten Verhaltensregeln**

Schritt 2: Höchstrahmen für Bußgelder

Vor 25. Mai 2018: BDSG

- § 43 Abs. 1 i.V.m. Abs. 3: 50.000 €; bei Unternehmen 500.000 €
  (§ 30 Abs. 2 Satz 3 OwiG)
- § 43 Abs. 2 i.V.m. Abs. 3: 300.000€; bei Unternehmen 3.000.000 €
  (§ 30 Abs. 2 Satz 3 OwiG)

Nach DS-GVO

- Art. 83 Abs. 4: 10.000.000 €; bei Unternehmen 2% des weltweiten Jahresumsatzes
- Art. 83 Abs. 5 und 6: 20.000.000 €; bei Unternehmen 4% des weltweiten Jahresumsatzes

Schritt 2: Höchstrahmen für Bußgelder

Unternehmen im Sinne der EU-DSGVO

Unternehmensbegriff i.S.d. Art. 101, 102 AEUV. Nach der ständigen Rechtsprechung des EuGH ist der weite, **funktionale Unternehmensbegriff**:

- Ein Unternehmen ist jede eine wirtschaftliche Tätigkeit ausübende Einheit, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung. Diese wirtschaftliche Einheit kann dabei nicht nur aus einem einzelnen Unternehmen i.S.e. Rechtssubjekts, sondern aus mehreren, natürlichen oder juristischen Personen bestehen.
- Vergleichbar mit dem Unternehmensbegriffs des europäischen Kartellrechts.

→ Anknüpfung an Marktverhalten der wirtschaftlichen Einheit insgesamt. Damit kann ein **ganzer weltweiter Konzern als ein Unternehmen** behandelt werden.

Schritt 3: Festsetzung des konkreten Bußgeldes

Möglicher Weg für die Zukunft!?

Einteilung wie bei der Finanzdienstleistungsaufsicht bei der BaFin:

1. Kategorisierung des Verantwortlichen in Größengruppen anhand seiner Marktposition. Die Einteilung erfolgt nach der Marktkapitalisierung zum Tatzeitpunkt.
2. Grundbeiträge bei betragsmäßigen Höchstbeträgen abhängig von der Kategorie des Verantwortlichen und der Tatumstände.

Einteilungsmatrix der BaFin als Beispiel

Kategorisierung des Emittenten anhand der Marktkapitalisierung						
Emittentengruppe	**A**	**B**	**C**	**D**	**E**	**F**
Marktkapitalisierung in Euro	über 20 Mrd.	über 4 Mrd. bis 20 Mrd.	über 500 Mio. bis 4 Mrd.	über 100 Mio. bis 500 Mio.	über 10 Mio. bis 100 Mio.	bis 10 Mio.

Quelle: https://www.bafin.de

Einteilungsmatrix der BaFin als Beispiel

Pflicht zur Veröffentlichung von Insiderinformationen nach Art. 17 Abs. 1 Unterabs. 1, Unterabs. 2 Satz 1 Marktmissbrauchsverordnung (EU) Nr. 596/2014
Bußgeldrahmen bis zu 2.500.000 Euro
(§§ 120 Abs. 18 Satz 2 Nr. 2, 120 Abs. 15 Nr. 6 und 7 WpHG)

Beträge in Euro		Emittentengruppe					
		A	B	C	D	E	F
Tatumstände	Außerordentlich schwer	2.000.000	1.750.000	1.500.000	1.250.000	1.000.000	750.000
	Sehr schwer	1.750.000	1.500.000	1.250.000	1.000.000	750.000	500.000
	Schwer	1.500.000	1.250.000	1.000.000	625.000	425.000	350.000
	Mittel	1.000.000	875.000	625.000	425.000	300.000	250.000
	Leicht	625.000	500.000	375.000	225.000	150.000	125.000

Quelle: https://www.bafin.de

Bisher gibt es weder auf nationaler noch auf europäischer Ebene einheitliche Vorgaben für die genaue Berechnung der Bußgelder!!!

Die folgenden Darstellungen sind Beispiele, wie Aufsichtsbehörden Bußgelder berechnen könnten:

Quelle: https://www.nelcartoons.de/tagein-tagaus/datenschutz-eugh-urteil.1327

Schritt 3: Festsetzung des konkreten Bußgeldes

a. **Festlegung des nominalen Grundbetrages**

b. **Anpassung des Grundbetrages mit Hilfe von tat- und täterbezogenen Zumessungskriterien an der konkreten Schuld des Verantwortlichen**

   anhand der Kriterien des Art. 83 Abs. 2 DS-GVO

c. **Berücksichtigung der wirtschaftlichen Verhältnisse des Verantwortlichen**

   (§ 17 OWiG) sowie Abschöpfung von wirtschaftlichen Vorteilen

Schritt 3b: Anpassung des Grundbetrags mit Hilfe von tat- und täterbezogenen Zumessungskriterien

Anpassung des Grundbetrags mit Hilfe von tat- und täterbezogenen Zumessungskriterien an der konkreten Schuld des Verantwortlichen anhand der Kriterien des Art. 83 Abs. 2 DS-GVO

a) Art und Dauer: 20 % bis 40 % Erhöhung

b) Vorsatz oder Fahrlässigkeit:

1. Absicht (dolus directus 1. Grades) und direkter Vorsatz (dolus directus 2. Grades): Keine Reduktion
2. Eventualvorsatz (dolus eventualis/bedingter Vorsatz): Reduktion um 25%
3. Fahrlässigkeit: Reduktion um 50%

c) Maßnahmen zur Minderung: Reduktion um 20% bis 40%; keine Maßnahmen führen nicht zur Erhöhung

d) Grad der Verantwortung: Reduktion oder Erhöhung um 10% bis 20%

Schritt 3b: Anpassung des Grundbetrags mit Hilfe von tat- und täterbezogenen Zumessungskriterien

Anpassung des Grundbetrags mit Hilfe von tat- und täterbezogenen Zumessungskriterien an der konkreten Schuld des Verantwortlichen anhand der Kriterien des Art. 83 Abs. 2 DS-GVO

e) **Frühere Verstöße:** Erhöhung um 20% bis 30%

f) **Zusammenarbeit mit der Aufsichtsbehörde:** Zusammenarbeit hat zur Vermeidung von Beeinträchtigung für betroffene Personen geführt: Reduktion um 10 %

g) **Kategorien p.b. Daten:** Erhöhung um 25% bis 50%

h) **Art und Weise wie der Verstoß der AB bekannt wurde:** Erhöhung um 25 %

i) **Einhaltung früher angeordneter Maßnahmen:** Reduktion um 10 %

j) **Einhaltung von genehmigten Verhaltensregeln:** Reduktion um 10 %

Berechnung des Bußgeldes an einem fiktiven Fall

Schritt 1: Entscheidung über Einleitung eines Bußgeldverfahrens (+)

Schritt 2: Festlegung des Höchstbetrages → Art. 83 Abs. 5 lit. a DS-GVO: 20.000.000 €

Schritt 3:

a) Jahresumsatz → 100 Mio. bis 1 Mrd.

b) Anpassung des Betrags

Nominalen Grundbetrag: schwerer Verstoß → Höchstbetrag 750.000 €

Anpassung des Grundbetrages:

Dauer: langer Zeitraum → Erhöhung um 30 % = + 30 %

Vorsatz: Eventualvorsatz → Reduktion um 25 % = - 25 %

Maßnahmen zur Minderung → (-)

Grad der Verantwortlichkeit → (-)

Frühere Verstöße → (-)

Berechnung des Bußgeldes für einen Fall aus der Praxis

Fortsetzung

Zusammenarbeit mit der Aufsichtsbehörde → (-)

Kategorien p.b. Daten → Erhöhung um 25 % = + 25 %

Art und Weise wie der Verstoß bekannt wurde: Erhöhung um 25 % = + 25%

Einhaltung früher angeordneter Maßnahmen: (-)

Einhaltung von genehmigten Verhaltensregeln: (-)

Ergebnis: Erhöhung um 45 % = 750.000 € + 45 % = **1.087.500 €**

Schritt 3 c): Berücksichtigung der wirtschaftlichen Verhältnisse (§ 17 OWiG)

Keine Anhaltspunkte für eine Verringerung

Vielen Dank für Ihre Aufmerksamkeit!

Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Sonja Wirtz

Referentin

beim Landesbeauftragten für den Datenschutz
und die Informationsfreiheit Rheinland-Pfalz

Postanschrift:	Postfach 30 40 55020 Mainz
Büroanschrift:	Hintere Bleiche 34 55116 Mainz
Telefon:	+49 (6131) 208-2573
Telefax:	+49 (6131) 208-2497
E-Mail:	s.wirtz@datenschutz.rlp.de
Web:	www.datenschutz.rlp.de