What is the GDPR?

The **General Data Protection Regulation** (**GDPR**) is a new regulation approved by the European Parliament and the Council regarding the handling of personal data of European Union citizens; it takes effect on 25 May 2018.

The goal of the GDPR is to unify data protection regulations across the European Union and to give EU citizens more power over their own personal data. To this end, the GDPR introduces new rights for citizens whose data is being collected (data subjects) as well as stricter cyber security requirements for data processing for companies that process and use private data of EU citizens (data processors and controllers).

All companies located inside the European Union as well as companies located outside the European Union who provide goods and services to EU citizens are **affected by the GDPR** regardless of where data processing takes place.

What is Ekran System?

Ekran System is an insider threat protection solution focused on user activity monitoring. Ekran System provides a full tamper-proof audit trail of everything that happens on each individual endpoint, including recordings of users' screens and corresponding metadata.

Ekran System also features robust alerting functionality, incident response features, custom and scheduled reporting, and different access management features allowing you to protect data, detect and investigate incidents, and achieve compliance with data protection regulations.

How Ekran System can help you comply with GDPR

There are four main areas in which Ekran System can help you achieve compliance with GDPR:

- **Proof of compliance.** Ekran System provides a tamper-proof centralized audit trail that can serve as definitive proof that your organization is complying with GDPR regulations.
- **Control over data processing.** Ekran System provides complete visibility over who enters personal data into the system and when they enter it, when data is accessed, and where and when data is transferred. This allows you to fully control all operations with sensitive data within your system and reliably confirm that data has been processed in accordance with the law and has not been misused by employees.
- **Additional layer of protection for personal data.** Ekran System serves as a reliable deterrent to malicious insiders and also allows you to quickly detect incidents as well as stop incidents as they happen by manually blocking ongoing sessions. Built-in access management functionality protects data from unauthorized access.
- **Powerful detection and investigation tool.** Ekran System features robust customizable alerting that allows you to quickly detect incidents as soon as they happen. Gathered monitoring data allows you to conduct quick and detailed investigations of any incident within the 72-hour timeframe situplated by the GDPR and then report to regulators exactly what happened.

Detailed example of how Ekran System can help you meet specific GDPR requirements

GDPR 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').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

As an insider threat protection solution, Ekran System focuses on securing your data from theft or damage by malicious insiders as well as from accidental loss or leakage by inadvertent insiders. Ekran System deters insider attackers, allows you to quickly detect incidents, and provides basic response tools including blocking of ongoing sessions if suspicious activity is detected.

Ekran System also provides several access control features, including two-factor authentication, that can reliably protect your data from unauthorized access.

GDPR 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.

Ekran System provides 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 individual session to a specific user.

This allows you to clearly demonstrate that data is processed according to GDPR requirements.

GDPR 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 required to do so by Union or Member State law.

Ekran System provides you with complete visibility over all user activity within each individual session by conducting video recordings of users' screens as well as collecting all corresponding metadata, including names of open applications and active windows, visited URLs, entered Linux commands, and so on. Powerful recording filters allow you to make sure that data is recorded only when necessary.

The robust user activity monitoring capabilities of Ekran System allow you to ensure that your employees are not leaking or stealing personal data and that personal data is processed in full accordance with all laws and regulations.

GDPR 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 action taken**. That documentation shall enable the supervisory authority to verify compliance with this Article.

Featuring robust and heavily customizable alerting, Ekran System allows you to quickly detect data breaches and leaks by legitimate employees as well as outside perpetrators using stolen credentials. If a suspicious activity is detected within an ongoing session, the session can be viewed live and manually blocked if necessary, mitigating potential damage.

Complete searchable video and metadata recordings serve as a great investigation tool, allowing you to quickly see exactly what happened without the need to involve IT specialists or go over technical software logs.