DATA ERASURE · DATA GOVERNANCE · COMPLIANCE · PRIVACY

WHITEPAPER · 2025

SURVIVING AND THRIVING IN THE AGE OF PRIVACY

Data Governance with Overty

Overty®

overtytech.com · Data Erasure & Governance

CONTENTS

Data Governance with Overty

$4.44M
COSTO PROMEDIO
average cost of a data breach IBM 2025

240+
DÍAS
detection and containment time

100%
CERTIFICADO
independently audited erasure

01

Introduction

Why does data erasure matter?

We live in a world where data management is strategic. Organizations generate, collect and process massive amounts of information: from personal identifiers and financial records to electronic communications and sensitive customer and employee data. However, not all of this information has permanent value for the business or a legal purpose that justifies keeping it indefinitely.

When data that should no longer exist remains stored, it not only wastes technological resources but also increases the risk of unwanted exposure. This accumulation of unnecessary information means every breach or unauthorized access can have a broader and more costly impact on the organization.

The risk is quantifiable and growing

The **IBM Cost of a Data Breach Report 2025** reports that the average global cost of a data breach is **USD $4.44 million** per incident. This cost includes:

— Immediate response costs

— Forensic investigations

— Regulatory fines

— Loss of revenue and customers

— Reputational damage

> ■ **Key fact**
>
> Breach detection and containment times often exceed
> 240 days, multiplying the total damage of the incident.
> The more data a company holds, the larger its attack surface.

Beyond security: privacy and trust

Deleting unnecessary data is a **measure of respect for people's privacy**. A database saturated with obsolete information can be exploited for identity theft, fraud or targeted phishing, and increases the likelihood of sensitive personal data being exposed.

Deleting unnecessary data **reduces the organization's "data footprint"**, enabling a stronger, more reliable and defensible privacy posture before regulators.

Section conclusion: Secure data erasure tangibly reduces the risk of costly breaches, optimizes infrastructure and reinforces the trust of clients, partners and auditors.

02

Current State

Tools without governance

In many organizations there is a **critical contradiction**: they have software licenses to erase data, but **lack a structured erasure management approach** as part of their data governance. This gap between technology and process has important consequences.

What is really happening?

While erasure tools can delete information individually, they do not by themselves solve the organizational challenges:

- **No formal documented processes** that establish how and when to erase each type of data.
- **No approved retention policies** with clear rules based on risks and regulations.
- **No integration with key business processes** such as backups, equipment leasing or staff offboarding.
- **No retention matrix exists** assigning deadlines by information type and regulatory framework.
- **No centralized traceability captured** nor auditable evidence to support deletion decisions.

Consequences of the structural gap

Erasure happens reactively, without formal criteria.
No documented evidence exists for audits or regulators.
Data minimization and quality principles go unmet.
Risk grows silently every day.

03

Regulatory Framework

The compliance imperative

The global regulatory landscape demands not only protecting data, but also managing its complete lifecycle — including timely and verifiable deletion. Organizations without formal erasure processes face growing sanctions.

GDPR (Europe)

Requires the "right to erasure" and data minimization. Retaining information without legitimate purpose violates the storage limitation principle.

ISO/IEC 27001

Requires formal controls over the information asset lifecycle and secure disposal of media and equipment. Annex A Control 8.10.

PCI-DSS

Requires cardholder data to be retained only when strictly necessary and deleted securely and verifiably. Requirements 3.1 and 3.2.

HIPAA (USA)

Establishes specific requirements for the disposal of protected health information, both physical and digital.

LFPDPPP (Mexico)

Provides the right of cancellation and requires suppression of data once the purpose for which it was collected has been fulfilled.

The critical difference

Compliance is not enough — you must DEMONSTRATE compliance.
Without documented evidence of deletion, there is no real compliance.
Regulators demand traceability, not just good intentions.

04

The Real Risks

Of ungoverned data lifecycle management

Every forgotten file, every unpurged historical backup, every reassigned device without formal control is a potential source of exposure. Ungoverned erasure is not a minor omission: **it is a structural risk**.

4.1 Compromised privacy

■ **Expands the attack surface**

Más datos almacenados significan más vectores potenciales de acceso. Attackers make no distinction between "active" and "forgotten" data.

■ **Amplifies breach exposure**

When an incident occurs, impact depends directly on the volume and sensitivity of compromised information. Retaining purposeless data amplifies the damage.

■ **Can trigger regulatory sanctions**

Data protection laws require retaining information only as long as necessary. Keeping data without justification may constitute non-compliance.

4.2 Real financial costs

The average breach cost reaches **USD $4.44 million**. With poor data governance, the impact is amplified by greater data volume compromised, additional regulatory scope, forensic complexity and more mandatory notifications.

■ Forensic and legal services

■ Loss of customer trust

■ Contract cancellations

■ Increased cyber insurance premiums

■ Long-term reputational damage

> ■ **The silent risk**
>
> The most silent risk is NOT DELETING data when required.
> Indiscriminate data accumulation is not digital strength.
> It is accumulated vulnerability — visible to attackers.

05

The Overty Solution

Governance, automation and traceability

Most organizations already have erasure tools. What they lack is **governance**. Overty proposes a paradigm shift: from reactive erasure to **governed, automated and auditable erasure**.

It is not just about deleting data. It is about turning deletion into a formal corporate process, aligned with regulation, risk and business strategy.

What makes Overty different?

✔ Política corporativa de retención y eliminación

Design and implementation of formal guidelines aligned with international regulations and best practices.

✔ Matriz de retención por tipo de dato

Clear definition of what is retained, for how long, and under which legal or regulatory basis.

✔ Integración con procesos críticos de negocio

Backup, leasing, tech refresh, migrations and offboarding are no longer blind spots.

✔ Trazabilidad centralizada y reportes auditables

Consolidated, verifiable evidence ready for internal or regulatory audits.

✔ Evidencia certificada de eliminación

Documentary support aligned with NIST 800-88, DoD 5220.22-M, ISO 27001, PCI-DSS and GDPR.

> **■ The value proposition**
>
> Overty does not just execute erasure.
> It turns it into a defensible corporate control.
> Structured governance + automation + traceability
> aligned with international regulatory frameworks.

06

Regulatory Compliance

Overty as an evidence enabler

The difference between complying and demonstrating compliance is critical. Lack of documented evidence can generate findings or sanctions under the most demanding regulatory frameworks.

ISO/IEC 27001

Requires formal controls over asset lifecycle. Overty generates evidence aligned with Annex A, Control 8.10.

PCI-DSS

Requires secure and verifiable deletion of sensitive data. Overty meets requirements 3.1 and 3.2.

CNBV and Banxico

Demand comprehensive technology risk management and evidence of control implementation.

GDPR / LFPDPPP

Overty's certified erasure supports the right to erasure and the minimization principle under both frameworks.

Without process, there is no control. Without evidence, there is no compliance. Overty closes the gap between the technical tool and the corporate process, integrating governance, automation and traceability in a single operational framework.

07

Conclusion

Privacy as a competitive advantage

Data is no longer just a technological or financial asset. It is a reputational, regulatory and strategic asset. Organizations are responsible for managing the complete lifecycle of their information, including its timely and verifiable deletion.

In an environment where regulations are increasingly strict, breaches more frequent and costly, and customers demand greater transparency, privacy becomes an element of **business trust** — not just compliance.

Organizations that govern the data lifecycle:

✔ Reduce their exposure to legal and financial risks

✔ Diminish the potential impact of security incidents

✔ Strengthen their posture before audits and regulators

✔ Build credibility with clients and investors

✔ Turn privacy into a sustainable competitive advantage

■ The result

Overty enables the shift from informal, reactive erasure
to a structured, automated and auditable model,
aligned with international regulatory frameworks.

In a market where trust is a scarce asset,
data governance becomes a competitive advantage.

Overty Corporation LLC · overtytech.com

Data Erasure · Data Governance · Compliance · Privacy