

DATENSCHUTZ

KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

E-Mail, Internet und Marketing

Auf dem Weg zur europäischen Cloud?

Interview mit Helmut Fallmann, Vorstand Fabasoft

Praxisprojekt: IT- und Datenschutz-Policies

Rainer Knyrim, Markus Oman

Kontrolle Internet/E-Mail am Arbeitsplatz

Wolfgang Goricnik

Checkliste E-Mail-Marketing

Hans-Jürgen Pollirer

Judikaturrückblick: Zustimmung und Werbung

Viktoria Haidinger

Rechtswidrige Weitergabe von Daten

Ernst M. Weiss



Rainer Knyrim

Rechtsanwalt und Partner bei Preslmayr Rechtsanwälte OG

Die neuen Pflichten nach der EU-Datenschutz-Grundverordnung im Überblick

Das künftige EU-Datenschutzrecht – Teil 5. Die am 15. 12. 2015 erfolgte politische Einigung zwischen Europäischem Parlament, Rat und Kommission bringt ein neues, direkt anwendbares Datenschutzrecht in ganz Europa. Es baut inhaltlich auf der Datenschutz-RL auf, führt aber teilweise weg von der bisherigen „papierlastigen“ Ausgestaltung bei der Umsetzung hin zu einer Datenschutz-Compliance, die eine intensive Befassung mit technischem und organisatorischem Datenschutz erfordern wird. Den Unternehmen bringt die DSGVO die von ihnen gewünschte Eigenverantwortlichkeit. Verstärkte Eigenverantwortung bedeutet aber nicht, dass man sich mit Datenschutz weniger befassen muss! Das Gegenteil ist der Fall: Unternehmen – wie auch die von der DSGVO genauso adressierten öffentlichen Auftraggeber – treffen zahlreiche neue Pflichten, die sie selbstständig in ihren Organisationen umsetzen müssen. Sollte dies nicht geschehen, wird durch exorbitant hohe Strafen vorgesorgt, dass die neuen Pflichten ernst genommen werden. Der **Strafrahmen beträgt 20 Mio Euro** für öffentliche Einrichtungen¹ und Unternehmen. Bei Unternehmen kann dieser Strafrahmen überschritten werden, es gilt ein Strafrahmen von maximal **4% des globalen Konzernumsatzes**.

Erweiterte und neue Betroffenenrechte

Die Betroffenenrechte werden durch die DSGVO deutlich erweitert und umgestaltet. So gibt es **deutlich aufwendigere Informationspflichten** bei der Datenerhebung, beim Erhalt oder dem Weiterleiten von Daten gegenüber den Betroffenen. Ebenso wurden die bekannten **Betroffenenrechte auf Auskunft, Richtigstellung und Löschung erweitert**, so ist zB die Speicherdauer künftig zu beauskunften und die Betroffenenrechte werden binnen eines Monats umzusetzen sein. Aufwendig wird auch das sog „**Recht auf Vergessen**“, ebenso die neue Verpflichtung, all jene, denen Daten weiterübermittelt wurden, über eine Richtigstellung, Löschung oder Einschränkung der Datenverarbeitung zu informieren.

Investitionen, insb technischerseits zur Schnittstellenprogrammierung, wird das vollkommen neue **Recht auf „Datenportabilität“** mit sich bringen. Dieses ermöglicht dem Betroffenen, seine Daten vom Auftraggeber zu verlangen. Die Daten müssen dabei vom Auftraggeber in einer strukturierten Form und in einem üblichen maschinenlesbaren Format zur Verfügung gestellt werden und der Betroffene kann, soweit technisch möglich, sogar verlangen, dass der Auftraggeber diese **Daten direkt(!) von einem Auftraggeber an einen anderen Auftraggeber überträgt**.

Verpflichtung zu Datenschutz durch Technik

Die neue Verpflichtung zu **Datenschutz durch Technik** besteht sowohl im Zeitpunkt, in dem die Mittel für die Datenverarbeitung festgelegt werden, als auch während der Datenverwendung selbst und kann durch technische und organisatorische Maßnahmen (zB Pseudonymisierung und Umsetzung der Datenschutzprinzipien wie etwa Datenminimierung und Einbau von Datensicherheitsmaßnahmen) umgesetzt werden.

HINWEIS

Eine ebenfalls neue Verpflichtung zu **datenschutzfreundlichen Voreinstellungen besteht unabhängig von den Implementierungskosten**. Der Auftraggeber ist verpflichtet, durch entsprechende technische und organisatorische Maßnahmen sicherzustellen, dass nur so viele Daten, wie für die **Zweckerreichung erforderlich sind, verarbeitet werden**.

Gemeinsame Auftraggeber

Dort, wo **zwei oder mehr Auftraggeber** gemeinsam die Zwecke und Mittel der Datenverarbeitung festlegen, gelten diese als **gemeinsame Auftraggeber** („joint controllers“). Diese sind künftig verpflichtet, in einer transparenten Art und Weise die

Umstände ihrer Zusammenarbeit, insb hinsichtlich der Rechte der Betroffenen und ihrer diesbezüglichen Informationspflichten, in einer vertraglichen Festlegung zwischen ihnen zu bestimmen.

Fehlende Dienstleisterverträge werden „teuer“

Wie schon die bisherige RL und das österr DSG enthält auch die DSGVO selbstverständlich **Regelungen über die Zusammenarbeit mit Dienstleistern**. Auch künftig muss zwischen dem Auftraggeber und dem Dienstleister ein **Dienstleistervertrag** abgeschlossen werden, mit einem Mindestinhalt, den die DSGVO vorgibt.

PRAXISTIPP

Auftraggeber sollten daher ein genaues Dienstleister-Vertragsmanagement betreiben, da die Nichteinhaltung der Dienstleisterregeln mit 10 Mio Euro oder 2% des konzernweiten Jahresumsatzes sanktioniert ist, im Vergleich zu € 10.000,- bisher im österr DSG.

¹ Sofern das nationale Recht der MS dies vorsieht. Die übrigen Zwangskompetenzen der Datenschutzbehörde wie Untersuchung oder Löschung treffen die öffentlichen Unternehmen aber jedenfalls.

Verfahrensverzeichnis statt Datenverarbeitungsregister – dieselbe Aufgabe in neuem Format

Statt dem Datenverarbeitungsregister führt die DSGVO das in Deutschland schon lange bestehende sog. „Verfahrensverzeichnis“ ein. Auftraggeber sind künftig verpflichtet, eine Übersicht über ihre Datenanwendungen zu führen; wobei dieses Verfahrensverzeichnis die eigenen Kontaktdaten wie Zwecke der Datenanwendungen, eine Beschreibung der in der Datenanwendung enthaltenen Datenkategorien, der Empfängerkategorien, weiters separat ausgewiesen Datentransfers in Drittstaaten und, soweit möglich, die geplante Speicherdauer sowie eine Allgemeinbeschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen enthalten muss. Abgesehen von der Speicherdauer entspricht das Verfahrensverzeichnis damit dem Inhalt der bisherigen DVR-Meldungen.

HINWEIS

Völlig neu ist allerdings, dass die Verpflichtung zum Führen eines Verfahrensverzeichnisses nun nicht nur Auftraggeber, sondern auch Dienstleister trifft.

Die Verpflichtung zur Führung des Verfahrensverzeichnisses trifft Unternehmen mit weniger als 250 Angestellten nur dann, wenn

- die Datenverarbeitung ein **hohes Risiko** für die Rechte und Freiheiten der Betroffenen bedeutet und die Datenverarbeitung **nicht nur gelegentlich erfolgt** oder
- wenn **sensible Daten** oder Daten über **strafrechtlich relevantes Verhalten** verarbeitet werden.

Datenmissbrauch als zeitliche Herausforderung

Mit der DSGVO wird die im DSG 2000 schon bekannte Verpflichtung zur **Informationspflicht bei Datenmissbrauch** europaweit eingeführt. Tritt ein Datenmissbrauchsfall ein, dann muss der Auftraggeber **unverzüglich**, und so weit möglich, **innerhalb von 72 Stunden** nach Kenntnis die zuständige **Datenschutzbehörde darüber informieren**, außer der Vorfall wird voraussichtlich kein Risiko für die Rechte und Freiheiten der Betroffenen herbeiführen. Schafft der Auftraggeber dies nicht innerhalb von 72 Stunden (man stelle sich das

Bekanntwerden eines solchen Vorfalls am Freitagnachmittag vor – dieser müsste bereits am Montagnachmittag der Behörde gemeldet werden), dann muss der Auftraggeber seine verspätete Meldung mit einer Begründung für die Verzögerung an die Datenschutzbehörde schicken. Bislang ist in Österreich nach dem DSG 2000 überhaupt keine Verständigung der Datenschutzbehörde vorgesehen.

Wenn der Datenmissbrauch ein hohes Risiko für die Betroffenen bewirken kann, ist der Auftraggeber verpflichtet, die **Betroffenen unverzüglich zu verständigen**.

PRAXISTIPP

Es sollte daher ein Maßnahmenkatalog umgesetzt werden, um das Unternehmen oder die öffentliche Einrichtung auf diesen Ernstfall vorzubereiten.

Völlig neu: Datenschutz-Folgenabschätzung

Die DSGVO führt eine völlig neue Verpflichtung zur Abschätzung der möglichen Folgen einer Datenverarbeitung ein, die „Datenschutz-Folgenabschätzung“ („Data Protection Impact Assessment“, kurz „DPIA“). Bei Datenverarbeitungen, insb wenn sie mit neuen Technologien arbeiten und im Hinblick auf ihre Art, Anwendungsbereich, Kontext und Zwecke möglicherweise ein hohes Risiko für die Privatsphäre der Betroffenen beinhalten, ist eine Abschätzung der Folgen durchzuführen.

Die Verpflichtung zielt hier nicht auf die Unternehmensgröße ab (dh es gibt **keine Ausnahmen für KMU**), sondern auf den Inhalt der Verarbeitung. Ein DPIA ist **va im Fall einer systematischen und extensiven Auswertung von persönlichen Aspekten**, insb durch **Profiling**, welche rechtliche Konsequenzen für die Betroffenen haben kann, durchzuführen; weiters ua bei einer **Verarbeitung von sensiblen Daten** oder der Verarbeitung von **strafrechtlich relevanten Daten** im großen Umfang.

HINWEIS

Das Ergebnis des DPIA kann die Konsultation der Datenschutzbehörde erforderlich machen.

Der Datenschutzbeauftragte ist da!

Durch die DSGVO wird nun ein **verpflichtender Datenschutzbeauftragter** einge-

führt, wobei sich die Pflicht am **Inhalt der Datenverarbeitung** des Unternehmens oder der öffentlichen Einrichtung **orientiert**.

Ein Datenschutzbeauftragter ist künftig verpflichtend dann zu bestellen, wenn

- die Datenverarbeitung durch eine **öffentliche Einrichtung** erfolgt oder
- die **Kerntätigkeit des Auftraggebers oder Dienstleisters** in Datenverarbeitung besteht, die aufgrund ihres Wesens, ihres Umfangs oder Zwecks eine **regelmäßige und systematische Beobachtung von Betroffenen in großem Umfang** erfordert, oder
- die **Kernaktivität des Auftraggebers oder Dienstleisters** in der Verarbeitung von sensiblen Daten oder strafrechtlich relevanten Daten in großem Umfang besteht.

Die Pflicht zur Bestellung eines Datenschutzbeauftragten trifft sowohl Auftraggeber als auch Dienstleister.

Der Datenschutzbeauftragte muss auf Basis seiner **beruflichen Qualität** und insb seines **Fachwissens im Datenschutzrecht und der Datenschutzpraxis** bestellt werden.

Internationaler Datenverkehr – komplex wie bisher

Die Regelungen für den internationalen Datenverkehr werden inhaltlich etwas erweitert und formal erleichtert. Das Grundprinzip, dass ein **Datentransfer in Drittstaaten** außerhalb der EU **grundsätzlich verboten** ist, soweit nicht eines der Datentransferinstrumente greift, bleibt.

Angemessenes Drittland: Wie bisher kann die EU-Kommission aber feststellen, dass ein **Drittstaat ein adäquates Datenschutzniveau hat** und danach ist ein Transfer ohne weitere Autorisierung möglich. **Standardvertragsklauseln**, die von der EU-Kommission erlassen werden, sowie (neu) Standardvertragsklauseln, die von der nationalen Datenschutzbehörde genehmigt und von der Europäischen Kommission akzeptiert wurden, können als Basis für einen Datentransfer dienen. „**Verbindliche Unternehmensvorschriften**“ (Binding Corporate Rules) für den Datentransfer sowie (neu) einmal genehmigte **Verhaltensregeln (Code of Conduct)** und (neu)

einmal genehmigte **Zertifizierungsmechanismen** können ebenfalls als Basis für einen Transfer ohne weiterer Autorisierung der nationalen Datenschutzbehörde dienen.

Bereits von nationalen Datenschutzbehörden erteilte Genehmigungen für den Datentransfer bleiben gültig.

Die DSGVO hält ausdrücklich fest, dass **bereits von nationalen Datenschutzbehörden erteilte Genehmigungen für den Datentransfer gültig bleiben**, soweit sie nicht geändert, ersetzt oder von der Behörde widerrufen werden. Somit bleiben sämtliche, von der österr. Datenschutzbehörde genehmigte Datentransfers auch künftig gültig und es besteht daher die **Möglichkeit, auch hier bereits aktiv Vorarbeit für 2018 zu leisten.**

Extremer Strafraumen als Daumenschrauben für die Unternehmen

Die Strafen sind künftig in zwei Stufen eingeteilt,

- einerseits bis 10 Mio Euro oder 2% des konzernweiten Umsatzes,
- andererseits bis 20 Mio Euro oder 4% des konzernweiten Umsatzes.

Mit dem **hohen Strafraumen** sind va die **Datenschutz-Grundprinzipien** wie Einhaltung des Zweckbindungsprinzips, des Datenminimierungsprinzips, das Prinzip der Begrenzung der Speicherdauer abgesi-

chert, was bedeutet, dass **grundsätzlich jeder Datenverarbeitungsvorgang auf Konformität mit diesen Grundprinzipien geprüft werden muss**, um nicht dem Risiko der hohen Strafe ausgesetzt zu sein. Weiters sind die **Betroffenenrechte** wie Recht auf Auskunft, Löschung, Richtigstellung, Datenportabilität und Recht auf Vergessen durch den hohen Strafraumen abgesichert sowie der **Datentransfer in Drittländer.**

HINWEIS

Neben den Verwaltungsstrafen sieht die DSGVO auch ein Beschwerderecht bei der Datenschutzbehörde sowie Klagerechte und Schadenersatzrechte für materielle und immaterielle Schäden vor.

Zum Thema

Über den Autor

Dr. Rainer Knyrim ist Rechtsanwalt und Partner bei Preslmayr Rechtsanwälte in Wien.
Tel: +43 (0)1 533 16 95, E-Mail: knyrim@preslmayr.at, Internet: www.preslmayr.at

Hinweis

Dieser Beitrag ist der 5. Teil der Serie zum künftigen EU-Datenschutzrecht. Bisher erschienen sind:

- Knyrim, Die Datenschutz-Grundverordnung: Entwicklung und Anwendungsbereich, Dako 2015/21;
- Pollirer, Die Datenschutz-Grundverordnung: Der Datenschutzbeauftragte, Dako 2015/37;
- Pollirer, Die Datenschutz-Grundverordnung: Die Datenschutz-Folgenabschätzung, Dako 2015/47;
- Wagner, Die Datenschutz-Grundverordnung: Die Betroffenenrechte, Dako 2015/59.

Die Serie wird im nächsten Heft fortgesetzt mit einem Beitrag von *Leissler/Wolfbauer*, Das One-Stop-Shop-Prinzip.

Inkrafttreten 2018

Die DSGVO tritt am 20. Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft, ist aber erst zwei Jahre nach diesem Datum anwendbar. Es wird damit gerechnet, dass die Beschlussfassung über die DSGVO im Europäischen Parlament und Europäischen Rat noch bis in das Frühjahr 2016 dauert, womit die DSGVO inklusive ihrer Strafen **im Frühling 2018 anwendbar** sein wird.

Bis dahin wird ein **straffer Zeitplan für öffentliche und private Auftraggeber sowie Dienstleister notwendig** sein, um fit für die DSGVO zu werden, denn es ist **keine Gnadenfrist** für den Eintritt der Strafen über 2018 hinaus vorgesehen.

Dako 2016/6