druva

Fünf Schritte zur Einhaltung der EU-Datenschutz-Grundverordnung (DSGVO)

Ein Leitfaden für die Entwicklung Ihrer zeitlichen Planung

Dieses Dokument bietet einen Rahmen für alle Unternehmen, die Kunden in Europa haben, da sie ihre eigenen Systeme vorbereiten müssen, um die neuen Anforderungen der DSGVO-Datenschutzbestimmungen vor 2018 zu erfüllen.

Fünf Schritte zur Einhaltung der EU-Datenschutz-Grundverordnung (DSGVO)

Bei der DSGVO geht es im Wesentlichen um die Regeln, die Unternehmen befolgen müssen, um sicherzustellen, dass persönlich identifizierbare Informationen (PII) in gutem Glauben geschützt werden. Ein Verstoß gegen diese Bestimmungen durch ein Unternehmen kann zu Geldstrafen und strafrechtlicher Verfolgung führen. Dies ist besonders in einer Umgebung besorgniserregend, die zunehmend mobil und Cloud-basiert ist. Warum? Da schützenswerte Daten, immer schwerer zu verfolgen sind und das Risiko, dass die Daten gefährdet sind und kompromittiert werden, immer größer wird, da sie sich nicht mehr hinter einer Firewall befinden.

Befolgen Sie diesen **Fünf-Punkte-Plan,** um Ihre eigenen Systeme darauf vorzubereiten, die neuen Anforderungen dieser Datenschutzbestimmungen vor 2018 zu erfüllen.

Was Sie zur Einhaltung der DSGVO benötigt:

1. Überprüfen Sie Ihr aktuelles Konzept zur Datenverwaltung, um Ihre aktuelle Position und Ihre Prozesse rund um den Datenschutz festzulegen

Sie sollten eine Prüfung aller Kundendatensätze im gesamten Unternehmen durchführen. Die Einführung neuer Prozesse oder die Stärkung des bestehenden Verfahrens ist nur dann möglich, wenn alle PII-Instanzen bekannt sind.

- Durch diese Prüfung können Unternehmen die aktuellen Geschäftsprozesse besser verstehen, die im Laufe der Zeit Kundendaten erzeugen oder verwenden
- Beziehen Sie Bereiche mit ein, in denen Kundendaten gegenwärtig möglicherweise nicht ausreichend geschützt sind oder verwaltet werden, beispielsweise bei einzelnen IT-Assets der Mitarbeiter. Diese Prüfung wird auch dazu beitragen, dass sichergestellt wird, dass alle Prozessänderungen durchgeführt werden, um zukünftige Anforderungen zu erfüllen

2. Bereiten Sie Führungskräfte innerhalb des Unternehmens hinsichtlich der Einhaltung des Datenschutzes vor

Die EU wird eine führende Datenschutzbehörde zur Verwaltung der DSGVO einsetzen, ebenso müssen Unternehmen intern eine Führungsposition für Datenschutz und Sicherheit besetzen. Dies wird eine IT-interne Rolle sein, beinhaltet aber die Zusammenarbeit mit den beiden anderen IT-Gruppen innerhalb der IT- sowie anderen Business-Teams/-Einheiten.

Diese Person sollte die Unterstützung des Senior Management Teams und der Person erhalten, die den Nachweis erbringt, dass die Regeln eingehalten werden.

- Diese Person kann Bemühungen delegieren, Back-up, Notfallwiederherstellung und Archivierungsprozesse zu überprüfen. Anstatt mehrere Werkzeuge für unterschiedliche Aufgaben rund um die Unternehmensdaten einzusetzen, sollte eine konvergente Lösung in Betracht gezogen werden, die einen einzigen Blick auf die Daten ermöglicht und somit die Replikation minimiert.
- Zukünftig müssen Sie Datenerstellung verfolgen und automatisch die entsprechenden Regeln auf persönliche Daten und Kundendatensätze anwenden. Druva InSync unterstützt die Automatisierung dieses Prozesses, ganz gleich, ob Daten innerhalb Cloud-Anwendungen, auf einzelnen Benutzergeräten erstellt oder zentral gespeichert werden.

3. Veröffentlichen des ersten Leitfadens für das Unternehmen

Die Unternehmen müssen sicherstellen, dass ihre internen Teams sich gleichermaßen ihrer Verantwortung bewusst sind. Aktualisieren Sie Ihre bestehende Business-Continuity-Richtlinien, sodass sie der DSGVO entsprechen. Allerdings sollte dieses Richtliniendokument auch an den Rest des Unternehmens weitergegeben werden. Dieses Bewusstsein kann die Akzeptanz neuer Prozesse sowie die Investition in neue Technologien unterstützen.

- Die Datenschutzbehörde wird Informationen zur Erfüllung der Anforderungen der DSGVO-Regel „Das Recht, vergessen zu werden“ bereitstellen. Dies umfasst das Löschen von Daten, wenn es angebracht ist und Kunden darum bitten und das berechtigte Aufbewahren von Daten, wenn Kunden umziehen oder den Service nicht mehr nutzen.
- Passen Sie Ihre eigenen Datenarchivierungsprozesse an, um diese Aufgabe zu erleichtern. Unternehmen in regulierten Branchen müssen möglicherweise Kundendaten jahrelang aufbewahren, auch wenn der Kunde dort keine Waren mehr kauft oder die Dienstleistungen nicht mehr in Anspruch nimmt. Bei einer Datenlöschanforderung kann es eine Überlappung zwischen den Daten für die Archivierung und denen zur Nutzung für die Kundendaten geben.

4. Konsolidierung, um den Schutz einfacher zu gestalten

Für viele Unternehmen existieren Daten über die geschäftlichen Aktivitäten hinaus und innerhalb verschiedener IT-Ressourcen. Heute erreichen rund 40 Prozent der Unternehmensdaten nie die zentralen IT-Plattformen. Um den DSGVO-Anforderungen gerecht zu werden, sollte man sich ansehen, wie all die Daten verwaltet werden, die Kundeninformationen beinhalten und wie dies reduziert werden kann.

- Schützen Sie Ihre Daten auf mobilen Endgeräten und in dezentralen Büros in die gleiche Weise, wie zentral aufbewahrte Informationen. Druva inSync kann Dateien und Daten für potenzielle PII- und andere sensible Datenrisiken scannen. Dieses Verfahren stellt sicher, dass das Unternehmen weiß, wo sich alle Daten befinden, und dass es die richtigen Sicherheitsmaßnahmen ergreifen kann, um sie zu schützen.
- Die Verschlüsselung von Daten auf mobilen Geräten ist wichtig, um Kundendaten zu schützen. Dies verhindert, dass Probleme auftreten, wenn Geräte verloren gehen oder gestohlen werden, was zu Compliance-Problem führen kann. Wenn ein Gerät verloren geht oder gestohlen wird, sollten die Informationen darauf auch über einen Remote-Befehl gelöscht werden können.
- Neben der Verschlüsselung von Daten auf den Geräten, müssen Unternehmen Daten auch zentral verschlüsseln. Für Unternehmen, die Daten in der Cloud speichern möchten, sollte auch eine Kontrolle über die zentralen Daten in Betracht gezogen werden. Achten Sie auf eine Verschlüsselung, die gewährleistet, dass nur das Unternehmen die relevanten Dateien entschlüsseln kann.
- Die Richtlinienverwaltung ist für Dateien wichtig - die Zentralisierung der Verwaltung gewährleistet, dass alle Schritte für die Einhaltung automatisch befolgt werden.

Plan für die regelmäßige Kommunikation

5. Die Einhaltung der DSGVO wird ab 2018 eine permanente Anforderung sein. Um den Anforderungen der DSGVO zu entsprechen, ist die Kommunikation zwischen dem IT-Team, das für den Datenschutz und die Sicherheit verantwortlich ist, und anderen Geschäftsfunktionen wie Compliance, Rechtsabteilung und Audit erforderlich.

Zudem sollten Sie in Erwägung ziehen, regelmäßig mit den Mitarbeitern im gesamten Unternehmen zu kommunizieren, um diese an ihre Aufgaben und Verantwortlichkeiten für Kundendaten zu erinnern.

- Definieren Sie eine Kommunikationsstrategie für Daten und den Datenschutz. Diese sollte den Mitarbeitern von Anfang an mitgegeben werden und immer wieder aufgefrischt werden, um Mitarbeiter bezüglich ihrer Verantwortlichkeiten auf dem Laufenden zu halten.
- Zudem sollte eine Kommunikationsstrategie für den Fall von Datenmissbrauch oder Datenverlust aufgestellt werden. Die lokale Datenschutzbehörde sollte über den Verstoß informiert werden; außerdem muss das Unternehmen dies seinen Kunden und der breiten Öffentlichkeit mitteilen.

Mit Druva inSync Kundendaten schützen und verwalten

Druva InSync kann die Erstellung neuer Dateien auf Laptops oder mobilen Geräten verfolgen und automatisch gewährleisten, dass Dateien mit Kundendaten und PII entsprechend Unternehmensregeln geschützt werden. Unternehmen wird Folgendes geboten:

- Zentrale Sichtbarkeit der Daten auf den Geräten und Cloud-Services, um Datenrisiken einzuschätzen und zu mindern.
- Werkzeuge für die Nachverfolgung und Identifizierung von möglichen Datenlecks, indem Unternehmen über mögliche Datenrisiken auf Geräten und Cloud-Services gewarnt werden.
- Die Möglichkeit, extern Daten auf mobilen Geräten zu löschen, um Expositionsrisiken zu minimieren, wenn ein Gerät verloren geht oder gestohlen wird
- Unternehmen erfahren, was sich auf einem Gerät befindet, das gestohlen wurde oder verloren wurde, um das Ausmaß der Exposition zu beurteilen.
- Erzwingen Sie die Verschlüsselung auf Geräten (nicht auf allen), um die Dateien zu schützen, die darauf gespeichert sind, für den Fall, dass das Gerät nicht bereits verschlüsselt ist

Von einer Cloud-Perspektive aus gesehen kann Druva inSync die Daten sicher speichern, die wir im EU-Raum sammeln, um die Wiederherstellung und tiefere Datenauswertung zu unterstützen.

Befolgen Sie diese Richtlinien, um hinsichtlich der regulatorischen Anforderungen auf der sicheren Seite zu sein, wenn Sie geschäftlich mit europäischen Kunden zu tun haben, und um Kosten bzgl, der Datensicherung und Notfallwiederherstellung zu senken.

Um mehr darüber zu erfahren, wie Druva dabei helfen kann, besuchen Sie
www.druva.com/proactivecompliance

Druva ist Marktführer für konvergenten Datenschutz. Das Unternehmen stellt Hochverfügbarkeits- und Verwaltungslösungen auf Data-Center-Niveau für mobile Mitarbeiter bereit. Druvas preisgekrönte Lösung kommt mit einer zentralen Übersicht für Back-up, Verfügbarkeit und Verwaltung aus, minimiert Auswirkungen auf das Netzwerk und ist für Endanwender transparent. Druva ist das industrieweit am schnellsten wachsende Unternehmen für Datenschutz. Über 4.000 globale Organisationen mit über 4 Mio. Geräten vertrauen Druva. Erfahren Sie mehr auf www.druva.com und beteiligen Sie sich an der Unterhaltung auf twitter.com/druvainc.

Q117-CON-10582

Druva, Inc.
1 888-248-4976
sales@druva.com
www.druva.com