Datenschutz-Grundverordnung (DSGVO) der Verordnung (EU) Nr. 2016/679

Die DSGVO-Frist rückt schnell näher. Sind Sie bereit?

Ab dem 25. Mai 2018 sind Unternehmen in Europa verpflichtet, der DSGVO-Verordnung (General Data Protection Regulation - GDPR) Folge zu leisten, was für eine Vielzahl an neuen Herausforderungen sorgt. Die Grundpfeiler dieser Verordnung können wie folgt zusammengefasst werden:

1. Sie gilt weltweit für jedes Unternehmen, vorausgesetzt dieses verfügt über personenbezogene Daten eines europäischen Staatsbürgers.
2. Die Verordnung betrifft hauptsächlich europäische Staatsbürger. Alle in ihr aufgeführten Anforderungen haben zum Ziel, diese zu schützen.
3. Sie beinhaltet eine Reihe von Grundsätzen, an die sich Unternehmen halten müssen. Örtliche Regulierungsbehörden werden NICHT NUR die Einhaltung der Regeln überwachen, sondern erwarten ebenfalls ein gewisses Maß an Eigeninitiative.
4. Bußgelder für die Nichteinhaltung der Grundsätze wurden auf höchstens vier Prozent des gesamten Jahresumsatzes eines Unternehmens oder 20 Millionen Euro festgelegt, je nachdem, welcher Wert größer ist.
5. Örtliche Aufsichtsbehörden müssen über jede Verletzung des Schutzes personenbezogener Daten schnellstens informiert werden, wenn möglich innerhalb von höchstens 72 Stunden. Betroffene Personen müssen umgehend von der Verletzung der Datensicherheit in Kenntnis gesetzt werden.
6. Kontrollierende und verarbeitende Unternehmen haften gemeinsam für Verletzungen des Datenschutzes.
7. Datenverschlüsselung wird ausdrücklich als risikominimierende Maßnahme hervorgehoben.

Das Hauptziel dieser Verordnung ist es, europäische Staatsbürger zu schützen. Unternehmen, die Zugang zu den personenbezogenen Daten europäischer Staatsbürger haben, müssen sicherstellen, dass diese Daten nur in ihre Systeme gelangen, wenn der Verarbeitung der Daten zugestimmt wurde. Darüber hinaus müssen die Systeme ausreichend sicher sein, um den Vorraussetzungen der Verordnung zu entsprechen. Unternehmen müssen außerdem notwendige Richtlinien und Rahmenbedingungen festlegen, um die laufende Sicherheit und Übertragbarkeit dieser Daten stets gewährleisten zu können. In der Verordnung wird ausdrücklich erwähnt, dass verwendete Systeme von Grund auf sicher entworfen sein sollten.

Wir bei Intralinks wissen, dass die Mehrheit der Unternehmen den Grundsätzen dieser Verordnung ohne große Umstrukturierung folgen können. Wir befinden uns jedoch in einem sich rasch wandelnden unternehmerischen Umfeld, in dem „Content in Motion“ ein grundlegendes unternehmerisches Risiko darstellt. Intralinks verfügt über ausreichend Ressourcen, um Ihr Unternehmen bei der Minimierung dieses Risikos zu unterstützen.

Unsere lange Unternehmensgeschichte ist ein Zeichen unserer Erfahrung in der Absicherung von hoch vertraulichen Inhalten innerhalb von stark regulierten Branchen und der Unterstützung von Unternehmen bei der Risikominimierung im Rahmen von komplexen Regulierungen, einschließlich der Datenschutz-Grundverordnung.

intralinks.com/de

Hier finden Sie eine Intralinks-Niederlassung in Ihrer Nähe:
intralinks.com/de/standorte

256582 DM

Überblick über den Intralinks Trust Perimeter™

Der Intralinks Trust Perimeter™ umfasst die folgenden Funktionen, um Kunden des Intralinks Content Collaboration Network zu unterstützen:

Intralinks Distributed Content Nodes: Physischer Standort

- Unsere Content-Nodes-Architektur ermöglicht es unseren Kunden, den physischen Standort für die Speicherung und Verarbeitung der Daten, die auf die Intralinks Plattform hochgeladen werden, einzuschränken, während sie gleichzeitig von den traditionellen Vorzügen einer Cloud-basierten Lösung profitieren.

Intralinks kundenseitig verwaltete Verschlüsselungs-Keys (CMK): Logischer Speicherort

- Die kundenseitig verwalteten Keys mit logischer Speicherort-Kontrolle bieten Kunden die komplette und alleinige Kontrolle über die Verschlüsselung, die ihre Daten in der Cloud schützt.

Intralinks Information Rights Management (IRM): Logische Kontrollen

- Plugin-freies Information Rights Management schützt Inhalte – während der Speicherung und Übertragung –, indem Kunden die Kontrolle über einzelne Dateien während des gesamten Lebenszyklus erhalten.

Rechtliche Möglichkeiten: Rechtliche Kontrollen

- Intralinks hat einen internationalen Data Privacy Officer ernannt, der in Zusammenarbeit mit Datenschutzexperten regelmäßig die neuen und sich ändernden weltweiten Datenschutzbestimmungen analysiert und bewertet. So können wir Kunden Einblicke und rechtliche Strategien rund um EU-Modellklauseln und den EU-US-Datenschutzschild anbieten.

Audit und Governance: Einblick

- Um diese Kontrollmaßnahmen zu unterstützen, beinhalten die Standardfunktionen der Intralinks-Plattform umfangreiche Audits und Berichte.

Der Intralinks Trust Perimeter kann folgende Services anbieten:

- vom Kunden verwaltete Verschlüsselungs-Keys für den Zugriff auf die Inhalte.
- Information Rights Management (IRM) – für eine granulare, lebenslange Kontrolle einzelner Inhalte.
- physische regionale Absicherung – Inhalte können in spezifischen Regionen gespeichert werden, ohne durch andere Regionen geleitet werden zu müssen (regionale Verarbeitung und Archiverstellung).
- juristische Hilfsmittel für den überregionalen Transfer persönlicher Daten – wir verwenden Musterverträge für die Weiterleitung persönlicher Daten in Länder, die sich außerhalb des Europäischen Wirtschaftsraums befinden und von der EU-Kommission als nicht „ausreichend“ befunden wurden. Wir sind nach dem EU-US-Datenschutzschild zertifiziert und haben die Genehmigung von verbindlichen Unternehmensregelungen (Binding Corporate Rules) beantragt.

Intralinks wird bereits zur Unterstützung folgender Anwendungsbeispiele verwendet:

Beaufsichtigung und Risikomanagement von Lieferanten:

Die Verwaltung von Lieferanten und Partnern zur Einhaltung regulatorischer Anforderungen, die Kunden und andere Beteiligte schützen sollen, ist noch immer mit Herausforderungen verbunden. Erfahren Sie, wie Sie mit Intralinks Folgendes erreichen können:

- den Fluss vertraulicher und personenbezogener Informationen (PII) von Kunden sichern
- die Einhaltung von Vertrags- und Compliance-Bedingungen überwachen und durchsetzen.

Management von Compliance:

Verwalten Sie unternehmensweit verfügbare Compliance-Daten mit granularen betrieblichen Kontrollmechanismen und Informationssicherheit bei der Zusammenarbeit mit internen und externen Stakeholdern. Mit Intralinks können Sie:

- nachweisen, wer wann welche Dokumente erstellt, geprüft und ausgetauscht hat
- eine einzelne Master-Kopie für Compliance-Handbücher, Richtlinien und Verfahrensbeschreibungen erhalten und intern und extern Beteiligten Zugriff gewährleisten

Risiko- und Compliance-Daten-Governance:

Die globale Finanzkrise hat den Bedarf an sofort verfügbaren, unternehmensweiten Risiko- und Compliance-Daten hervorgehoben. Regulierungsstellen erwarten von Unternehmen, dass diese Risiko- und Compliance-Daten vollständig, präzise und zeitnah bereitstellen. Intralinks bietet:

- eine zentrale globale Plattform, die geografische, geschäftsinterne und IT-basierte Grenzen überwindet
- allerhöchste Informationssicherheit beim Austausch von vertraulichen, aufsichtsrelevanten Daten mit Regulierungsstellen und anderen Parteien

Richtlinienkonforme Archivierung:

Ermöglichen Sie die Zusammenstellung, Optimierung und offizielle Einreichung regulatorischer Informationen über verschiedene Organisationsstrukturen und Informationsarten hinweg. Mit Intralinks können Sie:

- Informationen schützen, bevor diese öffentlich zur Verfügung gestellt werden
- Geschäftsabläufe zur besseren Einhaltung von Einreichungsfristen modernisieren
- die Rechenschaftspflicht in der gesamten Vorbereitungs- und Einreichungsphase verbessern

Um mehr über das Thema Datenhoheit in der Cloud zu erfahren, besuchen Sie bitte die Intralinks Trust Perimeter-Seite oder rufen Sie uns an: +44 (0) 20 7549 5200.

Über 99 % der Fortune-1000-Unternehmen haben Intralinks bereits ihre sensibelsten Daten anvertraut. Sie können es auch tun.