Secureworks

SOLUTION BRIEF

General Data Protection Regulation

The Challenge

In today's digitally connected, hybrid organizations, the landscape of systems actively holding, transferring and processing PII information is vast and complex. As the regulation brings new and strict enforcement powers for regulators with respect to personal data, ensuring you are taking the right steps towards GDPR-ready, appropriate security controls and practice requires expertise, resource and understanding beyond internal capability.

The Solution

Secureworks security and risk management experts partner with your organization to accompany you on your journey and ensure you are taking a pragmatic and risk-based approach to GDPR data security compliance.

The GDPR focuses on personal data protection: the right governance structure, policies and operational security practices, as well as processes for monitoring, detection and response. Organizations without a proactive, comprehensive information security readiness program will struggle in their compliance journey, and risk susceptibility to data breaches, which could incur financial penalties, possible damage to their brand, or worse, loss of data processing rights.

What is GDPR?

GDPR stands for General Data Protection Regulation, the most comprehensive overhaul of European data protection rules in more than twenty years, and perhaps the most significant regulatory framework to hit organizations since the Sarbanes-Oxley Act of 2002. Its purpose is to replace the varying implementations across Europe of the earlier European Union Data Protection Directive with a single, harmonized EU regulation. The intended outcome is a standardized set of expectations for an organization's management and protection of personally identifiable information (PII) on employees, clients and other applicable data subjects.

GDPR compliance becomes mandatory on 25th May, 2018, and while it is clearly EU focused, it is not limited to organizations based in the EU.

Strict enforcement powers for regulators and new requirements including privacy by design and default, defined penalties and fines, and mandated breach notification within 72 hours of detection will impact organisations and their personal data security strategy.

What is the GDPR Framework and Path to Compliance?

Unlike many checkbox-driven compliance programs, the GDPR is a risk-based framework. Because it covers personal data, the GDPR focuses on having the right governance structure, policies and operational practices, as well as processes for monitoring, detection and response. These are important implications for an organization's information security practice, and it's essential that all organizations impacted by the GDPR are prepared.

GDPR: At a Glance

- New requirements impacting information security including privacy by design and default, data portability and the right to erasure
- 72 hours to report a breach to the regulator after discovery
- Fines as high as 4 % of global annual turnover, or €20 million, whichever is greater

While virtually all organizations will have to implement some changes to become compliant, some will be able to take partial advantage of existing compliance with other mandates and frameworks, such as ISO 27001 and PCI, by extending those measures to the protection of personal data. However, despite having achieved compliance with other mandates, further work could still be required to comply with the GDPR.

The Secureworks Approach

In order to help organizations identify gaps and remediate to meet GDPR data security mandates, Secureworks has developed a four-step approach:

- **Know Your Data.** Understand and identify the scope of the GDPR's data security requirements for your specific operation
- **Assess Current State.** Assess the current state and identify gaps in your current operations and practices
- **Build the Program.** Build the right people, process and control strategies to meet the GDPR's data security mandates
- **Test, Operate and Manage.** Test, operate and manage in line with the GDPR data security requirements, and remove the workload from the security function, allowing security and privacy to be a business enabler

Secureworks GDPR Solutions

Secureworks partners with your organization to accompany you on the above four-step journey and ensure you are taking a pragmatic and risk-based approach to GDPR data security compliance. At any point in your organization's progress towards GDPR compliance, our trusted GDPR practitioners*, risk and security experts can advise you of the scope of data impacted by the GDPR, assess your current state, and define, build and realize a target state that suits your organization. Once implemented, the Secureworks portfolio of services also helps you continuously test, operate and manage your security operations and incident response processes to ensure they remain compliant with the GDPR.

Know Your Data, Assess Your Current State & Build the Program

Secureworks GDPR Advisory Services

GDPR Controls Assessment

The challenges of beginning your GDPR journey may be diverse. You may not know where to begin; you may not have the resources to act in the time remaining. In today's digitally-connected, hybrid organizations, the landscape of systems actively holding, transferring and processing PII information is vast and complex.

* To better advise you and ensure you have the guidance necessary to navigate the regulation, our GDPR Practitioners and risk management consultants have gone through a GDPR training course provided by IT Governance (ISO 17024-certificated).

Secureworks®

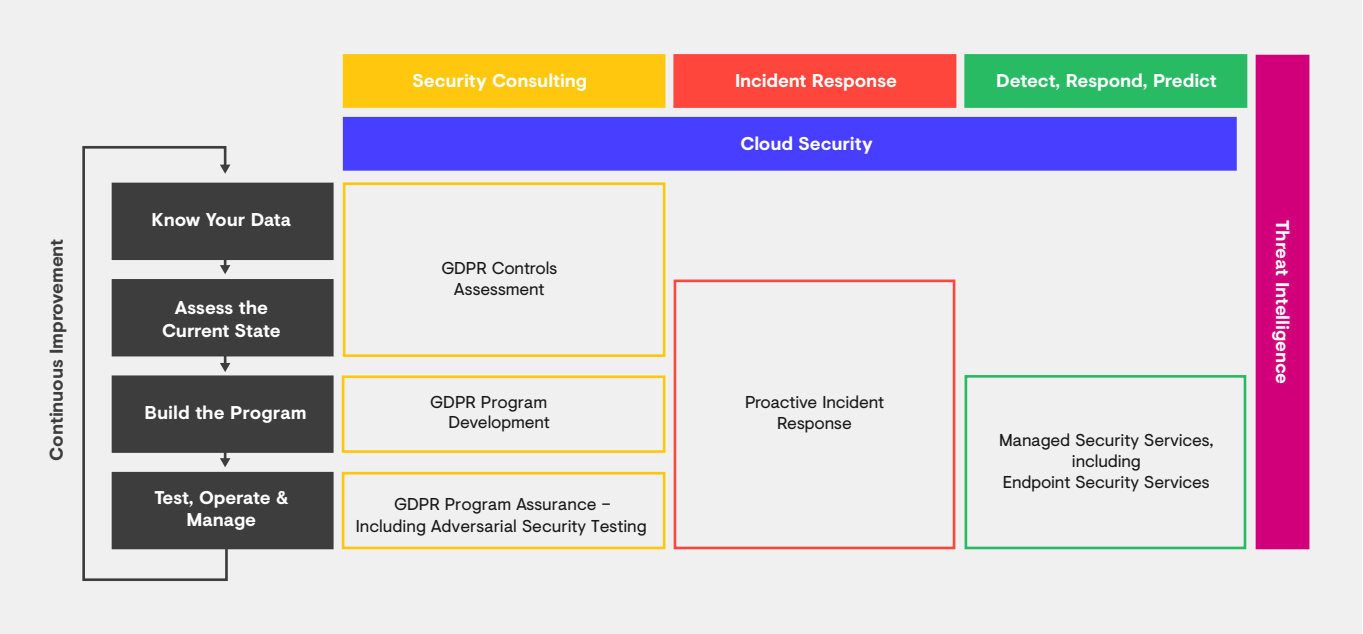

Figure 1. *Secureworks GDPR Solution – Aligning Security Expertise and Market-leading Information Security Services*

In addition, organizations have differing levels of in-house resource and skill to carry out assessments or build the business case that will ensure their information security operation is GDPR compliant. Our GDPR Controls Assessment is tailored to the progress and needs of your program.

A Secureworks GDPR Controls Assessment engagement enables your organization to understand its current state of readiness, and identify gaps in security practice against the GDPR. As part of this process, Secureworks begins by helping you identify data potentially in scope of the GDPR's data security requirements, and ends by providing a roadmap towards GDPR data security compliance. Two assessment options are available: a high-level assessment focused on creating Board awareness and building a business case, or a more detailed, in-depth assessment.

What do we help you answer?

- Which of my data and systems fall within the scope of the GDPR's data security requirements?
- How prepared is my organization's security for the GDPR?
- What are my current security gaps and weaknesses with respect to the Regulation?
- How will the data security changes required for the GDPR affect my organization?
- How best can I present this information to the Board?

GDPR Program Development

GDPR's risk-based approach means that there is no single set of security processes, policies and technical controls for organizations to enact.

For this reason, our Secureworks GDPR Program Development engagement is a highly tailored consulting service that builds GDPR data security compliance by designing and implementing appropriate measures specific to your organization's requirements. At the program's conclusion, your organization's privacy and security program will be ready for compliance with the GDPR.

What do we help you answer?

- What GDPR security strategy will ensure our compliance by 25th May 2018?
- What data security activities do I need to carry out to comply with the GDPR?
- How should I structure my data security team to meet the GDPR requirements?
- What is the level of detail required in the policies, procedures and workflows?
- How do I implement our GDPR data security program?
- How do I prove compliance to my senior management team?
- How do I monitor my ongoing GDPR data security compliance?

Test, Operate & Manage

Once implemented, our portfolio of services also helps you continuously test, operate and manage to ensure your security operations and incident response processes remain compliant with the GDPR.

Program Assurance

Our GDPR Program Assurance engagement is key to testing, operating and managing on-going compliance. Program Assurance includes testing system security, detection, and incident response capabilities on an ongoing basis. This engagement is designed to provide your organization with assurance or highlight any new or further gaps requiring remediation.

What do we help you answer?

- Are my organization's current personal data processing activities and measures resilient?
- Is the technical configuration of our systems hosting personal information secure and free of vulnerabilities?
- Have we identified and tested the scenarios in which personal data can be compromised from our key systems and have we put controls in place to address those scenarios?
- Do our current processes adequately and appropriately fulfill the GDPR data security requirements?
- How would our current personal data breach processes perform, and do they meet GDPR requirements for breach notification within 72 hours of detection?
- Can our current systems storing personal data withstand a targeted attack?

Secureworks Monitoring, Detection and Response Solutions

In addition to Advisory Services, Secureworks offers a portfolio of Monitoring, Breach Detection and Response Solutions to support the ongoing management and operation of information security best practice. The GDPR mandates that organizations have the right technical controls and processes to detect and respond to a personal data breach and, in certain instances, to share a formal report of the breach with the regulator within 72 hours of detection. We provide the managed service required to address the GDPR requirements for breach detection and response.

Service Offering	Methodology Stage	Service Features
GDPR Controls Assessment	Know Your Data	• Identify privacy data management systems potentially in scope (PII information) • Identify third party data processors • Identify information governance • Data flow analysis and mapping of privacy data (from collection to destruction)
	Assess Current State	• Gap analysis against GDPR data security requirements • Third party vendor assessment • Policy and architecture reviews • Assist in data protection impact assessments (DPIAs) • Road map development: define projects required to comply with GDPR. Includes risk-based prioritization.
GDPR Programme Development	Build the Program	• Define improvement program to address gaps identified • Extend existing privacy information management system or build the system (strategy, policies, procedures, roles and responsibilities, privacy by design methodology, training) • Implement technical controls for data management and security, monitoring and detection, response and remediation
GDPR Program Assurance Testing	Test, Operate and Manage	Investigate and highlight critical vulnerabilities in systems and processes collection, storing and sharing personal information, and remediation support. The Secureworks advisory, strategic and technical consulting portfolio is leveraged to help test and assure the GDPR program: • Secureworks Adversarial Security Testing includes penetration tests, application security testing, Red Team testing and more to test the security of systems that handle personal data • Secureworks Incident Response perform incident response testing of organisation's personal data breach handling process and notification procedure • Secureworks security and risk consultants perform mock-audits to test GDPR controls and identify areas of non-compliance before a formal audit takes place
Monitoring, Detection & Response Solutions	Test, Operate and Manage	• Data breach management — monitoring, detection and response • Incident Response Retainer • Vulnerability management — scanning and remediating vulnerabilities on the systems holding personal information

Managed Security Services

Secureworks Managed Security Services are designed to help organizations meet these specifications and better detect, validate and respond to a personal data breach across their infrastructure, whether on-premise or in the cloud.

With global visibility across more than 4,400 clients, once a threat is discovered, we use that knowledge to protect all of our clients, making us collectively smarter, exponentially safer. Our Counter Threat Platform™ (CTP) simplifies your security operations, so you can see more, know more and do more by connecting vast amounts of data across your existing security investments. Analyzing ~250 billion security events per day, CTP detects threats with high fidelity and provides you with actionable guidance to remediate.

Incident Response

Our Incident Response practice provides rapid containment and eradication of threats, minimizing the duration and impact of a security breach to your organization. Leveraging our cyber Threat Intelligence and global visibility, we can help you prepare for, respond to and recover from even the most complex and large-scale security incidents.

Our Incident Response experts understand that you have compliance obligations surrounding a breach. We help your compliance, privacy and legal teams make sense of the impact that the breach had, so intelligent decisions can be made to meet your obligations.

- Incident Response Retainer
- Proactive Incident Response Services

What do we help you answer?

- What can I do today to prevent fines and ensure sufficient breach notification compliancy?
- Does my organization have the right technology enabled services, controls and processes in place to detect and respond to a breach of personal data?
- How can an experienced security partner help me to alleviate the administrative and operational burdens of a GDPR program?
- What solutions and services are available to address the biggest risks, and how do they allow my organization to focus on business priorities?

Why Secureworks

Together or individually, the Secureworks portfolio of services and expertise combine to support you on your journey to GDPR compliance. We help you navigate the complexities of The Regulation and data privacy risk in our digitally connected world, enabling your unique business objectives and needs, strengthening your security posture and technical PII data security, and implementing effective data breach capabilities.

For more information, call **+1-877-838-7947** to speak to a Secureworks security specialist.

secureworks.com

About Secureworks

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world. We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Secureworks®