EU-Datenschutz: Die Unterpunkte haben es in sich

20.12.2015 | 17:57 | von Rainer Knyrim (Die Presse)

Die neue Grundverordnung bringt bürokratische Lasten, hohe Strafen und keine EU-weite Einheitlichkeit. Zusätzliche Unternehmerpflichten finden sich an versteckter Stelle.

Wien. Die politische Einigung über das neue EU-Datenschutzrecht wurde erzielt. Was kommt jetzt? Eine Datenschutz-Keule mit vielen kostenintensiven Detailbestimmungen für die Unternehmen. Und die nächste Lobbying-Welle?

Die vorige Woche in Brüssel vereinbarte Datenschutzreform wird ab 2018 die 20 Jahre alte Datenschutz-Richtlinie ablösen. Diese galt als zu bürokratisch und zu wenig harmonisierend. Die Unternehmen wollten mehr Selbstregulierung, weniger Behörden-Papierkram, einfache Regeln, weitreichende Ausnahmen für KMUs. Die EU-Kommission wollte eine Vollharmonisierung durch direkt anwendbares Recht. Das Detailstudium des 209 Seiten langen, für Durchschnittsbürger kaum verständlichen Textes der geplanten Datenschutz-Grundverordnung zeigt nicht das bis zuletzt erwartete Ergebnis. Heraus kam im Finale der Verhandlungen viel Selbst-Bürokratie und exorbitante Strafen für die Unternehmen und für die EU keine Vollharmonisierung.

Strafen 800 Mal höher

Markantester Einschnitt für die Unternehmen ist die Erhöhung des Strafrahmens von 25.000 auf 20 Mio. Euro, also das 800-Fache. Er ist zusätzlich nach oben offen, denn das Strafhöchstmaß kann bis 4 Prozent des globalen Konzernumsatzes betragen. Was bisher wenig beachtet wurde: Das neue Recht und die Strafen treffen nicht nur Facebook & Co., sondern jedes Unternehmen in Österreich, inkl. KMUs, deren Ausnahmewünsche aus dem ersten Entwurf fast alle gestrichen wurden.

Die Aufzählung der vielen neuen Pflichten der Unternehmen macht atemlos: Verzeichnis der Datenanwendungen führen; alle Betroffenen bei der Datenerhebung im Detail über die Datenverwendung informieren; Betroffenen auf Anfrage detailliert über die verarbeiteten Daten und deren Speicherdauer Auskunft geben; in bestimmten Fällen eine Datenschutz-Folgenabschätzung durchführen; nach einem Datenmissbrauch binnen 72 Stunden die Datenschutzbehörde informieren; bei Minderjährigen für eine Zustimmung der Eltern sorgen; wo „verhältnismäßig“, Datenschutz-Policies einführen. All diese Pflichten sind neue, interne Papiertiger. Dazu kommen technisch-organisatorische Pflichten wie die Umsetzung der neuen Rechte „auf Vergessen“ oder auf „Datenportabilität“ der Konsumenten, ebenso die Pflicht, Datenschutz durch Technik und Software-Voreinstellungen zu bieten, und die Pflicht, in bestimmten Fällen Datenschutzbeauftragte einzuführen. Die Unternehmen werden kaum bis zum Inkrafttreten 2018 fertig werden, wenn sie nicht rasch Projekte beginnen.

Teuflische Details verstecken sich meist in kleinen Unterpunkten. So bestimmt ein Punkt 2a) in Art 28 ganz nebenbei, dass auch jeder Dienstleister, der Daten verarbeitet, ein Verzeichnis der Datenanwendungen führen muss, wenn er sensible Daten verarbeitet. Das trifft z. B. externe Buchhalter, die Krankenstände berechnen, oder EDV-Dienstleister, die Daten der Buchhaltung hosten. Dienstleister waren bisher in Österreich von formalen Pflichten praktisch ganz verschont, werden aber nun auch von der Pflicht getroffen, bei bestimmten Verarbeitungen ebenfalls einen Datenschutzbeauftragten zu bestellen.

Interessenkonflikt droht

Apropos Datenschutzbeauftragter: Dieser muss natürlich nicht hauptberuflich angestellt sein, doch – hoppla! – eine kleine Ziffer 4a) in Art 36 besagt, dass seine sonstigen Aufgaben keinen

Interessenkonflikt auslösen dürfen. Da wird es schwierig – wie bisher üblich –, jemanden, mit dem künftig geforderten Expertenwissen im Datenschutzrecht, aus der EDV oder der Rechtsabteilung dazu zu bestellen.

Auch zunächst großzügig wirkende Einschränkungen wie bei der aufwendigen Datenschutz-Folgenabschätzungen, die nur bei der Verarbeitung sensibler Daten in großem Umfang durchzuführen sind, werden im selben Punkt (Art 33 2b) wieder relativiert, wenn dort anscheinend jegliche Verarbeitung strafrechtlich relevanter Daten doch eine solche Abschätzung erfordert. Dies könnte wegen des weit verbreiteten Sammelns von Strafregisterauszügen von Stellenbewerbern sehr viele Unternehmen treffen.

Solche Datenschutz-Folgenabschätzung sind überdies dann durchzuführen, wenn durch automatisierte Datenverarbeitung Personen kategorisiert werden, etwa bei negativen Bonitätsrankings, die dann verhindern, dass jemand einen Vertrag abschließen kann. Dieses „Profiling“ war bis zuletzt sehr umstritten, da hier die Unternehmen eine der wenigen Erleichterungen gegenüber bisher durchsetzen konnten: Es kann ohne vorherige Zustimmung durchgeführt werden, die Betroffenen haben nur ein Opt-out-Recht. Diese Erleichterung wird aber nun durch die Verpflichtung zur Folgenabschätzung in Punkt 2a) des Art 33 erschwert.

Während der vierjährigen Verhandlung fand die bisher beispielloseste Lobbyingschlacht in der Geschichte der EU statt, die u. a. in 4000 Änderungsanträgen im EU-Parlament endete. Diese ist trotz der Rechtsform der direkt anwendbaren EU-Verordnung, die nationale Änderungen nicht mehr zulässt, nicht zu Ende. Sämtliche vorgenannten Pflichten finden sich in den ersten 38 Artikeln des Textes. In diesen findet sich aber fast genauso oft das Recht der Mitgliedstaaten versteckt, die jeweilige Verpflichtung noch durch nationales Recht zu spezifizieren oder zu verändern. Der Schaffung von umfangreichem nationalem Datenschutzrecht, um noch eine Feinjustierung vorzunehmen – und damit einer zweiten Lobbyingwelle auf österreichischer Ebene – steht damit die Tür offen.

Rainer Knyrim ist Partner bei Preslmayr Rechtsanwälte OG, Wien, und Chefredakteur der Zeitschrift „Datenschutz konkret“.