Datenschutzgesetz-Novelle 2010: Neue Informationspflicht bei Datenmissbrauch

Österreich hat als zweites EU-Land die Pflicht von Unternehmen und öffentlichen Stellen eingeführt, bei Hacker-Attacken Betroffene zu informieren.

Von der Öffentlichkeit weitgehend unbeachtet ist neben den neuen Regeln zur Videoüberwachung am 1. Jänner 2010 mit der Novelle zum Datenschutzgesetz eine neue Informationspflicht bei Datenmissbrauch in Kraft getreten. Österreich übernimmt hier neben Deutschland wieder eine Vorreiterrolle bei der Weiterentwicklung des Datenschutzrechts.

Mit einer Bestimmung, die bloß zwei Sätze in einem neuen Absatz § 24 Abs 2a des Datenschutzgesetzes 2000 umfasst, wird privaten Unternehmen wie öffentlichen Stellen eine Informationspflicht bei „systematischer und schwerwiegend unrechtmäßiger Verwendung von Daten, bei der den Betroffenen Schaden droht“ eine Pflicht zur Information der Betroffenen auferlegt. Dies bedeutet, dass Vorfälle in der IT-Sicherheit wie etwa „Hacker-Attacken“, bei denen Kundendaten gestohlen wurden, nicht mehr unbemerkt von der Öffentlichkeit „unter den Tisch gekehrt“ werden dürfen.

Erpressung mit USB-Stick

Vielmehr ist künftig auch schon dann, wenn etwa ein USB-Stick verloren geht, zu prüfen, ob ein Missbrauch der auf diesem befindlichen Daten im Sinn dieser Bestimmung stattgefunden hat (etwa weil der Dieb oder zufällige Finder das Unternehmen nun mit einer Datenveröffentlichung zu erpressen versucht). Es muss überlegt werden, ob die Betroffenen zu informieren sind, also diejenigen, auf die sich die gestohlenen Daten beziehen (zB Kunden), wenn ihnen im Hinblick auf diesbezügliche Schritte des Diebs ein nicht bloß geringfügiger Schaden droht.

In den USA ist diese Informationspflicht seit einigen Jahren als sogenannte „Data Breach Notification Duty“ bekannt, und es gibt in den meisten US-Bundesstaaten mittlerweile ausdrückliche gesetzliche Regelungen dazu. In Europa wird die Einführung derartiger Regelungen in die Datenschutzrichtlinie seit kurzem diskutiert. Österreich hat nun im Zuge der DSG-Novelle 2010 mit 1. Jänner als zweites Land innerhalb der Europäischen Union eine solche Informationspflicht eingeführt.

Die österreichische Bestimmung ist allerdings nicht besonders geglückt, da sie voll von unklaren, nicht näher definierten Begriffen ist. So ist weder klar, was ein „systematischer“, noch was ein „schwerwiegender“ Datenmissbrauch genau ist. Ebenso unklar ist, was eine „geeignete“ Form der Verständigung der Betroffenen ist.

In den USA und ebenso in der seit 1. September in Deutschland gültigen Regelung ist als Form zunächst die direkte persönliche Verständigung des Betroffenen (etwa per Brief; denkbar sind aber auch E-Mail, Anruf etc.) vorgesehen. Wenn dies nicht möglich ist oder einen unverhältnismäßigen Aufwand bedeuten würde, sind Inserate in der Zeitung (in Deutschland zwei mindestens halbseitige Inserate in zwei bundesweit erscheinenden Tageszeitungen), in den USA teilweise sogar das Schalten von Informationspots im Fernsehen vorgesehen.

Was heißt „geringfügig“?

Eine Ausnahme von der Informationspflicht sieht der zweite Satz des § 24 Abs 2a DSG 2000 dann vor, wenn diese „angesichts der Drohung eines nur geringfügigen Schadens der Betroffenen einerseits oder der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert“. Es bedarf der Auslegung, was ein „geringfügiger“ Schaden ist. Ebenso unklar ist, ab wann die Informationskosten unverhältnismäßig wären. Die

sprachliche Wendung „einerseits . . . oder . . . andererseits“ ist wohl nur als ein schlichtes „oder“ zwischen den zwei Ausschließungsgründen zu lesen.

Interessant ist, dass die österreichische Datenschutzkommission entgegen dem Trend etwa in den USA oder der Diskussion in anderen Ländern der EU weder über einen Missbrauchsfall zu informieren ist noch sonst in irgendeiner Form in die Abwicklung eines solchen Missbrauchsfalles involviert wird.

Dies scheint für betroffene Unternehmen im ersten Moment zwar ein Vorteil zu sein, da es scheinbar die Möglichkeit offen lässt, Missbrauchsfälle eher „unter den Tisch zu kehren“. Bei näherer Betrachtung zeigt sich aber, dass Unternehmen letztlich bei der Beurteilung, ob und, wenn ja, in welcher geeigneten Form Betroffene über einen Missbrauchsfall zu informieren sind, vollständig allein gelassen sind.

Auch im Hinblick auf mögliche zivilrechtliche Haftungen wird hier dem Unternehmen eine erhebliche Selbstverantwortung auferlegt: Zu denken wäre etwa an einen Verstoß gegen Schadensminderungspflichten oder an mögliche Haftungsfreizeichnungen von Risikoversicherungen der betroffenen Unternehmen bei Ignorieren der Informationspflicht (Schutzgesetzverletzung!).

Für den Ernstfall vorbereiten

Dementsprechend ist es für Unternehmen wie öffentliche Stellen ratsam, einen möglichen Ernstfall nicht unvorbereitet auf sich zukommen zu lassen, sondern proaktiv Maßnahmen zu ergreifen, um vorbereitet zu sein. Vorbereitungsmaßnahmen sind nicht nur das Durchspielen unternehmenstypischer Risikoszenarien durch die Rechtsabteilung. Auch die gemeinsame Ausarbeitung von Notfallplänen mit verschiedenen anderen betroffenen Abteilungen, wie etwa der PR-Abteilung, der Unternehmens-IT, dem Krisenmanagement, der Geschäftsführung sowie möglicherweise betroffener Fachabteilungen gehören dazu.

Weitere Informationen zum Thema gibt es auf **www.preslmayr.at/datenschutz.php** und direkt beim Autor

Dr. Rainer Knyrim
Rechtsanwalt und Partner

knyrim@preslmayr.at

Pollirer · Weiss · Knyrim

DSG – Datenschutzgesetz

Von den Autoren des DSG-Kommentars kommt jetzt die **handliche Ausgabe** zum Datenschutzrecht:

- DSG aktuell – auf dem Stand der DSG-Novelle 2010
- informativ – mit präzis erläuternder Kommentierung, inkl. Materialien
- handlich – zum Mitnehmen und raschen Nachschlagen

Die Autoren:
Kommerzialrat **Hans-Jürgen Pollirer**, Gerichtssachverständiger und Geschäftsführer der SECUR-DATA GmbH.
Hofrat Dr. **Ernst M. Weiss**, Richter i.R.
Dr. **Rainer Knyrim**, Rechtsanwalt und Partner bei Preslmayr Rechtsanwälte mit Spezialgebiet Datenschutzrecht

Neue Partnerin

Mit Frau RA **Dr. Esther Hold** durften wir Anfang Februar 2010 eine Partnerin in unseren Reihen begrüßen. Sie war schon seit März 2007 als Rechtsanwaltsanwärterin Mitglied unseres Teams und vorwiegend im österreichischen und europäischen Kartellrecht, Medizinrecht, Arbeitsrecht und Vertragsrecht tätig.

Ihren Eintritt als Partnerin haben wir Anfang März 2010 in schon traditioneller Weise gemeinsam mit ihren Freunden und den Mitarbeitern gebührend gefeiert.