Muninn & GDPR

Contact us

Data breach, malware and hacker groups are words you hear in the news each day. Due to the vast amount of sensitive data, we store online, every company and every person are being targeted. This has led to the introduction of the GDPR, an effort of the European Union to hold businesses accountable for data privacy and data protection.

All companies that hold EU personal data, regardless of the nation of origin, must disclose breaches. Failure to comply with these rules will result in a fine of up to 4% global turnover (or 20 million Euros). These fines may seem severe, but they help businesses understand the data they collect and the severity of data protection more. Complying with these rules creates much needed trust between customers, employees, and businesses.

State of the art cybersecurity

Utilizing advanced Machine Learning and AI technologies, Muninn is able to detect, report, and prevent a wide range of anomalies, security incidents, and compliance breaches, ensuring the implementation of best practices for your network security.

GDPR Requirement	How Muninn helps fulfill this
Article 25 Data protection by design and by default … "the state of the art"...	Muninn is specifically designed to ensure data security through its advanced threat detection and immediate response mechanism. Today leading security analysts strongly recommend state-of-the-art protection tools like Muninn AI Detect and Muninn AI Prevent. Our cutting-edge technology enables continuous, autonomous, and intelligent monitoring and protection around the clock.
Article 32 (1) ...the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk...	Through constant monitoring for abnormalities, detection of non-compliance and sub-standard connections, Muninn empowers you to maintain the highest security standards. Moreover, when combined with a strong security partner, Muninn functions as a continuous pen-testing tool in specific areas of your IT infrastructure, helping you to enhance the security of your network consistently.
Article 33 Notification of a personal data breach to the supervisory authority	To report incidents within 72 hours of detecting a breach, Muninn: • Stores searchable logs of all data events, increasing the speedof reporting incidents. • Immediately stops data breaches and prevents further harm. • Unlike many other solutions, such as SIEM and Log Management, it includes actual raw data, not just metadata. • Enhances the speed of identifying advanced persistent threats, preventing breaches from occurring. • Reduces the need to spend money on incident recovery, thereby helping to save costs.
Also see Recitals 85, 87 & 88 Dealing with the forensics and whether adequate tooling was in place	Muninn provides continuous monitoring for anomalies, breaches, and suspicious activities on a network, including IoT devices. Our features to ensure GDPR compliance include: • Detecting, logging, and blocking file-sharing activities. • BitTorrent logging and blocking. • Logging and blocking of IoT activities. • Reporting on SSL, TLS, and certificate non-compliance, and best practices to follow in case of breaches.

Disclaimer: Muninn should not be solely relied upon to ensure your GDPR compliance, but rather should be used as a practical tool in conjunction with other legal compliance measures. The information provided in this document is intended for informational purposes only and should not be construed as legal advice. For advice regarding any specific issue or problem, please consult with your own legal counsel.