ZEITSCHRIFT FÜR DATENSCHUTZ

ZD

EDITORIAL

3/2016

Die DS-GVO – ein Compliance-Thema?

Lesedauer: 8 Minuten

Effektive Compliance-Management-Systeme (CMS) setzen wirksame Kontrollen voraus. Unternehmen müssen prüfen, ob sich Mitarbeiter und Geschäftspartner an die geltenden Regeln halten. Hier setzt der Datenschutz oft die Leitplanken, innerhalb derer Überwachungsmaßnahmen zulässig sind.

Bei Verstößen gegen die Vorgaben des Datenschutzrechts kann die Kontrolle selbst zum Compliance-Verstoß werden. Insofern gibt es zwischen Datenschutz und Compliance ein natürliches Spannungsfeld. Gelegentlich fällt in solchen Situationen auch schon einmal der Satz: „Manchmal muss man sich eben entscheiden – Datenschutz oder Datenverarbeitung." Auf Grund einer leicht zu übersehenden Regelung in der letzten Entwurfsfassung der DS-GVO dürfte bei solchen Abwägungen zwischen Persönlichkeitsrecht und Compliance die Rolle des Datenschutzes erheblich an Bedeutung gewinnen. Denn künftig werden sich die möglichen Bußgelder wegen Datenschutzverstößen teilweise im dreistelligen Millionenbereich bewegen.

Tim Wybitul
ist Rechtsanwalt, Fachanwalt für Arbeitsrecht und Partner der Kanzlei Hogan Lovells International LLP in Frankfurt/M. sowie Mitherausgeber der ZD.

Bisherige Bußgeldpraxis in Deutschland

Die tatsächlichen wirtschaftlichen Risiken möglicher Datenschutzverstöße waren bislang bekanntlich eher überschaubar. Die höchste Zahlung nach Verletzungen des BDSG in einem Unternehmen betrug € 1,9 Mio. Diese Summe setzte sich aus einem Bußgeld von € 1,3 Mio. und einer Stiftung von € 600.000,– für einen Datenschutz-Lehrstuhl zusammen. Verglichen mit Bußgeldern wegen Kartellverstößen, systematischem Steuerbetrug oder Korruption sind die bislang von deutschen Aufsichtsbehörden für den Datenschutz bei Verstößen veranschlagten Beträge eher bescheiden.

Millionenrisiken für Unternehmen?

Die bisherige Bußgeldpraxis ändert sich nun mit der bereits beschlossenen DS-GVO – mit drastischen Folgen für die Compliance-Bewertung datenschutzrechtlicher Risiken. Denn das kommende EU-weite Datenschutzrecht sieht drakonische Strafen vor. Es drohen Bußgelder von bis zu 4% des global erzielten Umsatzes des Vorjahrs.

Über einen wichtigen Punkt wurde hierbei bis zuletzt gestritten. Nämlich ob das Bußgeld nur auf der Grundlage des Umsatzes des verantwortlichen Unternehmens berechnet wird – oder auf Basis der Umsätze der gesamten Unternehmensgruppe. Bei Konzernen kann der Unterschied zwischen beiden Bemessungsmethoden gewaltig sein. Eine einzelne Landesgesellschaft oder eine kleine IT-Tochter eines global tätigen Konzerns werden teilweise keine gewaltigen Umsatzzahlen erwirtschaften.

Der nur auf Unternehmen bezogene Bußgeldrahmen wäre damit vergleichsweise überschaubar – bei internationalen Unternehmensgruppen ist das hingegen etwas anderes. Hier können 4% des gruppenweiten Unternehmensumsatzes durchaus dreistellige Millionenbeträge erreichen – wie die Bußgeldpraxis der *EU-Kommission* und anderer Behörden in Kartellverfahren eindrucksvoll zeigt. Und gerade der kartellrechtliche Unternehmensbegriff soll künftig auch beim Datenschutzrecht für die Berechnung von Bußgeldern gelten. Denn in der Entwurfsfassung der DS-GVO vom 15.12.2015 wurde zu den Sanktionen bei Datenschutzverstößen buchstäblich in letzter Sekunde noch eine recht versteckte Änderung aufgenommen.

Die letzte Fassung von Erwägungsgrund 120 verweist nämlich nun in Bezug auf die Bußgelder auf Art. 101 und 102 AEUV. Und diese Regelung legt den Begriff der wirtschaftlichen Einheit zu Grunde – vereinfacht gesprochen also den der Unternehmensgruppe. Dies würde auch zu der erklärten Absicht der *EU-Kommission* passen, ausgesprochen abschreckende Regelungen zu schaffen, um die Durchsetzung der Vorschriften des Datenschutzes sicherzustellen.

Voraussichtliche Position der Aufsichtsbehörden

Nun mag man zwar mit Recht bezweifeln, ob eine Vorgabe von derart fundamentaler Bedeutung überhaupt in einem Erwägungsgrund geregelt werden kann (vgl. hierzu *Faust/Spittka/Wybitul*, ZD 2016, 120 – in diesem Heft). Auch im Hinblick auf den in Deutschland u.a. in Art. 103 Abs. 2 GG festgeschriebenen Bestimmtheitsgrundsatz wäre eine solche Auslegung problematisch. Andererseits kann man wohl davon ausgehen, dass die Aufsichtsbehörden für den Datenschutz sich bei der Berechnung von Bußgeldern im Zweifelsfall eher an dem gruppenweiten Umsatz als an dem des Unternehmens orientieren werden.

Folgen der hohen Bußgelder für Unternehmen und deren Compliance-Abteilungen

Compliance ist letztlich regulatorisches Risikomanagement. Für die Wirtschaft hat die Regelung der Bußgelder in der kommenden DS-GVO erhebliche Folgen. Auf Grund der wohl ab 2018 drohenden ausgesprochen hohen Bußgelder wird der Datenschutz künftig zu einem ähnlich wichtigen Thema für Risikomanagement und Compliance-Abteilungen wie Verstöße gegen Kartell-, Korruptions- oder Steuerrecht.

Gefährdungsanalyse Datenschutz

Bei der Bewertung von Compliance-Risiken steht in aller Regel zunächst eine Gefährdungsanalyse im Vordergrund. Dabei geht es primär nicht um die rein juristische Bewertung der rechtlichen Zulässigkeit. Eine solche Analyse wäre in der Praxis bei den vielen Grauzonen im Datenschutz auch oft nur schwer umsetzbar. Aus Compliance-Sicht bewertet man hingegen zunächst die Risiken möglicher Fehler beim Umgang mit gesetzlichen oder sonstigen verbindlichen Vorgaben.

Neben möglichen Rufschäden, Schadensersatzforderungen, Beweisverwertungsverboten und den sonstigen bereits bekannten Risiken stehen nach der DS-GVO gerade die Bußgeldrisiken im Vordergrund. Hier bringt das neue Recht ganz erhebliche Verschärfungen mit sich. Diese sind i.R.e. auf das jeweilige Unternehmen bzw. auf die Unternehmensgruppe bezogenen Gefährdungsanalyse näher zu bestimmen.

Große Unternehmen werden ihre individuellen Bußgeldrisiken auf der Basis von 4% ihres gruppenweiten globalen Umsatzes des Vorjahrs berechnen müssen, um ihre eigene spezifische Gefährdungssituation beurteilen zu können. Wie bereits nach der bislang geltenden Rechtslage gelten die rechtlich festgelegten Sanktionen für einzelne Verstöße. Vereinzelte Übertretungen der rechtlichen Vorgaben sind aber beim Datenschutz in der Praxis eher selten.

Oftmals betreffen Datenverarbeitungen gleich eine Vielzahl von Personen bzw. Prozessen. In solchen Fällen bilden deutsche Behörden und Gerichte Gesamtbußgelder. Deren Höhe ist in aller Regel niedriger als die Summe der Bußgelder für einzelne Verstöße. Trotz dieses „Mengenrabatts" können solche Gesamtbußgelder ein Vielfaches des für einen einzelnen Verstoß angeordneten Maximalbußgelds erreichen.

Bußgeldbemessung nach der DS-GVO

Es spricht einiges dafür, dass die Datenschutzbehörden den Verweis auf Art. 101 und 102 AEUV zum Anlass nehmen werden, sich insgesamt an der bisherigen Bußgeldpraxis der Aufsichtsbehörden zu orientieren. In diesem Fall wäre es sehr unwahrscheinlich, dass die Behörden den im Einzelfall theoretisch möglichen Bußgeldrahmen auch in der Praxis voll ausschöpfen werden. Ein noch strengeres Vorgehen wäre auch im Hinblick auf das für die Verhängung von Bußgeldern maßgebliche Ordnungswidrigkeitenrecht problematisch.

Denn ähnlich wie im materiellen Datenschutzrecht ist auch bei der Verhängung von Bußgeldern der Verhältnismäßigkeitsgrundsatz entscheidend. Und es dürfte eindeutig unverhältnismäßig sein, Millionenbußgelder wegen vereinzelter oder weniger schwerwiegender Verstöße zu verhängen. Dabei werden Unternehmen mögliche Bußgelder nach Inkrafttreten der DS-GVO erst einmal nur näherungsweise bestimmen können. Eine genauere Analyse wird dann möglich, wenn sich eine einheitliche und abgestimmte Bußgeldpraxis der Datenschutzbehörden herausbildet.

Wie geht es weiter?

Sowohl bei der Auslegung der DS-GVO als auch bei der Bemessung von Bußgeldern wegen Datenschutzverstößen kommt den zuständigen Gerichten voraussichtlich eine deutlich wichtigere Rolle zu. In der Vergangenheit waren Gerichtsverfahren wegen Datenschutzfragen nicht sonderlich häufig. Insbesondere waren Rechtsstreitigkeiten wegen der Höhe verhängter Bußgelder die absolute Ausnahme. Das wird sich nun voraussichtlich ändern. Denn die massiv gesteigerten Bußgeldrahmen werden aller Voraussicht nach dazu führen, dass die Datenschutzbehörden auch deutlich höhere Bußgelder verhängen werden als bislang.

Unternehmen werden hierauf damit reagieren, dass sie öfter gegen verhängte Bußgelder rechtlich vorgehen. Gesellschafter, Aktionäre und Aufsichtsräte werden hohe Millionenstrafen aller Voraussicht nach nicht ohne weiteres akzeptieren. Ähnlich wie im Kartell- oder Korruptionsrecht werden Unternehmen auch Schadensersatzansprüche gegen verantwortliche Vorstände, Geschäftsführer und Beschäftigte prüfen und durchsetzen. Auch dies wird voraussichtlich viele Gerichtsprozesse wegen Haftungsfragen nach sich ziehen. Jedenfalls eine Folge der DS-GVO liegt bereits auf der Hand – Richter und Datenschutzanwälte mit Prozesserfahrung werden künftig viel zu tun haben.

Was kann die Wirtschaft jetzt schon tun?

Unternehmen können ihre derzeitigen Datenschutz-Strukturen bereits jetzt mit den künftigen Anforderungen der DS-GVO vergleichen. Auch Firmen oder Konzerne mit einem bereits ausgereiften und angemessen auf das BDSG ausgerichteten Datenschutz-Management-System (DMS) werden in Bezug auf die zusätzlichen Anforderungen des kommenden EU-weiten Datenschutzrechts noch deutlich nachbessern müssen – etwa in Bezug auf Transparenz, verständliche Datenschutzregelungen, Dokumentationspflichten („Accountability"), Standardsysteme („Privacy by Design") und Standardeinstellungen („Privacy by Default"). Auch datenschutzrechtliche Folgenabschätzungen („Privacy Impact Assessments") setzen entsprechende Strukturen und interne Planung voraus. Hier kommt auf deutsche und andere europäische Unternehmen voraussichtlich noch eine ganze Menge Arbeit zu.

Dabei sollte man auch nicht aus dem Blick verlieren, dass Unternehmen Veränderungen von Datenschutzstrukturen oftmals auch mit dem Betriebsrat abstimmen müssen. Gerade bei mitbestimmungspflichtigen Themen wie Datenschutzrichtlinien oder IT-Betriebsvereinbarungen können die notwendigen Verhandlungen mit dem oder den zuständigen Konzern-, Gesamt- oder lokalen Betriebsräten oft Monate oder sogar Jahre in Anspruch nehmen.