SecurityScorecard

Preparing For GDPR

AUGUST 2017

SecurityScorecard.com
info@securityscorecard.com

214 West 29th St, 5th Floor
New York, NY 10001
1.800.682.1707

70% of attacks are third-party security breaches.

– Why Third-Party Breaches Are On the Rise **(SecurityScorecard, 2016)**

The European Union's (EU) General Data Protection Regulation (GDPR), effective May 25, 2018, reaches far beyond the Continent's borders. GDPR imposes stringent legislation on every organization that handles Eu citizen data in order to deliver products or services. Inability to demonstrate compliance with GDPR will yield hefty penalties of 20+ million euros. That's a daunting prospect… but there's more. If an organization is compliant but its suppliers are not, the enterprise will be held accountable for all third-party violations of GDPR data privacy standards.

GDPR replaces the 1995 Data Protection Directive—a patchwork of 28 national laws—with a single legal framework. The new technical and organizational mandates are designed to protect the privacy and security of personal data as it traverses digital borders and is used by businesses worldwide. GDPR is part of a broader effort to strengthen and unify Europe's data regulation environment.

Personal Data: Any information relating to an individual's private, professional or public life, including a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address.

–European Commission

GDPR presents complex and formidable hurdles to companies doing business in Europe, but the regulation's scope extends beyond compliance. GDPR reinforces the need for more robust global security infrastructure. Regardless of GDPR and the array of other regulatory requirements in play, enterprises must step up and improve security posture—in their own environment as well as the vendor ecosystem. It's time to enhance data privacy and protection practices, fine tune alignment between business objectives and vendor risk management, and establish a vigilant and far-reaching cybersecurity defense built for today's digital economy and constantly evolving threat landscape.

GENERAL DATA PROTECTION REGULATION

Principles

- Lawful, fair, and transparent use of personal data
- Data collection restricted to specific, explicit, and legitimate purposes
- Minimum data retention limited to business purpose requirements
- Data security, confidentiality, and integrity
- Data controller responsibility for compliance

Goals

- Define privacy policies
- Protect personal data from breaches
- Establish consistent level of data protection across Europe
- Improve trust between citizens and businesses
- Increase organizational accountability for data practices
- Restrict use of personal data
- Restore control of personal information to individuals

Requirements

- Clear, specific, freely given, and withdrawable consent for use of personal information
- Adequate mitigation in place to minimize risk of data breaches
- Full transparency regarding how,when, and where personal data is used or shared
- Disposal of personal data upon request or withdrawal of consent to process

Enterprise Accountability Extends to Vendors

The 99 articles of GDPR mandate protection of all EU resident personal data everywhere. This translates to required compliance for any organization that touches EU citizen data. This includes controllers—organizations that collect and/or own personal data—and processors—third parties like cloud service providers that handle personal data or monitor user behavior on behalf of companies doing business with EU companies. GDPR identifies controllers as the entities responsible for personal data throughout the lifecycle. This is an increasingly difficult challenge as sophisticated cyber attackers skillfully target vulnerabilities in vendor and partner networks that manage essential business functions. Malicious perpetrators repeatedly exploit these security gaps in order to gain access to proprietary data on corporate networks.

GDPR Article 32: *The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.*

> *Controllers bear primary responsibility for ensuring that processing activities are compliant with EU data protection law.*
>
> –Obligations of Controllers
>
> Unlocking the EU General Protection Regulation

Vendor and partner supply chains continue to expand, complicating accountability in third-party ecosystems. When enterprises were more like impenetrable fortresses, every door was locked, and security teams and technologies could confidently ensure data security. But in today's distributed, hyper-connected environment, corporate, partner, and customer data mixes together in the cloud, opening those doors and escalating risk. Every new supplier potentially introduces additional risk. A third party's weak security posture jeopardizes enterprise infrastructure and increases vulnerability to cyber attacks.

Enterprises must continuously monitor security posture in-house and throughout their supply chains. This demands comprehensive visibility of user activity across the enterprise and vendor community, as well as restricted remote access based on device, location and data sensitivity. The ways in which personal data is gathered, stored, used, and shared will be under intense scrutiny. Privacy and protection are now required by default. This means security controls must be embedded in infrastructure rather than bolted on to systems and processes. In addition to stealth control mechanisms that align with risk levels and the potential harm caused by a breach, GDPR mandates rigorous data protection policies, procedures and reporting. For example, data breaches must be reported within 72 hours.

The magnitude of these challenges requires sophisticated security infrastructure. Unfortunately, the prevalence of legacy architectures, tools and technologies reveals a recipe for risk and an inability to keep pace with the emerging threats, complex targeted attacks, and pervasive ransomware that permeate today's cybersecurity landscape.

70% say existing security solutions are outdated and inadequate.*

The rapidly increasing number of devices with anytime/anywhere access to sensitive information compounds the data security dilemma. Heap on unapproved application deployments (shadow IT) and unmanaged data, including USB drives, files without expiration dates, and third-party information sharing, and the hurdles become higher.

*68% say organization's BYO devices may be allowing criminals to access corporate networks and data.**

Compliance is expensive and time consuming, with significant financial implications for GDPR nonadherence looming on the horizon. Organizations must carefully interpret what the EU data protection and privacy regulations mean in their environments and construct roadmaps that ensure adherence by next May.

*67% of global businesses are aware of GDPR, but only about half have started to prepare for the new requirements.**

By 2019, 30% of organizations will face significant financial exposure from regulatory bodies due to their failure to comply with GDPR requirements to protect personal data on mobile devices.

*The Need for a New IT Security Architecture: Global Study on Compliance Challenges & Security Effectiveness in the Workplace (Ponemon Institute, March 2017)

Accelerate GDPR Compliance Efforts with SecurityScorecard

Always Know Your Data Is Safe

GDPR specifies stricter standards related to personal data privacy, consent, processing, access, loss and disposal. Compliance requires real-time visibility of security status inside and outside the enterprise.

SecurityScorecard, provider of the most trusted cybersecurity risk ratings platform, empowers companies to instantly, accurately and continuously self-monitor security health as well as assess vendor and partner security posture. With this intelligence snapshot, security professionals gain insight faster. Workflows enable transparent collaboration with internal and external business partners to quickly evaluate risk and effectively remediate critical security issues.

The SecurityScorecard platform maps the entire Internet every second of every day—every IP address and every open port—using proprietary sensors to collect real-time data from hacker forums, social engineering exploits and data breaches, monitoring millions of signals to discover vulnerabilities.

SecurityScorecard's extensive executive reporting capabilities enable security practitioners to speak the language of the Board of Directors and deliver an abridged view of enterprise security posture. Users can instantly create easily digestible performance reports that facilitate benchmarking comparisons with industry peers and competitors, track threats averted, and demonstrate return on security investments. Executives are most concerned about brand reputation, growth, competitive advantage, and the bottom line. SecurityScorecard's reporting tools make it easy to keep senior management informed and give them only the information they need for high-level decision-making.

- **Additional Features & Benefits**
- Automate risk management
- Gather intelligence data and instantly grade companies across 10 critical security categories
- Receive immediate alerts about new risks in vendor ecosystem
- View, report, and collaborate on security risk from one platform
- Map security issues to GDPR and demonstrate compliance
- Measure impact of security investments
- Establish portfolios for low-risk, high-risk, critical, and rotating vendors
- Prioritize partner assessments and due diligence based on scorecards
- Scrutinize vendors depending on risk level and value add
- Reduce remediation from weeks to days
- Demonstrate efforts to mitigate third-party risk
- Strengthen security posture of suppliers
- Enhance security without impeding productivity
- Improve risk management without additional resources

Savvy organizations understand that enterprise security is only as strong as the third-party security that forms its foundation. GDPR compliance will be achieved through a continuous collaborative dialogue throughout the supply chain.

SecurityScorecard is fundamentally changing these security conversations. Find out how we can help you and your partners build and maintain a defensible security posture for GDPR.

Know now.
See your security posture at:
instant.securityscorecard.com