41 Geldbußen in Deutschland, drei Geldstrafen in Österreich. Wie verhält man sich bei Datenschutzvorfällen richtig?

Die **Kooperation** mit der Aufsichtsbehörde (in Ö: Österreichische Datenschutzbehörde) ist wesentlich und wichtig, und führt dazu, dass eine Geldstrafe nicht zu hoch ausfällt.

In **Deutschland** wurde im **November 2018** ein erstes Bußgeld bekannt. Das Chat-Portal „knuddels.de" erhielt eine Geldbuße von EUR 20.000,--. Bei diesem Verfahren hat das Unternehmen kooperiert.

In **Österreich** hat die DSB am **12.09.2018 in** einem **Straferkenntnis eine GmbH**, die an einem von mehreren Standorten eine Videoüberwachung in der Art betrieben hat, dass auch der Parkplatz (als öffentlicher Raum) unzulässigerweise überwacht wurde, die Speicherdauer mit mehr als 72 Stunden gewählt wurde, und keine Protokollierung erfolgte, wurde eine Geldstrafe von (lediglich) EUR 4.800,-- (gesamt) verhängt. Die DSB hat dabei die Rechtslage vor Geltungsbeginn der DSGVO angewendet, da aufgrund des § 69 Abs 5 DSG ein „Günstigkeitsvergleich" anzustellen ist, und daher liegt die maximale Geldstrafe nach § 52 Abs 2 DSG 2000 bei EUR 10.000,00, weil der überwiegende Teil des strafbaren Verhaltens vor dem 25.05.2018 gelegen ist. Für Beurteilungen von Geldstrafen nach der DSGVO ist daher diese erste veröffentlichte österreichische Entscheidung nicht sehr maßgeblich. Der Verantwortliche im österreichischen Verfahren hat sich daran nicht beteiligt, und keine Stellungnahme abgegeben, obwohl diesem diese Möglichkeit einzuräumen war. Geht man von der Maximalstrafe von EUR 10.000,-- aus, dann ist die Geldstrafe von EUR 2.400,-- (für die Verletzung der Grundsätze der DSGVO, weil die Verarbeitung nicht angemessen und nicht auf das nötige Maß beschränkt ist, und die fehlende Rechtsgrundlage) mit 24% des Strafrahmens als hoch zu bewerten. Ich denke, dass bei einer Kooperation des Unternehmens mit der Behörde, die Geldstrafe wesentlich niedriger ausgefallen wäre.

Über weitere Verfahren in Österreich wurde bereits unter Verweis auf den Newsletter 01/2019 der DSB informiert.

Deutsche Medien berichten von den Verfahren, die zu Geldbußen geführt haben. So schreibt zB das Handelsblatt über **41 verhängte Geldbußen**:

> „Die meisten Bußgelder verhängte Nordrhein-Westfalen (33), gefolgt von Hamburg (3) und Baden-Württemberg und Berlin (jeweils 2) und dem Saarland (1). Allein beim Bayerischen Landesamt für Datenschutzaufsicht (BayLDA), das die Einhaltung des Datenschutzrechts in privaten Wirtschaftsunternehmen, bei Freiberuflern, in Vereinen und Verbänden sowie im Internet überwacht, laufen derzeit 85 Bußgeldverfahren nach der DSGVO.
>
> Mit Blick auf die Höhe der Bußgelder besteht derzeit offenbar noch Schonfrist. So verhängte der Landesdatenschutzbeauftragte von Baden-Württemberg mit 80.000 Euro bislang die höchste Einzelstrafe. Im konkreten Fall landeten aufgrund unzureichender interner Kontrollmechanismen Gesundheitsdaten im Internet. Hamburg verhängte insgesamt Bußgelder in Höhe von 25.000 Euro, Nordrhein-Westfalen von knapp 15.000 Euro."
> (https://www.handelsblatt.com/politik/deutschland/datenschutzgrundverordnung-behoerden-verhaengen-erste-bussgelder-wegen-verstoessen-gegen-dsgvo/23872806.html?ticket=ST-509069-fy31DrwD7iRKpy2w4b1T-ap1, abgerufen am 19.1.2019)

Der Rechtsanwalt, der das deutsche Unternehmen im Verfahren vor dem LfDI Baden-Würtemberg vertreten hat, Tim Wybitul mit seinem Team von der Kanzlei Latham & Watkins führte dazu u.a. aus: *„Die niedrige Höhe des Bußgeldes trägt der Tatsache Rechnung, dass unsere Mandantin nach Aufdeckung des Hackerangriffs schnell und richtig gehandelt hat. Entscheidend war auch die Verteidigungsstrategie, umfassend und transparent mit der Datenschutzbehörde zu kooperieren*“ (Auszug aus der Homepage, abgerufen am 19.1.2019: https://de.lw.com/news/LW-veteidigt-Chatportal-erfolgreich-in-Datenschutzverfahren)

In der Pressemeldung der Aufsichtsbehörde wurde auf die Kooperation des Unternehmens mit derselben hingewiesen: **Kooperation mit Aufsicht macht es glimpflich.**

Was ist nötig, um eine Geldstrafe (in D: Bußgeld) im Rahmen zu halten?

1. Meldung der Datenschutzverletzung an die Behörde (siehe auch Art 33 DSGVO):

Wenn die Organisation, die einem Hackeranagriff ausgesetzt ist, oder auf andere Art und Weise Daten verliert, die Datenschutzverletzung erkennt, dann ist diese verpflichtet unverzüglich, längstens aber binnen 72 Stunden die Datenschutzverletzung der Aufsichtsbehörde (in Österreich: Österreichische Datenschutzbehörde) zu melden.

Die Österreichische Datenschutzbehörde bietet ein Formular zur Meldung auf der Website an:

Meldungen von Verletzungen des Schutzes personenbezogener Daten:

Dieses Formular dient zur Meldung einer Verletzung des Schutzes personenbezogener Daten (eines "Data Breach") durch den Verantwortlichen selbst. Das Formular ist nicht für Beschwerden geeignet.

- Meldungen von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DSGVO (PDF, 416 KB)

In **Art 83 DSGVO** (Allgemeine Bedingungen für die Verhängung von Geldbußen) ist in **Abs 2 lit e** als ein **Kriterium für die Höhe der Geldbuße** u.a. die *„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*“.

Die Meldung bewirkt daher keine „Straffreiheit“, ist aber im Rahmen der Bemessung der Geldstrafe von der Behörde jedenfalls zu berücksichtigen.

In § 19 VStG sind keine derartigen Kriterien für die Strafzumessung festgelegt, sondern haben die Verwaltungsstrafbehörden folgende gesetzlichen Vorgaben für die Strafbemessung:

- **Bedeutung des strafrechtlich geschützten Rechtsgutes**
- **Die Intensität der Beeinträchtigung**
- **Ausmaß des Verschuldens**

Des Weiteren verweist § 19 Abs 2 VStG explizit auf die Bestimmungen der §§ 32 bis 35 StGB, sohin

§ 32 StGB: allgemeine Grundsätze der Strafbemessung

§ 33 StGB: Besondere Erschwerungsgründe

§ 34 StGB: Besondere Milderungsgründe

§ 35 StGB: Berauschung.

Nach **§ 34 (1) Z 17 StGB** ist das **Ablegen eines reumütigen Geständnisses** sowie **das wesentliche Beitragen zur Wahrheitsfindung** ein besonderer Milderungsgrund, unter den auch die „Selbstanzeige" des Art 33 DSGVO zu subsumieren wäre.

2. Vollständige Transparenz und Kooperation mit der Aufsichtsbehörde

Im Anlassfall eines derartigen Verfahrens, das zu einer Geldstrafe führen kann, ist es mE wesentlich, dass „mit offenen Karten gespielt" wird. Insbes. wenn Daten „nach außen" gehen, dann ist zu erwarten, dass diese auch irgendwann verwendet werden, und so im Rahmen von Veröffentlichungen über das Datenleck berichtet wird. Die Transparenz gegenüber der Behörde und die Zusammenarbeit mit dieser ist daher von grundsätzlicher Bedeutung für die Höhe der Geldstrafe, da zu erwarten ist, dass der Sachverhalt, der nach der DSGVO eine Geldstrafe rechtfertigt ohnehin durch die Behörde ermittelt werden wird.

„Die Transparenz des Unternehmens war ebenso beispielhaft wie die Bereitschaft, die Vorgaben und Empfehlungen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit, Dr. Stefan Brink, umzusetzen." (Pressemitteilung).

Nach Art 83 Abs 2 lit f DSGVO ist bei der Höhe der Geldstrafe auch auf der „**Umfang der Zusammenarbeit mit der Aufsichtsbehörde**, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern" beachtlich.

3. Maßnahmen setzen, um weitere, gleichartige Datenschutzverletzungen zu vermeiden

Ein weiteres wesentliches Element im Zusammenhang mit Datenschutzverletzungen und im Verfahren mit einer Aufsichtsbehörde ist es, zu dokumentieren welche konkreten Schritte bereits eingeleitet wurden, um gleichartige Verletzungen des Datenschutz(rechts) zu verhindern, sowie welche Maßnahmen gesetzt wurden, um einen Schaden bei den betroffenen Personen zu verhindern und/oder zu mildern.

Bereits in **Art 33 Abs 3 lit d DSGVO** wird normiert, dass der Verantwortlich im Rahmen der Meldung gegenüber der Behörde die ergriffenen oder vorgeschlagene Maßnahmen darlegt, um die Verletzung zu beheben, und Maßnahmen beschreibt, die die möglichen nachteiligen Folgen der Datenschutzverletzung abmildern.

Die gesetzten Maßnahmen sollten der Behörde gegenüber offengelegt werden, und auch deren Ratschläge – sofern diese erteilt werden – berücksichtigt werden.

4. Ausarbeitung / Definition eines „Maßnahmenplans" für Datenschutzverletzungen

Um die kurzen Fristen bei Datenschutzverletzungen einhalten zu können, und jedenfalls rechtzeitig gegenüber der Aufsichtsbehörde eine vollumfängliche Meldung erstatten zu können, ist es wichtig, diese

Situation auch einmal „durchzuspielen“, um auch etwaige Schwachpunkte in der eigenen Organisation zu erkennen, und beseitigen zu können.

Es gibt viele **Fragen**, die sich im Zusammenhang mit eine Meldung an die Österreichische Behörde, stellen; hier nur einige davon:

1. Wer setzt die Meldung ab?
2. Ist eine Genehmigung durch die Geschäftsführung nötig? Welches Mitglied der Geschäftsführung ist für die Erteilung der Genehmigung zuständig (Recht, Organisation, IT).
3. Wer kann welche Inhalte für eine Meldung beitragen?
4. Wie wird mit der Öffentlichkeit kommuniziert? Wer ist Ansprechpartner für Medien, die sich eventuell melden?
5. Wer entscheidet, ob auch betroffene Personen zu kontaktieren sind, oder eine Meldung an die Aufsichtsbehörde ausreicht?

Das **Datenschutz-Management-System** einer Organisation sollte daher **nicht nur eine Dokumentation der Verarbeitungsvorgänge** sein, sondern auch eventuelle **Pläne für die Bewältigung von Datenschutzverletzungen und Maßnahmen nach Datenschutzverletzungen** beinhalten.