

Der Pfad zur DSGVO-Konformität

Erfahren Sie, wie Ihre Sicherheitslösungen zum Schutz der Daten von EU-Bürgern beitragen können.



Was ist die DSGVO?

Bei der Datenschutz-Grundverordnung (DSGVO) handelt es sich um einen Satz an Vorschriften, mit denen geregelt wird, wie Organisationen personenbezogene Daten von Bürgern der Europäischen Union (EU) erfassen, nutzen und freigeben. Die DSGVO verleiht nicht nur Einzelpersonen mehr Kontrolle über ihre Daten, sondern gilt auch international für alle Organisationen, die Daten von EU-Bürgern verarbeiten, und sieht bei Verstößen hohe Geldstrafen vor. Mittlerweile nutzen auch viele andere staatliche Stellen die DSGVO als Maßstab für die Einführung eigener strenger Datenschutzgesetze.



20 Mio. €

oder 4 % des Jahresumsatzes, je nachdem, welcher Betrag höher ist, können bei Nichteinhaltung der Datenschutzbestimmungen anfällig sein.

2.000+

Bußgelder wurden seit Mai 2018 von DSGVO-Aufsichtsbehörden gegen Organisationen verhängt, was einem Gesamtbetrag von 4,48 Milliarden Euro entspricht.

73 %

der Benutzer von physischen Sicherheitslösungen waren 2024 von Vorschriften zum Schutz personenbezogener Daten, zur Wahrung der Privatsphäre und zur Gewährleistung der Cyber-Resilienz betroffen.

Wie sind Sie von der DSGVO betroffen?

Personenbezogene Daten im Bereich der physischen Sicherheit

Wahrscheinlich erfasst Ihre Organisation täglich personenbezogene Daten von EU-Bürgern. Dabei handelt es sich um Daten, die direkt oder indirekt Rückschlüsse auf die Identität einer Person zulassen. Von physischen Sicherheitssystemen werden unter anderem folgende personenbezogene Daten erfasst:

- Von Überwachungskameras erfasste Videos von Personen
- Informationen zu Karteninhabern und von Zutrittskontrollsystemen verfolgte Aktivitäten
- Von einer automatischen Nummernschilderkennung erfasste Kfz-Kennzeichen

Grundlagen der DSGVO

Nach der DSGVO muss Ihre Organisation die Rechte Einzelner in Bezug auf personenbezogene Daten wahren. Darüber hinaus müssen Sie Mindestanforderungen an Cybersicherheit, Datenverarbeitung und die Meldung von Datenschutzverletzungen erfüllen. Nachfolgend finden Sie einige grundlegende Richtlinien:

- Sorgen Sie für vollständige Transparenz, indem Sie über die Erhebung von Daten informieren und Ihre Datenschutzerklärung öffentlich machen.
- Sofern die Verarbeitung nicht aus anderen Gründen gerechtfertigt ist, holen Sie vor der Erhebung personenbezogener Daten die gültige und ausdrückliche Einwilligung der betroffenen Personen ein.
- Speichern Sie personenbezogene Daten nur für den erforderlichen Zeitraum.
- Löschen Sie personenbezogene Daten auf Anfrage der betroffenen Person unverzüglich, sofern gesetzlich nichts anderes vorgeschrieben ist.
- Stellen Sie den betroffenen Personen gegebenenfalls ihre personenbezogenen Daten in einem gebräuchlichen Format zur Verfügung.
- Delegieren Sie den Zugriff auf personenbezogene Daten, insbesondere auf Videos, an bestimmte Personen bzw. beschränken Sie diesen.
- Anonymisieren und redigieren Sie Videoinhalte, um Identitäten beim Austausch von Informationen zu schützen.
- Verwenden Sie verschiedene Verschlüsselungsmethoden zum Schutz personenbezogener Daten, auch in Videos und Kommunikationsmitteln.

- Dokumentieren Sie, wer wann auf personenbezogene Daten zugreift.
- Informieren Sie Behörden und gegebenenfalls Nutzer innerhalb von 72 Stunden über Verstöße im Zusammenhang mit personenbezogenen Daten.

Festlegung von Rollen und Verantwortlichkeiten

Alle Organisationen, die Daten von EU-Bürgern erheben oder verarbeiten, unterliegen der DSGVO. Ihre Organisation ist nicht nur für die Einhaltung dieser DSGVO-Vorgaben verantwortlich. Sie müssen auch sicherstellen, dass alle Ihre Partner, die Zugriff auf Ihre Daten haben, diese ebenfalls einhalten.

Datenverantwortliche

Jede Organisation, die entscheidet, welche personenbezogenen Daten zu welchem Zweck erhoben und auf welche Weise verarbeitet werden, beispielsweise ein Unternehmen, das Informationen zu Karteninhabern erfasst oder Videos aufzeichnet. Verantwortlichkeiten:

- Sicherheitsüberprüfung der Vertriebspartner und Lieferanten, mit denen Sie zusammenarbeiten
- Kontrolle darüber, auf welche Daten Ihre Partner Zugriff haben
- Beurteilung der Art und Weise, wie Ihre Partner Daten verwalten, speichern und schützen
- Gewährleistung, dass Ihre Partner Best Practices einhalten und ihren Verpflichtungen nachkommen

Auftragsverarbeiter

Jede Organisation, die personenbezogene Daten im Auftrag von Datenverantwortlichen verarbeitet, beispielsweise Cloud-Dienstleister oder Unternehmen, die Sicherheitssysteme hosten. Verantwortlichkeiten:

- Rechenschaftspflicht für technologische Leistungen und andere Verpflichtungen
- Wahrung der Transparenz beim Umgang mit personenbezogenen Daten und deren Schutz
- Übernahme der Verantwortung für alle eigenen Handlungen (einschließlich der ihrer jeweiligen Lieferanten), die sich auf Ihr Unternehmen auswirken können

Wie können Ihre physischen Sicherheitslösungen helfen?

① Sichere Weitergabe personenbezogener Daten auf Anfrage

Unter der DSGVO haben Personen gegebenenfalls das Recht, eine Kopie der personenbezogenen Daten anzufordern, die Ihr Unternehmen über sie gespeichert hat. Mit Genetec Clearance™, der Plattform für das digitale Beweismanagement, können Sie schnell auf solche Anfragen reagieren. Die Lösung bietet ein sicheres webbasiertes Portal, über das Sie Videos und andere personenbezogene Daten einfach erfassen und austauschen können. Die Empfänger erhalten einen Link zu der freigegebenen Datei und können das Video nur mit Ihrer Genehmigung ansehen.

Vorteile für Ihr Unternehmen:

- Der Einsatz unsicherer physischer Datenträger wie USB-Sticks und DVDs erübrigt sich.
- Über dasselbe Portal können Sie fallbezogene Dateien mit Prüfern oder Anwälten austauschen, wobei die Privatsphäre aller Beteiligten gewahrt bleibt.
- Durch End-to-End-Verschlüsselung und eine strenge Kennwortverwaltung wird die Sicherheit der freigegebenen Daten gewährleistet.

Verwaltung von Zugriffsanfragen mit Clearance

② Einschränkung des Zugriffs auf vertrauliche Daten von einem zentralen Ort aus

Gemäß der DSGVO müssen Systeme so konzipiert sein, dass die Erfassung, Aufbewahrung und Zugänglichkeit von personenbezogenen Daten begrenzt werden. Das Security Center ist eine zentralisierte Sicherheitsplattform, mit der Sie festlegen können, wer Zugriff auf personenbezogene Daten hat, insbesondere auf spezielle Kategorien personenbezogener Daten (in der Regel vertrauliche Daten), und wie lange Videos und personenbezogene Daten aufbewahrt werden. So können Sie verhindern, dass Unbefugte auf die im Sicherheitssystem übertragenen und gespeicherten Videos und personenbezogenen Daten zugreifen.

Vorteile für Ihr Unternehmen:

- Sie können Benutzerzugriff und Speicheranforderungen für alle Sicherheitsanwendungen an einem Ort verwalten.
- Die Datenintegrität und der Datenschutz werden durch Multi-Faktor-Authentifizierung und integrierten Kennwortschutz verbessert.

- Autorisierte Benutzer können Prüfprotokolle und Berichte erstellen, aus denen hervorgeht, wer auf Dateien zugegriffen hat.

So aktivieren Sie Cybersicherheitsfunktionen

③ Automatisierung des Datenschutzes bei Echtzeitvideos

Wenn eine Person in das Sichtfeld Ihrer Kamera tritt, werden deren Bild und damit auch deren personenbezogene Daten sofort erfasst. Das KiwiVision™-Modul Privacy Protector im Security Center sorgt in Live-Videos und Aufzeichnungen für eine automatische Anonymisierung von Personen. Durch die Speicherung einer sicheren Kopie des ursprünglichen Bildmaterials, die nur befugten Benutzern zugänglich ist, sorgen Sie gleichzeitig für den Schutz von Beweismitteln und Daten.

Vorteile für Ihr Unternehmen:

- Die Privatsphäre wird geschützt, während Nutzer dennoch sehen können, was geschieht.
- Bewegungen, Handlungen und Ereignisse bleiben in Live-Videos und Aufzeichnungen erkennbar.
- Autorisierte Nutzer können bei Bedarf auf die Originalvideodateien zugreifen.

Entdecken Sie die einzige Lösung mit EuroPriSe-Zertifizierung

④ Widerstandsfähigkeit gegen Cyberangriffe dank innovativer Tools

Die Umsetzung von Best Practices für Cybersicherheit ist für die Einhaltung der DSGVO unerlässlich. Daher sind starke Verschlüsselungsmethoden unabdingbar. Sie tragen dazu bei, Videos und personenbezogene Daten vor dem Zugriff unbefugter Nutzer zu schützen und die Kommunikation zwischen Clients und Servern zu sichern. Weitere integrierte Hardening-Tools warnen Sie vor Systemschwachstellen, vereinfachen kritische Updates und helfen Ihnen, Maßnahmen zur Verbesserung der Systemresilienz zu ergreifen.

Vorteile für Ihr Unternehmen:

- Sie genießen umfassenden Schutz auf allen Ebenen der Video- und Zutrittskontrollarchitektur.
- Sie profitieren von einem Höchstmaß an End-to-End-Verschlüsselung für Widerstandsfähigkeit gegen Cyberangriffe.
- Ihr System ist zu jeder Zeit optimiert, sicher und auf dem neuesten Stand.

Weitere Informationen zu sicherer Zutrittskontrolle

⑤ Erweiterung Ihrer Bereitstellung mit einer Hybrid-Cloud

Durch Investitionen in cloudbasierte Lösungen können viele Cybersicherheitsaufgaben automatisiert werden. Wenn Sie sich beispielsweise für eine Lösung mit physischer Sicherheit als Service (PSaaS) entscheiden, werden die neuesten Versionen und Fehlerbehebungen automatisch auf Ihr System übertragen. Außerdem erhalten Sie Zugriff auf Cybersicherheits- und Datenschutzfunktionen, sobald diese verfügbar sind.

Vorteile für Ihr Unternehmen:

- Sie können den Zustand Ihrer Systeme und Datenschutzkontrollen von jedem beliebigen Standort aus fernüberwachen.
- Ihre Systeme für physische Sicherheit sind immer auf dem neuesten Stand und geschützt.
- Ihre IT- und Sicherheitsteams werden von der Belastung durch ständige Wartung und Absicherung befreit.

Vorteile einer allumfänglichen Hybrid-Cloud mit SaaS



Was bedeutet es, in integrierten Datenschutz bzw. „Privacy by Design“ zu investieren?

Die Datenschutz-Grundverordnung (DSGVO) verpflichtet Organisationen zur Einhaltung strenger Datenschutzvorgaben und sieht bei Verstößen Geldbußen vor. Der Schutz der von Ihnen erfassten personenbezogenen Daten vor unautorisiertem Zugriff ist daher ein zentraler Bestandteil der Compliance. Ebenso entscheidend ist die Auswahl von Technologiepartnern, die Ihre datenschutzrechtlichen Standards und Werte konsequent mittragen. Genetec entwickelt physische Sicherheitslösungen mit einem klaren Fokus auf Datenschutz und Informationssicherheit. Unser „Privacy by Design“-Ansatz stellt sicher, dass regulatorische Anforderungen nicht nur erfüllt, sondern proaktiv berücksichtigt werden – und unterstützt Sie dabei, das Vertrauen von Kunden, Mitarbeitenden und weiteren Stakeholdern nachhaltig zu stärken.

Unser Ansatz zum Datenschutz:

- Wir verpflichten uns, sichere und konforme Lösungen zu entwickeln, damit Sie Ihre Organisation vor physischen Bedrohungen und Cyberangriffen schützen können.
- Wir bieten integrierte Tools und Services, mit denen Sie höchste Datenschutz- und Sicherheitsstandards erreichen und aufrechterhalten können.
- Ein Spezialteam für Cybersicherheit ermittelt in aktiver Kooperation mit Branchenexperten neue Schwachstellen und kann zügig Gegenmaßnahmen einleiten.
- Unser Managementsystem zur Informationssicherheit (Information Security Management System, ISMS) wurde geprüft und entspricht den Anforderungen verschiedener Standards von Behörden und Branchen.
- Wir kommunizieren offen und transparent und arbeiten bei der Produktentwicklung und entlang der gesamten Lieferkette ausschließlich mit vertrauenswürdigen Partnern zusammen.

Aspekte des integrierten Datenschutzes:

- ✓ Verschlüsselte Übertragung und Speicherung von Videos und allen Systemdaten
- ✓ Integrierte Authentifizierung zum Schutz Ihrer Videos und anderer Daten vor unbefugtem Zugriff
- ✓ Kontrolle der Benutzeraktivitäten durch umfassendes Autorisierungsmanagement auf Einzelpersonen- und Gruppenbasis

Wir gehen noch einen Schritt weiter:

Vertrauenswürdige Lösungen – Wir halten zahlreiche Cybersicherheitszertifizierungen, darunter ISO/IEC 27001, ISO/IEC 27017, SOC 2 Typ II und weitere.

Sichere und zuverlässige Integrationen – Unser Ökosystem aus Technologiepartnern basiert auf Vertrauen und Transparenz. Wir legen größten Wert auf Sicherheit und Datenschutz bei den Organisationen, mit denen wir zusammenarbeiten.

Verantwortungsbewusster Einsatz künstlicher Intelligenz – Für unsere Entwickler stehen Datenschutz, Data Governance, Transparenz, Sicherheit und menschliche Kontrolle an erster Stelle, um Verzerrungen zu minimieren und fundierte Entscheidungen zu treffen.

Durchgängige Transparenz – Wir lassen unsere Produkte regelmäßig von externen Unternehmen auf Sicherheitslücken prüfen und veröffentlichen die Ergebnisse. Außerdem verfolgen wir ein strenges Programm zum Schwachstellenmanagement.

Weitere Informationen zu unseren Konzepten im Bereich Cybersicherheit und Datenschutz finden Sie im Trust Center.

DSGVO und Videoüberwachung

Zertifizierungen im Bereich Cybersicherheit

Datenschutz und Privatsphäre