

2018 will see the most stringent Cyber Security and Digital Privacy mandates go into enforcement; with many more public safety and national security requirements soon to follow. Is your business performing its due diligence?

COMPLIANCE



PREP THREAT MODEL



Hippogriff LLC

Computer Technology Protection Services

Hippogriff.TECH | Enterprise
Hippogriff.IO | SMB & SP

GDPR

General Data Protection Regulation Act

Introductory Overview:

- ❖ The European Union's (E.U.) General Data Protection Regulation (GDPR) takes effect the 25th of May 2018 and applies to any company that handles personal data of European residents. It covers all companies operating in the E.U., even if there is no physical presence in the E.U.
- ❖ The rules cover almost any data that can be linked to a individual, such as: mailing address, credit card numbers, travel records, web search history, computer ID codes, biometric data, etc.
- ❖ The world's 500 largest corporations are on track to spend \$7.8 billion in complying with GDPR in the months before its implementation – and after.
- ❖ The most serious violations of GDPR will result in fines of up to 20 Million Euros or 4% of a company's global revenue, whichever is higher. Criminal prosecution and civil complaint against board members may arise from chronic lack of information system(s) protections.
- ❖ GDPR specifies organizations must designate a technical and policy manager for data protection, certifying that data collection governance is minimizing the impact on privacy rights, collect only data that is needed immediately, and not stockpile information for later use.
- ❖ GDPR also specifies that companies must disclose data collection policies clearly rather than burying them in legal documents. In addition, they must report the loss, damage, or theft of data to regulators within 72 hours of such incidents.
- ❖ Individuals may demand to know what personal information an organization holds about them and can invoke “right to erasure” asking a business to delete their data for almost any reason. This mandate specific mirrors current E.U. regulation under the Right to Be Forgotten Act – as well as the ePrivacy Act.

Threat Modeling:

In order to properly achieve compliance for GDPR – and all other current and next generation technology controls – executives must allow for the utilization of the same knowledge and skills that adversaries are employing against their commercial operations. Hippogriff Technologists are ready to carry out ethical and essential actions on behalf of clients – so consumers, employees, and connected vendors are granted the assurance market trends are bringing to their attention.

Conducting a Threat Model is a crucial step in a complete assessment of not only companies information technology networks, but also utilities/applications present on operating systems – and webspace virtual environments. This process will determine the initial starting position of firms' data security, or complete lack thereof. Threat Modeling gets business managers on course to having their organization become GDPR compliant.

Threat Modeling is a process by which potential threats, such as structural vulnerabilities, can be identified, enumerated, and prioritized – all from a hypothetical attacker's point of view. The purpose of Threat Modeling is to provide defenders with a systematic analysis of the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker. Threat Modeling answers the questions: 1) Where are the high-value assets? 2) Where is a targeted organization most vulnerable to attack? 3) What are the most relevant threats? 4) Is there an attack vector that might go unnoticed?

Hippogriff will identify all potential issues with a parent organization's data security, as well as subsidiaries and third-parties – and will grant a true result to mitigate risks across software, hardware, and human domain variables. This is accomplished through a remote and/or on-premises presence by Hippogriff Technologists fielding Information Security (InfoSec) methodology standards and proprietary mechanisms; in cooperation with the client's in-house technical staff and sub-contracted support entities.

Total Capability:

Once a Threat Model is complete, then Hippogriff can proceed to nurture responsible data stewardship for an organization by way of tri-layer advisement, training, monitoring, and testing solutions – that will keep firms across all sectors being seen as safe and reliable goods or services providers.

Hippogriff team members understand the concerns of our clients and their goals. This is why no single solution can be granted to achieve compliance or make ready when responding to a cyber security related incident; it takes people to be involved in every way, all the time. Even though people can be the weakest link in allowing for exploitation to occur – resulting in damage to property and reputation – they are also the most vital component in staving off ever more escalating and destructive cyber attacks. All of the following capabilities are afforded to our customers when relevant:

- Cyber Security Policy and Procedure Development
- System Protection, Continuity and Contingency Planning
- Cyber Security Architecture Design and Implementation
- Network Security Testing and Evaluation
- Incident Response Management and Reporting
- Cyber Security Operations and Management
- Assessment and Authorization Services
- Cyber Security Awareness Training
- Risk and Vulnerability Assessment/Mitigation
- Identity Assurance and Management
- Cloud Preparedness Solutions
- Web and Mobile Application Scanning
- Virtual Intelligence Services
- Forensic Investigation and Data Retrieval

Achieving Compliance:

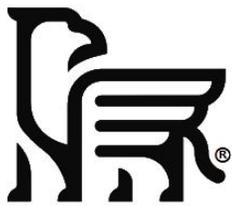
Things to consider. Things that Hippogriff is available to see through:

- ✓ Create and maintain a registry of cyber incidents. Update or create cyber security breach procedures.
- ✓ Consider taking out a cyber insurance policy or adding additional coverage to an existing policy.
- ✓ Has everyone in your database explicitly consented to receive electronic marketing? Confirm that each customer or business contact can opt out of future unsolicited marketing.
- ✓ Delete all non-essential personal data to eliminate liability.
- ✓ Carry out data auditing and add a privacy policy to make it clear how data is collected and how it will be used.
- ✓ Put processes in place to deal with requests from individuals seeking to enforce their rights within the shorter period permitted for response, including a designated team to deal with such requests. A clear plan will minimize waste of company time and resources.
- ✓ Consider which of your service providers are acting as data processors and which are acting as controllers. Make sure that business contacts reflect the position and contain the necessary GDPR elements.
- ✓ For new projects, do not collect personal data unless you can justify your purposes for doing so and you have conducted, and documented, privacy impact assessments.
- ✓ Make sure that data protection policies are up to date and that data processing is transparent.
- ✓ Assess whether appointing a data protection executive director is acceptable.

About Us:

The Hippogriff is an ancient mythological creature that is half Eagle and half Horse. By these traits Hippogriff is ever vigilant, ever elegant, and ever loyal; with the endurance to make unauthorized entities challenged in their interest of information technology materials. Hippogriff is Global, Innovative – Computer Technology Protection Services.

Spaces that Hippogriff is engaged in include but are not limited to: Healthcare IT & Medical Devices · Connected Smart Vehicles · Mainframes · Maritime Vessel & Shore Establishment Safety · FinTech · IoT Risk Mitigation · Website Integrity Control · Autonomous Robotics Countermeasures · Entertainment & Sports · Onsite Energy Facility Systems Monitoring · Anti-Terror · Conflict Zone Forensics, Aerospace · Cyber Concepts Enactment · Civil Liberties & Privacy Guardianship · Anti-Malware Research · Schools/University & Municipal Protection · Gameplay Safety Oversight, and much more...



Hippogriff LLC

Computer Technology Protection Services

Contact: inquiry@hippogriff.tech | 1-866.273.4831

GDPR Information Portal - www.gdpreu.org

European Commission - www.ec.europa.eu

Copyright © 2015-2023 | All rights are reserved.