ELEARNINGNEWS ARTICLE

Year 9 - number 320 Wednesday 05 february 2025

Privacy and GDPR training: questions and answers 2025

Explore answers to common questions about Privacy and GDPR training and discover how to protect your company data while maintaining compliance.

The **General Data Protection Regulation (GDPR)** came into force in 2018, radically transforming the landscape of personal data protection in Europe. In 2025, its relevance remains intact, with an even deeper impact thanks to increasing digitalization and the pervasive use of online technologies.

Why is it essential for companies and what are the implications for training?

Privacy and GDPR training is not just a regulatory requirement but serves to ensure compliance and mitigate risks. Through a deep understanding of the regulation, employees can prevent errors that could lead to violations, fines, and reputational damage. Furthermore, GDPR promotes ethical data management, fundamental for company credibility. Training isn't just about formal obligations but also about adopting a responsible corporate culture that values data protection as an integral part of company culture.

Privacy and GDPR: clearing every doubt

Is GDPR training mandatory?

Yes, it's a legal obligation. Every company that processes personal data must ensure that its staff is trained to understand:

- The **fundamental principles** of GDPR.
- The **internal procedures** for managing and protecting data.
- How to **prevent and react** to security breaches.

Lack of training is not just operational negligence but can be considered a violation of GDPR itself, with economic and legal consequences.

What is the best approach to train employees?

An effective program must **adapt to roles and responsibilities**. For high-risk roles, such as DPOs and data processors, advanced and personalized training is recommended. For other employees, online training can offer:

- **Accessibility**: modules accessible anywhere and anytime.
- **Microlearning**: short content to maintain high attention.
- **Interactivity**: simulations and quizzes to reinforce knowledge.

A practical example could be a module that simulates a data breach, allowing participants to identify errors and correct them.

What are the consequences of non-compliance?

Non-compliance with GDPR represents not only an economic risk but also a reputational one. The **sanctions** provided by the regulation can reach up to 4% of annual global turnover or 20 million euros, whichever is greater. However, the impact of controls and sanctions is not limited to large companies but also affects smaller entities.

Beyond economic implications, customer trust is often compromised. Consumers are increasingly mindful of how their personal data is managed, and a violation can generate a loss of credibility that's difficult to recover.

Moreover, the absence of adequate security measures can expose companies to **cyberattacks**, with additional costs related to system restoration and compensation. Investing in training, therefore, also means **protecting company value in the long term**.