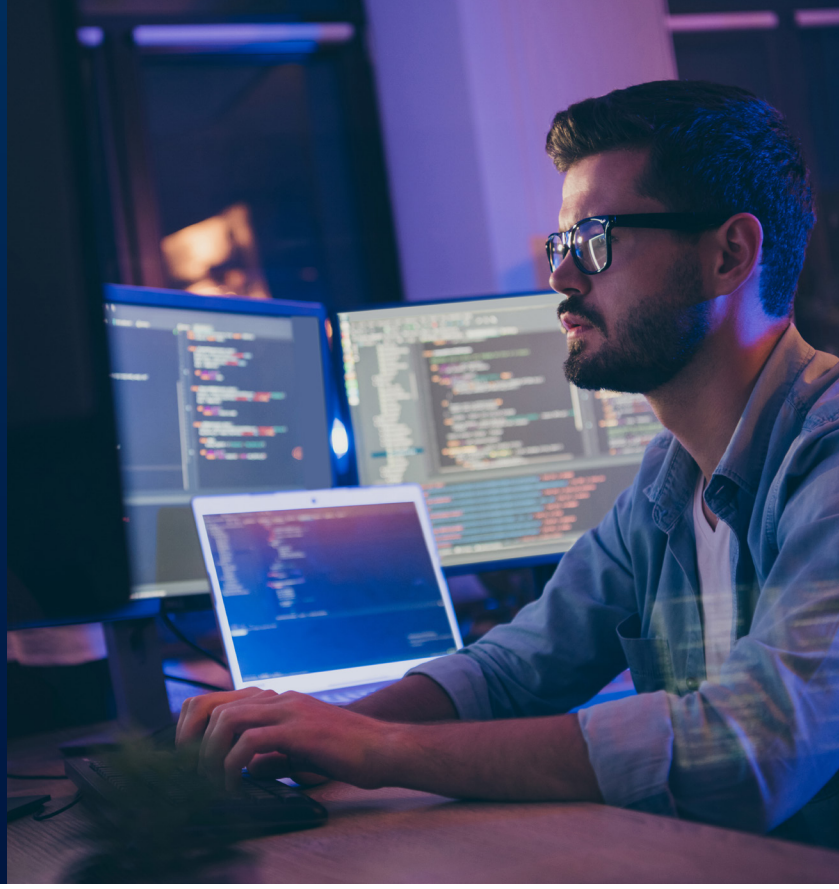
Brown & Brown



PROPERTY & CASUALTY

GDPR For Risk Managers

The Basics

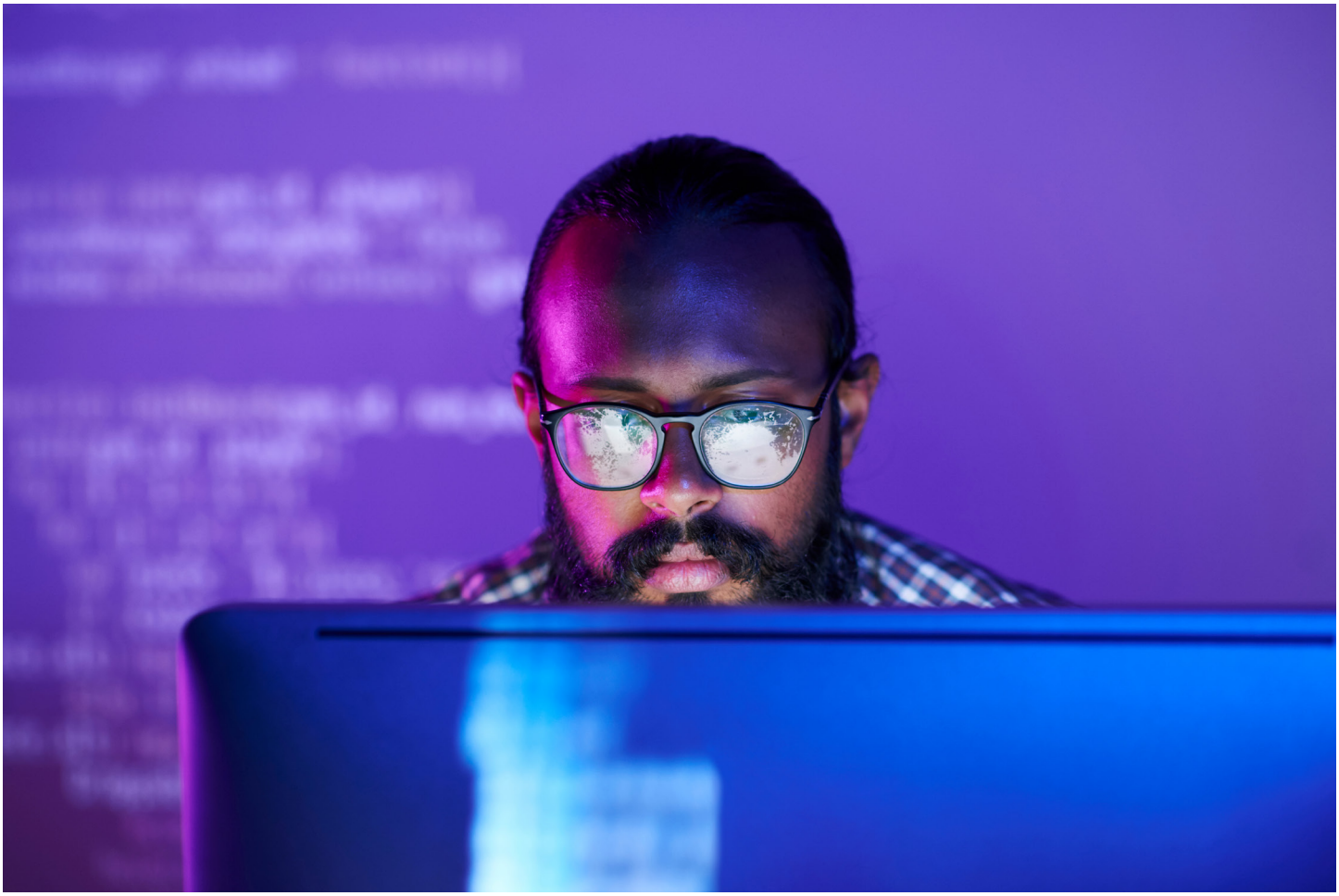
Authored by Jessica Slater and Chris Keegan

The General Data Protection Regulation (GDPR), effective May 25, 2018, requires any company collecting, storing or processing data of European Union residents to comply with data privacy and protection regulations, which change rapidly. Key components of GDRP include regulation around record keeping, control systems and breach notification requirements. To be GDPR compliant, companies must maintain records of all personal data, detailing how the data is used, where it is sent and how it is protected. Data subjects have the right to request information about the use and dissemination of personal data and the right to withdraw their data.

Maintaining appropriate records requires obtaining and properly documenting informed consent. This applies to data collected both before and after the GDPR effective date. Additionally, companies must design systems and controls tailored for data protection. Examples of these controls include implementing codes of conduct and training, developing data breach response preparedness guidelines and hiring a fully trained data protection officer designated to ensure regular and systematic monitoring of data privacy systems. In the event of a personal data breach, companies must promptly notify the proper supervisory authority and possibly the affected individuals.

Since the GDPR entered into force, over 2,000 cases have been created in the European Data Protection Board's case register, and 711 final decisions have been taken. In some cases, imposed fines have reached hundreds of millions of euros. Updated rules designed to streamline enforcement between EU states came into effect in July 2023. The European Commission expects that these will bring swifter case resolutions, meaning quicker remedies for individuals and more legal certainty for businesses.

Compliance with regulations is critical to avoid fines and penalties, handle the changing regulatory landscape and better protect customer data. Noncompliance with GDPR core principles could result in fines and penalties of up to 20 million euros or 4% of global revenue, which could lead to customer dissatisfaction and reputational harm.



Traditional non-cyber insurance policies are unlikely to cover claims brought by consumers, individuals or government agencies enforcing the claims including costs of defending investigations. Cyber policies can provide coverage; however, they must cover all results caused by the failure to conform with GDPR requirements. To obtain the broadest coverage, companies should first make sure they are compliant. Prioritizing compliance helps avoid breaches, litigation and claims.

Examples

Since GDPR was imposed, fines have reportedly reached over 4 billion euros collectively. Examples of larger fines imposed to date, and the company's industry include:

- Technology Company (1.2 billion euros)
- E-Commerce Company (746 million euros)
- Retail Company (35.25 million euros)
- Telecommunications Company (27.8 million euros)
- Airline (22.4 million euros)
- Hospitality Company (20.45 million euros)

How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving program.

Brown & Brown

Find Your Solution at BBrown.com