

Die Presse, **Vorreiter bei Informationspflicht – mit kleinen Stolperern**

Rechtspraxis, 1. 2. 2010, 8

VON RAINER KNYRIM

Österreich verpflichtet als zweites EU-Land Unternehmen und öffentliche Stellen, bei Datenmissbräuchen die Betroffenen zu informieren.

WIEN. 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 eine Vorreiterrolle.

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 schwerwiegender 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 diesen befindlichen Daten im Sinn dieser Bestimmung stattgefunden hat (etwa,

weil der Dieb oder zufällige Finder das Unternehmen nun mit einer Datenveröffentlichung zu erpressen versucht); und es muss überlegt werden, ob die Betroffenen zu informieren sind.

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 der Datenschutzrichtlinie seit Kurzem diskutiert. Österreich hat nun im Zuge der DSGVO-Novelle 2010 mit 1. Jänner als zweites Land innerhalb der Europäischen Union eine solche Informationspflicht eingeführt und übernimmt daher gemeinsam mit Deutschland wieder eine Führungsrolle bei der Weiterentwicklung des Datenschutzrechtes.

Die österreichische Bestimmung ist allerdings nicht besonders glücklich, 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 bedeutete, sind Inserate in der Zeitung (in Deutschland zwei mindestens halbseitige Inserate in zwei bundesweit erscheinenden Tageszeitungen), in den USA teilweise sogar das Schalten von Informationsspots im Fernsehen vorgesehen.

Was heißt „geringfügig“?

Eine Ausnahme von der Informationspflicht sieht der zweite Satz des § 24 Abs 2a DSGVO 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“. Unklar ist hier, was ein „geringfügiger“ Schaden ist – so könnten zum Beispiel 50 Euro als

drohender Schaden für einen wohlhabenden Bankkunden unbedeutend, für einen Mindestrentner hingegen bedeutend sein. Ebenso unklar ist, ab wann die Informationskosten unverhältnismäßig wären. Schon die sprachliche Wendung „einerseits... oder... andererseits“ ist nicht unbedingt gut gelungen, kann wohl aber nur als „oder“ zwischen den zwei Ausschließungsgründen gelesen werden – und nicht (obwohl dies vom Sprachgebrauch indiziert wäre) als „und“.

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 Missbrauchsfalls involviert wird. Dies scheint für betroffene Unternehmen im ersten Moment zwar ein Vorteil zu sein, da es scheinbar die Möglichkeit offen lässt, Missbrauchsfälle „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 Haftungsverzeichnungen 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 unternehmens-typischer 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.

Dr. Rainer Knyrim ist Partner bei Preslmayr Rechtsanwälte, Wien.