EBMI 2026

ITAD CONFERENCE

WHEN DATA BECOMES WASTE

The Hidden Liability and Opportunity in Every Device

Angelos Ginis

CEO

GreenFence–MetalLogic S.A.

GreenFence | MetalLogic

WHO WE ARE

GREENFENCE - METALLOGIC S.A.

GREENFENCE

Secure Data Destruction

- GDPR-Compliant Destruction
- Certified Processes (DIN 66399)
- ITAD Services
- Full Traceability & Reporting
- Confidential Destruction Bins
- Data Security Audit & Consulting

GreenFence | MetalLogic

YOUR TRUSTED PARTNER

SINCE 1972

METALLOGIC

Precious Metals Recovery

- Electronic Waste
- x-Ray Films
- Catalytic Converters
- Advanced Sampling & Refining
- Industrial & Hazardous Waste Refining
- On-site Material Sorting Services

ONE PARTNER.

TWO DIVISIONS.

FULL SOLUTION.

WHY THIS MATTERS

Data does not disappear when a device becomes waste.

SENSITIVE DATA OFTEN REMAINS ACCESSIBLE
Even after a device reaches the recycling stream.

DATA PROTECTION OBLIGATIONS DO NOT END AT DISPOSAL
Risk continues beyond the asset's useful life.

REGULATORS AND CUSTOMERS EXPECT ACCOUNTABILITY
Proof of secure handling is becoming essential.

SECURITY AND CIRCULARITY MUST WORK TOGETHER
Data protection and resource recovery are no longer separate challenges.

THE EVIDENCE

42% **Sensitive data** found on used drives

€3.87M **Germany:** Average breach cost per incident

443 **Personal data breach** notifications per day in Europe

€1.2B **GDPR Fines** issued in 2025

Sources:
Blancco / Ontrack study (159 used drives purchased across US, UK, Germany & Finland), DLA Piper, GDPR Fines and Data Breach Survey: January 2026; IBM, Cost of a Data Breach Report 2025

SECURE DATA HANDLING PROTECTS PEOPLE, BUSINESSES AND THE PLANET

THE CORE CONFLICT

Data Destruction vs. Waste Regulation

WEEE

PROTECT THE ENVIRONMENT

- Collection
- Recycling
- Recovery
- Traceability

VS

GDPR

PROTECT THE DATA

- Confidentiality
- Security
- Accountability
- Compliance

01.

WEEE & Waste Legislation

Pushes data-bearing devices into recycling streams. Focuses on environmental treatment and material recovery — not data security.

02.

GDPR & Data Protection Laws

Hold organizations — including recyclers — legally responsible for any personal data that survives disposal. Liability does not disappear at the collection point.

THE RESPONSIBILITY GAP

Who Controls This Gap? In Practice, No One.

Producers & EPR Systems

Fund recycling but routinely **exclude data destruction** from their scope and budgets.

Collection Points & Retailers

Accept devices without verifying whether data has been sanitized — **no questions asked**.

Consumers & Companies

Assume "recycling" automatically means "data deleted." **It does not.**

Regulators

Intervene **after breaches occur** — not preventively within recycling flows where the risk originates.

This is where the recycler becomes exposed.

The Gap Between Theory and Practice

In theory, end users should delete data before disposal. In practice, **this cannot be guaranteed.** Devices enter the recycling stream with data intact as users forget, don't know how, or assume recycling handles it.

ICO 2024 Findings Highlight the Limits of User-Led Erasure

- 14 million UK adults do not know how to erase data from old devices
- Average person keeps 3 unused devices at home
- 1 in 5 keep old devices due to personal-data concerns

⚠ **This is where the recycler becomes exposed.**

Data-protection principles are clear: personal data cannot move through the recycling chain without control. The risk defaults to the recycler — not by design, but by omission. Recyclers are already carrying this responsibility, **whether they want it or not.**

DPIA as a protection tool

A Data Protection Impact Assessment helps recyclers show they have identified and mitigated risks before something goes wrong. GDPR Article 32 requires controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

Authorities expect evidence of control, not perfection.

Key Questions to Answer

What data-bearing devices do we receive?
Identify device types and quantities

What types of data may be inside?
Assess data sensitivity and risk level

Who has access to the devices?
Control access to sensitive materials

Where are they stored?
Secure storage and location tracking

Destruction Methods

Wipe
Software erasure

Degauss
Magnetic destruction

Shred
Physical destruction

Crush
Mechanical damage

Evidence Requirements

- Verification results
- Destruction certificates
- System logs

Chain of custody

6-Step Workflow for Secure Data Destruction

Secure Transportation

Controlled collection & traceable movement of data-bearing material.

01

Reception & Verification

Confirm material received, quantities, batches, & identify data-bearing devices.

02

Secure Storage

Segregated storage in restricted-access areas until destruction.

03

Method Selection & Destruction

Choose the appropriate method for each media type and perform destruction.

04

Documentation & Verification

Record the method, date, operator, result, and any exceptions.

05

Certificate of Destruction

Issue final proof linked to the customer, batch, or asset.

06

DATA DESTRUCTION IS NOT ONLY THE FINAL DELETION STEP.
IT IS A CONTROLLED WORKFLOW FROM COLLECTION TO DOCUMENTED PROOF.

Personnel Security

Worker Compliance & Training

Implement comprehensive workforce controls to ensure data security and GDPR compliance throughout the recycling process.

Essential Controls

NDA/Confidentiality Agreement
Workers sign additional confidentiality agreements

GDPR & Data Training
Comprehensive data protection training

Data-Handling Policy
Acceptable-use and data-handling policy

Background Screening
Criminal/background checks where permitted

Training Requirements

Annual

GDPR fundamentals	Required
Data handling procedures	Required
Security awareness	Pending

Value Preservation

Destroy the Data, Not the Value

Data destruction is not one action — it is a chain of control.
Compliance is proven by the process around it, not just the final deletion step.

Principles

Value Preservation

HIGH VALUE

1. **Identify device types and quantities**
   Data-bearing devices have high precious-metal value
2. **Dismantle Separately**
   Process high-grade materials before low-grade
3. **Match Method to Media**
   Choose appropriate destruction technique
4. **Document Everything**
   Keep records for compliance and verification

Examples

Implementation

PRACTICAL

1. **HDD PCB Removal**
   Prevents plug-and-play recovery
2. **Wiping Tools**
   Free/low-cost options available
3. **Degaussing**
   New degaussers -> 3 seconds per piece for HDDs
4. **Simple Shredding**
   Any kind of shredding, damaging can be considered as data destruction

Security Framework

Minimum Viable Data-Security System

Implement a minimum viable data-security system that protects sensitive information while maintaining operational efficiency and cost-effectiveness.

01.

Physical Security

- **Separate at receiving**
  Identify data-bearing devices immediately
- **Locked storage**
  CCTV monitoring for secure areas
- **Access control**
  Limit to trained personnel only

02.

Training

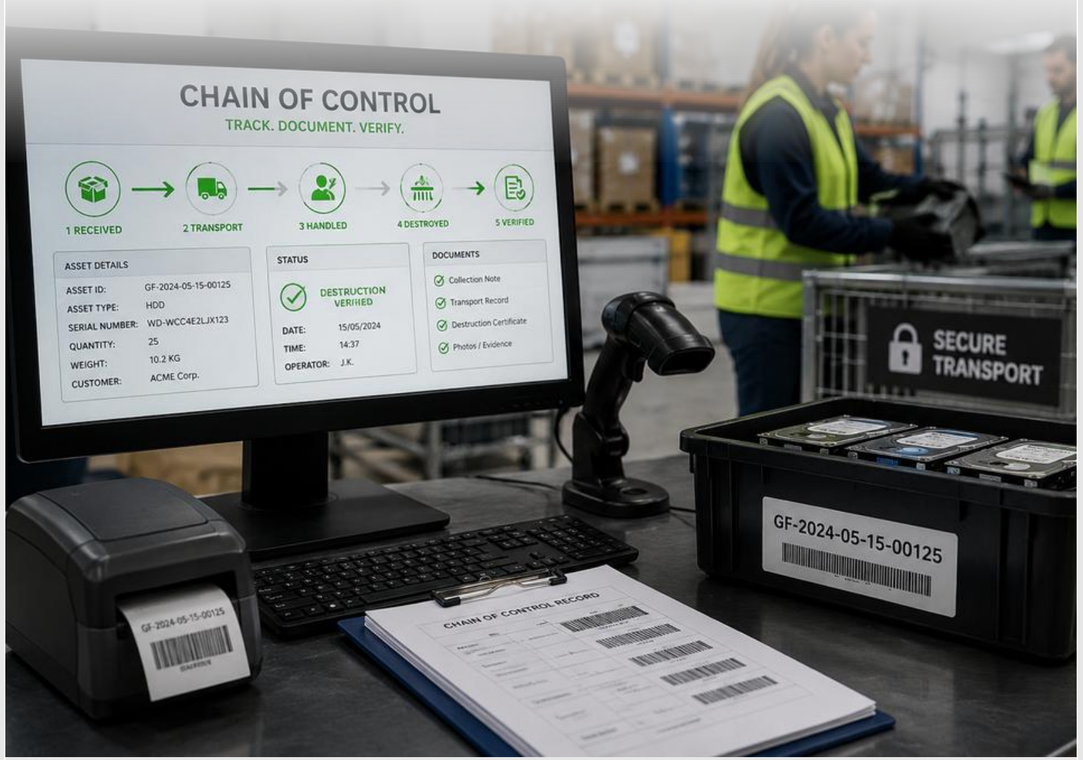
- **Worker training**
  Annual refresher training
- **Access logging**
  Track who handles devices
- **Security audits**
  Regular compliance checks

03.

Documentation

- **Documented destruction**
  Simple but documented methods
- **Record retention**
  Keep records for defined period
- **Exception handling**
  Handle missing devices/failed wipes

Chain of Control
Documentation



A recycler must be able to prove the full chain of control.

Without documentation, data destruction is only a statement.
With documentation, it becomes evidence.

What Came In
STEP 1

Customer: Device source
Device Type: HDD, SSD, Mobile
Quantity: Count/Weight
Serials: Batch numbers

Where It Went
STEP 2

Transport: Record route
Storage: Location ID
Area: Restricted access

Who Handled It
STEP 3

Operator: Trained personnel
Access: Controlled entry
Responsibility: Assigned roles

How Destroyed
STEP 4

Method: Wipe/degauss/shred/other
Verification: Destruction proof
Dismantle: Component separation

When It Happened
STEP 5

Date: Destruction date
Time: Specific timestamp
Frequency: Destruction schedule

What Proof Exists
STEP 6

Certificate: Destruction proof
Logs: System records
Photos: Visual evidence
Transfer of Custody: Downstream recycler, handover record, destruction proof

High-Risk Assets

Strategic Device Analysis - Risk vs Value

DEVICE TYPE	DATA RISK	VALUE	RECOMMENDED ACTION	STATUS
HDD	High	Medium/High	Degauss or shred, then recover metals	• Active
SSD	High	Medium	Do not degauss; shred or verified sanitization	• Active
MobilePhones	Very High	High	Secure storage, dismantle, destroy memory-bearing parts	• Active
Laptops	High	High	Remove drive, process separately	• Active
Servers	Very High	High	Asset-level tracking, serials, customer certificate	• Active
Printers/Copiers	Medium-Low	Low	Check internal HDD/SSD/memory	• Check
Network Equipment	Medium-High	High	Reset/sanitize, remove storage where present	• Active
USB/SD Cards	High	Medium	Physical destruction	• Active

Commercial Opportunity

Is Data Destruction Worth It?

Analyzing the cost-benefit equation of secure data destruction services and their impact on business value.

Do customers want data destruction?
Yes Most customers don't actively seek it

Do customers pay for it?
No Willing to pay for security

Does it attract new customers?
Yes Security creates competitive advantage

Cost vs. return?
Positive When bundled with services

Trust & Retention
improves customer loyalty

Contracting
Better contract terms

Compliance
Regulatory protection

CLOSING

Key Takeaways

Waste Vs Data

When a device becomes waste, the data inside is not waste.

Recycler’s Threat

A recycler is authorized to recover the material — metals, plastics, components — not to access, use, copy, or allow others to access the data inside.

Reduce Risk

The solution does not have to be complicated: simple, risk-based, well-documented procedures can significantly reduce the risk.

Thank you!

Angelos Ginis
CEO
GreenFence–MetalLogic S.A.

GreenFence | MetalLogic