Das künftige EU-Datenschutzrecht – Neue Anforderungen an die unternehmerische Compliance

Europa ringt seit Jahren um die Erneuerung der veralteten Datenschutzgesetze. Beispielloses Lobbying hat den Beschluss einer verbindlichen Grundverordnung verzögert. Langsam kristallisieren sich aber doch Kernpunkte des Reformwerks heraus. Dabei zeigt sich, dass Datenschutz verstärkt ein Thema für die Unternehmens-Compliance werden wird. Nicht zuletzt wegen der drohenden, drakonischen Bußgelder.

Von Rainer Knyrim | Gerald Trieb

1. Stand des Entwurfs für das künftige EU-Datenschutzrecht

Ende Jänner 2012 hat die EU-Kommission einen lange erwarteten Vorschlag für die Reform des europäischen Datenschutzrechts vorgelegt. Intention ist, das Datenschutzrecht in Europa zu vereinheitlichen. Der Vorschlag für die Reform besteht aus zwei Teilen: einem Vorschlag für eine Richtlinie, die sich an die Behörden wendet, die Daten im Zusammenhang mit Straftaten verarbeiten,[1] und einem Vorschlag für eine „Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr", kurz „Datenschutz-Grundverordnung" (DSGVO), die sich an die Unternehmen und sonstigen Behörden wendet.[2]

Dieser Beitrag beschäftigt sich ausschließlich mit der DSGVO. Der Vorschlag für die DSGVO enthält 91 Artikel auf 113 Textseiten. Sie soll als direkt anwendbare EU-Verordnung das bisherige, auf der EU-Datenschutzrichtlinie aus 1995 basierende nationale Datenschutzrecht ersetzen. Über diesen Vorschlag hat sich das Europäische Parlament im Jahr 2013 eingehend beraten. Dabei kam es zu einem bisher beispiellosen Lobbying: über 3.000 Änderungsanträge wurden eingebracht. Der sogenannte LIBE-Ausschuss des Parlaments hat schließlich im Oktober 2013 aus diesen über 3.000 Änderungsanträgen eine „Entschließung" mit 113 Änderungen verabschiedet.[3] Der Inhalt dieser Entschließung wurde erst vor kurzem, am 12. März 2014, vom Parlament mit großer Mehrheit angenommen. Auch die Vertreter der Mitgliedstaaten arbeiten sich im Rat der EU seit Monaten intensiv durch den Entwurf, wobei Bestimmungen, die stark in die nationale Souveränität eingreifen, wie etwa das sogenannte „One-Stop-Shop"-Prinzip, im Fokus stehen. Noch vor dem Sommer soll ein „Trilog" zwischen Parlament, Rat und Kommission gestartet werden. Der „offizielle" Zeitplan sieht derzeit vor, dass Ende 2014 die Endfassung der DSGVO vorliegt und zwei Jahre später in Kraft tritt.

2. Künftige Rechtslage nach der DSGVO

Auch wenn der Text der DSGVO noch im Entwurfsstadium ist, haben sich in den über zweijährigen Verhandlungen bereits einige für die Unternehmens-Compliance bedeutenden Punkte herauskristallisiert, die zwar noch Änderungen unterworfen sein werden, aber offensichtlich Kernpunkte der Reform bilden werden.

3. Drakonische Strafen

Schon der Vorschlag der Kommission sah eine enorme Strafhöhe von maximal einer Mio Euro oder zwei Prozent des weltweiten Konzernumsatzes vor.[4] Das Parlament hat die Strafhöhe sogar auf maximal 100 Mio Euro oder fünf Prozent des weltweiten Konzernumsatzes des Unternehmens (je nachdem, was mehr ist) hinaufgesetzt. Die endgültigen Strafhöhen werden sich nach einem politischen Kompromiss wohl zwischen diesen Werten befinden. Ab sofort und somit schon vor Inkrafttreten der DSGVO wird Datenschutzrecht besonders bei den vielen Unternehmen in Österreich, die sich noch immer nicht oder nicht ausreichend mit diesem befasst haben, dadurch zu einem der wichtigsten Compliance-Themen. Es gilt, bisher Versäumtes nachzuholen und sich auf die künftigen, neuen Anforderungen einzustellen.

3.1. Compliance wird strafmildernd wirken

Die DSGVO soll den Unternehmen – teilweise verpflichtend – Maßnahmen vorgeben, die Datenschutzverstöße schon im Vorhinein verhindern sollen. Diesbezüglich wird von Unternehmen die Einhaltung der Prinzipien „Privacy by Design" und „Privacy by Default", das Durchführen von Datenschutz-Folgeabschätzungen vor der Einführung datenverarbeitender Systeme sowie die Erarbeitung und Festlegung von Richtlinien für den Umgang mit und die Reaktion auf Datenschutzverstöße verlangt. Diese „vorbeugenden Maßnahmen" können im Falle des Verstoßes und eines darauffolgenden behördlichen Strafverfahrens die Geldbuße drastisch reduzieren. Neben möglichen Erschwerungsgründen bei der Strafzumessung (besonders achtloser Umgang mit personenbezogenen Daten, völliges Fehlen von Datensicherheitsmaßnahmen, etc) können also in Zukunft von Unternehmen vorab gesetzte Compliance-Maßnahmen als Milderungsgründe geltend gemacht werden. Datenschutz-Compliance soll sich also nicht nur als Risikominimierung im Vorfeld, sondern auch im „Ernstfall" strafmildernd auswirken.

3.2. Eigenverantwortung der Unternehmen wird gestärkt

Die DSGVO soll die Eigenverantwortung der Unternehmen deutlich stärken. So sollen Meldeverfahren auf spezifische Anwendungsfälle reduziert (zB im Fall der Verwendung sensibler Daten, bei Videoüberwachung, Massendatenverarbeitungen etc), den Unternehmen dafür aber höhere interne Dokumentationspflichten (ab einem bestimmten Schwellenwert) auferlegt werden. Den Unternehmen wird also nicht erspart bleiben, sich einen Überblick über die betriebenen Datenanwendungen zu verschaffen. Gerade in größeren und verflochtenen Unternehmensgruppen ist dies eine der schwierigsten Aufgaben in Datenschutz-Compliance-Projekten und wird daher oft gar nicht oder nicht ordentlich durchgeführt, was bei den künftigen Strafhöhen teuer werden könnte.

Unternehmen, die Datenbanken betreiben, in denen Daten von zumindest 5.000 Betroffenen gespeichert sind, sollen laut Abstimmung im EU-Parlament verpflichtet werden, einen Datenschutzbeauftragten in ihrem Unternehmen zu benennen. Diese Verpflichtung wird wohl viele datenverarbeitende Unternehmen insbesondere in Bezug auf ihre Kundendatenbanken treffen, denn schon bei mehr als 5.000 Kunden im Newsletter-Verteiler wäre diese Grenze überschritten. Der ursprüngliche Entwurf der Kommission hatte vorgesehen, dass ein Datenschutzbeauftragter erst ab 250 Beschäftigten zwingend einzurichten ist – ein Kriterium, das nur 0,3 Prozent der österreichischen Unternehmen erfüllt hätten. Nach welchem Kriterium und in welcher Höhe die Grenze schließlich politisch ausgehandelt werden wird, bleibt noch abzuwarten.

Als „Gegenpol" zur gestärkten Eigenverantwortung steht die Drohung der bereits erwähnten Geldbußen von 100 Mio Euro oder fünf Prozent des weltweiten Konzernumsatzes (die durch eine schriftliche Verwarnung im Falle eines ersten und nicht vorsätzlichen Verstoßes ersetzt werden kann). Überdies sollen Unternehmen bei Datenschutzverstößen nach Art 79 des Entwurfs auch regelmäßig Überprüfungen betreffend die Einhaltung von Datenschutzvorschriften drohen.

Daneben soll auch die – in Österreich bereits seit der Novelle zum Datenschutzgesetz im Jahr 2010 verpflichtende – „Data Breach Notification Duty" (also die Pflicht, Datenschutzverstöße zu melden) europaweit eingeführt werden. Die Unternehmen werden also verpflichtet, die von ihren Datenanwendungen Betroffenen selbst über Sicherheitslücken zu informieren.

In die Richtung, Unternehmen einen höheren Grad an Eigenverantwortung bei der Verwendung von personenbezogenen Daten zu geben, geht auch der Vorschlag des Parlaments, Unternehmen standardisierte Symbole (Piktogramme) für die Verwendung auf Homepages oder sonstigen kommerziellen Kommunikationsmedien zur Verfügung zu stellen. Die Art der Verwendung personenbezogener Daten durch das jeweilige Unternehmen und die mit ihr verbundenen Schutzmaßnahmen sollen Usern auf diese Weise plakativ dargestellt werden.

3.3. Risikobasierter Compliance-Ansatz

Die vorgesehenen Sanktionen und die neuen Pflichten für Unternehmen durch die kommende DSGVO legen es nahe, bei der Datenschutz-Compliance einen „Risk-Based-Approach", also einen risiko- bzw haftungsorientierten Ansatz zu wählen. Das bedeutet, dass für das Setzen von Compliance-Maßnahmen zur Risikominimierung die Ausgestaltung der Strafbestimmungen als Orientierungsmaßstab dient.

Eine nähere Betrachtung der zentralen Strafbestimmungen in Art 79 des Entwurfs für die DSGVO ist daher angezeigt. Diese zeigt, dass nach Artikel 79 Abs 2c DSGVO ein ganzer Katalog von Faktoren im Fall der Verhängung von Sanktionen für deren Höhe bzw Intensität maßgeblich ist (die Anmerkungen stammen von den Autoren):

a) Die Art, Schwere und Dauer des Verstoßes;
b) der vorsätzliche oder fahrlässige Charakter des Verstoßes;
c) der Grad der Verantwortung der natürlichen oder juristischen Person und frühere Verstöße dieser Person;
d) der Wiederholungscharakter dieses Verstoßes (Anm: dies dürfte sich zumindest teilweise mit dem Faktor unter c) überschneiden);
e) der Umfang der Zusammenarbeit mit der Aufsichtsbehörde zur Wiedergutmachung des Verstoßes und zur Minderung seiner möglichen negativen Auswirkungen (Anm: auch nach der Begehung des Verstoßes ist somit gegenüber der Behörde kooperatives und gegenüber den (potenziell) Geschädigten schadensminimierendes bzw -gutmachendes Verhalten angezeigt);
f) die spezifischen Kategorien personenbezogener Daten, die von dem Ver-

stoß betroffen sind (Anm: dies hält Unternehmen auch dazu an, nur jene personenbezogenen Daten zu verarbeiten, die man auch tatsächlich benötigt);

g) der Umfang des Schadens, auch des immateriellen Schadens, für die betroffenen Personen;

h) die von dem für die Verarbeitung Verantwortlichen (Anm: = Auftraggeber) oder dem Auftragsverarbeiter (Anm: = Dienstleister) getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;

i) direkt oder indirekt aus dem Verstoß entstandene beabsichtigte oder erlangte finanzielle Vorteile oder vermiedene Verluste (Anm: dies wird vor allem bei Datenmissbrauch aus finanziellen Überlegungen sowie bei Verstößen im Zusammenhang mit der Verwendung von Daten für Marketingmaßnahmen relevant sein);

j) die technischen und organisatorischen Maßnahmen und Verfahren gemäß
   - Art 23 der DSGVO (Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Anm: Prinzip des „Privacy by Design" und „Privacy by Default"));
   - Art 30 (Sicherheit der Verarbeitung);
   - Art 33 (Datenschutz-Folgenabschätzung);
   - Art 33a (Überprüfung der Einhaltung der Datenschutzbestimmungen (Anm: darunter sind die ohnehin verpflichtenden, regelmäßig durchzuführenden „Datenschutz-Audits" zu verstehen));
   - Art 35 (Benennung eines Datenschutzbeauftragten – Anm: gemeint wohl, wenn nach den Bestimmungen dieser DSGVO nicht ohnehin verpflichtend)

k) die Weigerung, mit der Aufsichtsbehörde zusammenzuarbeiten oder die Behinderung von ihr gemäß Art 53 durchgeführter Nachprüfungen, Überprüfungen und Kontrollen (Anm: wohl bereits durch Punkt e) (teilweise) abgedeckt);

l) jegliche anderen erschwerenden oder mildernden Umstände im Einzelfall (Anm: jede weitere positive Datenschutz-Compliance-Handlung kann sich somit positiv auf die Strafbemessung auswirken).

Zur Risikominimierung bzw Linderung der finanziellen Auswirkungen eines Datenschutzverstoßes sollte dieser Katalog somit strikt beachtet und jene Maßnahmen durchgeführt werden, die das Strafmaß reduzieren können. Besonders hervorzuheben ist auch, dass das Erlangen des Gütesiegels für Unternehmen den Vorteil bringen soll, dass nach Artikel 79 Abs 2b des Entwurfes für eine DSGVO nur dann eine Geldbuße über ein Unternehmen zu verhängen ist, wenn der Verstoß bei Vorsatz oder Fahrlässigkeit des Unternehmens geschehen ist, was eine erhebliche Risikominimierung bedeutet.

Datenschutz-Gütesiegel sollen von den nationalen Datenschutzbehörden bzw durch von diesen akkreditierte externe Prüfern verliehen werden (siehe Art 39 des Entwurfes). Für die Erlangung solcher Gütesiegel, die für die Zertifizierung von Dienstleistungen und Produkten, die mit der Verwendung personenbezogener Daten einhergehen, verfügbar sind und die Einhaltung des europäischen Datenschutzrechts attestieren, ist es erforderlich, (unabhängige) Datenschutzexperten aus den Bereichen „Technik" und „Recht" mit der Evaluierung der Einhaltung des Datenschutzrechts in einem Unternehmen bzw der Beachtung von datenschutzrechtlichen Grundsätzen von IT-Systemen zu beauftragen. Deren Prüfbericht muss von der Zertifizierungsstelle bestätigt werden, die sodann das Gütesiegel verleiht. Klar ist aber, dass das Gütesiegel nur dann ein Grund für das Absehen von der Geldbuße sein kann, wenn auch die Anforderungen an das Aufrechtbleiben der Zertifizierung (durch Durchführung der vorgeschriebenen Audits, etc) eingehalten werden.

4. Vorbereitung auf die DSGVO aus Sicht der unternehmerischen Compliance

In Anbetracht des Ziels der EU, die DSGVO bis Ende 2014 politisch auszuverhandeln und zwei Jahre später, also Ende 2016, in Kraft zu setzen, hat die Uhr für die Vorbereitung auf die DSGVO bereits laut zu ticken begonnen: erfahrungsgemäß ist der Aufbau einer gut funktionierenden Datenschutz-Compliance in einem Unternehmen ein Prozess, der sich bis über mehrere Jahre hinziehen kann. Kernelement der Vorbereitung auf die DSGVO sollten aus heutiger Sicht ua folgende sein:[5]

- Aufbau einer Datenschutzstruktur im Unternehmen/Konzern durch Benennung und Ausbildung von Datenschutzbeauftragten und Aufbau von Datenschutzrechtswissen in der Rechtsabteilung.
- Schaffung eines Überblicks über die im Unternehmen betriebenen Datenanwendungen (welche Arten von Daten werden zu welchem Zweck von wem im Unternehmen verwendet und wer hat auf die Daten intern/konzernintern/extern Zugriff? Welche Dienstleister sind intern/konzernintern/extern im Einsatz?
- Abarbeitung des derzeit geltenden materiellen und formellen Datenschutzrechts, um einen Compliance-Ist-Stand herzustellen, auf dem weiter aufgebaut werden kann (materiell: ua Einhaltung der Grundprinzipien des § 6 DSG 2000 wie das Wesentlichkeitsprinzip, das Zweckbindungsprinzip, das Prinzip der Datenlöschung; Prüfung der Rechtsgrundlage der Verarbeitung nach §§ 7 ff DSG 2000 inklusive Einholung korrekt formulierter Zustimmungserklärungen zur Datenverarbeitung nach §§ 8 und 9 DSG 2000; formell: Meldung beim Datenverarbeitungsregister,[6] wenn Meldepflicht vorliegt; Einholung der allenfalls erforderlichen Genehmigungen für den internationalen Datenverkehr nach § 13 DSG 2000; Abschluss von datenschutzrechtlichen Dienstleisterverträgen mit den Dienstleistern nach §§ 10 und 11 DSG 2000).
- Schulung der Belegschaft im Datenschutzrecht und in der Datensicherheit (je nach Tätigkeitsbereich inhaltlich angepasst und intensiv durch Seminarbesuche, interne persönliche Schulungen, e-Learning-Tools etc).

- Erarbeitung und Aktualisierung von Policies zur Datenverwendung, Datensicherheit und Verwendung der IT durch die Mitarbeiter.
- Regelmäßige interne Datenschutz-Compliance-Audits, um den Compliance-Status zu ermitteln und dafür zu sorgen, dass ein einmal erreichtes Compliance-Niveau gehalten wird.
- Erlangung eines Datenschutz-Gütesiegels für das Unternehmen oder einzelne Datenanwendungen des Unternehmens. Ein solches kann das Unternehmen weitgehend vor der Verhängung von Sanktionen bewahren.
- Erarbeitung eines ausführlichen und detaillierten „Data-Breach-Konzepts", um auf den Ernstfall eines Datenmissbrauches (§ 24 Abs 2a DSG 2000) vorbereitet zu sein.
- Absicherung der Wahrung der Betroffenenrechte (Auskunfts-, Richtigstellungs- und Löschpflichten – §§ 27 ff DSG 2000 – etwa durch Schulung der Mitarbeiter, Erarbeitung eines Ablaufkonzepts, Erstellung von Antwortmustern).
- Sicherstellung der Einhaltung der organisatorischen und technischen Datensicherheitsmaßnahmen und ihrer Dokumentation in einem Datenschutzhandbuch (§ 14 DSG 2000).
- Arbeitsverfassungsrechtlich ist überdies auf die Pflicht zum Abschluss von Betriebsvereinbarungen bei bestimmten Datenverarbeitungsvorhaben (siehe §§ 96 und 96a ArbVG) hinzuweisen, die aus heutiger Sicht unberührt bleiben wird, da Art 82 DSGVO eine generelle Ausnahme im Hinblick auf das Arbeitsrecht vorsieht (Entwurf der Kommission) und diesen Rechtsbereich weiterhin den nationalen Gesetzgebern überlassen möchte (nach Beschluss des Parlaments allerdings in einem vordefinierten Basis-Rechtsrahmen). Das Vorliegen der notwendigen Betriebsvereinbarungen (oder Zustimmungen der einzelnen Mitarbeiter nach § 10 AVRAG bei Nichtbestehen eines Betriebsrates) sollte daher geprüft und Fehlendes nachgeholt werden.

5. Compliance bei künftigen Projekten unter der DSGVO

Spätestens ab Inkrafttreten der DSGVO, aber insbesondere bei langfristigen und kritischen neuen Projekten sollte schon heute jedenfalls auf folgende Prinzipien geachtet werden:

- Grundprinzipien des Datenschutzrechts wie Zweckbindungsprinzip; Wesentlichkeitsprinzip; „Datensparsamkeit" und Datenlöschung;
- Privacy by Design and by Default – das eingesetzte Hard- oder Softwareprodukt sollte datenschutzfreundlich konzipiert sein und datenschutzfreundliche Grundeinstellungen vorsehen; Durchführung von Datenschutz-Folgeabschätzungen (Privacy Impact Assessment), die bei der Einführung bestimmter Systeme ohnehin verpflichtend vorgesehen wird;
- Prüfung der Einhaltung der technischen und organisatorischen Datensicherheitsmaßnahmen (auch bei Dienstleistern – die Praxis zeigt, dass oft nur einige wenige Mitarbeiter und die „Peripherie" des Unternehmens (externe Dienstleister) das Problem sind, nicht die Sicherheit der zentralen Server im Unternehmen);
- Abschluss der notwendigen Betriebsvereinbarungen.

6. Fazit

Auch wenn der Entwurf der DSGVO noch in Verhandlung steht, zeichnen sich die Eckpfeiler der kommenden Verordnung schon deutlich ab. Unternehmen sollten daher bereits heute beginnen, sich mit der Umsetzung der künftigen DSGVO zu befassen. Sie sollten ein Maßnahmenpaket überlegen und einen Zeitplan erstellen, um für die neuen Anforderungen auf dem Gebiet der Datenschutz-Compliance gewappnet zu sein und die Zahlung künftiger hoher Geldstrafen zu vermeiden. Mit dem Setzen „vorbeugender Maßnahmen" sollte jedenfalls besser früher als später begonnen werden. Die Praxis zeigt, dass die Umsetzung solcher Maßnahmen und die Herstellung der Compliance – von der unternehmensinternen Evaluierung der einzelnen Datenanwendungen und der Datenflüsse bis hin zur Registrierung der Anwendungen und Genehmigung von internationalen Datentransfers – gut ein bis zwei Jahre, manchmal auch länger in Anspruch nehmen kann.

---

1) http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A52012PC0010.
2) http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf.
3) http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=DE&ring=A7-2013-0402.
4) In Österreich liegt die Maximalstrafe nach § 52 DSG 2000 dzt bei Euro 25.000,00.
5) Siehe zu diesen Kernelementen näher in *Knyrim*, Praxishandbuch Datenschutzrecht², insbes 303ff.
6) Der Meldestand des eigenen oder jedes meldepflichtigen fremden öst Unternehmens kann anonym und kostenlos sehr einfach im Internet im Online-Datenverarbeitungsregister unter https://dvr.dsb.gv.at abgefragt werden.

Foto Preslmayr

Die Autoren

RA Dr. Rainer Knyrim (links im Bild) ist Partner bei Preslmayr Rechtsanwälte. Er ist Autor des „Praxishandbuch Datenschutzrecht" und Mitherausgeber des größten österreichischen Datenschutz-Kommentars. Dr. Knyrim ist Mitglied der „Task Force on Privacy and the Protection of Personal Data" der Internationalen Handelskammer (ICC) Paris sowie wissenschaftlicher Beirat der Zeitschrift jusIT und Mitglied des Programmkomitees des Österreichischen IT-Rechtstages.

RA Dr. Gerald Trieb (rechts im Bild) ist Partner bei Preslmayr Rechtsanwälte. Er ist vorwiegend im Datenschutz- und Datensicherheitsrecht tätig. Weitere Tätigkeitsschwerpunkte liegen im Bankrecht, Insolvenzrecht und Unternehmenssanierungen, Verwaltungsrecht und Verfassungsrecht sowie Zivilprozessrecht und Schiedsgerichtsverfahren.

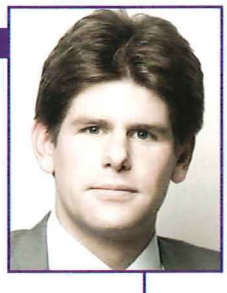

Foto Preslmayr