CB-EDITORIAL

DSGVO – Heikle Compliance-Reform am offenen Herzen

Noch knapp 100 Tage, bis die neue EU Datenschutz-Grundverordnung in Kraft tritt. Die Spannung steigt – und die Nervosität. Mit Bußgeldern, die dem Kartellrecht angelehnt wurden und bis zu 20 Millionen Euro und 4 Prozent des weltweiten Umsatzes eines Konzerns betragen können, genießt das Thema nun schließlich eine hohe Aufmerksamkeit bis in die Führungsebene von internationalen Unternehmen. Diese Situation ist auch kein rein europäisches Thema mehr, sondern faktisch bereiten sich alle globalen Großkonzerne auf das neue Recht vor, auch wenn ihre Zentralen in Asien oder Nordamerika liegen.

Unternehmen müssen eine Datenschutz-Compliance aufbauen, wie sie für andere Compliance-Bereiche in den letzten Jahren üblich geworden ist. Das neue Prinzip der Rechenschaftspflicht – englisch präziser „Accountability" – verlangt, dass man künftig das Recht nicht nur einhält, sondern dessen Einhaltung stets aktiv nachweisen kann. Dies führt zu mehr Papier: Richtlinien und interne Verhaltensanweisungen müssen entworfen und Mitarbeiter entsprechend geschult werden. Das kommt Compliance-Verantwortlichen wahrscheinlich sehr bekannt vor. Das neue Recht ist gleichzeitig auch sehr kleinteilig in seinen Anforderungen. Unternehmen müssen jede einzelne Datenverarbeitung in ihren Häusern erfassen und katalogisieren (das sog. Data Mapping). Die hieraus erstellte Übersicht ist quasi die Grundvoraussetzung, das neue Recht einhalten zu können: Wenn man nicht weiß, wo welche Daten für welchen Zweck, wie lange und von wem gespeichert werden, ist kaum sicherzustellen, dass die Daten immer im Einklang mit den Grundprinzipien verarbeitet werden. Nur aus einer vollständigen Übersicht kann man die Daten zusammentragen, die notwendig sind, um Mitarbeiter und Kunden umfassend zu informieren.

Diese notwendige Erfassung aller Datenverarbeitungen stellt Großunternehmen vor erhebliche Herausforderungen. Viele haben hierfür Beraterteams ins Haus geholt, die mit Personal-, IT-, Marketing-Verantwortlichen und vielen anderen Interviews führen, wo welche Daten verarbeitet und gespeichert werden. Je größer Unternehmen sind, umso schwieriger wird es aber, alles im Detail zu erfassen. Die komplette Erfassung von Datentransfers gleicht einer Sisyphos-Aufgabe. Ein Unternehmen kann nur eine gewisse Komplexität praktisch managen – man kann also kaum jede Excel-Liste mit Geburtstagen der Abteilungskollegen erfassen, auch wenn man es theoretisch vielleicht müsste. Dieser Spagat führt zu Kompromissen – von denen niemand weiß, ob sie eine Behörde künftig so akzeptieren wird.

Komplette Erfassung von allen Datenverarbeitungen im Konzern ist eine Sisyphos-Aufgabe.

Aufgrund der Kleinteiligkeit und Komplexität sind viele Unternehmen bei den Vorbereitungen auf das neue Recht noch nicht weit genug. Viele haben das Thema wohl auch unterschätzt und zu spät angefangen.

Die kurzfristige Lösung liegt in der Priorisierung der Einzelaufgaben. Das Erfassen aller Datenverarbeitungen und die Erstellung des Verzeichnisses sollten nun fertig werden – dann kann man in den kommenden knapp 100 Tagen zumindest die Benachrichtigungen entwerfen und Einwilligungsformulare aktualisieren. Die Details einer Datenschutz-Folgenabschätzung für hochriskante Verarbeitungen gilt erst mal nur für neue Verfahren, die nach Mai eingeführt oder geändert werden. Das kann man also noch etwas schieben. Auch jede interne Datenschutz-Richtlinie muss wohl nicht bis Mai fertig werden.

Oder vielleicht doch? Keiner weiß, wie streng die Verwaltung das neue Recht ab Tag eins einfordern wird. Letztlich wird diese Thematik auch in Europa entschieden: Der neue EU-Datenschutz-Ausschuss kann bindende Vorgaben machen, wie die insoweit nicht mehr so unabhängigen Behörden das neue Recht vollziehen müssen. Limitierender Faktor bleibt ein anderer: Die Personalstärke der 17 deutschen Behörden wächst bis Mai nicht in dem Maße, dass diese eine flächendeckende Beaufsichtigung ab Tag eins erlaubt. Dies wird langfristig sicherlich anders, wenn die Behörden mehr Bußgelder eintreiben, als sie Personalkosten haben – also aus Sicht der Landes-Finanzminister zum Profit Center werden.

Im Mai werden also nur die wenigsten Unternehmen wirklich zu 100 Prozent auf das neue Recht vorbereitet sein. Sie können wohl in gewissem Maße entspannt bleiben, wenn sie ihr Projekt auf einem guten Weg haben. Gleichzeitig wachen manche jetzt erst auf und nehmen das neue Recht erstmalig zur Kenntnis. Oder sie reagieren erst, wenn die ersten Bußgelder durch die Presse gehen. In diesen Fällen werden die Behörden dann wohl nicht ganz so großzügig sein.

AUTOR

Dr. Christoph Ritzer, *RA, ist Partner bei Norton Rose Fulbright Frankfurt. Er berät seit über 10 Jahren als spezialisierter Anwalt zum Datenschutzrecht, Informationstechnologie-Recht sowie zum Outsourcing und begleitet eine Vielzahl von deutschen und internationalen Unternehmen dabei, sich auf das neue EU-Recht vorzubereiten.*