MAXXYS

EU DSGVO

LÖSUNGSBOX

Die Box

Kompetenz durch Erfahrung
Wir begeistern durch Know-how im Bereich Softwareintegration. Nach einer umfassenden Analyse Ihres Unternehmens in Bezug auf die Einführung der DSGVO, unterstützen wir Sie bei der Auswahl und Implementierung der richtigen Softwarelösungen.
Die MAXXYS DSGVO Lösungsbox enthält ingesamt 10 Module. Sie können, ganz nach dem ermittelten Bedarf, die für Sie relevanten Module auswählen und individuell zusammenstellen.

Die MAXXYS AG

Seit unserer Gründung im Jahr 2002 sind wir Spezialisten für Software Systemintegration und IT-Softwaremanagement mit Sitz in Wetzlar. Wir bieten eine umfassende Analyse Ihrer IT-Infrastruktur, kundenorientiertes Consulting und Customizing an, sowie die Implementierung von IT-Software und die Inbetriebnahme und Pflege der IT-Infrastrukturen und Systeme. Als unabhängiger Systemintegrator vertreiben wir Softwareprodukte und Managementsysteme verschiedener führender Hersteller. Wir passen diese individuell an oder erweitern sie – so integrieren wir die Systeme optimal in die IT-Infrastruktur Ihres Unternehmens. Dabei greifen wir auf die langjährige Erfahrung und Expertise unserer Mitarbeiter zurück. Zu unseren Kunden zählen mittlere und größere Unternehmen aus der Industrie und dem Handel, sowie Banken, Versicherungen und öffentliche Verwaltungen.

Inhalt

Die Einführung der EU Datenschutz-Grundverordnung verunsichert viele Unternehmen und stellt sie vor große Herausforderungen.
Mit unserem ganzheitlichen Beratungskonzept, der MAXXYS DSGVO Lösungsbox, helfen wir Ihnen diese Herausforderungen zu managen.

Folgende Anforderungen der EU DSGVO gilt es umzusetzen:

Die Verarbeitung personenbezogener Daten sollte rechtmäßig und für die betroffene Person auf nachvollziehbare Weise verarbeitet werden: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz.

- Rechenschaftspflicht und Anzeigepflicht bei Datenschutzverstößen
- Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- Führen eines Verzeichnisses von allen Verarbeitungstätigkeiten
- Dokumentation der implementierten Prozesse
- Management von Zugriffskontrollen nicht ausschließlich von privilegierten Anwendern
- Verarbeitung von Testdaten in Ihrem Software-Lebenszyklus

Zur Umsetzung der EU-DSGVO benötigen Sie einen durchgängigen Prozess; unterstützt durch die Zusammenarbeit mit a.) einem rechtlichen Berater, b.) einem Datenschutzbeauftragten und c.) IT-Spezialisten.

Prozess zur Umsetzung EU DSGVO

- **Detaillierte Untersuchung, welche Bereiche der Unternehmensstruktur, -prozesse mit der neuen EU DSGVO übereinstimmen**
  - Aufdecken von Lücken
- **Identifikation von persönlichen Daten und Umgang mit diesen**
  - Wo sind diese überall gespeichert und welchem Zweck dienen sie (Werbung, Kunde, Support...)
  - Wer hat Zugriff auf diese Verzeichnisse (Zugriffkontrollen)
  - Wie erfolgt die Verarbeitung (Anonymisierung, Pseudonymisierung)
  - Datenportabilität
  - Recht auf Vergessenwerden und Löschung
- **Umsetzung zum Schutz der Daten und Berückigsichtigung im Reporting**
- **Auswahl der richtigen Security Lösungen, um in der Lage zu sein**
  - Sicherheitsrichtlinien durchzusetzen
  - Die Einhaltung von Vorschriften zu gewährleisten
  - Den Schutz sämtlicher IT-Ressourcen zu ermöglichen

DSGVO Artikel

Rechenschaftspflicht bei der Verarbeitung personenbezogener Daten
DSGVO Artikel 5, 24, 30

- Einholen der Einwilligung der betroffenen Person für bestimmte Datenverarbeitungstätigkeiten
- Nachvollziehbare Verarbeitung personenbezogener Daten
- Verarbeiten der Daten beschränkt auf den Zweck der Erhebung
- Löschung bzw. Berichtigung von personenbezogenen Daten, die im Hinblick auf den Zweck ihrer Verarbeitung unrichtig sind
- Zeitliche Aufbewahrung der Daten nur so lange, wie es für die Zwecke der Verarbeitung erforderlich ist
- Umsetzung geeigneter Datenschutzrichtlinien und -prozesse
- Benennen eines Verantwortlichen, welcher für die Verarbeitung zuständig ist; gegebenenfalls Benennen eines Datenschutzbeauftragten
- Führen eines Verzeichnisses aller Verarbeitungstätigkeiten

Rechte betroffener Personen DSGVO Artikel 4, 15, 16, 17, 18, 20, 21, 87, 88

- Auskunftsrecht zu personenbezogenen Daten
- Berichtigen, Löschen („Recht auf Vergessenwerden“) und Einschränken der Verarbeitung
- Recht auf Datenübertragbarkeit und Berichtigung
- Einlegen von Widerspruch gegen die Verwendung der Daten
- Gewährleistet den Schutz der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Daten im Beschäftigungskontext

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen DSGVO Artikel 25, 35

- Die Maßnahmen sind dafür ausgelegt, Datenschutzgrundsätze wie die Datenminimierung und die Pseudonymisierung wirksam umzusetzen und die notwendigen Garantien (Schutzmaßnahmen) in die Verarbeitung aufzunehmen (privacy by design)
- Personenbezogene Daten werden durch Voreinstellungen standardmäßig privatisiert und können nur durch das Eingreifen der betroffenen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden (privacy by default)

Anforderungen

Eine Übersicht grundlegender Artikel der neuen EU DSGVO.
Diese Anforderungen gilt es einzuführen und umzusetzen.

Meldung von Datenschutzverletzungen DSGVO Artikel 33, 34

- Die Aufsichtsbehörde ist binnen 72 Stunden zu informieren
- Der Auftragsverarbeiter meldet die Verletzung unverzüglich dem Verantwortlichen
- Die betroffene Person ist unverzüglich über die Datenschutzverletzung zu informieren (hiervon gelten einige Ausnahmen)

Anonymisierung und Pseudonymisierung DSGVO Artikel 25, 89

- Entsprechend den Grundsätzen zum „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ bei der Verarbeitung personenbezogener Daten
- Betrifft Daten bzw. deren Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

Grenzüberschreitende Datenübertragungen und verbindliche unternehmensinterne Datenschutzvorschriften DSGVO Artikel 42, 44, 45, 47, 49

- In Länder außerhalb des Europäischen Wirtschaftsraums (EWR), die kein „angemessenes Schutzniveau“ gewährleisten
- Verbindliche unternehmensinterne Datenschutzvorschriften und Standardvertragsklauseln (oder Modellklauseln), die von der Europäischen Kommission ausgegeben wurden, bleiben gültige Instrumente, um die Einschränkungen der EU für die Datenübertragung einzuhalten

Zertifizierungen, Verhaltenskodizes und Siegel DSGVO Artikel 40, 42

- Unternehmen können Zertifizierungsverfahren nutzen, um nachzuweisen, dass sie bestimmte Garantien bieten und entsprechende Vorschriften einhalten

IDS CA Identity Suite

Die CA Identity Suite (IDS) deckt folgende Anforderungen der DSGVO ab:

Anforderungen	DSGVO Artikel
Rechenschaftspflicht bei der Verarbeitung personenbezogener Daten	5, 24, 30
Rechte betroffener Personen	4, 15, 16, 17, 18, 20, 21, 87, 88
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen	25, 35
Meldung von Datenschutzverletzungen	33, 34
Anonymisierung und Pseudonymisierung	25, 89
Grenzüberschreitende Datenübertragungen und verbindliche Unternehmensinterne Datenschutzvorschriften	42, 44, 45, 47, 49
Zertifizierungen, Verhaltenscodies und Siegel	40, 42

Leistungen

IDS

Die CA Identity Suite kombiniert CA Identity Manager und CA Identity Governance mit einer einfachen, intuitiven unternehmensorientierten Oberfläche dem CA Identity Portal.

Identity Manager

- Identitätsverwaltung
- Provisionierung/Deprovisionierung, Anwender-Self-Service
- Auditing und Reporting im Hinblick auf die Compliance Unterstützung bei der Einführung einheitlicher Security-Richtlinien für Identitäten => Richtlinienmanagement
- Die Vereinfachung der Compliance und die Automatisierung wichtiger Prozesse => Workflow Management

Identity Governance

- Nutzt Analysefunktionen und Workflows, um Prozesse der Identity Governance zu automatisieren
- Bereinigung von Berechtigungen, Zertifizierungen, Aufgabentrennungen und Rollenmanagement
- Durch die Automatisierung dieser Prozesse und Steuermechanismen werden Risiken gesenkt, die Compliance verbessert und die Unternehmenseffizienz gesteigert => Richtlinienerzwingung
- Zertifizierungskampagnen für Datenschutzbeauftragte

Identity Portal

- Über einen intuitiven „Einkaufswagen“ werden die Zugriffe für Anwender in Unternehmen beträchtlich vereinfacht
- Die Anwender können bequem, die für ihre Arbeit erforderlichen Rollen und Berechtigungen auswählen, aktuelle Zugriffsberechtigungen anzeigen und den Status früherer Anforderungen überprüfen
- Die Risikoanalyse und Zertifizierungsprozesse werden automatisiert
- Vorbeugende Richtlinienerzwingung, Audit-Performance und Risikomanagement
- Die Mobile Device Oberfläche bietet ein vollständiges Branding sowie ein Launchpad für Webanwendungen und APP Anwendungen

PAM CA Privileged Access Management Suite

mit Threat Analytics for PAM (TAP)

Das CA Privileged Access Management (PAM) deckt folgende Anforderungen der DSGVO ab:

Anforderungen	DSGVO Artikel
Rechte betroffener Personen	4, 15, 16, 17, 18, 20, 21, 87, 88
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen	25, 35
Meldung von Datenschutzverletzungen	33, 34
Anonymisierung und Pseudonymisierung	25, 89

CA Threat Analytics for PAM deckt folgende Anforderungen der DSGVO ab:

Anforderungen	DSGVO Artikel
Meldung von Datenschutzverletzungen	33, 34

Leistungen

PAM Privileged Access Management ermöglicht den Schutz sämtlicher IT-Ressourcen, gewährleistet die Einhaltung von Vorschriften und minimiert die Kosten.

TAP Mit Threat Analytics wird das Zugriffsverhalten privilegierter Identitäten analysiert. Auf diese Weise können Datenschutzverletzungen im Sinne der DSGVO proaktiv erkannt werden und verhindert.

CA Privileged Access Management

- Transparenz und Management von Zugriffen nicht nur privilegierter Accounts
- Passwortmanagement und Session-Aufzeichnung
- Kontrolle der Aktivitäten privilegierter Nutzer für Compliance-Zwecke

CA Threat Analytics for PAM

- Erstellung von Nutzungsprofilen nicht nur für privilegierte Anwender auf Basis des beobachteten Verhaltens
- Erkennen von Abweichungen in der Nutzung und bei verdächtigem Verhalten
- Proaktive Erkennung von Datenschutzverletzungen durch Analyse des Zugriffsverhaltens privilegierter Identitäten

DLS DriveLock Suiten

DriveLock Suiten decken folgende Anforderungen der DSGVO ab:

Anforderungen	DSGVO Artikel
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen	25, 35
Meldung von Datenschutzverletzungen	33, 34

Leistungen

DLS

DriveLock ermöglicht u.a. die Verschlüsselung von Daten auf Wechseldatenträgern, internen Festplatten oder Dateien. Auf diese Weise kann der unbefugte Zugriff durch Dritte unterbunden werden.

Standard

Reporting & Forensik:
- Identifizierung und Vorbeugung aller Schwachstellen und Gefahrenstellen
- Abschließende Analyse aller Aktivitäten in Ihrem IT-Umfeld

Encryption-2-Go:
- Flexible Verschlüsselung externer Wechseldatenträger (z. B. USB-Sticks) per Container- oder Datei/Ordner-Verschlüsselung

Device Control:
- Umsetzung von Unternehmensrichtlinien für den Gebrauch aller Schnittstellen am Gerät (z.B. USB, Bluetooth)
- Überwachung aller Zugriffe externer Geräte oder Wechseldatenträger

Security Awareness:
- Identifizierung aller Schwachstellen und Gefahrenstellen
- Abschließende Analyse aller Aktivitäten in Ihrem IT-Umfeld

Premium

Standard Suite
+
Application Control
- Nicht genehmigte Programme werden gestoppt, bevor sie Schaden anrichten können
- Festgelegte Regeln bleiben nach Software Upgrades bestehen

Inventory

Executive

Standard und Premium Suite
+
Disk Protection
- Unabhängige Festplattenverschlüsselung für integrierte Festplatten mit Betriebssystem
- Von Bitlocker unabhängige eigene Verschlüsselung mit Pre-Boot-Authentication

UDP Arcserve Unified Data Protection und Archiverung

Arcserve Unified Data Protection und Archivierung deckt folgende Anforderungen der DSGVO ab:

Anforderungen	DSGVO Artikel
Rechte betroffener Personen	4, 15, 16, 17, 18, 20, 21, 87, 88
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen	25, 35

Leistungen

UDP

Arcserve UDP unterstützt durch regelmäßige Datensicherungen, Wiederherstellungstests und Reports. Diese Standard Reports belegen welche Datensicherungen laufen und welche Daten wie und wo gesichert werden.

Unified Data Protection

- Verschlüsselung schützt die Kopien der Datensicherung und entsprechend die Daten nach DSGVO Vorgaben
- Flexible Wiederherstellungsoptionen ermöglichen eine Verwaltung der Datensicherungen
- Vorbehaltungsoptionen unterstützen eine langfristige und gesetzeskonforme Aufbewahrung sowie rechtlich unbedenkliche Content-Entsorgung
- Optionen zum Testen, Messen und Reporten von Wiederherstellungsprozessen zur Einhaltung der DSGVO Vorgaben

Unified Data Protection Archivierung

- Diese Technologie zur E-Mail Archivierung stellt sämtliche Funktionen bereit um die Archivierung von E-Mails DSGVO-konform zu gestalten
- Arcserve UDP Archivierung ist eine speziell entwickelte Lösung zur regulierungskonformen E-Mailarchivierung und stellt diverse Funktionen bereit, um schnell auf die DSGVO Anforderungen reagieren zu können
- Sie unterstützt eine mandantenfähige Architektur und ermöglicht daher multinationalen und dezentralisierten Unternehmen die Suche nach E-Mails per Standort, Bereich oder Abteilung.
- Für den Fall, dass eine Person seine Einwilligung zurückzieht, verfügen Administratoren über integrierte eDiscovery Optionen um rasch nach allen empfangenen und versandten E-Mails dieser Person zu suchen, identifizieren und sie zu löschen.
- Administratoren haben Zugriff auf detaillierte Archivierungsprotokolle die sämtliche Aktionen belegen und als Beweis der Löschung dienen. Diese Protokolle widersprechen nicht den Konformationsanforderungen der DSGVO - auch wenn es dazu keine eindeutige Angaben gibt

IMPRESSUM

MAXXYS AG
Frankfurter Straße 76
35578 Wetzlar

Fon: +49 (0) 64 41 / 2 10 04 - 0
Fax: +49 (0) 64 41 / 2 10 04 - 20

info@maxxys.de
www.maxxys.de

Vorstand
Bernhard Bock

Handelsregister
Amtsgericht Wetzlar
HRB 2551
USt. ID Nr. DE 221 290 739