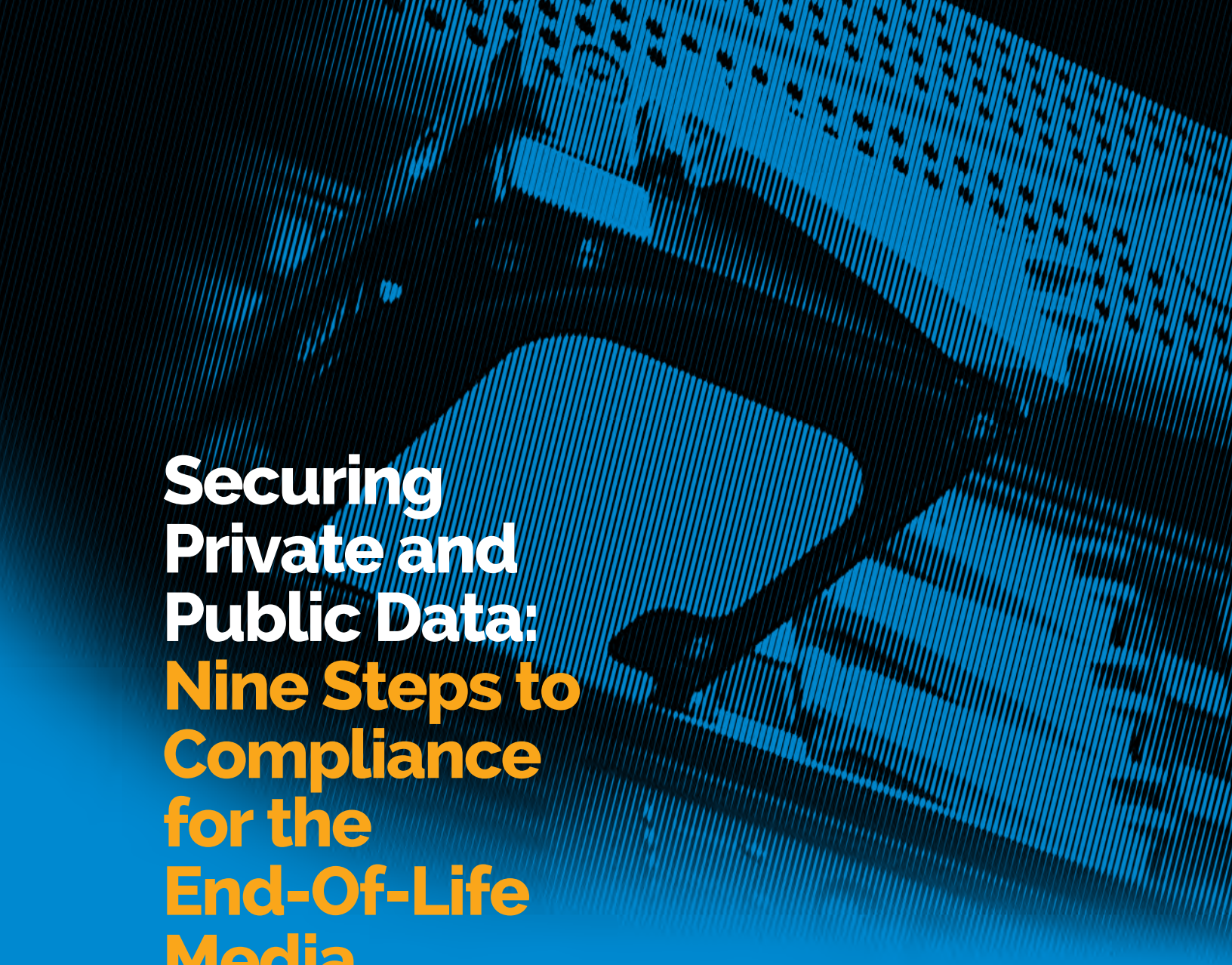

Securing Private and Public Data: Nine Steps to Compliance for the End-Of-Life Media Ecosystem

tech2

Securing Private and Public Data: Nine Steps to Compliance for the End-Of-Life Media Ecosystem

Contents

Securing Private and Public Data: Nine Steps to Compliance for the End-Of-Life Media Ecosystem

Securing Private and Public Data: Nine Steps to Compliance for the End-Of-Life Media Ecosystem

The Challenges in Data Security

How successful are you at securing data in an adverse environment of enterprise facilities, datacenter decommissioning and secure transport operations? Are you trying to make outmoded processes compliant? Do you have confidence that you have control of the data you possess during these operations?

Maybe you did survive another year where the internal compliance auditors did not ask the tough questions. Will you endure through the harder compliance audits being launched this year by federal and state agencies? Will your process survive the Cybersecurity Whistleblowers?

How long can you hide the facts that your current processes are not tied to Cybersecurity regulations concentrating on Risk Management, Planning, Training, and Compliance?

Wherever you are in the process, this whitepaper can help you. It explores the nine steps in securing public and private data when you are performing data destruction, decommissioning a datacenter or secure transport operations.

Threats to personal and public data

Just as organizations enjoy the automation benefits that the As A Service distributors offer, cyber criminals do also. Today's cyber attackers increasingly infiltrate datacenter environments and take advantage of the fact that their impersonator will not be recognized by datacenter staff.

IBM estimates the data loss in physical breaches as a result of unauthorized access at $400 billion *annually*.

The risks of unauthorized access to data are reported as:

1. Risk One: The Insider Threat
2. Risk Two: The Outsider Threat
3. Risk Three: The Seemingly Innocent Personal Item
4. Risk Four: Poor or Nonexistent Identity Verification

These startling results highlight the frequency with which cybercriminals are targeting datacenters using sophisticated techniques. The challenge for security teams lies in identifying and securing potential vulnerabilities and stopping an attack in its tracks.

With the General Data Protection Regulation (GDPR) in effect, data management is paramount when destroying data, decommissioning, or moving customer data.

"GDPR has expanded the responsibility of protecting critical data to any entity that is a 'controller' of the data," says Charles Robbins, Compliance Officer at TechR2. "As such, traditional Chain of Custody concepts will no longer protect an organization from regulatory reach."

12477 Broad Street SW, Pataskala, Ohio 43062 | **614.322.2222** | clientrelations@techr2.com | **techr2.com**

Securing Private and Public Data: Nine Steps to Compliance for the End-Of-Life Media Ecosystem

Maintaining compliance standards

When your customers and your cybersecurity auditor interact with you, do they tell you that your policy, procedures, execution, verification, and monitoring is exceptional? In a world of customers fearing a partner breach of their data, what people say about you will determine whether you receive another contract extension or more.

Data security is a top decision-making attribute with more and more enterprises and with all levels of government.

12477 Broad Street SW, Pataskala, Ohio 43062 | **614.322.2222** | clientrelations@techr2.com | **techr2.com**

Securing Private and Public Data: Nine Steps to Compliance for the End-Of-Life Media Ecosystem

NNine Steps to Securing Private and Public Data

Step 1: Governance and global mandates

The EU General Data Protection Regulation (GDPR) that went into effect on May 24, 2018, has changed the landscape of data protection for tracking.

Article 33 and Recital 85 require controllers to notify the supervisory authority of a personal data loss no later than 72 hours after having become aware of it.

Article 25 and Recital 87 state that it should be ascertained whether all appropriate technological protection and organizational measures have been implemented to establish immediately whether a personal data breach has taken place.

Cybersecurity Framework (CSF) Compliance is required for companies doing federal work.

The Federal Acquisition Regulation (FAR) governs all federal government acquisitions and contracting procedures; DFARS is the special supplement for DoD-related contracts. The FAR Final Rule 52.204-21 on "Basic Safeguarding of Contractor Information Systems," which became effective June 15, 2016, contains 15 controls that are considered the minimal baseline for federal contractors. These controls resonate with basic security objectives contained in NIST SP 800-171 Revision 2.

Starting this year, the compliance model will begin to move from self-attestation (i.e., the current NIST SP 800-171 compliance model) to third-party validation in accordance with the new, three-level Cybersecurity Maturity Model Certification (CMMC 2.0).

The majority of US States adopted the NIST Cybersecurity Framework (CSF), specifically NIST SP 800-53 R5 for their agencies, contractors and subcontractors. Media Protection (MP) is one section of the NIST CSF that has been scrutinized by the US Inspector General for failing the control.

NIST SP 800-53 MP-6(1) MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

Industry rules require businesses to be subject to mandatory compliance standards imposed by the government (such as HIPAA, SOX, PCI DSS). These standards often stipulate how businesses should secure Personally Identifiable Information (PII), and other sensitive data. A Data Loss Prevention (DLP) policy is a basic first step to compliance, and most DLP tools are built to address the requirements of common standards.

HIPAA requires strict control of medical data which eliminates the possibility of shipping loose media and decommissioned data bearing devices offsite.

FFEIC Handbook Rules for Banks and Financial Institutions require extraordinary tracking and containing of data and data bearing devices.

Payment Card Industry (PCI) - Credit card processors are required to notify the card associations on a quarterly basis to identify any merchant who is not PCI compliant. Merchants can face penalties and fines by the credit card associations for not being compliant and may even have their ability to accept credit card payments terminated.

12477 Broad Street SW, Pataskala, Ohio 43062 | **614.322.2222** | clientrelations@techr2.com | **techr2.com**

Securing Private and Public Data: Nine Steps to Compliance for the End-Of-Life Media Ecosystem

IBM Own Cloud Compliance Policy

Compliance - Last Updated: 2019-07-31

IBM® Cloudant® for IBM Cloud provides a trustworthy and secure cloud database system. The service is built on best-in-industry standards, including ISO 27001:2013.

HIPAA - IBM Cloudant, when deployed on dedicated hardware on IBM Cloud, meets the required IBM controls that are commensurate with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security and Privacy Rule requirements.

International Organization for Standardization (ISO) - IBM Cloudant and IBM Cloudant Dedicated Cluster are audited by a third-party security firm and meet ISO 27001, ISO 27017, and ISO 27018 requirements.

SOC 2 Type 2 Certification - IBM provides a Service Organization Controls (SOC) 2 Type 2 report for Cloudant.

General Data Protection Regulation (GDPR) - The GDPR seeks to create a harmonized data protection law framework across the EU and aims to give citizens back the control of their personal data, while imposing strict rules on those hosting and 'processing' this data, anywhere in the world.

Step 2: Plan for multi-step processes

You will find that Cybersecurity Frameworks (CSF) follow logical data security steps to Identify, Protect, Detect, Respond and Recover. Control of your data in a datacenter is part of this multi-step sequence.

1. Complete a Risk Assessment (RA) of the Data Destruction, Sanitization for Refreshes, Decommissioning or Secure Transport operation
2. Create data destruction / decommissioning / secure transport plan that meets or exceeds the parameters of the RA
3. Project managers create timelines, review data security processes that meet RA and legal requirements
4. Employees and vendors comply with the cybersecurity checklist
5. Data Destruction, Decommissioning or Secure Transport work is completed in accordance with the Project Management guidelines within the cybersecurity framework
6. Data Destruction Event is conducted with reconciliation, audit, destroy data, Certificate of Destruction (CoD) and ISO 14001 recycling
7. Close Project and transmit CoD, Audit and Green Reports, and Certificate of Recycling

Step 3: Global view

You need data control that is a cradle to grave solution for tracking, containing and destroying Data at Rest and is a proven technique used by large financial, healthcare, retail and hospitality industries. The solution should be a far right and far top choice in data security and helps you pass your internal regulatory audits, since the solution is fully compliant and certified for ISO 27001, 9001, 45001, 14001 and 31000.

12477 Broad Street SW, Pataskala, Ohio 43062 | **614.322.2222** | clientrelations@techr2.com | **techr2.com**

Securing Private and Public Data: Nine Steps to Compliance for the End-Of-Life Media Ecosystem

Step 4a: Follow Track – Contain – Destroy – Verify for Data Destruction and Datacenter Decommissioning

By now, you should be aware of the Federal and State NIST CSF requirements that require you to control the data in the datacenter. You must:

- Track your data-bearing devices using a technological method such as RFID and establish a real time inventory and audit trail via tailored customer portal.
- Contain data-bearing devices securely in a locked Appliance, only accessible by certified staff.
- Destroy data onsite, within the four walls of your facility, and receive a Certificate of Destruction prior to the departure of the dual technicians.
- Verify data destruction via dual controlled teams and electronic reporting to reconcile internal data bases/asset inventories.

Step 4b: Follow Track – Contain – Verify for Secure Transport

By now, you should be aware of the Federal and State NIST CSF requirements that require you to control the data in transit. You must:

- Track your data-bearing devices using a technological method such as RFID and establish a real time inventory and audit trail via tailored customer portal.
- Contain data-bearing devices securely in locked containers, only accessible by certified staff.
- Verify data bearing devices throughout the transit via dual controlled teams and electronic reporting to reconcile internal data bases/asset inventories.

Step 5: Automate your processes

When a company experiences a Data Security incident, which solution do you think a CISO wants? A completely digital solution that actually meets the NIST regulation or a something someone locally just contrived. Look at your documents and compare them to the NIST standard and you will be shocked that your old solution is not compliant.

Besides compliant reports, your data security team will appreciate the ease of conducting internal audits on your systems without the necessity of flying to each location. Your internal auditors can view current data 24-7 through a Customer Portal.

Step 6: Accept ISO and Worldwide Compliance

It is 2022 and non-compliant data security companies are selling their products and services to you. How do you separate those third-party providers who will cause you to fail your audits from those who will not? Innovation in solving your problems is number one. Proof of cybersecurity compliance is the next.

The ISO compliance system is your way to know that the data security, quality management, environmental services, health and safety, and risk management programs are internally and externally audited to worldwide standards.

Is the company compliant to NIST 800-171? These are questions to ask before there is a problem.

ISO 27001 ISO 14001 ISO 45001 ISO 31000 ISO 20243 ISO 9001

12477 Broad Street SW, Pataskala, Ohio 43062 | **614.322.2222** | clientrelations@techr2.com | **techr2.com**

ISO 27001 ISO 14001 ISO 45001 ISO 31000 ISO 20243 ISO 9001

TEAR-A-BYTE TECHR2 IS NIST COMPLIANT MBE Ohio Achieve GDPR COMPLIANCE ZERO TRUST MODEL

 226-07/24

Securing Private and Public Data: Nine Steps to Compliance for the End-Of-Life Media Ecosystem

Step 7: Environmental Acceptance

Responsible technology recycling is essential for end-of-life data bearing equipment. Improper disposal can lead to fines, litigations, and most importantly a data breach. But such disposal is more than mere self-protection – it is a moral imperative. Your recycler should lead the charge to honor the environment. Your research, your expectations, and your reactions to changes in data and environmental law and practice may affect you – operationally, financially, and ethically.

Your recycler should keep a vigilant eye on the global business and environmental culture so that you are better able to understand and fulfill your role while maintaining optimum value. As stewards of the environment and a student of sound business practices, your choice should develop strategic alliances with organizations that share your environmental goals.

Honoring the environment™

Step 8: Make the Cybersecurity Transition

In the coming years, companies and their third-party providers must all comply with Cybersecurity Framework (CSF) programs. Where most companies in the world are not compliant, those who take data security seriously for their clients have held their CSFs for many years.

Step 9: Grow your Security

As part of any Cybersecurity Framework (CSF) program, annual Risk Assessments, Planning and Training will create a multi-layered data security system that will also inspire growth in your other data security programs. You know that you cannot stay at the status quo. Data security is either growing or failing. Partnering with world-class data security professionals will enhance your program.

12477 Broad Street SW, Pataskala, Ohio 43062 | **614.322.2222** | clientrelations@techr2.com | **techr2.com**

ISO 27001 ISO 14001 ISO 45001 ISO 31000 ISO 20243 ISO 9001

TEAR-A-BYTE TECHR2 IS NIST COMPLIANT MBE Ohio Achieve GDPR COMPLIANCE ZERO TRUST MODEL

226-07/24

techr2.com **614.322.2222**

Securing Private and Public Data: Nine Steps to Compliance for the End-Of-Life Media Ecosystem

TechR2 as your Data Security Partner

The Challenge

In the Business-to-Business world, 'As A Service' representatives use to have large list of partners to perform any IT operation. But wait a second. Laws like GDPR and US federal regulations prevent data from being controlled by non-compliant, non-cybersecurity certified, untrained truck drivers and movers to interact with hard drives, solid state devices and digital systems. This decade, many data controllers found that their procedures were flawed when brought to court.

The Solution

Enter TechR2, a top compliant, cybersecurity certified datacenter destruction, datacenter decommissioning vendor trusted by IBM, Kyndryl and other many Fortune 500 companies. Externally audited annually to six (6) worldwide ISO certificates, and NIST Compliant to the DFARS standard. Externally assessed to HIPAA and financial compliance. Organizations know that these multiple frameworks have helped to build TechR2 staff into a trusted entity when you are the most vulnerable and data is on the loose.

Next Steps

Contact our experienced TechR2 staff to learn more.

Contributing Authors

Sepp Rajaie
CEO and President, TechR2

35 years Executive Level Management
Visionary Entrepreneur
Patent Holder
Cyber Warrior

Charles Robbins
Senior Compliance Officer, TechR2

47 years in Software and System Development
Retired Infantry and Armor Officer
Prolific Author and College Teacher
Cyber Warrior

We offer **one** standard of service: **Excellence.**

Innovation	100%
Experience	100%
Compliance	100%
Customer Focus	100%

Call 614.322.2222
clientrelations@techr2.com

12477 Broad Street SW, Pataskala, Ohio 43062 | **614.322.2222** | clientrelations@techr2.com | **techr2.com**

ISO 27001 ISO 14001 ISO 45001 ISO 31000 ISO 20243 ISO 9001

TEAR-A-BYTE | TECHR2 IS NIST COMPLIANT | MBE Ohio | Achieve GDPR COMPLIANCE | ZERO TRUST MODEL

226-07/24