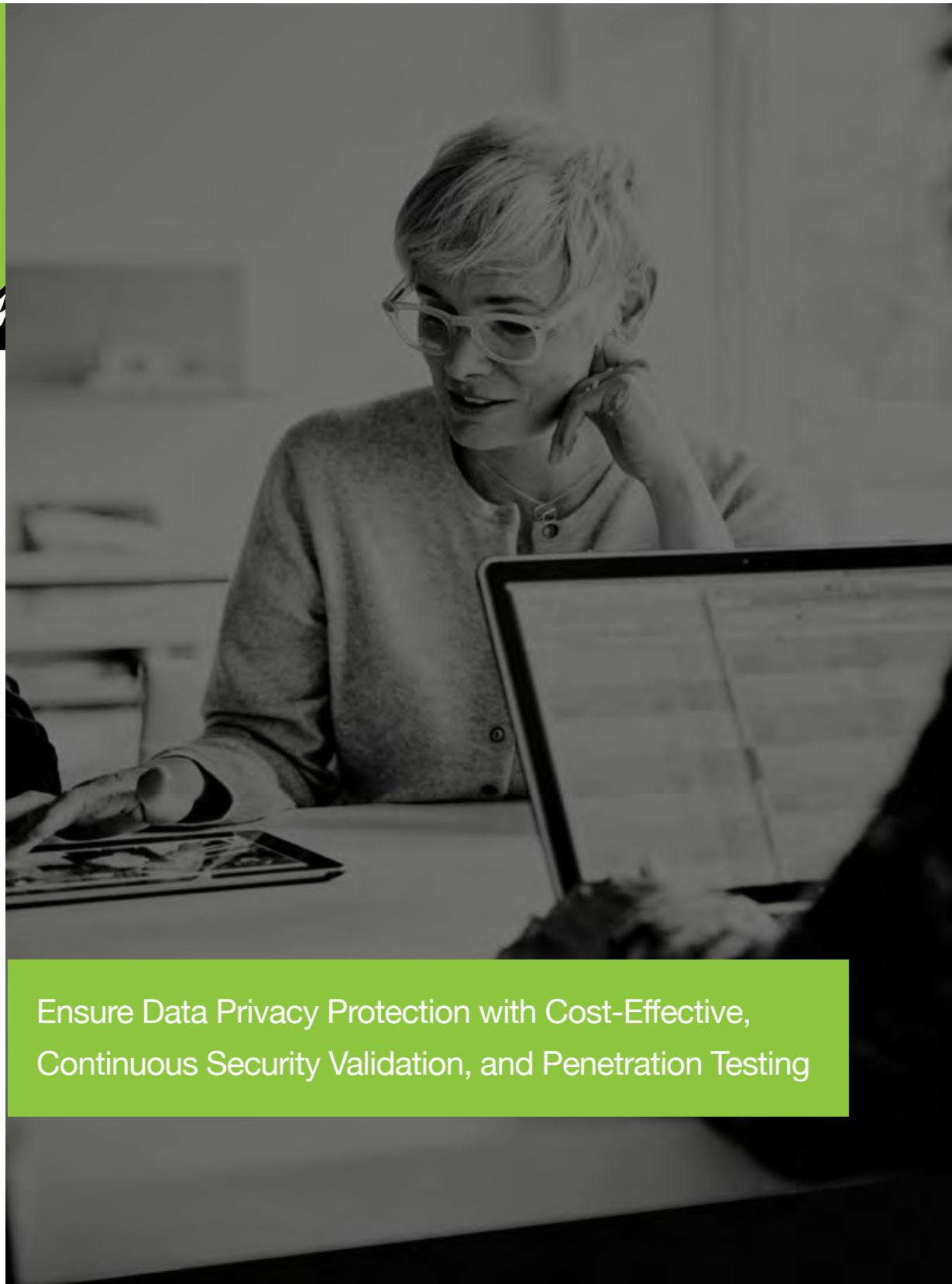
GDPR and Worldwide Data Privacy Compliance

Using RidgeBot™

RIDGE SECURITY



Ensure Data Privacy Protection with Cost-Effective, Continuous Security Validation, and Penetration Testing

Abstract

This white paper discusses how RidgeBot™ security validation and penetration testing can help organizations comply with legal requirements concerning the digital privacy and security of sensitive personal information. The paper focuses on GDPR, the data privacy legislation of the EU, along with coverage of POPIA (South Africa), LFPDPPP (Mexico), and LGPD (Brazil).

While each country's law is different and specific to its region, the technical security requirements are generally similar across the board. They follow the same general themes of what to do and how to ensure adequate protection. The information in this document is, therefore, applicable to technical compliance of data privacy laws worldwide.

Introduction

Over the last half-century, the world has experienced the relentless digitization of citizens' financial and personal lives. We are experiencing the ever-increasing interconnectedness of the global economy and the marketing, sale, use, and abuse of sensitive electronically-stored personal data. Many countries worldwide have pursued or revised legislation to keep sensitive data stored and shared safely and out of the hands of malicious perpetrators who use personal data for identity theft and many other fraudulent and exploitative purposes.

In 2016, the European Union (EU) enacted the General Data Protection Regulation (GDPR), a law that stipulates data privacy requirements, regarded as the gold standard for data privacy worldwide. GDPR replaced the older 1995 European Data Protection Directive law and has been fully implemented and enforced in EU member states since May 2018. The majority of countries worldwide maintain national data privacy laws targeting goals similar to those of GDPR: the "protection of natural persons concerning the processing of personal data and on the free movement of such data."

Much of the GDPR provisions' legal content—and related laws in other countries—is geared towards non-technical considerations. Considerations like organizational processes, administrative responsibilities, clauses to be incorporated in contracts, establishing legal justifications for collecting and storing personal data, requiring breach notifications, and governing the retention time of time-sensitive data. But there is also a set of technical requirements regarding the storage, processing, transmission, and access of sensitive data (electronic or otherwise) that puts data-and-network security front-and-center to legal compliance. Data privacy cannot exist without data security.

Data and Network Security

The digital transformation of worldwide economic, business and government operations has seen rapid growth in security defense technologies such as encryption, Next-gen firewalls, filtering methods, malware screening, multi-factor authentication, and surveillance.

Despite advances in these defensive technologies, networks, hosts and applications are continuously under attack by increasingly creative and sophisticated methods. Breaches are continually growing in number, size, and damages inflicted by attackers.

Industry Trends

Traditional defensive security mechanisms have failed to adequately protect networks, data centers, hosts, and applications from infiltration, attacks, and breaches. The effectiveness of traditional defensive security mechanisms pivots largely on the concept of border security—while increasingly, industry trends in SaaS, IaaS, cloud computing, IoT, virtualization, and mobility have blurred or erased borders in networks and computer processing and storage systems.

Security posture is also distressed because, while attacks have escalated in number, subtlety, and precision, IT resources for security measures, audits, and protective activities have tightened.

Penetration Testing

Rapidly increasing threat incidences and sophistication have made it imperative to harden security postures with active, offensive methods. Not supplanting, but in addition to traditional defensive measures, such as penetration testing probes for vulnerabilities, they are addressed before they are exploited.

Breach Prevention Traditional Defense 2002 | **Post Breach Detection 2012** | **Pre-Breach Offensive Defense 2020**

Penetration testing is typically an expensive, resource-intensive, disruptive, and often manual process executed periodically (for example, annually). Or when there is an upcoming audit or other collateral need to gain or reaffirm compliance with one of the many worldwide standards and regulations regarding financial, personal, health, or additional sensitive information. Periodical testing leaves your environment vulnerable during the often-lengthy periods in between audits doing scheduled pen-testing validation.

Automated Continuous Validation with RidgeBot

RidgeBot is an intelligent robot that provides low-cost continuous, automated security validation services to harden your security posture ongoing and deliver always-on compliance monitoring. It has built-in collective real-time knowledge of the latest threats, vulnerabilities, exploits, and state-of-the-art AI/ML-assisted hacking methods and techniques. It scales as needed and runs as a VM, on an appliance, or as SaaS.

RidgeBot automates penetration testing, making it an ongoing high-use tool integral to your security policy and procedures instead of an expensive one-time test exercise. RidgeBot is your personal robot assistant that details how and where a hacker can successfully compromise your assets. It recommends step-by-step how to build and maintain your assets in a secure, protected manner.

RidgeBot does much more than a pen-test: it auto-discovers assets and then proceeds to probe them continuously, iteratively, fully automated, at scale, and exploits the vulnerabilities found. In its report, it alerts you to the ranked short-list of dangerous, successfully exploited vulnerabilities as well as a list of lower-priority non-exploited vulnerabilities. This means your network is always locked down, always patch-up-to-date, always ready for audit, and always prepared to submit proof of security posture—all at minimal cost and human intervention.

RidgeBot provides the following key capabilities:

- **Discovery**: Automatically crawls through your environment to identify and document types of assets (including networks, hosts, applications, plug-ins, images, IoT devices, and mobile devices) and the attack surfaces of those assets.
- **Scanning**: Assets and attack surfaces are mined for vulnerabilities by leveraging RidgeSecurity's leading-edge Threat Intelligence Platform—a collective vulnerability knowledge database—that includes more than 2-billion pieces of security intelligence data, 100 million attack libraries, and 150K exploit libraries.
- **Exploit**: AI/ML-assisted attack techniques/modes automatically exploit vulnerabilities found. Findings are documented along with remediation recommendations in accurate, reliable, and usable reports. AI/ML algorithms draw on an expert knowledge base to guide RidgeBot in attack-path-finding and path-selection to launch iterative attacks based on learning along the path. Attacks achieve much wider test coverage and deeper inspection than traditional pen-test methods.
- **Post-exploit Risk Prioritization**: RidgeBot visualizes the kill-chain and quantifies risks based on multiple factors to give organizations a detailed and specific ranking of the most dangerous vulnerabilities. Focusing on specific exploitable vulnerabilities (a single-digit percentage), RidgeBot's analytics drastically reduce the manual work required to rank and remediate vulnerabilities.

GDPR Overview

The General Data Protection Regulation (GDPR) is a law adopted by the European Union (EU) in April 2016, and effective as of May 25, 2018, with Regulation (EU) 2016/679 as the current version. GDPR targets the security and protection of EU individuals' personal data and replaces the older 1995 Data Protection Directive. The GDPR provisions comprise a far-reaching change in data privacy regulation in the EU, and span a broad scope of operational, administrative, procedural, and technical requirements.

Type of Requirement: GDPR is an EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA).

Geographic Applicability: The law was drafted and passed by the European Union (EU), but it is extraterritorial. It imposes obligations onto organizations worldwide if they target or collect data related to EU individuals. For example, any organization recording or storing an online account or profile of an EU individual is subject to GDPR compliance, regardless of the company's physical location or ownership. Specifically, GDPR applies to any organization which:

- has a business presence in the EU
- offers goods or services to EU individuals
- collects and stores data about an EU individual, or the individual's behavior and preferences

Ownership: European Union (EU) Parliament.

Compliance Verification and Enforcement: GDPR is enforced by the individual regulatory enforcement agency, or Supervisory Authorities (SA), of each EU member country. The SA advises businesses on how to comply, conduct audits, carry out investigations, review certifications, impose administrative fines, and take other actions to verify or enforce compliance.

More information:

- GDPR general information and resources: gdpr.eu
- Text of the articles of the GDPR law: gdpr-info.eu

Data Privacy Laws in Other Countries

South Africa: POPIA Overview

The Protection of Personal Information Act (POPIA) is legislation to safeguard the integrity and sensitivity of private information. The law intends to promote the right to privacy contained in the South African Constitution while at the same time protecting the flow of information and advancing the right of access to, and protection of, information.

The section of the law applicable to technical data-and-network security measures and safeguards appears in Chapter 3 “Processing of personal information in general”, Part A “Processing of personal information in general”, Condition 7 “Security safeguards”, Section 19 “Security measures on integrity and confidentiality of personal information” and Section 22 on breach notification “Notification of security compromises.”

Type of Requirement: POPIA is a South African law on data protection and privacy.

Geographic Applicability: POPIA applies to every type of company either based in South Africa or based outside South Africa but processes personal information within South Africa.

Ownership: POPIA was established by the South African Parliament in November 2013, with a general commencement date of July 1, 2020 (while a few small sections have different dates).

Compliance Verification and Enforcement: The POPIA law includes establishing an Information Regulator that has powers and duties to enforce the law.

More information:

- Protection of Personal Information (POPI) Act: https://popia.co.za/

Mexico: LFPDPPP Overview

The Mexico federal LFPDPPP law (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*) protects personal data held by private parties and became effective July 6, 2010. The law was revised and augmented with additional legislation in 2011, 2013, 2014, and 2018. The LFPDPPP law governs how the private sector can collect, process, and reveal individuals' personal data.

The use of all personal data must be justified, and the law follows nine principles: legitimacy, consent, information, quality, purpose, loyalty, proportionality, and accountability. Technical, physical, and administrative safeguards, security policies, and security responsibilities to guarantee the safety of personal information fall under the "Accountability" principle.

Unlike GDPR, the LFPDPPP law applies only to private individuals or legal entities that process personal data and those that disclose the data for commercial use. It does not cover the government or credit reporting companies governed by the Law Regulating Credit Reporting Companies or entities collecting and storing personal data purely for personal use.

Type of Requirement: LFPDPPP is a Mexican federal law on data protection and privacy.

Geographic Applicability: The law applies primarily inside Mexico. Businesses located outside Mexico are subject to the law only when personal data collected in Mexico is transferred outside of Mexico.

Ownership: LFPDPPP was established by the Mexican Congress in April 2010.

Compliance Verification and Enforcement: The law is enforced by the National Institute for Transparency, Access to Information and Personal Data Protection (INAI), which investigates reported violators and applies fines.

More information:

- LFPDPPP Law (in Spanish): http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf
- National Institute for Transparency, Access to Information and Personal Data Protection (INAI): https://home.inai.org.mx/

Brazil: LGPD Overview

Brazil's General Law for the Protection of Personal Data (LGPD) (*Lei Geral de Proteção de Dados*) was passed August 14, 2018 and became effective in February 2020. The law covers the processing of personal data, including digital media, by a natural or legal person to protect the fundamental rights of freedom and privacy.

Type of Requirement: LGPD is a Brazilian law on data protection and privacy.

Geographic Applicability: As with GDPR, LGPD applies extraterritorially to any business or organization that processes the personal data of people in Brazil, regardless of the location of that business or organization.

Ownership: LGPD was established by the Brazilian government in August 2018.

Compliance Verification and Enforcement: The National Data Protection Authority (ANPD) was created to oversee the implementation of the law.

More information:

- GDPR—LGPD comparison: https://gdpr.eu/gdpr-vs-lgpd/
- LGPD Law (in Portuguese): https://www.gov.br/defesa/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd

GDPR Legal Compliance

GDPR consists of 99 articles and 173 recitals, the content of which can be accessed here. The articles comprise the legal requirements organizations must follow to demonstrate compliance, while the recitals provide additional supportive information to supplement the articles.

Seven principles form the foundation of the GDPR—outlined in Article 5. The principles where the digital data security measures and safeguards offered by RidgeBot can be of help to comply fall under "Integrity and confidentiality" (#7) and "Accountability" (#8).

1. Lawfulness
2. Fairness and transparency
3. Purpose limitation
4. Data minimization
5. Accuracy
6. Storage limitation
7. Integrity and confidentiality
8. Accountability

Article 5 [1f] states that "personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality')."

Article 5 [2] states that "the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

GDPR Content Outline

To provide perspective on where RidgeBot can help with compliance, the GDPR structural outline below highlights specific articles concerning digital data security and integrity protection.

Chapter 1: General Provisions

— Article 1: Subject-matter and objectives

— Article 2: Material scope

— Article 3: Territorial scope

— Article 4: Definitions

Chapter 2: Principles

— **Article 5: Principles relating to the processing of personal data**

— Article 6: Lawfulness of processing

— Article 7: Conditions for consent

— Article 8: Conditions applicable to a child's consent relative to information society services

— Article 9: Processing of special categories of personal data

— Article 10: Processing of personal data relating to criminal convictions and offenses

— Article 11: Processing which does not require identification

Chapter 3: Rights of the Data Subject

Section 1: Transparency and modalities

— Article 12: Transparent information, communication, and modalities for the exercise of the rights of the data subject

Section 2: Information and access to personal data

— Article 13: Information to be provided where personal data is collected from the data subject

— Article 14: Information to be provided where personal data has not been obtained from the data subject

— Article 15: Right of access by the data subject

Section 3: Rectification and erasure

— Article 16: Right to rectification

— Article 17: Right to erasure ('right to be forgotten')

— Article 18: Right to restriction of processing

— Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing

— Article 20: Right to data portability

Section 4: Right to object and automated individual decision-making

— Article 21: Right to object

— Article 22: Automated individual decision-making, including profiling

Section 5: Restrictions

— Article 23: Restrictions

Chapter 4: Controller and Processor

Section 1: General obligations

— Article 24: Responsibility of the controller

— **Article 25: Data protection by design and by default**

— Article 26: Joint controllers

— Article 27: Representatives of controllers or processors not established in the Union

— Article 28: Processor

— Article 29: Processing under the authority of the controller or processor

— **Article 30: Records of processing activities**

— Article 31: Cooperation with the supervisory authority

Section 2: Security of personal data

— **Article 32: Security of processing**

— **Article 33: Notification of a personal data breach to the supervisory authority**

— **Article 34: Communication of a personal data breach to the data subject**

Section 3: Data protection impact assessment and prior consultation

— **Article 35: Data protection impact assessment**

— Article 36: Prior consultation

Section 4: Data protection officer

— Article 37: Designation of the data protection officer

— Article 38: Position of the data protection officer

— Article 39: Tasks of the data protection officer

Section 5: Codes of conduct and certification

— Article 40: Codes of conduct

— Article 41: Monitoring of approved codes of conduct

— Article 42: Certification

— Article 43: Certification bodies

Chapter 5: Transfers of Personal Data to Third Countries or International Organizations

- Article 44: General principle for transfers
- Article 45: Transfers on the basis of an adequacy decision
- Article 46: Transfers subject to appropriate safeguards
- Article 47: Binding corporate rules
- Article 48: Transfers or disclosures not authorized by Union law
- Article 49: Derogations for specific situations
- Article 50: International cooperation for the protection of personal data

Chapter 6: Independent Supervisory Authorities

Section 1: Independent status

— Article 51: Supervisory authority

— Article 52: Independence

— Article 53: General conditions for the members of the supervisory authority

— Article 54: Rules on the establishment of the supervisory authority

Section 2: Competence, tasks and powers

— Article 55: Competence

— Article 56: Competence of the lead supervisory authority

— Article 57: Tasks

— Article 58: Powers

— Article 59: Activity reports

Chapter 7: Cooperation and Consistency

Section 1: Cooperation

— Article 60: Cooperation between the lead supervisory authority and the other supervisory authorities concerned

— Article 61: Mutual assistance

— Article 62: Joint operations of supervisory authorities

Section 2: Consistency

— Article 63: Consistency mechanism

— Article 64: Opinion of the Board

— Article 65: Dispute resolution by the Board

— Article 66: Urgency procedure

— Article 67: Exchange of information

Section 3: European data protection board

— Article 68: European Data Protection Board

— Article 69: Independence

— Article 70: Tasks of the Board

— Article 71: Reports

— Article 72: Procedure

— Article 73: Chair

— Article 74: Tasks of the Chair

— Article 75: Secretariat

— Article 76: Confidentiality

Chapter 8: Remedies, Liability, and Penalties

- Article 77: Right to lodge a complaint with a supervisory authority
- Article 78: Right to an effective judicial remedy against a supervisory authority
- Article 79: Right to an effective judicial remedy against a controller or processor
- Article 80: Representation of data subjects
- Article 81: Suspension of proceedings
- Article 82: Right to compensation and liability
- Article 83: General conditions for imposing administrative fines
- Article 84: Penalties

Chapter 9: Provisions Relating to Specific Processing Situations

- Article 85: Processing and freedom of expression and information
- Article 86: Processing and public access to official documents
- Article 87: Processing of the national identification number
- Article 88: Processing in the context of employment
- Article 89: Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
- Article 90: Obligations of secrecy
- Article 91: Existing data protection rules of churches and religious associations

Chapter 10: Delegated Acts and Implementing Acts

- Article 92: Exercise of the delegation
- Article 93: Committee procedure

Chapter 11: Final Provisions

- Article 94: Repeal of Directive 95/46/EC
- Article 95: Relationship with Directive 2002/58/EC
- Article 96: Relationship with previously concluded Agreements
- Article 97: Commission reports
- Article 98: Review of other Union legal acts on data protection
- Article 99: Entry into force and application

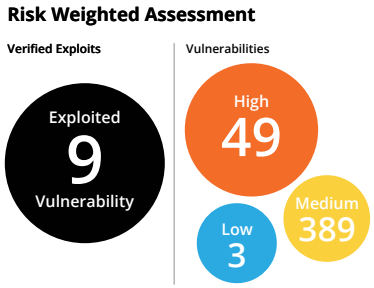
OVERVIEW

How RidgeBot Can Help

In a general sense, RidgeBot finds security deficits in your assets and provides guidance on how to immediately resolve exposures. Moreover, RidgeBot helps maintain, on a continuing basis, a security posture that is always in compliance with data security—and by implication, data privacy—regulations and expectations.

Some of RidgeBot's key benefits to your organization's security posture include:

- **Improve and Simplify Security Activities and Process**
  - — Discover, inventory, and document system components, assets, and attack surfaces. Because RidgeBot is fully automated, you can do this continuously or at much more frequent intervals than previous periodic manual processes.
  - — Reports help document vulnerabilities found, exploited, remediated, and validated.
  - — Reports provide clear risk ranking to focus manual remediation activity on the highest risk vulnerabilities.
  - — RidgeBot's flexibility allows you to run attack testing from inside and outside your environment.



  - — RidgeSecurity's Threat Intelligence Platform knowledgebase ensures that you are always up to date with industry-leading security vulnerability information.
  - — Run RidgeBot attacks and scans as a standard part of your ongoing security policy.

- **Continuous Security Validation**
  - — RidgeBot provides no-cost iterative, continuous hardening, and asset inventory. You can run different scans periodically or continuously—because it is fully automated, no manual intervention is required until a vulnerability is reported.
  - — Continuous monitoring and asset discovery protect against hacker intrusion caused by an employee (or any other person) accidentally or maliciously connecting untrusted or unplanned IoT, wireless, or other unauthorized devices to the environment.
  - — Scan reports provide a shortlist of must-fix exploitable vulnerabilities to document and resolve. Report output ensures all software patches and updates needed to resolve dangerous vulnerabilities are installed on all affected assets.
- **DevOps/SecOps Software Development and Release Testing**
  - — Use RidgeBot during the software development process to ensure that dangerous coding practices that introduce vulnerabilities never ship in new software releases.
  - — Use RidgeBot to harden software patches, software upgrades, new devices, and any configuration changes before pushing them into the production environment.
- **Security Posture Validation**
  - — Continuously and iteratively attack the production environment. Maintain security posture and discover misconfigurations in wireless or defensive security appliances or services such as firewall rules or UTM appliances.
  - — Continuously monitor and harden login credentials on sensitive assets.
- **Compliance Audit**
  - — Continuous asset discovery scanning and attack and exploitation attempts (and the reports issued) mean your environment is always audit-ready.
  - — Use RidgeBot reports submitting evidence of vulnerabilities probed, remediated, and resolved.
- **Security Incident Response**
  - — Scan reports, containing recommended solutions for each vulnerability found, provide critical information to your security incident response/escalation team.
  - — Risk ranking of vulnerabilities feeds into the priorities and procedures for incident response.
  - — RidgeBot AI/ML exploitation attacks provide forensic capabilities to investigate the origin and path taken by a breach and step-by-step guidance on how to resolve the entry point vulnerability.

RidgeBot includes several template scans that you can use and the flexibility to customize your scans completely. The system templates include:

- **Full scan**: This test launches numerous attack techniques used by real-world hackers. Based on threat intelligence and an exploit knowledge base, RidgeBot profiles assets, mines vulnerabilities, and launches attacks against target assets, which may be internal or external to your environment, in a private or public environment.
- **Weak password scan**: This test launches direct or iterative attacks based on sensitive information collected via weak credentials or unauthorized access vulnerabilities. Attack targets include redis, elasticsearch, ActiveMQ, database, web login, and other applications.
- **Struts 2 scan**: This test launches direct or iterative attacks based on known 1-day or n-day vulnerabilities detected on targets using the Struts 2 framework.
- **Weblogic scan**: This test launches direct or iterative attacks based on known 1-day or n-day vulnerabilities detected on targets using Weblogic middleware.
- **Web scan**: This test launches cyberattacks against target websites, web applications, and all related attack surfaces. Gain control of the target website for both self-developed and contact management system-based websites.
- **Host scan**: This test launches direct or iterative attacks from inside a corporate network to validate the security system's response to an internal threat. Target systems include all network-accessible internal hosts and servers.

How RidgeBot Can Help with Data Privacy Compliance

Much of the text of the worldwide data privacy laws—many influenced by the EU's GDPR and containing requirements similar in spirit and intent if not in exact phrasing—focus on administrative, organizational, and process stipulations. GDPR is often more comprehensive and specific than other laws.

The GDPR's technical requirements, where they exist, contain recurring themes in different chapters and sections. These unique technical themes—as distilled from the detailed GDPR articles and recitals enumerated in the section following this one—yield a series of generic, non-country-specific data privacy requirements discussed in this section. RidgeBot's penetration testing, vulnerability ranking, risk assessment, AI/ML-assisted vulnerability exploitation, recommended remediation steps, and rigorous reporting can harden your network and help comply with the legal data privacy stipulations of your region.

Fundamentally, data privacy cannot exist independent of data security, and RidgeBot capabilities ensure asset (including data) security.

Data Privacy by Design and Default

GDPR Article 25 requires the cost-effective implementation of appropriate technical data protection principles, as well as the integration of necessary safeguards into all aspects of data processing activities. Both external infrastructure with PII (Personally Identifiable Information) such as CRM, payroll, and email systems, as well as internal infrastructure with PII such as internal servers, networking equipment and end user devices (laptops and desktops etc.) must be subject to vulnerability assessments to confirm that systems are up-to-date, correctly configured and free of malware.

USING RidgeBot TO COMPLY

- RidgeBot's automated asset discovery can help inventory and document all data processing assets and attack surfaces while preparing for data privacy compliance. Running this scan iteratively discovers and documents any changes in the presence of assets that should be included in the inventory.
- RidgeBot's automated asset discovery can additionally verify on an ongoing basis, that no new, unplanned devices are connected to the infrastructure that introduce vulnerabilities. For example, an attacker might set up a rogue wireless access point or install an IoT device that allows remote access to the internal network.
- Run a pen-test scan against all internal systems as well as any provider- or cloud-hosted assets and services.
- Run full scans, with exploitation turned on for the vulnerabilities found, as a regular part of your policy/process for hardening software patches, software upgrades, new devices, and any configuration changes before pushing them live into the production environment.
- Run full scans, with exploitation turned on for the vulnerabilities found, as a regular part of the software development and software validation processes.

Protect Against Accidental or Malicious Access, Destruction, Leakage, and Tampering

Data privacy laws require you to implement and ensure protection against any accidental, unlawful, or malicious destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data. One obvious remedy is to use encryption wherever possible and necessary.

USING RidgeBot TO COMPLY

- Run a weak password scan against all assets to document and resolve login credential vulnerabilities.
- Ensure that a scan specifically targeting encryption-related vulnerabilities is part of the policy for cryptographic controls.
- Penetration testing can reveal weak points in physical security processes and systems that could grant an attacker physical or electronic access to secure systems or areas or allow tampering with surveillance cameras or stored footage.

TECHNICAL REQUIREMENTS

Ongoing Confidentiality and Resilience

The verbiage in data privacy laws not only require compliance but require ongoing compliance. This could be an expensive proposition if you have to hire an outside firm to do one-time penetration testing.

USING RidgeBot TO COMPLY

- RidgeBot's fully automated pen-test capabilities can be run cost-effectively as frequently as necessary, rather than doing occasional one-time tests. This ensures peace of mind that your assets are continually locked-down and that new vulnerabilities are detected immediately after—or often before—they're introduced into your production environment.
- Run regular automated asset discovery scans to ensure all assets and attack surfaces are identified and documented. These scans can additionally verify, on an ongoing basis, that no new, unplanned devices the introduce vulnerabilities connect to the infrastructure.

Documentation and Records

A key requirement of the data privacy laws is to document everything: activities, events, measures taken, safeguards instituted, vulnerabilities found, risk assessments, impact assessments, remedial steps taken, etc. Unlike compliance with industry standards, there is no "certification" process with data privacy laws. These are legal requirements and therefore apply on a continuous basis, and as with other laws, it is your responsibility to ensure ongoing compliance. In the event of an audit, complaint, investigation, or breach, you should be prepared to provide documentary evidence and justifications of your security posture and legal vigilance.

USING RidgeBot TO COMPLY

- RidgeBot's scan reports—results from the same scan repeatedly run on a fixed schedule—can assist you in compiling consistent and comparable documentation of vulnerabilities found, vulnerability ranking, successful exploits, and the mitigation and remedial steps taken.
- The recommended remedial steps in the RidgeBot reports provide evidence that risks are being adequately found, measured, reviewed, and treated.
- Run a scan to ensure that all systems or devices used to document events and activities are secure from weak credentials or other software/malware vulnerabilities.Vulnerabilities where a hacker can get access to erase or alter logs, video surveillance footage, or audit trail information.

Risk Assessment and Effectiveness

The data privacy laws require regularly testing, assessing, and evaluating the effectiveness of your security measures. In practice, this means doing continuous vulnerability scanning and penetration testing. Vulnerability scanning evaluates each system visible on the public internet and checks that operating systems, software, and patches/security are installed and up-to-date. You are required to keep and have available, upon request, objective risk and impact assessments, evaluations, and mitigation measures envisaged to address the risks.

While impact assessments are primarily administrative or managerial tasks, risk assessment is based on your assets' digital assessment. Moreover, the laws recognize that the digital economy changes over time and require you to be ahead of technology advances to keep up with new additions and changes in the threat landscape.

USING RidgeBot TO COMPLY

- RidgeBot's pen-test capabilities identifies, analyzes, and evaluates all risks found. The scan reports provide a ranked list of vulnerabilities found based on each vulnerability's likelihood to be exploited, including those successfully exploited during the test. Reports also evaluate with granular steps to remediate each vulnerability.
- Run full scans, with exploitation turned on for the vulnerabilities found, as a regular part of your policy/process for hardening software patches, software upgrades, new devices, and any configuration changes before pushing them live into the production environment.
- RidgeBot's built-in AI/ML exploitation engine uses RidgeSecurity's industry-leading knowledge base of attack techniques and ensures that your assets are always hardened with the most up to date vulnerability intelligence. It is the best way to detect emerging technical vulnerabilities in a structured and systematic way.

Breach Notification and Forensic Responsibility

A common requirement in the data privacy laws is the obligation to make breaches public within a specific time frame and inform impacted persons of their data exposed in the breach. The EU's GDPR requires notification within 72 hours of finding out about the breach. Clearly, the notification obligation is simplified and assisted by the speed with which you can get detailed and accurate forensic information from your systems.

USING RidgeBot TO COMPLY

- The pen-test scan reports—which include recommended solutions for each vulnerability—provide critical information for your security incident response/escalation or forensics team to ensure timely and effective handling of all situations.
- A forensic scan—after a security incident has occurred—can help determine where and how the breach was perpetrated. From there, it can extrapolate which systems and what data was exposed.

TECHNICAL REQUIREMENTS

GDPR Articles and Recitals

Salient extracts of the GDPR requirements that pertain to technical data-and-network security posture are given below. The full text of the GDPR-EU law can be viewed here.

Article 25 "Data Protection by Design and by Default"

Article 25 [1] states that "Taking into account… the cost of implementation… as well as the risks of varying likelihood and severity… posed by the processing, the controller shall… **implement appropriate technical** and organizational **measures**… designed to implement data-protection principles… in an effective manner and to **integrate the necessary safeguards** into the processing…"

Article 30 "Records of Processing Activities"

Article 30 [1] states that "Each controller… shall maintain a **record of processing activities** under its responsibility."

Article 32 "Security of Processing"

Article 32 [1] states that "…the controller… shall implement appropriate technical… **measures to ensure** a level of **security** appropriate to the risk, including [a] the… encryption of personal data; [b] **the ability to ensure the ongoing confidentiality**, integrity, availability and resilience of processing systems and services."

Article 32 [2] states that "In assessing the appropriate level of security, account shall be taken… of the risks that are presented by processing… from **accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data** transmitted, stored or otherwise processed."

Article 33 "Notification of a Personal Data Breach"

Article 33 [1] states that "In the case of a personal data breach, the controller shall, …not later than 72 hours after having become aware of it, notify the… supervisory authority..."

Article 33 [3a] states that "The notification… shall… describe the nature of the personal data breach including… the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned…"

Article 34 "Communication of a Personal Data Breach to the Data Subject"

Article 34 [3a] states that "The communication to the data subject… shall not be required if any of the following conditions are met… the controller has **implemented appropriate technical** and organizational **protection measures**, and those measures were applied to the personal data affected by the… data breach… in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption…"

Article 35 "Data Protection Impact Assessment"

Article 35 [7d] states that "The assessment shall contain… the **measures envisaged to address the risks**, including **safeguards**, **security measures** and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation…"

Recital 6 "Ensuring a High Level of Data Protection Despite the Increased Exchange of Data"

Recital 6 states that "Rapid technological developments and globalization have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organizations, **while ensuring a high level of the protection** of personal data."

Recital 39 "Principles of Data Processing"

Recital 39 states that "Personal data should be processed in a manner that **ensures appropriate security and confidentiality of the personal data**, including for **preventing unauthorized access** to or use of personal data and the equipment used for the processing."

Recital 49 “Network and Information Security as Overriding Legitimate Interest”

Recital 49 states that “The processing of personal data to the extent strictly necessary and proportionate for the purposes of **ensuring network and information security**, i.e. the ability of a network or an information system to **resist**, at a given level of confidence, **accidental events or unlawful or malicious actions** that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems… This could, for example, include preventing unauthorized access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.”

Recital 76 “Risk Assessment”

Recital 76 states that “Risk should be evaluated on the basis of an **objective assessment**… [to establish] whether data processing operations involve a **risk or a high risk**.”

Recital 78 “Appropriate Technical and Organizational Measures”

Recital 78 states that “…the controller should **adopt internal policies and implement measures** which meet in particular the principles of data protection by design and data protection by default. Such measures could consist of… enabling the controller to create and improve security features. When **developing, designing, selecting and using applications, services and products**… producers of the products, services and applications should… take into account the right to data protection when developing and designing such products, services and applications, and… make sure that controllers and processors are able to fulfil their data protection obligations.”

Recital 82 “Record of Processing Activities”

Recital 82 states that “Each controller… should… **make records**, on request, available to [the supervisory authority]…”

Recital 83 “Security of Processing”

Recital 83 states that “…controller… should **evaluate the risks** inherent in the processing and implement measures to mitigate those risks, such as encryption…”

Recital 84 “Risk Evaluation and Impact Assessment”

Recital 84 states that “…the controller should be responsible for the **carrying-out of a data protection impact assessment** to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should… [determine] the appropriate measures to be taken in order to demonstrate that the processing of personal data complies…”

Recital 90 “Data Protection Impact Assessment”

Recital 90 states that “…a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the… likelihood and severity of the high risk… and the sources of the risk. That impact assessment should include… the **measures, safeguards and mechanisms envisaged for mitigating that risk**…”

Recital 91 “Necessity of a Data Protection Impact Assessment”

Recital 91 states that “This should in particular apply to large-scale processing operations [that] process a considerable amount of personal data at [a] regional, national or supranational level and which could affect a large number of data subjects and which are likely to **result in a high risk**…, where… **a new technology is used** on a large scale, as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects…”

Company Profile

Ridge Security delivers ethical, efficient and affordable pen testing solutions to enterprises, small and large. We ensure our customers stay compliant, alerted and secure at all times in the cyber world. The management team has many years of networking and security experience. Ridge Security is located in the heart of Silicon Valley and is expanding into other areas including Latin America, Asia and Europe.

RidgeBot, a robotic penetration testing system, fully automates the testing process by coupling ethical hacking techniques to decision-making algorithms. RidgeBots locate, exploit and document business risks and vulnerabilities discovered during the testing process, highlighting the potential impact or damage.

Ridge Security Technology Inc.
www.ridgesecurity.ai