PROTEGRITY® FOR GENERAL DATA PROTECTION REGULATION (GDPR)

Data Protection for the Data-Driven organization

Protegrity's Data Protection Platform helps data-driven organizations comply with the EU's General Data Protection Regulation (GDPR) by implementing enterprise-wide privacy data protection that meets compliance expectations without compromising business processes.

Protegrity is the only enterprise data security software platform that helps brands honor obligations to protect personally identifiable information (PII) while maintaining its value and usability on-premises, in the cloud, and by third parties, regardless of operating system or application.

GDPR mandates that organizations must know where and how the private data of European citizens is stored and accessed, then prove that it is appropriately protected "by design and by default" throughout its lifecycle with, "the existence of appropriate safeguards, which may include encryption or pseudonymization."

THAT IS PRECISELY WHAT PROTEGRITY DOES.

Data Protection that Delivers

Customer-centric and digitally-disruptive organizations that uphold privacy as a brand value increasingly rely on Protegrity's innovative solutions to thwart internal and external threats to PII without compromising the analytic value of the data or compliance with regulatory requirements.

Protegrity's data-centric approach to protecting PII for GDPR compliance provides businesses with centralized control and management so they can create rule-based security policies to handle these data-centric operational needs:

- Which data shall be protected?
- How shall the data be protected?
- Who shall have access to it?
- Where shall the policy be enforced?
- Audit of access and attempts by whom, to what, where and when?

Once organizations see where data resides and what its purpose is, they can choose from a variety of data protection methods that Protegrity has developed and refined over the past two decades: the tokenization and encryption processes that hide, or pseudonymize, elements of data; or the privacy models that strip elements of data out of data sets, effectively anonymizing some data elements so data scientists and third parties can never access the sensitive data.

With this detailed level of control, enterprises can select a type of protection that best suits business objectives. A retailer, for example, can pseudonymize aspects of a customer's personal information so that a customer service representative sees a name and address but only meaningless digits and characters in place of a national or social identification number—a step that should soothe customers who are concerned about privacy. Similarly, by choosing to anonymize certain data—whether it's PII, PHI, or PCI—organizations can point to how even if the larger data set is ever breached, the sensitive data is nowhere to be found.

Key Terms

Pseudonymisation

A method of de-identifying PII, advocated by GDPR, to protect individuals' rights during data processing. The pseudonymization of sensitive data can be done in one of two ways: tokenization or encryption.

Tokenization

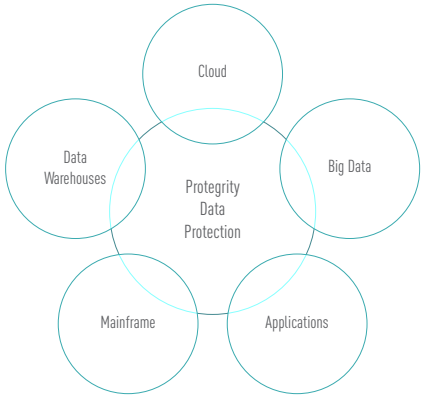
A non-mathematical, reversible method of pseudonymisation that substitutes PII with random fake data that preserves data type, length and format, allowing legacy architecture underneath to remain operational. Tokens can keep the data's integral value fully or partially visible, enabling secure data processing and analytics.

Encryption

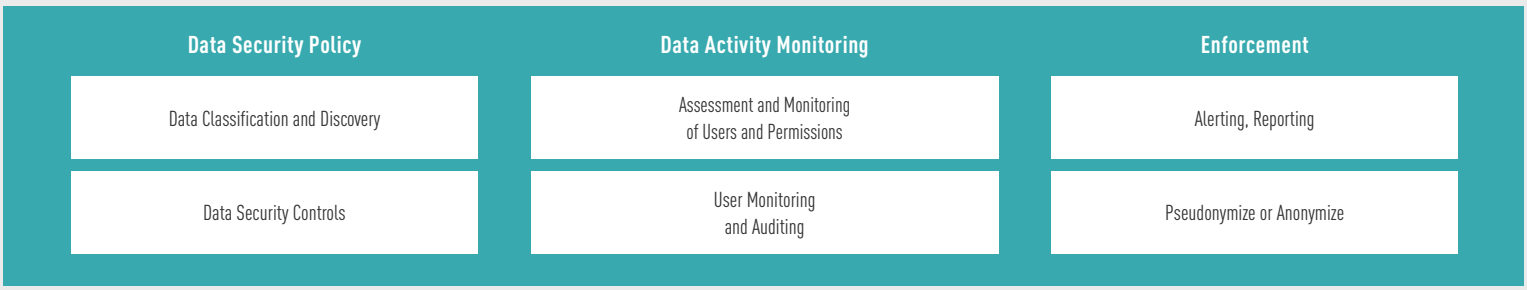
A mathematical method of rendering PII unintelligible to any person without the authority to access it.

Anonymization

The opposite of pseudonymization: privacy models essentially irreversibly strip bare data elements that organizations don't want seen by data analysts, business partners or data marketplaces.



Data Protection that Simplifies Compliance



Codes of Conduct

GDPR requires organizations to create and apply codes of conduct to demonstrate protection of PII. Protegrity enables organizations to easily and consistently manage and control access to PII by centrally-enforcing data protection policies based on codes of conduct via user-friendly interfaces so that it remains protected throughout the entire data flow.

Privacy by Default & Design

Under GDPR, organizations are required to, "implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access." Protegrity's data security software platform mitigates internal and external threats to PII on-premises and in the cloud by empowering organizations to enforce separation of duties and protect and control access to data.

Breach Notifications

Protegrity helps organizations mitigate the impact of GDPR's breach notification requirements by protecting PII so that should a breach occur, data no longer identifies people or any sensitive information.

Rights of Individuals

GDPR gives consumers more control over their personal information including: "Right to be Informed, Right of Access, Right to Rectification, Right to Erasure/to be Forgotten, Right to Restrict Processing, Right to Data Portability, Right to Object and Rights in Relation to Automated Decision Making and Profiling." regarding how and why their data is being processed. Protegrity's encryption technology helps organizations meet these obligations without impeding their ability to extract value from data.

Third Parties and Cross Border

With Protegrity, organizations can confidently and compliantly embrace cloud technology and share large datasets with third parties and across borders by de-identifying PII. Masked or tokenized data can be embedded with business intelligence analytical programs without the need for third parties to re-identify individuals.

Protecting Against Penalties for Failure to Comply

A data-centric audit and protection approach to GDPR significantly reduces the likelihood of fines of up to four percent of global revenues for failure to comply. Thanks to the Protegrity Data Protection Platform's centralized management of access controls, monitoring, auditing, and reporting, organizations can simplify their observance of GDPR.

Key benefits

- Simplified compliance with GDPR, PCI DSS, IPA, internal policies and other data regulations, by design and by default.
- Central policy control and management of automated sensitive data protection and access, monitoring, auditing and reporting, in transit, at rest, in use and across borders.
- Minimal disruption to internal and third-party users, processes and applications, on premises and in the cloud.
- Dynamic, transparent de-identification of PII with vaultless tokenization, encryption, and anonymization.
- Flexible deployment across databases, applications, file servers, applications.

Protegrity USA, Inc.
(Global Headquarters)
1165 E Wilmington Avenue
Suite 200
Salt Lake City, Utah 84106
1.203.326.7200
1.650.431.7000

Email: info@protegrity.com
www.protegrity.com