CYBERSAFE SOLUTIONS

10 Tips to Help Clients Comply with GDPR

The General Data Protection Regulation (GDPR) was first enforced in 2018 to significantly enhance the protection of EU citizens' personal data.

The law shifted more of that responsibility to organizations that collect or process personal data. The provisions in the GDPR call for harsh penalties for violations and put the citizens' rights at the forefront. What's important to note is a company may be physically based outside of the EU's jurisdiction but still meet the criteria. That's why it's crucial for MSPs to understand the GDPR and provide the right guidance, service, and solutions for their clients to ensure compliance. **Here are 10 talking points to discuss with clients.**

1. Understand the Law

Before getting too deep into the details of GDPR, consult an attorney. They can provide explanations and legal guidance on achieving compliance for you and your clients. Once you have a basic understanding, you can better communicate how your services ensure compliance.

2. Be Proactive in Communication

Don't wait for your clients to ask about GDPR compliance. Be proactive in communicating with them. In doing so, you can educate them on what the law means while reinforcing that you have their best interests in mind and the right tools to achieve compliance.

3. Define Covered Data

You are a resource in addition to a service provider. That's important to remember. Be ready to discuss what constitutes "covered data" as it pertains to GDPR, because it might not be obvious. Personal data includes anything that can be used to identify an individual such as IP addresses, location data, mobile devices ID, and cookies.

4. Implement Monitoring

While GDPR doesn't specifically require monitoring, it does call for certain security controls to be in place. Implementing 24/7/365 monitoring allows you to gain visibility into your clients' cybersecurity posture, so you can be proactive in detecting threats before they become breaches. Visibility into their environment (network, cloud assets, and endpoints) is crucial to preventing and responding to threats.

5. Centralize Security Management

GDPR requires organizations to have a privacy compliance framework, which could combine monitoring with the services of a security operations center (SOC). That way, cybersecurity experts can provide analysis—by looking at logs and trends in the industry—in addition to solutions.

6. Track Real-Time Alerts

When your clients suffer a breach, they are required by GDPR to report it to the authorities within 72 hours and notify affected parties "without undue delay." The only way to fulfill that mandate is with real-time threat alerts. These not only keep your clients compliant but also allow you to identify, contain, and respond to threats as quickly as possible.

7. Conduct Tests

You need to understand where your clients are most vulnerable. Conduct tests to determine the effectiveness of their security measures, identify places for improvement, and provide assurance that clients remain GDPR compliant. You should run simulated tests at least four times a year.

8. Have an Incident Response Plan in Place

If your client were breached, what would they do? An incident response plan covers every stage of a cyber incident from identification to response and recovery— who is in charge, chain of command and communication channels, priorities, and more. Education and preparedness are keys to limiting potential damage and keeping your clients' businesses up and running.

9. Invest in Threat Detection Tools

Threat detection is about preventing incidents from becoming breaches. You need a team of experts to track trends, isolate potential compromises, and stay ahead of bad actors as much as possible.

10. Respond to Breaches Quickly

Small problems become big, expensive problems if they're not dealt with quickly. That's especially true in cybersecurity. The longer breaches last, the more expensive they are, shutting down operations, damaging reputations, and resulting in GDPR fines. Don't hesitate when breaches occur.

CYBERSAFE
SOLUTIONS®

Access Cybersafe's senior-level security experts with 20+ years of experience and a state-of-the-art Security Operations Center.

For more information, call
1-800-897-CYBER (2923)