»Bei den Strafhöhen wird es ordentlich scheppern«

Datenschutzexperte Rainer Knyrim kommentiert einen veröffentlichten Bescheid der Datenschutzbehörde und erwartet im Jahr zwei der Verordnung ein Ende der Schonfrist für Unternehmen.

(+) PLUS: Die DSGVO ist seit einem Jahr anwendbar. Was hat sich in diesem ersten Jahr getan?

Rainer Knyrim: Der irrsinnige Medienhype um das Thema DSGVO, der vor einem Jahr bestanden hat, ist zum Glück verflogen, denn er hat nicht nur positive Auswirkungen gehabt. Viele Unternehmen gerieten durch diesen in Panik und haben teilweise konzeptlos irgendetwas »hingebastelt«, damit es so aussieht, als hätten sie sich mit dem Thema ausreichend beschäftigt. Wie sich nun zeigt, reicht dies der Datenschutzbehörde aber nicht.

(+) PLUS: Was wurde nachgeprüft?

Knyrim: Ein sehr interessanter Fall ist jener eines Allergie-Tageszentrums. Dieses hatte letzten Sommer zunächst zweimal an die Datenschutzbehörde Datensicherheitsverletzungen – »Data Breaches« – gemeldet. Die Behörde wurde offensichtlich stutzig, dass die Schreiben von einer als Datenschutzkoordinator benannten Person kamen, dieselbe Person auf der Webseite des Unternehmens aber als Datenschutzbeauftragter benannt wurde. Dies sind zwei unterschiedliche Funktionen, die nicht zusammenpassen. Die Behörde leitete ein amtliches Prüfverfahren ein und stellte dem Unternehmen verschiedene Fragen. Unter anderem, ob nun ein Datenschutzbeauftragter – wie auf der eigenen Webseite behauptet – bestellt sei oder nicht.

(+) PLUS: Das Unternehmen hat die Fragen beantwortet?

Knyrim: Teilweise ja. Hinsichtlich des Datenschutzbeauftragten hat das Unternehmen aber der Datenschutzbehörde eine Frage zurückgestellt, nämlich, dass es sich nicht sicher sei, ob ein Datenschutzbeauftragter zu bestellen sei, da es von der eigenen Kammer im Laufe der letzten Monate unterschiedliche Informationen dazu erhalten habe. Es bat die Datenschutzbehörde dazu um Beratung.

(+) PLUS: »Beraten statt Strafen« war ja einer der Slogans, der hinsichtlich der Tätigkeit der Datenschutzbehörde gefordert wurde.

Knyrim: Tatsächlich gibt es diesen Grundsatz »Beraten statt Strafen« nicht, im Gesetz festgehalten ist die Möglichkeit der Datenschutzbehörde, statt zu bestrafen zu verwarnen. Die Datenschutzbehörde hat in diesem Fall aber auch nicht verwarnt, sondern dem Unternehmen erklärt, dass es durch Studium der Rechtsgrundlagen und begleitender Unterlagen dazu selbst zum Ergebnis hätte kommen müssen, dass aufgrund seiner Tätigkeit im Gesundheitsbereich und mit der Beschäftigung einer größeren Anzahl von Ärzten die Bestellung eines Datenschutzbeauftragten erforderlich gewesen wäre. Die Datenschutzbehörde hat daher im Ergebnis festgehalten, dass das Unternehmen seine Verpflichtung zur Bestellung eines Datenschutzbeauftragten verletzt habe und diesem aufgetragen, binnen acht Wochen bei sonstiger Exekution einen zu bestellen.

(+) PLUS: Hat die Datenschutzbehörde auch eine Strafe verhängt?

Knyrim: Noch nicht, laut Jahresbericht der Datenschutzbehörde ist aber ein separates Verwaltungsstrafverfahren anhängig.

(+) PLUS: Können Sie kurz zusammenfassen, worum es in den anderen Punkten ging?

Knyrim: Wichtigster Punkt, der alle Unternehmen betrifft, ist dass die Datenschutzbehörde festgehalten hat, dass es Aufgabe der Unternehmen ist, selbst zu beurteilen, welche Datensicherheitsmaßnahmen erforderlich sind und diese dann entsprechend umzusetzen. Dies kann zum Beispiel die Verschlüsselung von E-Mails betreffen. Wenn Gesundheitsdaten oder sonstige besondere Datenkategorien übermittelt werden, muss das Unternehmen, das diese aussendet, von sich aus beurteilen, ob die E-Mail zu verschlüsseln ist. Was unzulässig ist, die Allergie-Tagesklinik aber gemacht hat, ist, die Patienten um Einwilligung zu fragen, ob es für sie in Ordnung ist, dass die E-Mails mit den Befunddaten unverschlüsselt an sie geschickt werden. In diesem Fall ergreift das Unternehmen nämlich selbst keine Sicherheitsmaßnahmen, sondern hängt dem Kunden das Sicherheitsproblem um. Dies hat die Datenschutzbehörde für unzulässig erachtet.

(+) PLUS: Müssen E-Mails nun immer verschlüsselt werden?

ZUM UNTERNEHMEN

Knyrim Trieb Rechtsanwälte wurde von Rainer Knyrim und Gerald Trieb 2017 gegründet. Die Kanzlei ist auf Datenschutzrecht, IT-Recht, E-Commerce-Recht, Arbeitsverfassungsrecht und Vertragsrecht spezialisiert. Rainer Knyrim ist zudem Chefredakteur der Zeitschrift Datenschutz konkret, Herausgeber des »DatKomm«, Chief Information Privacy Manager und zertifizierter Experte für das Datenschutzgütesiegel EuroPriSe.

Rainer Knyrim: »Datenschutzrecht sollte wie jedes andere Compliance-Thema in der DNA eines Unternehmens verankert werden.«

Knyrim: Nein, die Datenschutzbehörde hat in dieser Entscheidung auch ausdrücklich festgehalten, dass die DSGVO nicht fordert, dass E-Mails immer verschlüsselt werden müssen. Es ist eben die Aufgabe des verantwortlichen Unternehmens, sich selbst die Frage zu stellen, ob es die E-Mails, die es aussendet, aufgrund deren Inhalts verschlüsseln sollte oder nicht. Und mit dieser Aufgabe muss sich das Unternehmen befassen.

(+) PLUS: Welche Fehler hat die Datenschutzbehörde noch festgestellt?

Knyrim: Die Datenschutzbehörde hat weiters festgehalten, dass die Informationspflichten nach der DSGVO vom Unternehmen verletzt wurden, weil auf dessen Webseite intransparente Informationen enthalten waren. So wurden etwa berechtigte Interessen als Rechtsgrundlagen für Datenverarbeitungen angesprochen, aber nicht näher beschrieben und es war auch unklar, inwieweit das Unternehmen nur eigene Daten verarbeitet oder ob es auch Daten von Dritten erhält und was es mit diesen macht. Weiters wurden Verletzungen gegen die Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung bei mehreren der vom Unternehmen betriebenen Datenanwendungen festgestellt. Die Entscheidung zeigt den Unternehmen insgesamt, dass sie sich intensiv mit der Materie des Datenschutzrechts befassen müssen und nicht darauf hoffen können, dass sie mit halbherzigen Lösungen und Texten bei der Datenschutzbehörde durchkommen oder ihnen diese dann im Prüfverfahren ihre Hausausgaben abnimmt.

(+) PLUS: Spektakulär war die Strafe über 50 Millionen Euro, die die französische Datenschutzbehörde gegen Google verhängt hat. Warum wurde diese Strafe verhängt?

Knyrim: Das ist gerade das Spektakuläre an der Strafe: Wenn man die 50 Millionen Euro in der Zeitung liest, möchte man glauben, dass die französische Datenschutzbehörde nun das Böse schlechthin bei Google entdeckt hat. Der Grund für die Strafe war aber banaler: Auch bei der französischen Datenschutzbehörde ging es darum, dass dieser die Informationen, die Google auf der Webseite zur eigenen Datenverarbeitung hatte, nicht transparent und nutzerfreundlich genug waren. Die französische Datenschutzbehörde bekrittelte etwa, dass man bis zu sechs Links anklicken muss, um zur Gesamtinformation zu gelangen, das sei für die Nutzer zu komplex. Es ging also auch hier um die Transparenz über die Datenverarbeitung, nicht um die Zulässigkeit des Inhalts der Datenverarbeitung selbst.

(+) PLUS: Gibt es auch in Österreich solch drakonische Strafen?

Knyrim: Von der absoluten Strafhöhe her nicht, es gibt also noch keine Millionenstrafen. Das heißt aber nicht, dass Unternehmen und Einzelpersonen nicht bereits jetzt streng bestraft werden. Die Behörde hat bislang erst sehr kleine Unternehmen bestraft, diese aber durchaus hart. So erhielt ein kleines Wettbüro in Graz rund 5.000 Euro Strafe, weil es den Gehsteig und den Parkplatz neben dem Wettlokal mit einer Videokamera überwacht hatte und damit verbotenerweise öffentlichen Raum.

Ein Döner-Stand-Betreiber erhielt eine Strafe über zirka 1.000 Euro, weil er eine Videokamera installiert hatte und den Platz vor dem Döner-Stand filmte. Man kann sich ausrechnen, dass dieser mehrere hundert Döner verkaufen wird müssen, um diesen Betrag wieder hereinzuspielen.

Die im Verhältnis härteste Strafe traf aber eine Einzelperson: Diese hatte aus ihrer Wohnung mit zwei Kameras in einem Mehrparteienhaus Parkplätze, Gehwege, Zugangsbereiche und Gartenflächen gefilmt. Die Datenschutzbehörde verhängte hier inklusive Verfahrenskosten eine Strafe von 2.420 Euro, wobei sie von einem durchschnittlichen Nettoeinkommen des Beschuldigten von 1.800 Euro monatlich ausgegangen war. Die Summe betrug also deutlich mehr als ein Monatseinkommen und bei dieser Einkommenshöhe ist davon auszugehen, dass die bestrafte Person nun deutliche Einbußen in ihrer finanziellen Lebensgestaltung im heurigen Jahr erleiden wird.

(+) PLUS: Wie hoch darf die Strafe maximal sein?

Knyrim: Bei Einzelunternehmen maximal 20 Millionen Euro, bei Unternehmen höchstens vier Prozent vom Jahresumsatz. Legt man die vorher genannte Strafe gegen die Einzelperson auf das Jahreseinkommen mit 14 Gehältern um, so betrug der Strafrahmen gegen diese Einzelperson nicht 4 %, sondern 10 %. Dies zeigt, dass die Datenschutzbehörde schon jetzt ziemlich hart straft. Es ist daher davon auszugehen: Straft die Datenschutzbehörde erstmalig ein großes Unternehmen, wird dabei auch eine entsprechend hohe, medienwirksame Strafe herauskommen.

(+) PLUS: Wie wird es im zweiten Jahr der DSGVO weitergehen?

Knyrim: Die deutschen Behörden haben zum Jahresanfang deutlich gesagt, dass die Schonzeit nun vorbei sei. Ich gehe davon aus, dass es in ganz Europa und auch in Österreich heuer bei den Strafhöhen immer öfter ordentlich scheppern wird. Die Aufregung darüber in den Medien wird wieder zu hektischen Reaktionen bei den Unternehmen führen und zu weiteren Hauruck-Aktionen hinsichtlich der Datenschutz-Compliance. Tatsächlich gefragt ist aber seriöse, laufende Arbeit im Datenschutzrecht, die nur über die Schaffung eines Datenschutz-Management-Systems, Ausbildung entsprechender Personen und Zurverfügungstellung entsprechender Kapazitäten und Budgets erreicht werden kann. Wir sehen in der Beratung, dass dies bei immer mehr Unternehmen auch tatsächlich stattfindet, wenn auch der Weg dorthin lange dauert.

Letztendlich muss aber Datenschutzrecht wie jedes andere Compliance-Thema in der DNA des Unternehmens verankert werden und schlicht als Thema laufend abgearbeitet werden. Nur dann funktioniert Datenschutz-Compliance und man muss sich nicht vor behördlichen Untersuchungen fürchten, weil man datenschutzrechtliche Leichen – nämlich vor allem Daten – im Keller hat. ■

Foto: Kynrim Trieb