



VORBEREITUNG FÜR DIE DSGVO-COMPLIANCE FÜR ENDPUNKT- UND MOBILE DATEN

Die Umsetzung der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union (EU) gilt für alle globalen Organisationen, die personenbezogene Daten von EU-Datensubjekten verarbeiten. Im Bezug auf Ihre Endpunkt- und mobile Umgebung sollten Sie folgende Fragen sicher beantworten können:

- Wo werden Daten gespeichert
- Werden Daten sicher gespeichert
- Werden sie in Übereinstimmung mit den Vorschriften und Bestimmungen gespeichert
- Verbleiben Ihre Unternehmensdaten im Land
- Wie wird der Datenschutz: für Endbenutzer gewährleistet

Es geht nicht mehr nur um Ihre Sicherheit. Sie betrifft auch Ihre Mitarbeiter, Partner und Kunden. Handeln Sie also überlegt.



Datensicherung (Containment): Stellen Sie sicher, dass Ihr Anbieter Sicherheitsmechanismen anbietet, die es ermöglichen, Daten auf einem Gerät, statt auf Servern, zu speichern, und verhindern, dass interne Teams des Anbieters Einblick in die Daten nehmen können. Darüber hinaus ist sicherzustellen, dass personenbezogene Daten, die dort gespeichert werden, im Umfang auf den tatsächlichen Bedarf beschränkt sind, darunter Name, Anschrift und Telefonnummern.



Datenverschlüsselung: Achten Sie darauf, dass Ihr Anbieter die AES-256 CTR Verschlüsselungsalgorithmen zur Verschlüsselung aller Anwendungs- (App-) Daten in Bewegung und in Ruhe nutzt. Achten Sie beim Apple iOS auf die integrierte CommonCrypto FIPS 140-2-konforme Verschlüsselung; bei Google Android achten Sie auf SQLCipher mit OpenSSL (AES-256) FIPS 140-2-konformen Crypto-Modulen. Dies sorgt für eine umfassende Verschlüsselung der Datenbanken, nicht nur ihrer Inhalte.



Lokale Präsenz: Zweck der DSGVO-Anforderungen ist es, dass alle Daten, mit denen Ihre Organisation in Berührung kommt, sicher sind. Wählen Sie eine Lösung, deren Rechenzentren kontextabhängig gestaltet sind und regionale Bestimmungen beachten. Auf diese Weise können Kunden und Endbenutzer die Flexibilität ihrer globalen mobilen Datenübertragung ausweiten.



Kognitive Erkenntnisse und Analysen: Der Einsatz erweiterter Intelligenz, um zu sehen, was passiert, was passieren kann und was getan werden sollte, kann, immer unter Berücksichtigung der eigenen Umgebung, dazu beitragen, gesetzliche Compliance-Bestimmungen proaktiv zu realisieren. Ein umfangreicher Kontext Ihrer Endpunkt- und mobilen Daten kann Entscheidungsfindungsprozesse verbessern und IT- und Sicherheitsverantwortlichen bei der Umsetzung der DSGVO-Compliance helfen.



Unified Endpoint Management (UEM): Eine UEM-Lösung mit robuster Unterstützung für herkömmliche und innovative Endpunkt- und mobile Plattformen kann die Anpassung an die DSGVO-Anforderungen erleichtern. Die Auswahl einer Cloud-basierten Plattform mit direkter Unterstützung der jeweils neuesten Betriebssystemversions-Updates sorgt für solide Sicherheit Ihrer Datenbanken.

Unterstützung gesetzlicher Bestimmungen durch einen Branchenführer

► **IBM® MaaS360® mit Watson™ kognitives UEM** bietet ein Fenster zur Verwaltung und Sicherung Ihrer mobilen Geräte, Laptops und Desktops, einschließlich ihrer Nutzer, Apps, Inhalte und Daten. MaaS360 unterstützt Ihre DSGVO-Compliance-Ziele mit Merkmalen wie Containment, kognitive Erkenntnisse und kontextbezogene Analysen.

► **MaaS360 Kunden sind** in den USA geschützt durch Gesetze wie den Federal Information Security Management Act (FISMA) und das Federal Risk and Authorization Management Program (FedRAMP) – zusätzlich zu ISO 27001, AICPA SOC 2 Type II und die FIPS 140-2 Datenverschlüsselungsstandards.

IBM MaaS360 | mit Watson

Wir unterstützen Organisationen bei der Einhaltung der globalen Datenschutzanforderungen

MaaS360 prüft die zentralen DSGVO-Anforderungen von Endpunkt- und mobilen Daten und ist so der optimale UEM-Partner für Organisationen, die ihre Compliance vorbereiten.

Merkmale und Funktionalitäten	MaaS360
Lokale Datenspeicherungseinheit, die den Umfang der personenbezogene Daten auf den tatsächlichen Bedarf beschränkt	✓
Übergreifende Verwaltung für mobile Geräte und Laptops mit UEM	✓
Kontextbezogene Erkenntnisse/Analysen	✓
Volle Verschlüsselung inaktiver und aktiver Daten	✓
Möglichkeit zur Entfernung von personenbezogenen Daten auf Wunsch	✓
Möglichkeit der Datencontroller, eine elektronische Kopie der erfassten Daten eines Benutzers auf Wunsch bereitzustellen	✓
Verfügbarkeit vollständiger Data Maps für Kunden	✓
Benutzerzustimmung durch Annahme von Servicevereinbarungen und Endbenutzerlizenzvereinbarungen	✓
Bestehende Datensubjektzugriffs- und berichtigungsverfahren	✓
Bestehende Datenverletzungsmaßnahmen- und -benachrichtigungsprotokolle	✓
Einbeziehung des Datenschutzes in Produkte und Verfahren ab der Entwicklungsphase	✓
Ernennung eines Datenschutzbeauftragten	✓
Auditkompetenzen und -verfahren zur Unterstützung der Datenschutzbehörden (DPA)	✓

IBM MaaS360 | mit Watson

WEITERE INFORMATIONEN. Erfahren Sie, wie MaaS360 Ihre Ziele bei der Umsetzung der DSGVO unterstützt.

Testen Sie 30 Tage kostenlos AB SOFORT.

Kunden sind selbst dafür verantwortlich, alle für sie gültigen Gesetze und Vorschriften einzuhalten. Dazu gehört unter anderem die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union. Kunden müssen sich hinsichtlich der Ermittlung und Interpretation geltender Gesetze und Vorschriften, die die Geschäfte des Unternehmens betreffen, auf eigenen Antrieb hin rechtlich beraten lassen – auch hinsichtlich der Maßnahmen, die sie ergreifen müssen, um alle Gesetze und Vorschriften einzuhalten. Die hierin beschriebenen Produkte, Dienstleistungen und anderen Funktionen eignen sich nicht für alle Kundensituationen und sind möglicherweise nur eingeschränkt verfügbar. IBM bietet weder rechtliche, buchhalterische noch revisionsbezogene Beratung an. Des Weiteren übernimmt IBM keine Garantie dafür, dass die von IBM bereitgestellten Services oder Produkte die Einhaltung gesetzlicher Bestimmungen oder Vorschriften durch den Kunden sicherstellen.

Informieren Sie sich [hier](#) über IBMs eigenen Weg in Sachen GDPR-Bereitschaft und lernen Sie unsere GDPR-Funktionen und Angebote kennen, mit denen wir Ihren Compliance-Pfad unterstützen.

