EKRAN®

VERWENDUNG VON EKRAN SYSTEM ZUR GEWÄHRLEISTUNG DER DSGVO-COMPLIANCE

Verwendung von Ekran System zur Gewährleistung der DSGVO-Compliance

Die **Datenschutz-Grundverordnung (DSGVO)**, die vom Europäischen Parlament und dem Rat verabschiedet wurde, zielt darauf ab, den Datenschutz in der EU zu vereinheitlichen und EU-Bürgern und Einwohnern mehr Macht über ihre personenbezogenen Daten zu geben.

Die DSGVO definiert Rechte für diejenigen, deren Daten erhoben werden **(betroffene Personen)**, und legt strenge Anforderungen an die Cybersicherheit für Unternehmen fest, die personenbezogene Daten von EU-Bürgern und Einwohnern der EU erheben und verarbeiten **(Datenverarbeiter und für die Verarbeitung Verantwortliche)**.

Wenn Ihr Unternehmen innerhalb der EU ansässig ist oder wenn es außerhalb der EU ansässig ist, aber Waren oder Dienstleistungen an EU-Bürger oder Einwohner der EU liefert, müssen Sie die DSGVO-Anforderungen erfüllen.

Ekran System ist eine Plattform zur Verwaltung von Insider-Bedrohungen, die den gesamten Zyklus abdeckt und Insider-Bedrohungen wirksam abwehrt, aufspürt und unterbricht. Dank seiner umfangreichen Funktionalität kann Ekran System helfen, verschiedene Anforderungen an die Einhaltung der Cybersicherheit zu erfüllen, einschließlich der in den **Artikeln 5, 24, 32, 33, 35 und 39 der DSGVO** festgelegten Anforderungen.

Artikel	Beschreibung	Wie Ekran System bei der Einhaltung unterstützt
Artikel 5 Grundsätze für die Verarbeitung personenbezogener Daten	1. Personenbezogene Daten müssen a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden	Robuste Überwachungsfunktionen zeigen Ihnen **genau, wie Benutzer Daten verarbeiten**. Mit Ekran System können Sie die Aktivitäten verschiedener Arten von Benutzern überwachen, darunter • Drittanbieter • Externe und interne Mitarbeiter • Reguläre und privilegierte Benutzer

	(„Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“); f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“); 2. Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).	Ekran System bietet darüber hinaus Zugriffskontrollfunktionen, einschließlich Zwei-Faktor-Authentifizierung und Einmalpasswörter, die **Ihre Systeme** zuverlässig **vor unberechtigtem Zugriff schützen** können. In der Zwischenzeit können Sie mithilfe der Sekundär-Authentifizierung genau wissen, wer sich bei einem gemeinsam genutzten Konto anmeldet. Als zusätzliche Sicherheitsebene verwendet Ekran System ein KI-gestütztes Modul zur Analyse des Benutzer- und Entitätsverhaltens (UEBA), um eine **sichere Datenverarbeitung** zu gewährleisten. Das UEBA-Modul erkennt anormale Aktivitäten und informiert sofort den Sicherheitsbeauftragten. Nutzen Sie die umfangreichen Berichtsfunktionen von Ekran System, um ein Protokoll zu erstellen und diesen als eindeutigen Nachweis für **die Einhaltung der DSGVO-Anforderungen** zu verwenden.
Artikel 24 Verantwortung des für die Verarbeitung Verantwortlichen	1. Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.	Mit Ekran System können die für die Datenverarbeitung Verantwortlichen mehrere **wesentliche technische Maßnahmen ergreifen um eine konforme und sichere Datenverarbeitung zu gewährleisten**: • Audio- und Videoaufzeichnung von Benutzersitzungen • Online- und Offline-Benutzerüberwachung • Kontrolle über alle an Unternehmenssysteme angeschlossenen Geräte Um Ihnen dabei zu helfen, **nachzuweisen, dass Sie Daten in**

	2. Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.	**Übereinstimmung mit der DSGVO verarbeiten**, bietet Ekran System ein vollständig manipulationssicheres Protokoll aller Benutzeraktionen innerhalb jeder überwachten Sitzung. Dieses Protokoll zeigt deutlich, wie sensible Daten verarbeitet wurden, während die Sekundär-Authentifizierung von Ekran System es Ihnen ermöglicht, jede Sitzung eindeutig einem bestimmten Benutzer zuzuordnen.
Artikel 32 Sicherheit der Verarbeitung	4. Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.	Damit Sie feststellen können, ob Benutzer **Daten gemäß Ihren Anweisungen verarbeiten**, bietet Ekran System einen vollständigen Überblick über alle Benutzeraktivitäten. • Erhalten Sie vollständige Video- und Audioaufzeichnungen von Benutzersitzungen • Beobachten Sie Benutzeraktivitäten online • Sammeln Sie alle Metadaten für Benutzersitzungen (gestartete Anwendungen, aktive Fenster, besuchte URLs, ausgeführte Befehle, angeschlossene Geräte, Tastenanschläge) Leistungsfähige Aufzeichnungsfilter ermöglichen es Ihnen, **Daten nur bei Bedarf aufzuzeichnen**. Wählen Sie Anwendungen, die aufgezeichnet werden sollen, oder erstellen Sie eine Liste von privaten/nicht-kritischen Anwendungen und URLs, die Sie nicht überwachen müssen. **Sichern Sie personenbezogene Daten** vor unsachgemäßer Verarbeitung und Diebstahl mit:

		• Überwachung, Steuerung und Blockierung von angeschlossenen USB-Geräten • Temporärer Zugriff auf sensible Daten nur für autorisierte Benutzer und aus triftigem Grund • Vordefinierte und benutzerdefinierte Regeln, um Sitzungen zu blockieren oder Warnungen an Benutzer zu senden, wenn verdächtige Aktivitäten entdeckt werden
Artikel 33 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde	1. Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. 2. Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich. [...] 5 Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation ermöglicht der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels.	Ekran System hilft Datenverarbeitern und für die Verarbeitung Verantwortlichen, **Datenverletzungen** und **Datenlecks** durch rechtmäßige Mitarbeiter und externe Täter, die gestohlene Zugangsdaten verwenden, **schnell zu erkennen**. 1. Profitieren Sie von anpassbaren Echtzeit-Warnmeldungen, die Sicherheitsbeauftragte über verdächtige Aktivitäten informieren und es ihnen ermöglichen, sofort zu reagieren. 2. Untersuchen Sie durchsuchbare Videoaufzeichnungen, um zu erfahren, was vor, während und nach einem Vorfall geschah, ohne dass IT-Spezialisten hinzugezogen oder technische Softwareprotokolle durchgesehen werden müssen. Ekran System kann **den für die Datenverarbeitung Verantwortlichen** auch **bei der Dokumentation von Verletzungen personenbezogener Daten** und der damit verbundenen Informationen **helfen**. • Nutzen Sie umfangreiche Reporting-Funktionalitäten, um mit wenigen Klicks individuelle Berichte zu erstellen

		• Dokumentieren Sie nur wesentliche Informationen • Erstellen Sie einen praktischen Zeitplan für den Erhalt regelmäßiger Berichte • Exportieren Sie Daten in einem geschützten Dateiformat für Untersuchungen und forensische Aktivitäten
Artikel 35 Datenschutz-Folgenabschätzung	1. Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.	Damit Sie **die Auswirkungen von Verarbeitungen** auf den Schutz personenbezogener Daten **umfassend beurteilen** können, bietet Ekran System tiefe Einblicke in die Art und Weise, wie und von wem auf die Daten zugegriffen wird. Entdecken Sie unsere **umfassenden Prüfungs-, Statistik- und Reporting-Funktionen** zur Analyse: • Welche Benutzer auf welche Daten zugreifen und wie oft • Wie Benutzer mit personenbezogenen Daten interagieren • Welche Anwendungen und Webseiten Benutzer besuchen • Wie sich die Benutzeraktivität im Laufe der Zeit verändert Anpassen der Warnhinweise zur Verfolgung Ihrer Anforderungen
Artikel 39 Aufgaben des Datenschutzbeauftragten	1. Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben: a) Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung	Ekran System unterstützt Datenschutzbeauftragte bei der **Aufklärung der Benutzer über sichere und gesetzeskonforme Datenverarbeitung** mit Warnungen, die durch vordefinierte und benutzerdefinierte Regeln ausgelöst werden. Benutzer können diese Warnungen erst nach einer angemessenen Verzögerung schließen,

	sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten; b) Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;	um sicherzustellen, dass sie ihre Handlungen bestätigt haben. Mit Ekran System können Sie **die Überwachung der Einhaltung erleichtern**: • Überwachung von Benutzersitzungen offline, falls die Netzwerkverbindung ausfällt • Extrahieren detaillierter Berichte über Benutzeraktivitäten • Erhalten von sofortigen Warnungen bei Sicherheitsvorfällen • Nachverfolgung des Zugriffs auf sensible Daten aus jedem System innerhalb Ihres Unternehmens • Verhinderung unsachgemäßer Datenverarbeitung mit dem UEBA-Modul

GET MORE DETAILS

Contact us

General inquiries: info@ekransystem.com
Partner program: partner@ekransystem.com

www.ekransystem.com

Ekran System®