Datenschutzrecht: Schluss mit der Bürokratie

Ein Ovum-Bericht im Auftrag von Intralinks

ovum

INTRA LINKS™

ovum

Inhalt

Zusammenfassung 1

Einleitung 2
Compliance-Herausforderungen für Unternehmen 4
Cloud-Lösungen sind weiter auf dem Vormarsch 4
Unternehmen fehlen die Grundlagen zum Schutz vertraulicher Inhalte 5
Datenschutzbestimmungen sind uneinheitlich, sodass Unternehmen rund um den Globus anfällig für Verstöße sind 6
Geplante EU-Datenschutzrichtlinien werden Maßstäbe für den internationalen Datenschutz setzen, können aber zum Hemmschuh für die EU-Wirtschaft werden 7
Der Speicherort von Daten ist das wichtigste Kontrollkriterium, aber schwer zu definieren 8
Vorschriften verursachen hohe Kosten 9
Unternehmen mit Sitz in den USA stehen unter Drck 9

Empfehlungen 10

Anhang 11
Methodik 11
Autor 11
Ovum Consulting 11
Copyright und Haftungsausschluss 11

INTRA LINKS

Zusammenfassung

Neue internationale Datenschutzbestimmungen stellen ernstzunehmende Risiken für Unternehmen und die Wirtschaft dar.

Verschiedene Landesregierungen erlassen neue, strenge Datenschutzrichtlinien, um die Daten ihrer Bürger zu schützen, nationalstaatliche Sicherheitsinteressen zu wahren und die heimische Industrie anzukurbeln. Der zunehmend komplexe Schutz vertraulicher Inhalte und personenbezogener Daten wird zum Hemmschuh für gängige Strategien, Verfahren und Prozesse internationaler Unternehmen. Intralinks hat im dritten Quartal 2015 eine internationale Umfrage unter 366 IT-Entscheidungsträgern bei Ovum in Auftrag gegeben, um die Auswirkungen der Datenhoheit und Datenschutzbestimmungen zu untersuchen.

Die wichtigsten Erkenntnisse:

Datenschutzbestimmungen stehen in direktem Konflikt mit der geschäftlichen Nutzung von Cloud-Diensten, Software-as-a-Service (SaaS) und mobilen Geräten.

Cloud-Computing ist mittlerweile aus der Unternehmens-IT nicht mehr wegzudenken. Es ist davon auszugehen, dass dieser Trend in den nächsten zehn Jahren weiter steigen wird. Unternehmen mit einem hohen Informationsaufkommen setzen auf SaaS. Kombiniert mit einer Umstellung auf mobile Plattformen erschwert dies die Kontrolle über den Datenstandort und die Einhaltung von Datenschutzbestimmungen. Dennoch planen 78 % der Befragten, in den kommenden drei Jahren cloud- und SaaS-basierte Anwendungen für die Speicherung und den Austausch vertraulicher und regulierter Inhalte zu nutzen.

Führungskräfte sehen den möglichen Konsequenzen der neuen Datenschutzbestimmungen sehr pessimistisch entgegen.

Unsere Umfrage ergab, dass Unternehmen um das Problem Datenschutzrecht wissen, aber unsicher sind, welche Maßnahmen sie diesbezüglich ergreifen sollen. In Bezug auf die geplante europäische Datenschutz-Grundverordnung gaben 52 % der Befragten an, dass sie mit Geldstrafen für ihr Unternehmen rechnen. Zwei Drittel gehen davon aus, dass ihre Geschäftsstrategie in Europa angepasst werden muss.

Die Kosten für die Einhaltung gesetzlicher Auflagen sind extrem hoch, die Kosten für Compliance-Verstöße sind aber weitaus höher.

Mehr als 70 % der Befragten erwarten höhere Ausgaben, um die Anforderungen rund um das Thema Datenhoheit erfüllen zu können. Über 30 % rechnen damit, dass Budgets in den kommenden zwei Jahren um mehr als 10 % steigen. Von den Unternehmen, die ihre Datenschutzstrategie in den nächsten drei Jahren aktualisieren möchten, wollen 38 % entsprechende Experten beauftragen, 27 % möchten einen Chief Privacy Officer (CPO) einstellen.

Unternehmen mit Sitz in den USA sind besonders gefährdet.

Es gibt ihn wirklich, den Snowden-Effekt. Von 20 Industrienationen wird den USA das wenigste Vertrauen entgegengebracht. Die Befragten schätzen, dass dort die Wahrscheinlichkeit unerlaubter Zugriffe auf vertrauliche Inhalte am größten ist – dicht gefolgt von China und Russland. Durch die neuen Gesetze ergeben sich für US-Unternehmen mehr Nachteile. 63 % der Befragten glauben, dass die geplante europäische Datenschutz-Grundverordnung US-Unternehmen den Wettbewerb erschweren wird. 70 % sind der Ansicht, dass die neue Gesetzgebung in Europa ansässige Unternehmen begünstigt.

Der Großteil der Unternehmen nutzt Datenschutztechnologien nicht effizient genug.

Viele Unternehmen nutzen keine der verfügbaren Technologien zum Schutz vertraulicher Inhalte. Nur 44 % der Befragten überwachen die Aktivitäten ihrer Anwender und nutzen automatische Benachrichtigungen für Richtlinienverstöße. Lediglich 53 % klassifizieren Informationen gemäß entsprechender Zugangskontrollen. Etwa die Hälfte (47 %) der Befragten verfügt weder über Richtlinien noch über Kontrollen bezüglich der Nutzung cloud-basierter Consumer-Tools für File-Sharing, wie z. B. Dropbox.

International tätige Unternehmen benötigen eine gezielte Strategie für das Thema Datenhoheit, die für Menschen, Prozesse und Technologien gleichermaßen gilt.

Führungskräfte haben erkannt, dass ein ausgewogenes Konzept für Datenhoheit und Datenschutz erforderlich ist. 55 % der zu Investitionsstrategien befragten Unternehmen gaben an, dass sie neue Schulungen für Mitarbeiter planen. 51 % möchten ihre Richtlinien anpassen, und 53 % wollen neuen Technologien einführen.

Unternehmen müssen zahlreiche internationale Datenschutzrichtlinien einhalten, die sich widersprechen. Sie benötigen Technologien, die alle Eventualitäten abdecken.

Durch die neuen Entwicklungen in puncto Datenhoheit droht eine „Balkanisierung“ der Technologielandschaft, in der verschiedene, inkonsistente und oftmals inkompatible Vorschriften für die Speicherung, Verarbeitung und gemeinsame Nutzung von personenbezogenen Daten vorherrschen. Das ist nicht nur unübersichtlich, sondern sorgt auch für Verunsicherung. Wichtige Fragen bleiben unbeantwortet, z. B. die Auslegung der Anforderungen an Datenstandorte. Unternehmen benötigen Technologien, mit denen sie schnell auf neue Richtlinien und Vorschriften reagieren können.

Einleitung

Der Datenschutz war bereits vor den Enthüllungen von Edward Snowden zur elektronischen Überwachung durch die NSA ein Thema auf internationalem Parkett. Durch Regierungsspionage und massive Datenlecks mussten Landesregierungen in den letzten Jahren erkennen, dass das aktuelle Datenschutzrecht im digitalen Zeitalter nicht mehr zeitgemäß ist und entsprechend angepasst werden muss. In der Folge gab es so viele neue Gesetze wie nie zuvor, die vorschreiben, wie bestimmte vertrauliche Inhalte erfasst, gespeichert, verarbeitet und ausgetauscht werden dürfen.

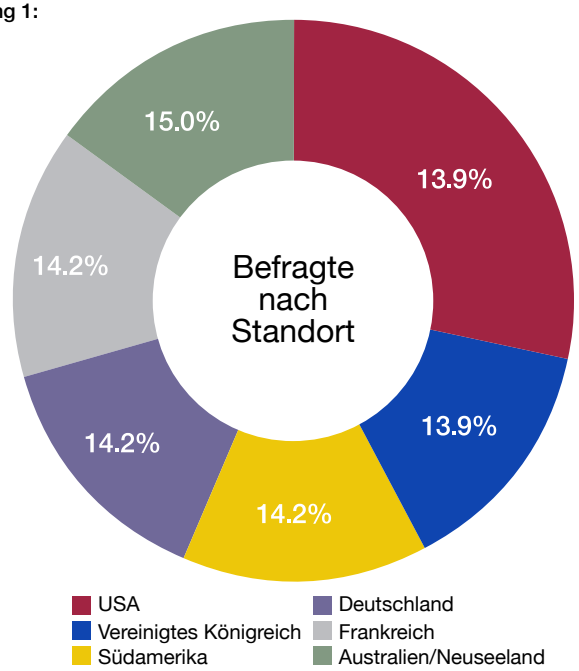
Die Regelungen in Ländern wie Brasilien, Singapur und Russland werden immer strenger. Die EU hat die langwierige Prüfung der diesbezüglichen Gesetzgebung fast abgeschlossen. Davon betroffen sind alle Unternehmen der Mitgliedsstaaten. Die neuen Vorschriften sind notwendig, da Unternehmen grenzüberschreitend und zunehmend mobil arbeiten und auf cloud-basierte IT-Systeme umsteigen. Die neuen Compliance-Anforderungen werden immer komplexer – insbesondere für Unternehmen, die in verschiedenen Rechtsprechungen tätig sind. Hier muss die Frage gestellt werden, wie Gesetze und Vorschriften für Daten gelten, die in Cloud-Anwendungen vorgehalten werden.

Intralinks, ein führender Anbieter von cloud-basierten Lösungen für die unternehmensweite Nutzung von Inhalten, hat im dritten Quartal 2015 eine internationale Umfrage bei Ovum in Auftrag gegeben, um die Auswirkungen der Datenschutzbestimmungen auf weltweit tätige Unternehmen zu untersuchen. Dabei wurden folgende Fragen gestellt:

- Wie stellen sich Unternehmen zum Thema Datenhoheit auf?
- Welche Auswirkungen haben die neuen Datenschutzbestimmungen?
- Welche Anpassungen nehmen Unternehmen im Zuge der neuen Datenschutzverpflichtungen vor?
- Wie unterscheiden sich die Meinungen in verschiedenen Ländern und Rechtsprechungen?
- Welche technologischen Entscheidungen werden im Zuge der Datenschutzbestimmungen getroffen?
- Welche Best Practices gibt es, um sich an neue gesetzliche Vorgaben anzupassen?

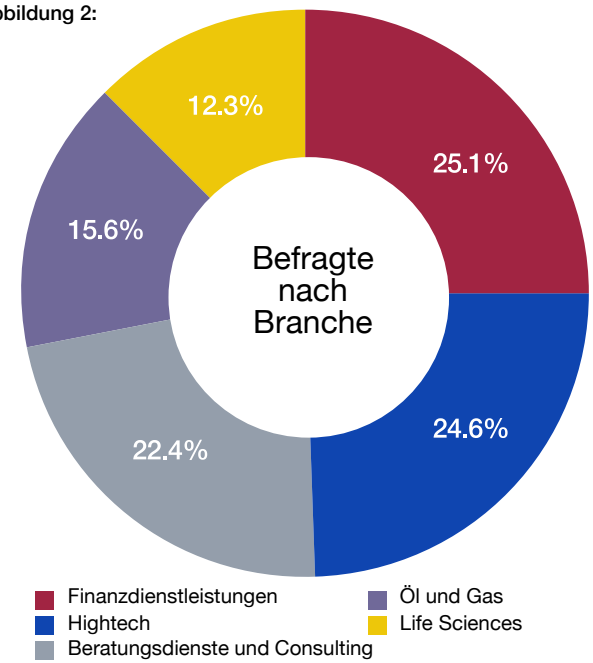
Ovum hat 366 international tätige Unternehmen verschiedener Größen und Branchen befragt (siehe Abbildungen 1, 2 und 3). Diese Demografie wurde bewusst ausgewählt, um verschiedene Unternehmensarten und Standorte berücksichtigen zu können, die von Datenhoheitsverpflichtungen und Datenschutzbestimmungen betroffen sind.

Abbildung 1:



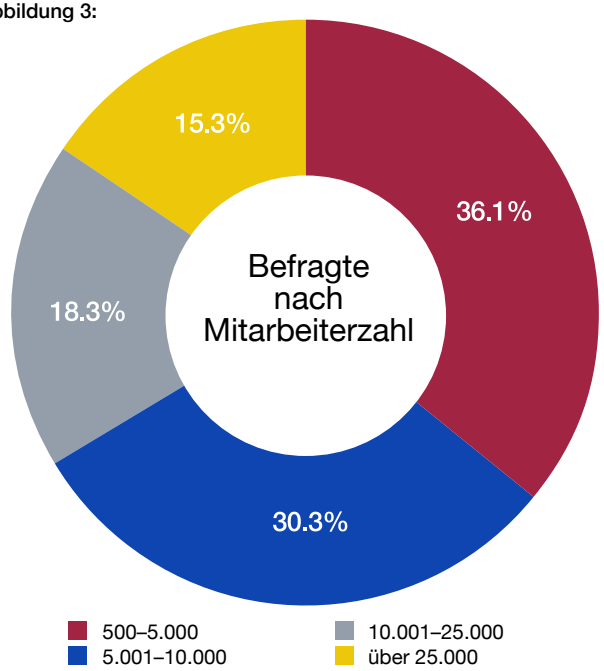
Quelle: Ovum

Abbildung 2:



Quelle: Ovum

Abbildung 3:



Quelle: Ovum

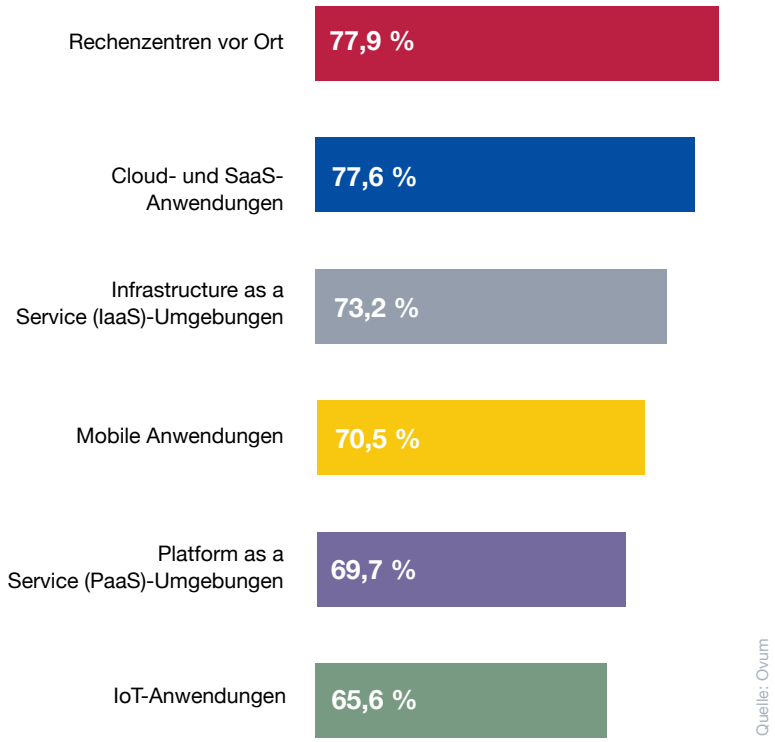
Compliance-Herausforderungen für Unternehmen

Cloud-Lösungen sind weiter auf dem Vormarsch.

Sie steigern die Produktivität in modernen Unternehmen und verbinden alle Mitarbeiter, ermöglichen Geschäftsbeziehungen zu anderen Unternehmen, Partnern und Kunden und verbinden uns auch auf sozialer Ebene. Wir kommunizieren und übermitteln Informationen heute grundlegend anders. Das führt auch in etablierten Unternehmen und bei der Handhabung von IT-Budgets zu Veränderungen. Eine kürzlich von Ovum durchgeführte Umfrage ergab, dass ein Sechstel des gesamten IT-Budgets von Unternehmen im Regelfall auf SaaS entfällt und die Ausgaben für cloud-basierte Lösungen sehr wahrscheinlich steigen werden. Etwa vier Fünftel der Unternehmen nutzen oder planen die Nutzung cloud-basierter Lösungen (private, öffentliche und Hybrid-Modelle) und Services (IaaS, PaaS, SaaS). Anfang 2014 waren es noch zwei Drittel. Der Markt wächst mit der neuen Anwendergeneration. Die zweite Welle hat ihren Höhepunkt erreicht, und eine dritte Welle von Nachzüglern ist im Kommen.

Die Umfrage zum Thema Datenhoheit liefert neue Erkenntnisse darüber, wie viele Unternehmen mittlerweile auf Cloud-Anwendungen setzen, um regulierte und vertrauliche Inhalte vorzuhalten. Das steht im deutlichen Gegensatz zur Situation vor ein paar Jahren, als man sich fragte, ob die Cloud überhaupt vertrauenswürdig sei. Heute geht man davon aus, dass dort gespeicherte, vertrauliche Inhalte zuverlässig geschützt werden (siehe Abbildung 4). Cloud-Dienste werden für ihren positiven Beitrag in Unternehmen geschätzt. Die Umfrage ergab auch, dass 58 % der Befragten Cloud-Lösungen geschäftlich nutzen – und das trotz der möglichen Auswirkungen neuer Datenschutzrechte, die rund um den Globus neue Vorschriften für das Speichern, Übertragen und Verarbeiten von Daten vorsehen. Cloud-Computing hat also einen festen Platz eingenommen und lässt sich auch durch neue Richtlinien und Vorschriften nicht verdrängen. Dennoch wird die Regulierung der in der Cloud gespeicherten Inhalte für Juristen, Politiker und Unternehmen, die Datenschutz, Zugriff und Produktivität ins Gleichgewicht bringen wollen, immer mehr zum Problem.

Abbildung 4: Antworten auf die Frage „In welchen IT-Umgebungen werden sich Ihre regulierten und vertraulichen Inhalte in den kommenden drei Jahren (bis Mitte 2018) befinden?“



Ovum ist der Ansicht, dass die steigende Beliebtheit von Cloud-Computing auf fehlende Ressourcen zurückzuführen ist. Es ist hinlänglich bekannt, dass es Unternehmen oft an Ressourcen mangelt, um einen geeigneten Schutz für regulierte und vertrauliche Inhalte zu schaffen und bei einer internen Speicherung die Compliance nachzuweisen. So wird der Datenschutz selbst zum Wachstumsmotor für Cloud-Lösungen, da Kunden davon ausgehen, dass die Serviceanbieter für die bestmögliche Sicherheit sorgen.

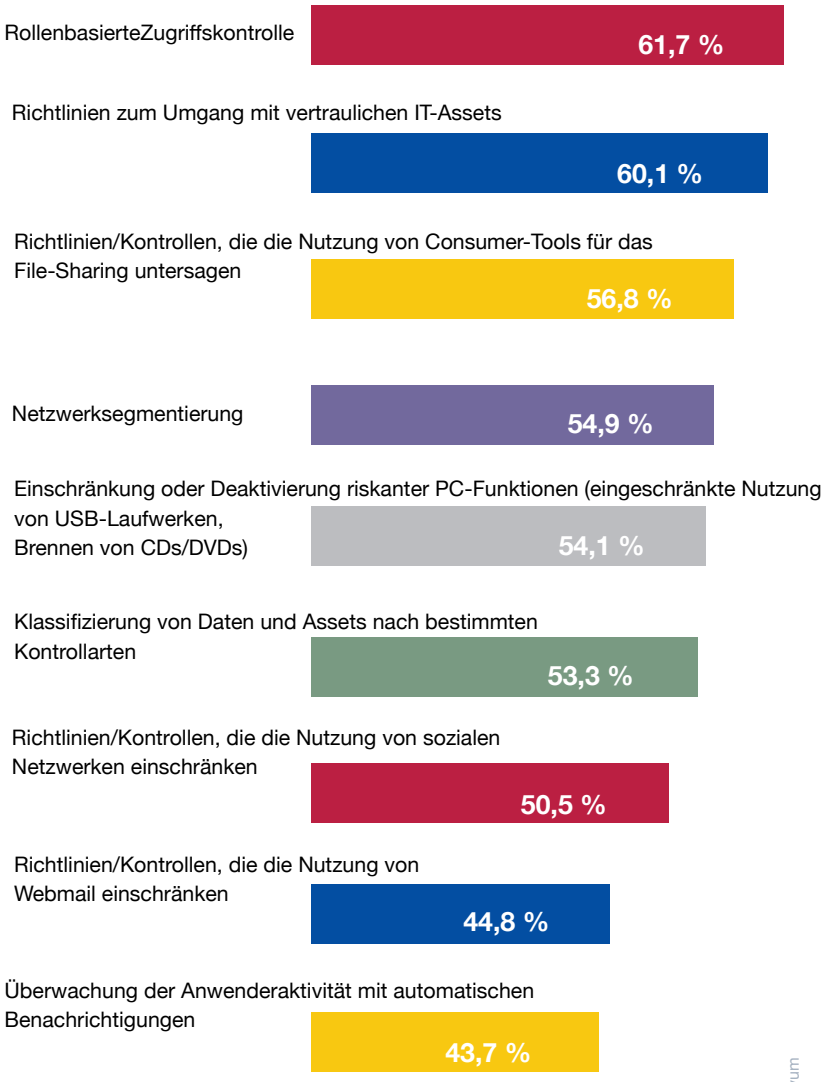
Unternehmen fehlen die Grundlagen zum Schutz vertraulicher Inhalte.

Unsere Umfrage ergab außerdem, dass viele der Befragten nicht einmal grundlegende Maßnahmen ergreifen, um Compliance-Anforderungen einzuhalten (siehe Abbildung 5). Nur 44 % der Befragten überwachen die Aktivitäten ihrer Anwender und nutzen automatische Benachrichtigungen, und lediglich 62 % verfügen über rollenbasierte Zugriffskontrollen. Nur etwas mehr als die Hälfte (53 %) klassifiziert Inhalte, um die Kontrolle zu erleichtern. Lediglich 54 % der befragten Unternehmen deaktivieren riskante Rechnerfunktionen wie externe Laufwerke, und nur 57 % sperren den Zugriff auf Consumer-File-Sharing-Tools wie z. B. Dropbox, für die es keine Unternehmensrichtlinien gibt.

Unternehmen, die derartige Sicherheitslücken aufweisen, wenden sich eher an Cloud-Anbieter, statt selbst Zeit und Ressourcen in die Problembehebung zu investieren. Die Umfrage ergab auch, dass ein mangelnder Datenschutz besonders in kleinen und mittleren Unternehmen zu finden ist. Dieses Ergebnis könnte sich dadurch erklären, dass diese Unternehmen überproportional mehr investieren müssten, um ihre Schutzmaßnahmen entsprechend aufzurüsten.

Kunden aus verschiedenen Unternehmen kennen sich immer besser mit steigenden Compliance-Anforderungen an den Datenschutz aus und behalten entsprechende Gesetze daher genau im Blick. Die notwendigen Technologien werden von Cloud- und SaaS-Anbietern bereitgestellt.

Abbildung 5: Antworten auf die Frage „Welche Richtlinien, Prozesse und Kontrollen nutzt Ihr Unternehmen momentan, um Daten zu schützen und Missbrauch zu vermeiden?“



Quelle: Ovum

Datenschutzbestimmungen sind uneinheitlich, sodass Unternehmen rund um den Globus anfällig für Verstöße sind.

Unternehmen, in denen selbst grundlegende Maßnahmen zum Datenschutz fehlen, sind mit neuen, strengeren Datenschutzgesetzen überfordert. Diese Gesetze werden lokal erlassen. Es gibt keine universal gültige Rechtsprechung. International tätige Unternehmen, die in verschiedenen Rechtsprechungen tätig sind, müssen zahlreiche verschiedene Gesetze einhalten, die unterschiedliche Maßnahmen vorschreiben (siehe Tabelle 1). Es ist unklar, inwieweit sich bestehende Gesetze ändern werden. Nehmen wir z. B. Safe Harbor. Das 15 Jahre alte Abkommen regelt die Datenübertragung zwischen der EU und den Vereinigten Staaten und wurde kürzlich für ungültig erklärt. Betroffen sind über 4.000 Unternehmen, denen es nun nicht mehr möglich ist, Daten ohne rechtliche Vorgaben wie Standardvertragsklauseln oder verbindliche Unternehmensrichtlinien legal in die USA zu übermitteln. International tätige Unternehmen und besonders solche, die in Europa vertreten sind, wissen also nicht mehr, welches Vorgehen am sichersten ist, und fürchten Gesetzesverstöße.

Tabelle 1: aktueller Stand der Datenschutzgesetzgebung

Land/Region	Definition personenbezogener Daten	Art der Einwilligung zur Handhabung personenbezogener Daten	Richtlinien für die Übertragung personenbezogener Daten ins Ausland	Anforderung öffentlicher Stellen zur Herausgabe von Daten	Strafen
EU	Information zu einer bekannten oder unbekannten natürlichen Person. Gesetzesentwurf beinhaltet IP-Adressen.	Eindeutige Einwilligung. Gesetzesentwurf soll ausdrückliche Einwilligung einführen.	Die EG und ihre Mitgliedsstaaten entscheiden, ob ein Drittland ausreichenden Schutz bietet. Ist dies nicht der Fall, müssen entsprechende Maßnahmen ergriffen werden.	Unklar nach Aufhebung der Richtlinie zur Vorratsdatenspeicherung. Nationale Gesetze haben weiterhin Bestand.	Über Strafen entscheidet jedes Land selbst. Gesetzesentwurf schlägt Geldstrafen von bis zu 2 % des Jahresumsatzes von Unternehmen vor.
USA	Unklar. Variiert je nach Act/Branche.	Vorherige Einwilligung in schriftlicher oder elektronischer Form gemäß Communications Act.	Keine spezifischen Richtlinien. Laut Federal Trade Commission (FTC) gelten US-Gesetze auch dann, wenn Daten die USA verlassen.	Gerichtsbeschluss erforderlich. Ausnahmen für das FBI und andere Behörden im Rahmen des USA PATRIOT Act.	Strafen variieren je nach Act.
Australien	Eine wahre oder unwahre, materielle oder nicht-materielle Information oder Meinung über eine bestimmte identifizierte Person oder eine Person, die sich identifizieren lässt.	Unternehmen müssen den Umständen entsprechende Schritte einleiten, um die Person über die Erfassung von Daten in Kenntnis zu setzen.	Die übertragenden Unternehmen müssen angemessene Schritte unternehmen um sicherzustellen, dass die geltenden Richtlinien befolgt werden, wenn Daten in ein Drittland übermittelt werden.	Behörden dürfen personenbezogene Daten nur dann erfassen, wenn diese für eine oder mehrere Funktionen oder Aktivitäten erforderlich sind.	Für ernstzunehmende und wiederholte Verstöße gegen Richtlinien können zivilrechtliche Sanktionen von bis zu 1,57 Mio. US-Dollar (1,7 Mio. AUD) verhängt werden.
Singapur	Wahre oder unwahre Daten einer Person, die sich anhand der fraglichen Daten oder durch andere Daten identifizieren lässt, auf die das Unternehmen Zugriff hat.	Die Einwilligung sollte in Schriftform oder in anderer Form erfolgen, die gespeichert werden kann. Sie kann auch mündlich erteilt werden.	Eine Übertragung in Drittländer ist dann zulässig, wenn das Empfängerland ein vergleichbares Schutzniveau aufweist.	Staatliche Stellen und Unternehmen, die im Auftrag einer staatlichen Stelle handeln, sind vom Personal Data Protection Act (PDPA) ausgenommen.	Es kann eine Geldstrafe von maximal 799.000 US-Dollar (1 Mio. SGD) verhängt werden.
Brasilien	Unklar. Das zivilrechtliche Internet-Rahmenabkommen (Marco Civil da Internet) wird durch eine detaillierte Gesetzgebung ergänzt.	Freiwillige, informierte und ausdrückliche Einwilligung. Künftige Gesetze gehen u. U. mehr ins Detail.	Die Übertragung in Drittländer ist gestattet, Unternehmen müssen aber brasilianische Gesetze einhalten, wenn Daten in Brasilien erfasst/verarbeitet werden.	Die Aufbewahrungsfrist für ISP-Verbindungsregister beträgt ein Jahr, für Anwendungsanbieter sind es sechs Monate. Für die Polizei oder Gerichte kann die Frist u. U. verlängert werden.	Bis zu 10 % des Unternehmensumsatzes vor Steuern sowie temporäre oder vollständige Aussetzung der Datenerfassung und -verarbeitung.

Quelle: Ovum und Gesetzestexte

Geplante EU-Datenschutzrichtlinien werden Maßstäbe für den internationalen Datenschutz setzen, können aber zum Hemmschuh für die EU-Wirtschaft werden.

Laut der Weltbank und dem Weltwährungsfonds ist die EU gemessen am BIP die weltweit größte Volkswirtschaft. Aus diesem Grund kann sie in puncto Regulierung durchaus Maßstäbe für andere Länder setzen. Die europäische Gesetzgebung nimmt zwangsläufig Einfluss auf alle international agierenden Unternehmen. Der Datenschutz in der EU wurde erstmals in der Datenschutzrichtlinie von 1995 festgeschrieben. Vor ein paar Jahren kamen die EU-Behörden überein, dass angesichts des technologischen Fortschritts ein neues Regulierungssystem (die geplante Datenschutz-Grundverordnung) erforderlich ist, das die Nutzung von Smartphones, Tablet-PCs, Breitbandanbindungen und Cloud-Diensten in Unternehmen berücksichtigt. Tabelle 2 fasst die wichtigsten Änderungen der Datenschutz-Grundverordnung zusammen.

Unsere Umfrage zeigt, dass international tätige Unternehmen beabsichtigen, ihre Geschäftsabläufe in einigen europäischen Ländern zu ändern, sobald die neue Datenschutz-Grundverordnung in Kraft tritt. 78 % der US-Unternehmen, 62 % der Unternehmen im Vereinigten Königreich, 46 % der südamerikanischen, 71 % der deutschen, 58 % der französischen und 71 % der Unternehmen in Australien und Neuseeland wollen ihre Strategien überprüfen. Das könnte zu einem schweren wirtschaftlichen Einbruch in der EU führen, deren Wohlstand vom internationalen Handel abhängt. Diese Entscheidung wird außerdem vom Kostenfaktor untermauert. 68 % der befragten Unternehmen glauben, dass die neue Datenschutz-Grundverordnung die Handelskosten in der EU drastisch in die Höhe treiben wird. Außerdem sind 85 % der US-Unternehmen der Meinung, dass sich der Wettbewerb mit europäischen Unternehmen verschärfen wird. Das könnte bedeuten, dass weniger US-Unternehmen in der EU tätig sein werden. Diese Ergebnisse verdeutlichen die große Skepsis in Bezug auf die neue Datenschutz-Grundverordnung. Unternehmen befürchten negative Auswirkungen auf das internationale Geschäft und die EU-Wirtschaft.

Die befragten Unternehmen äußerten auch Bedenken zu möglichen Sanktionen. Die in der neuen Datenschutz-Grundverordnung vorgesehene Geldstrafe für Verstöße beträgt 2 % des weltweiten Unternehmensumsatzes. In großen Unternehmen können das mehrere Milliarden US-Dollar sein. Unserer Umfrage zufolge glauben mehr als 50 % der weltweit agierenden Unternehmen, dass sie im Rahmen der neuen Datenschutz-Grundverordnung eine Strafe zahlen müssen.

Tabelle 2: die wichtigsten Änderungen der Datenschutz-Grundverordnung im Überblick

Problem	Neuerung	Auswirkungen
Zentrale Anlaufstelle	Unternehmen müssen ihre Compliance mit einer zentralen EU-Regulierungsstelle statt mit einer im Mitgliedstaat ansässigen Stelle abstimmen.	Vereinfachung der Compliance. Hinweis: Es steht derzeit nicht fest, ob dies so umgesetzt wird.
Datenverarbeiter	Datenschutzrechte werden ausgehend vom Eigentümer der Daten um den Verarbeiter der Daten erweitert.	Anbieter von Cloud-Services, SaaS-Anbieter usw. müssen das EU-Datenschutzrecht einhalten.
Exterritorialität	Das Gesetz gilt für Unternehmen mit Hauptsitz außerhalb der EU, wenn sie Daten von EU-Bürgern erfassen.	Serviceanbieter außerhalb der EU müssen beispielsweise in regionale Rechenzentren investieren.
Datenportabilität	Daten zu EU-Datensubjekten dürfen ohne entsprechenden Rechtsrahmen nicht außerhalb des EWR übertragen werden. (Die neue Datenschutz-Grundverordnung wird als Scheitern von Safe Harbor interpretiert. Weitere Informationen dazu im Fließtext.)	Siehe oben
Daten-Profiling	Wenn Daten zu Profiling-Zwecken an dritte Datenverarbeiter weitergeleitet werden, müssen die betroffenen Personen zuvor einwilligen.	Dies könnte sich auf Datenverarbeiter auswirken, wenn diese Daten verwenden oder an andere Datenverarbeiter weiterleiten bzw. die Daten selbst zu Profiling-Zwecken nutzen. Hinweis: Es steht noch nicht fest, ob die Einwilligung ausdrücklich oder stillschweigend erfolgen muss.

Quelle: Ovum

Nach Land und Region sieht dies wie folgt aus: 62 % der deutschen, 59 % der US-amerikanischen, 42 % der französischen und 32 % der südamerikanischen Unternehmen, 53 % der Unternehmen im Vereinigten Königreich und 56 % der Unternehmen in Australien und Neuseeland rechnen im Rahmen der Datenschutz-Grundverordnung mit Geldstrafen. Der Großteil der globalen Unternehmen (57 %) ist der Ansicht, dass die neue Datenschutz-Grundverordnung eine Überreaktion auf die von Edward Snowden enthüllten Informationen zu Überwachungs- und Spionagepraktiken von Geheimdiensten ist. Die befragten europäischen Unternehmen stimmten dieser Aussage zu. 57 % der deutschen, 46 % der französischen und 51 % der befragten Unternehmen im Vereinigten Königreich sehen die neue Datenschutz-Grundverordnung als Überreaktion auf das Datenschutzproblem an. Auch hier sind die Antworten wohl wieder auf den Kostenfaktor zurückzuführen, der durch Geldstrafen und Anpassungen der Geschäftsstrategien entsteht.

Der Speicherort von Daten ist das wichtigste Kontrollkriterium, aber schwer zu definieren.

Vom gesetzgeberischen Aspekt her ist der Speicherort der Daten besonders wichtig. In der Diskussion zum Thema Datenhoheit sind der Datenspeicherort und die eindeutige Definition der Kontrolle über personenbezogene Daten äußerst problematisch. Unsere Umfrage zeigt, dass diese vermeintlich offensichtlichen Konzepte zu einer gewissen Verunsicherung führen. Die Datenhoheit für Unternehmensdaten (Zugriffskontrolle) und Einhaltung von Compliance-Vorgaben hängen stark vom Speicherort der Inhalte ab. Er bestimmt u. a., welche Rechtsprechung für die Daten gilt und in welchem Umfang der Zugriff möglich ist. Viele Unternehmen können den Speicherort ihrer Daten nur schwer mitbestimmen, da die meisten Systeme (und insbesondere cloud-basierte Systeme) das Konzept des Datenspeicherorts nicht als geschäftliche Entscheidung ansehen. Dieses Problem wird noch verschärft, da die genaue Definition des Datenspeicherorts zu Compliance-Zwecken je nach Rechtsprechung variiert und juristische Auslegungssache ist. Unternehmen, die compliant sein möchten, müssen also den physischen, logischen, rechtlichen und politischen Speicherort ihrer Daten kontrollieren können. Tatsächlich wird das Thema bereits an Gerichten rund um den Globus diskutiert. Wo werden Daten gespeichert und kontrolliert, und welche Rechtsprechung gilt für Inhalte? Ein gutes Beispiel ist hier das Verfahren gegen Microsoft, das von einem US-Richter bezüglich der Herausgabe von Daten angestrebt wurde, die in einem Rechenzentrum in Dublin (Irland) vorgehalten wurden.

Laut unserer Umfrage (siehe Tabelle 3) gibt es keinen klaren Konsens zur Frage des Datenspeicherorts. Die Hälfte der befragten Unternehmen plant, ihren primären Ansatz zu diesem Kriterium in den kommenden drei Jahren zu ändern. Dieses Ergebnis kann als Unsicherheit bezüglich der Anpassung der aktuellen kundenseitigen Ansätze an künftige Anforderungen und die zu verfolgende Strategie interpretiert werden. Außerdem lässt sich schlussfolgern, dass Unternehmen auf einen neuen Standard warten. Das spricht sehr für einen Ansatz, der verschiedene technische Optionen anbietet, z. B. die Möglichkeit der Kontrolle des physischen und logischen Datenspeicherorts.

Tabelle 3: Aktuelle/mögliche Datenschutzmaßnahmen der Befragten

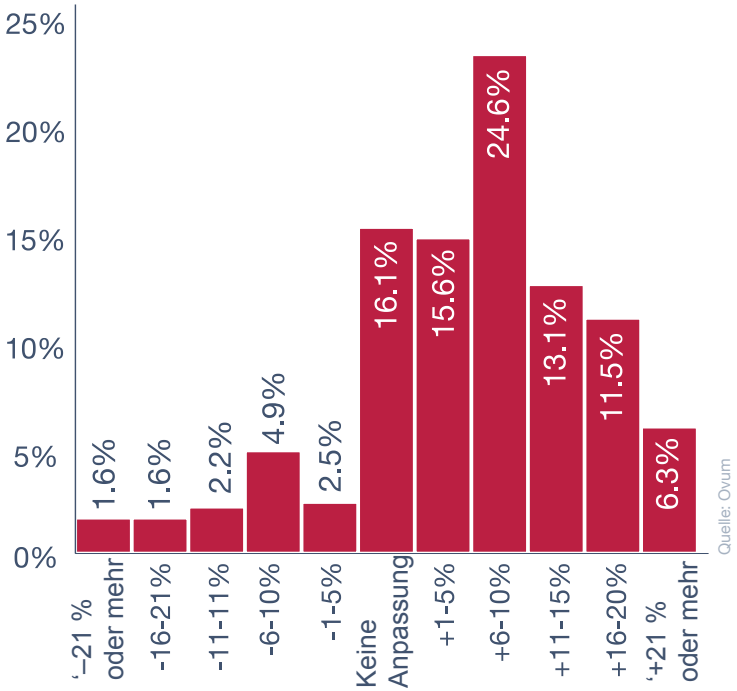
Antwort	Aktuelle primäre Maßnahmen	Maßnahme wird erwogen
Wir entscheiden je nach Rechtsstandort unserer Daten über den Datenschutz. (Diese Aussage bezieht sich auf ein Land bzw. Länder, die für die Daten zuständig sind, und auf die Rechtsprechung, gegen deren Gesetze verstoßen wird, wenn Dritte gegen Ihren Willen auf Daten zugreifen.) Anders ausgedrückt: ein Land, das für die eigenen diesbezüglichen Gesetze verantwortlich ist.	26 %	27 %
Wir entscheiden je nach logischem Standort unserer Daten über den Datenschutz. (Der geografische Standort, von dem aus die Kontrolle über eine bestimmte Rechenfunktion erfolgt, d. h. der Standort, an dem die Verschlüsselung stattfindet.)	27 %	33 %
Wir entscheiden je nach physischem Standort unserer Daten über den Datenschutz. (Üblicherweise der bzw. die Standorte, an denen Daten tatsächlich gespeichert werden.)	33 %	24 %
Wir entscheiden je nach politischem Standort unserer Daten über den Datenschutz. (Der Standort, an dem Regierungen Druck ausüben, damit Inhalte herausgegeben werden.) Z. B. USA oder EU.	14 %	15 %

Quelle: Ovum

Vorschriften verursachen hohe Kosten.

Von der Veränderung des regulatorischen Umfelds, z. B. in Hongkong, Singapur und Russland, sind auch Budgets betroffen. Datenschutzgesetze sind seit jeher ein rechtliches Problem. Da sie jetzt aber auch die Technologie und Compliance betreffen, zeigt unsere Umfrage, dass viele Unternehmen davon ausgehen, hierfür neue Mitarbeiter einstellen zu müssen, um sie einhalten zu können. Im Einzelnen heißt das, dass 19 % der Befragten zusätzliche Kräfte in der Rechtsabteilung, 31 % neue Mitarbeiter in der IT und 34 % Zusatzkräfte für die Compliance einstellen müssen. Dies wiederum wirft neue Fragen zu veränderten Rollen in diesen drei Bereichen auf, deren Wert angesichts der Einführung neuer Vorschriften nicht zu unterschätzen ist.

Abbildung 6: Antworten auf die Frage „Wie müssen Sie Ihr Budget in den kommenden zwei Jahren anpassen, um auf neue internationale Richtlinien für den Datenschutz und die Datenhoheit zu reagieren?“



Der Umfrage zufolge glauben die Befragten, dass Technologie- und Compliance-Experten am besten geeignet sind, um dieses rechtliche Problem anzugehen. In den kommenden Jahren werden wir sicherlich mehr Experten sehen, die ihr Know-how zu Datenschutzgesetzen ausweiten. In der Folge steigen natürlich auch die Kosten. Unsere Umfrage verdeutlicht die voraussichtlichen Auswirkungen auf das Gesamtbudget (siehe Abbildung 6). Über 30 % der Befragten gehen davon aus, dass Budgets um mindestens 10 % steigen werden. Etwa ein Viertel rechnet mit einer Steigerung von 6 % bis 10 %. Insgesamt erwarten über 70 % der Befragten aufgrund der neuen Datenschutz-Grundverordnung steigende Budgets.

Unternehmen mit Sitz in den USA stehen unter Druck.

Durch die Enthüllungen von Edward Snowden zur Überwachung durch die NSA wird den USA ein gewisses Misstrauen entgegengebracht. Wir wollten von den Umfrageteilnehmern wissen, welche große Industrienation am ehesten unbefugt auf Unternehmensdaten zugreifen würde. Die USA liegen an erster Stelle, China und Russland auf Platz zwei bzw. drei. Tatsächlich aber gibt es in den Vereinigten Staaten einen strengen Datenschutz, der besser ist als der einiger europäischer Länder. Die Umfrageergebnisse sind wohl auf die Medienberichterstattung über Edward Snowden zurückzuführen.
Durch neue Regelungen in Europa ergeben sich Nachteile für US-Unternehmen. 63 % der Befragten glauben, dass die geplante europäische Datenschutz-Grundverordnung US-Unternehmen den Wettbewerb erschweren wird. 70 % sind der Ansicht, dass die neue Gesetzgebung europäische Unternehmen begünstigt.

Empfehlungen

Probleme hinsichtlich der Datenhoheit durch die Gesetzgebung werden sich stark auf zahlreiche Unternehmen auswirken, die international tätig sind. Unternehmen müssen ihre geschäftlichen und rechtlichen Anforderungen sowie Verbraucherwünsche ins Gleichgewicht bringen, wenn es um die Handhabung personenbezogener Daten geht. Folgende Maßnahmen sind jetzt ratsam:

Schaffung einer Datenhoheitsstrategie

Internationale Unternehmen, die personenbezogene Daten erfassen, unterliegen den Datenschutzbestimmungen in allen Ländern, in denen sie tätig sind. Sie können auch dann noch zur Verantwortung gezogen werden, wenn die Datenverwaltung durch einen externen Cloud-Anbieter erfolgt. Der erste Schritt ist, diese Verantwortung anzuerkennen und eine entsprechende Reaktionsstrategie zu erarbeiten. Diese sollte durch ein entsprechendes Führungsteam, das für die Schaffung unternehmensweiter Kontrollen, Richtlinien und Verfahren zur Einhaltung der Compliance zuständig ist, verwaltet werden. Vielleicht hat Ihr für GRC (Governance, Risiko und Compliance) zuständiges Team bereits entsprechende Schritte eingeleitet. Die Unternehmensführung sollte aber hinter einer solchen Strategie stehen.

Risikobewertung des Datenschutzes

Eine gute Unternehmensführung berücksichtigt immer auch die geschäftlichen Risiken. Der Kontext ist besonders wichtig, wenn es darum geht, Datenschutzrisiken zu bewerten. Für bestimmte Branchen wie z. B. Life Sciences und Versicherungen gelten besonders strenge Auflagen. Am Anfang einer Bewertung sollte die Einteilung der Informationen in bestimmte Kategorien stehen (z. B. personenbezogene Daten, vertrauliche Unternehmensdaten). Diese sollten dann mit bestehenden Geschäftsprozessen und zugehörigen Regionen abgeglichen werden. Außerdem sollten Sie die relevanten Datenschutzvorschriften aller Rechtsprechungen, in denen Sie tätig sind, kennen und prüfen. Stellen Sie sich darauf ein, Geschäftsprozesse zu ändern, um regulatorische Anforderungen erfüllen zu können. Vielleicht verfügen Sie bereits über geeignete Lösungen, die Ihnen bei der Bewertung Ihrer Inhalte helfen (z. B. Datenklassifizierungstools wie Atlas). Gleichzeitig nutzen Sie aber vielleicht auch Technologien, die Ihr Risiko erhöhen (z. B. Consumer-Tools für das File-Sharing wie Dropbox).

Einbeziehung des Faktors Mensch

Bei der Bewertung der Auswirkungen der Datenhoheit können sich rechtliche und technologische Probleme ergeben. Datenschutz und Datenhoheit sind komplexe Themen, die Ihr gesamtes Unternehmen betreffen. Die Schulung Ihrer Mitarbeiter ist ebenso wichtig wie die Implementierung von Technologien zum Verwalten des Datenflusses. Es ist finanziell nicht tragbar und rechtlich nicht einwandfrei, sich nur auf eine Technologie, einen Prozess oder eine Mitarbeiteraktivität zu konzentrieren, da alle drei eine wichtige Rolle spielen.

Reden ist Gold

Fragen Sie Ihre Technologie- und Serviceanbieter danach, wie sie mit neuen gesetzlichen Vorgaben umgehen werden. Erfahrende Anbieter sind gut vorbereitet und bieten entsprechende Datenschutz-Optionen. Diese Optionen sind wichtig, da sich die Gesetzgebung der einzelnen Länder unterscheidet und schnell ändert. Anbieter sollten Fragen zum logischen und physischen Datenspeicherort beantworten können und über Serviceverträge verfügen, die eine rechtliche Flexibilität bieten.

Anhang

Methodik

Die Ovum-Umfrage wurde im dritten Quartal 2015 durchgeführt. Befragt wurden 366 Unternehmen verschiedener Größen an unterschiedlichen Standorten, die in diversen Branchen tätig sind. Die Untersuchungsergebnisse wurden im Kontext der laufenden Beratung von Ovum-Kunden, Gesprächen mit Branchenanbietern und sekundären Untersuchungen analysiert.

Autor

Alan Rodger, Senior Analyst, Enterprise ICT Management
alan.rodger@ovum.com

Ovum Consulting

Wir hoffen, dass Ihnen die Untersuchung dabei hilft, Geschäftsentscheidungen zu treffen. Wenn Sie Fragen haben, steht Ihnen das Beratungsteam von Ovum gerne zur Verfügung.

Weiter Informationen zum Beratungsangebot von Ovum erhalten Sie über consulting@ovum.com.

Copyright und Haftungsausschluss

Die Inhalte dieses Dokuments unterliegen internationalen Urheberrechtsgesetzen, Datenbankrechten und anderen gewerblichen Schutz- und Urheberrechten. Eigentümer dieser Rechte sind Informa Telecoms und Media Limited, angeschlossene Unternehmen und andere Drittlizenzgeber. Alle in diesem Dokument genannten Produkt- und Unternehmensnamen und alle abgebildeten Logos sind Marken, Dienstleistungsmarken oder Handelsnamen ihrer jeweiligen Inhaber (einschließlich Informa Telecoms und Media Limited). Das vorliegende Dokument darf ohne vorherige Genehmigung von Informa Telecoms und Media Limited nicht kopiert, vervielfältigt, verteilt oder veröffentlicht werden.
Die Richtigkeit und Vollständigkeit der Informationen mit Stand des Datums der Erstveröffentlichung dieses Dokuments wurden in angemessenem Umfang überprüft. Informa Telecoms und Media Limited und andere von Informa Telecoms und Media Limited beschäftigte oder beauftragte Personen übernehmen keine Verantwortung für eventuelle Fehler, Auslassungen und andere Ungenauigkeiten. Leser sollten alle Daten und Fakten unabhängig prüfen, da hierfür keine Verantwortung übernommen wird. Die volle Verantwortung und das Risiko für die Verwendung der Informationen und Inhalte liegen allein beim Leser.

Alle hier genannten Ansichten oder Meinungen sind die persönlichen Ansichten und Meinungen des Autors und anderen Mitwirkenden und geben nicht notwendigerweise die Ansichten und Meinungen von Informa Telecoms und Media Limited wider.

ovum

KONTAKT

www.ovum.com
askananalyst@ovum.com

NIEDERLASSUNGEN

Peking
Dubai
Hongkong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
São Paulo
Tokio

INTRA LINKS