The General Data Protection Regulation (GDPR) imposes rules on the collection, processing and management of personally identifiable information (PII) of EU Citizens. GDPR has implications for every organisation from SMEs through to multinationals even if the organisation is not physically located in Europe.

Personal data includes profiles for marketing, sales and communications, eMail and postal addresses, phone numbers or a range of other data that may have been acquired during business transactions or use of a service.

GDPR is in force since MAY 25, 2018. Non-compliant organisations risk fines of up to 20 million Euros or 4% of annual global revenue. Most organisations and all healthcare entities also handle sensitive personal data (Article 9). Non-compliance is not an option.

GDPR requires clear demonstrable processes and policies on Collection, Storage, Processing, Retention and Deletion of personal identifier information. GDPR compliance can be complex:

- Right to Forgotten (Article 17)
- Data Protection by Design (Article 25)
- State of the Art (Articles 25 & 32)
- Ensure ongoing confidentiality, integrity, availability & resilience (Article 32)
- 72 hours data breach notification (Articles 33 & 34)
- Data minimisation principle (Article 25)
- Data Transfers (Articles 44-50)
- Data Portability (Article 20)

GDPR non-compliance for small SMEs (~€2 million revenue) carries a minimum risk of €80,000 does not include potential revenue loss, possible legal exposure and reputational damage.

Educate4Health follows gold standard globally recognised (ANSI, ISO & IAPP) best practices to:

- Simplify the GDPR compliance process
- Audit and assess your specific circumstances
- Document recommendations to achieve GDPR compliance
- Provide excellent Rol (invest €2k-€4k to remove €80k risk)
- Train staff in GDPR best practices
- Deliver tailored ongoing support if required, costs agreed in advance