- Ausfertigung -

Baden-Württemberg

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT

- Bußgeldstelle -

LfDI Baden-Württemberg · Postfach 10 29 32 · 70025 Stuttgart

Datum 21. November 2018
Name [redacted]
Durchwahl 0711/615541-0
Aktenzeichen O 1018/115
(Bitte bei Antwort angeben)

[redacted] und [redacted]
Knuddels GmbH & Co. KG
Kaiserstraße 146
76133 Karlsruhe

Bußgeldverfahren gegen Knuddels GmbH & Co. KG wegen Verstoßes gegen Artikel 32 Abs. 1 lit. a DSGVO
(Speicherung von ungehashten Passwörtern)
hier: Bußgeldbescheid
Anlage: 1 Überweisungsträger, Kassenzeichen Nr. 1885260000100

Sehr geehrter Herr [redacted]
sehr geehrter Herr [redacted],

der Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI) Baden-Württemberg – Bußgeldstelle – erlässt gegen die Knuddels GmbH & Co. KG den folgenden

Bußgeldbescheid:

1. Gegen die Knuddels GmbH & Co. KG wird ein

   Bußgeld in Höhe von **20.000,- Euro** festgesetzt.

2. Daneben hat die Knuddels GmbH & Co. KG eine Gebühr in Höhe von 1.000,- Euro zu bezahlen.

Gründe:

1. Sachverhalt

Die Knuddels GmbH & Co. KG (im Folgenden Knuddels) betreibt als Unternehmen seit 2002 eine Internetplattform, über welche sich Nutzer unter Pseudonymen in sog. Chats austauschen können. [redacted]

[redacted] Dabei war Knuddels spätestens seit 2012 bewusst, dass eine ungesicherte Speicherung von Passwörtern nicht (bzw. nicht mehr) dem Stand der Technik entsprach. Denn zu dieser Zeit führte Knuddels für die Login-Daten ihrer Nutzer die Sicherung mittels Hashverfahren ein.

[redacted] In Ansehung des Wirksamwerdens der EU-Datenschutz-Grundverordnung (DSGVO) entschied Knuddels, die Datei mit Passwörtern im Klartext auch nach dem 25.05.2018 zu unterhalten, um auch zukünftig ein „Abfischen" der Passwörter der Nutzer durch Dritte zu verhindern.

Mit zwei Angriffen am 12.07.2018 und am 14.07.2018 erbeutete ein bislang nicht ermittelter Täter, der sich Zugriff auf die Daten von Knuddels verschafft hatte, insgesamt 1,8 Mio. Datensätze, darunter auch die Datei mit den unverschlüsselten Passwörtern. Von den entwendeten Datensätzen wurden im Zeitraum vom

05.09.2018 bis 07.09.2018 zunächst 8.000 Nutzerdaten, darunter auch Passwörter und E-Mailadressen, auf der Plattform „Pastebin“ veröffentlicht. Ein weiterer Datensatz mit 1,8 Mio. Nutzerdaten, darunter Pseudonyme, Passwörter und E-Mail-Adressen, wurde im selben Zeitraum auf der Plattform „mega.nz“ veröffentlicht.

Nachdem Knuddels am Abend des 05.09.2018 Kenntnis von der Veröffentlichung erhielt und so erstmals auf den vorangegangenen erfolgreichen Hacker-Angriff aufmerksam wurde, informierte Knuddels am Freitag, den 07.09.2018, seine Nutzer über den Vorfall und forderte zur Änderung des Passwortes auf. Am 08.09.2018 veröffentlichte Knuddels zudem im Rahmen einer Pressemitteilung und über verschiedene soziale Netzwerke das Ausmaß des Hackerangriffs und entschuldigte sich bei ihren Nutzern für den Vorfall. Am selben Tag erstattete Knuddels eine Datenpannenmeldung gegenüber der zuständigen Datenschutzaufsichtsbehörde sowie eine Strafanzeige bei der Staatsanwaltschaft Karlsruhe. Am Montag, den 10.09.2018, erläuterte Knuddels in einem öffentlichen Forum auf seiner Homepage zudem, aus welchem Grund in der Vergangenheit Passwörter ungehasht gespeichert wurden und dass diese Praxis am 07.09.2018 beendet worden sei. Interne Überprüfungen von Knuddels ergaben, dass die erbeuteten Nutzerdaten insgesamt 330.000 Personen betrafen.

Seit der Veröffentlichung der gehackten Nutzerdaten wandte Knuddels circa [redacted] für die kontinuierliche Verbesserung ihrer IT-Sicherheitsmaßnahmen auf. Weitere [redacted] werden bis Jahresende in den darüber hinausgehenden Ausbau der bestehenden Sicherheitsinfrastruktur investiert. Ein Missbrauch der entwendeten Datensätze konnte bislang nicht festgestellt werden.

2. Beweiswürdigung

Der Sachverhalt steht fest aufgrund der glaubhaften Angaben von Knuddels sowie aufgrund des Ermittlungsergebnisses des LfDI. Auf den Inhalt der Bußgeldakte wird vollumfänglich Bezug genommen.

3. Rechtliche Würdigung

Durch das Abspeichern von unverschlüsselten Passwörtern [redacted] gegen ihre Pflicht zur Gewährleistung der Datensicherheit bei der Verarbeitung personenbezogener Daten gem. Artikel 32 Abs. 1 lit. a DSGVO.

Bei den ungesicherten Passwörtern handelt es sich um personenbezogene Daten, nachdem mittels dieser Passwörter, der zugehörigen Nutzernamen und E-Mail-Adressen, die ebenfalls abgespeichert waren und gehackt wurden, eine zumindest indirekte Bestimmbarkeit der jeweiligen Personen möglich war. Das Bekanntwerden der tatsächlichen Namen der betroffenen Nutzer ist dagegen nicht erforderlich (vgl. zur indirekten Bestimmbarkeit: BeckOK Datenschutzrecht Wolff/Brink, DSGVO Artikel 4 Rn. 17). Entgegen ihrer Verpflichtung als verantwortliche Stelle sicherte Knuddels diese Daten nicht durch geeignete technische und organisatorische Maßnahmen gem. Artikel 32 DSGVO ab, um einen Zugriff durch unbefugte Personen zu verhindern. Wie Knuddels bekannt war, entspricht es bereits seit vielen Jahren dem Stand der Technik, die Passwörter von Nutzern nur verschlüsselt bzw. gehasht abzuspeichern. Aus diesem Grund stellte Knuddels bereits im Jahr 2012 seine Chatlogins auf gehashte Passwörter um. [redacted]

Dieser Verstoß ist der Knuddels GmbH & Co. KG auch zurechenbar. Denn das Anlegen und Fortführen der Datei mit ungesicherten Passwörtern erfolgte auf Veranlassung, jedenfalls aber in Kenntnis und mit ausdrücklicher Billigung der beiden Geschäftsführer [redacted] und [redacted]. Der Datenschutzverstoß wurde somit von vertretungsberechtigten Organen der Knuddels GmbH & Co. KG in zumindest mittelbarer Weise begangen, sodass die pflichtwidrige Handlung unabhängig von der Frage einer etwaigen funktionalen Verantwortlichkeit des Unternehmens jedenfalls nach § 30 Abs. 1 Nr. 1 OWiG der Knuddels GmbH & Co. KG zuzurechnen ist.

4. Bußgeldbemessung

Der Bußgeldrahmen ist Art. 83 Abs. 4 DSGVO zu entnehmen, der eine Geldbuße von bis zu 10 Mio. Euro oder 2 % des Umsatzes des vorangegangenen Geschäftsjahres vorsieht.

Bei der Bemessung der Geldbuße im Konkreten waren zu Gunsten von Knuddels die nachfolgenden Umstände zu sehen: Die Übertragung der Nutzerdaten an einen unberechtigten Dritten erfolgte nicht auf Veranlassung von Knuddels, sondern durch einen externen Hackerangriff. Durch dieses rechtswidrige Eindringen und Entwenden von Daten seitens unbekannter Dritter erlitt Knuddels selbst einen nicht

unerheblichen Vermögens- und Rufschaden. Nach Bekanntwerden des Hackerangriffs bemühte sich Knuddels um schnellstmögliche und umfassende Transparenz sowohl gegenüber ihren Nutzern als auch gegenüber der Aufsichtsbehörde. Dadurch trug Knuddels in ganz erheblichem Maße dazu bei, den Sachverhalt vollumfänglich aufzuklären und substanzielle Fortschritte bei der Datensicherheit der Nutzerinnen und Nutzer zu erzielen. Im Rahmen der Bußgeldbemessung war überdies als bußgeldmildernd zu berücksichtigen, dass Knuddels durch den eingetretenen Verstoß keinerlei wirtschaftliche Vorteile gezogen hat oder dies beabsichtigt gewesen wäre. Zudem investierte Knuddels innerhalb weniger Wochen nach dem Vorfall, ohne hiervon durch die Aufsichtsbehörde ausdrücklich angehalten worden zu sein, einen Betrag von [redacted] in IT-Sicherheitsmaßnahmen, sodass die Sicherheitsarchitektur nun dem aktuellen Stand der Technik entspricht. Weitere [redacted] wird Knuddels für zusätzliche IT-Sicherheitsmaßnahmen bis Jahresende investieren, um den erreichten Sicherheitsstandard weiter zu verbessern. Darüber hinaus hat sich Knuddels bereit erklärt, sämtliche Vorgaben der Aufsichtsbehörde (soweit nicht bereits geschehen) zügig umzusetzen, die ebenfalls weitere Mehrkosten verursachen werden. Die sehr gute Kooperation mit der Aufsichtsbehörde und die transparente Offenlegung der eigenen Überlegungen, Strukturen und Versäumnisse war dabei als besonders positiv zu bewerten. Daneben war zu Gunsten von Knuddels zu sehen, dass ihre Datenverarbeitung in der Vergangenheit keinerlei Beanstandungen ausgesetzt war. Zu Lasten von Knuddels war freilich zu sehen, dass personenbezogene Daten in nicht unerheblichem Umfang betroffen waren und dass Knuddels die gegenständlichen Passwörter wissentlich im Klartext abgespeichert hatte. [redacted]

Nach Abwägung aller für und gegen Knuddels sprechenden Zumessungskriterien erschien insbesondere aufgrund des sehr positiven Verhaltens seit Bekanntwerden des Verstoßes sowie des für Knuddels eingetretenen Schadens ein Bußgeld im unteren Bereich des Bußgeldrahmens angemessen.

Unter Würdigung aller maßgeblichen Umstände war gegen die Knuddels GmbH & Co. KG deshalb ein

Bußgeld in Höhe von 20.000,- Euro

als wirksam, abschreckend und verhältnismäßig im Sinne des Art. 83 Abs. 1 und 2 DSGVO festzusetzen. [redacted]

[redacted]

5. Gebühren und Auslagen

Neben der festgesetzten Geldbuße hat Knuddels auch die Kosten des Verfahrens zu tragen (§§ 105, 107 OWiG i.V.m. § 464 Abs. 1, § 465 StPO). Die Verfahrensgebühr beträgt 5% der Geldbuße, jedoch mindestens 25,- Euro und höchstens 7.500,- Euro (§ 107 Abs. 1 S. 3 OWiG).

Gegen die Knuddels GmbH & Co. KG war deshalb eine

Gebühr von 1.000,- Euro

festzusetzen.

Auslagen sind nicht angefallen.

Rechtsbehelfsbelehrung:

Dieser Bußgeldbescheid wird rechtskräftig und vollstreckbar, wenn Sie nicht innerhalb von 2 Wochen nach seiner Zustellung Einspruch einlegen. Der Einspruch ist schriftlich oder zur Niederschrift beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) Baden-Württemberg, Bußgeldstelle, Königstraße 10a, 70173 Stuttgart einzulegen. Die Frist ist nur dann gewahrt, wenn der Einspruch vor Ablauf der Frist beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit in Stuttgart eingeht. Falls wir den Bußgeldbescheid nach Einspruchserhebung aufrechterhalten, entscheidet das Amtsgericht Stuttgart über Ihren Einspruch.

Zahlungsaufforderung:

Sie werden aufgefordert, den zu zahlenden Gesamtbetrag von 21.000,- Euro auf das Konto der Landesoberkasse Baden-Württemberg bei der BW-Bank, BIC: SOLADEST600, unter der IBAN DE02 6005 0101 7495 5301 02 anzuweisen. Bitte geben Sie als Verwendungszweck unbedingt das oben aufgeführte Kassenzeichen (1885260000100) an, da Ihre Zahlung anderenfalls nicht zugeordnet werden kann.

[redacted]

[redacted]

Bei Zahlungsunfähigkeit ist dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) unter eingehender Begründung rechtzeitig vor Ablauf der (jeweiligen) Zahlungsfrist mitzuteilen, warum die fristgemäße Zahlung nach den wirtschaftlichen Verhältnissen nicht zuzumuten ist. Geeignete Nachweise (z.B. Bilanzen) sind beizufügen.

Falls weder die Zahlungsfristen eingehalten werden, noch die Zahlungsunfähigkeit rechtzeitig dargelegt wird, wird der fällige Betrag zwangsweise beigetrieben. Auch kann das Amtsgericht zur Beitreibung der Geldbuße Erzwingungshaft anordnen.

Mit freundlichen Grüßen
Im Auftrag
gez.
[redacted]

Ausgefertigt
Stuttgart, den 21.11.2018