EKRAN®

USING EKRAN SYSTEM TO ENSURE GDPR COMPLIANCE

Using Ekran System to Ensure GDPR Compliance

The **General Data Protection Regulation (GDPR)**, approved by the European Parliament and the Council, aims to unify data protections across the EU and give EU citizens and residents more power over their personal data.

The GDPR defines rights for those whose data is collected (data subjects) and sets strict cybersecurity requirements for companies that collect and process the personal data of EU citizens and residents (**data processors and controllers**).

If your company is located inside the EU or if it's located outside the EU but provides goods or services to EU citizens or residents, you must comply with GDPR requirements.

Ekran System is a full-cycle insider threat management platform that effectively deters, detects, and disrupts insider threats. Thanks to its extensive functionality, Ekran System can help you meet various cybersecurity compliance requirements, including those set forth in **GDPR Articles 5, 24, 32, 33, 35, and 39.**

Article	Description	How Ekran System helps you comply
Article 5 **Principles relating to processing of personal data**	1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'). (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').	Robust monitoring functionality shows you **exactly how users process data**. With Ekran System, you can monitor the activity of various types of users, including: • Third-party contractors • Remote and in-house employees • Regular and privileged users Ekran System also provides access control features, including two-factor authentication and one-time passwords, that can reliably **protect your systems from unauthorized access**. Meanwhile, secondary authentication lets you know exactly who logs in to a shared account.

	2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').	As an additional layer of security, Ekran System uses an AI-powered user and entity behavior analytics (UEBA) module to **make sure data is processed securely**. The UEBA module detects abnormal activity and immediately informs security officers. Leverage the extensive reporting functionality of Ekran System to gather an audit trail and use it as clear evidence to **demonstrate compliance with GDPR requirements**.
Article 24 **Responsibility of the controller**	1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. 2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.	With Ekran System, data controllers can take several **essential technical measures to ensure compliant and secure data processing**: • Audio and video recording of user sessions • Online and offline user monitoring • Control over all devices connected to corporate systems To help you **demonstrate that you process data in accordance with the GDPR**, Ekran System offers a full tamper-proof audit trail of all user actions within each monitored session. This audit trail clearly shows how sensitive data was processed, while the Ekran System secondary authentication feature allows you to clearly assign each session to a specific user.
Article 32 **Security of processing**	4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is	To help you identify whether users **process data according to your instructions**, Ekran System provides you with complete visibility of all user activity. • Get complete video and audio recordings of users' sessions • Watch user activity online

	required to do so by Union or Member State law.	• Collect all metadata for user sessions (launched applications, active windows, visited URLs, executed commands, connected devices, keystrokes) Powerful recording filters allow you to **record data only when necessary**. Choose applications to be recorded or create a list of private/non-critical apps and URLs you don't need to monitor. **Secure personal data** from inappropriate processing and theft with: • Monitoring, controlling, and blocking of connected USB devices • Temporary access to sensitive data only for authorized users and for a valid reason • Predefined and custom rules to block sessions or send warnings to users when suspicious activity is detected
Article 33 Notification of a personal data breach to the supervisory authority	1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. 2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach. [...] 5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial	Ekran System helps data processors and controllers **quickly detect data breaches** and leaks by legitimate employees and outside perpetrators using stolen credentials. 1. Benefit from customizable real-time alerts that notify security officers about suspicious activity and allow them to react immediately. 2. Explore searchable video records to know what happened before, during, and after an incident without the need to involve IT specialists or go over technical software logs. Ekran System can also **assist data controllers with documenting personal data breaches** and associated information.

	action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.	• Use extensive reporting functionality to create customized reports in a few clicks • Document only essential information • Set up a convenient schedule to receive regular reports • Export data in a protected file format for investigation and forensic activities
Article 35 **Data protection impact assessment**	1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.	To help you **fully assess the impact of processing operations** on the protection of personal data, Ekran System provides deep insights into how data is accessed and by whom. Explore our **comprehensive auditing, statistics, and reporting functionality to analyze**: • Which users access which data and how often • How users interact with personal data • What apps and sites users visit • How user activity changes over time Customize alert rules to track what you need.
Article 39 **Tasks of the data protection officer**	1. The data protection officer shall have at least the following tasks: (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data,	Ekran System helps data protection officers **educate users about secure and compliant data processing** with warnings that are triggered by predefined and custom rules. Users can close these warnings only after a reasonable delay to make sure they have acknowledged their actions. With Ekran System, you can **facilitate compliance monitoring**: • Monitoring user sessions offline in case the network connection goes down

	including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;	• Extracting detailed reports on user activity • Getting instant alerts on security incidents • Tracking access to sensitive data from every system within your organization • Preventing inappropriate data processing with the UEBA module

GET MORE DETAILS

Contact us

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

www.ekransystem.com

Ekran System®