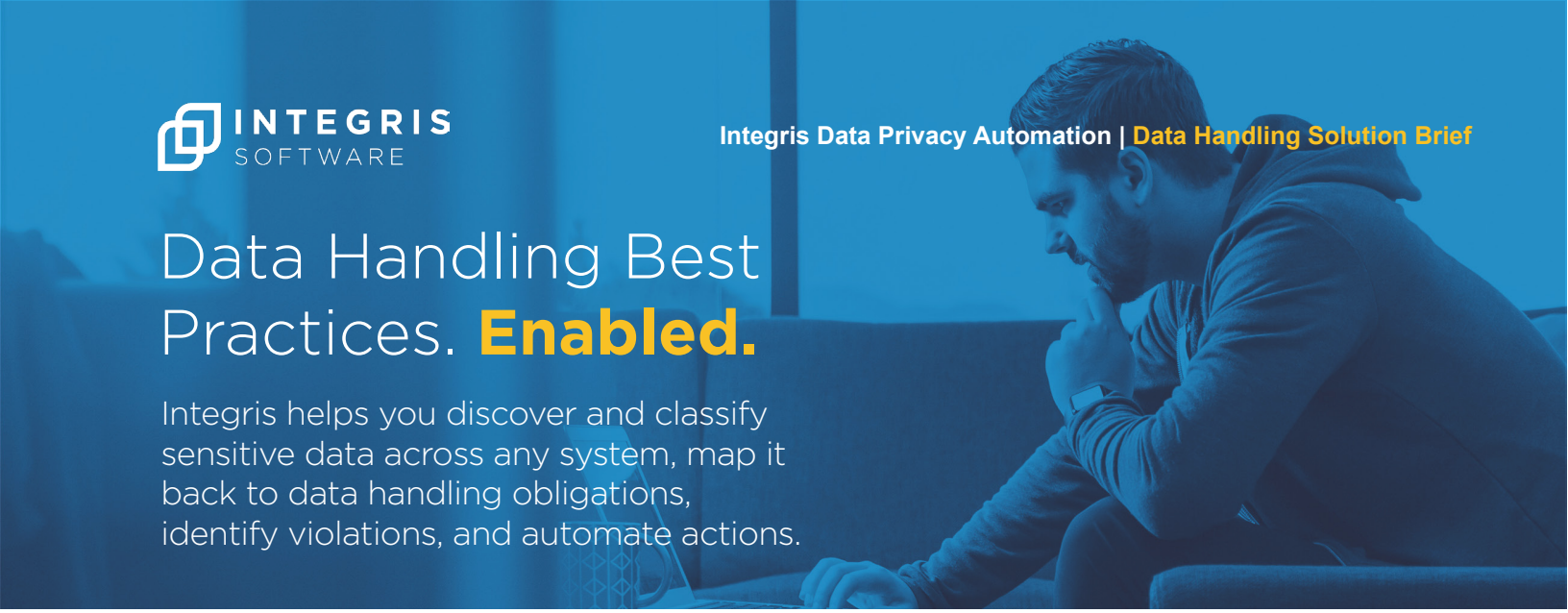
Data Handling Best Practices. **Enabled.**

Integris helps you discover and classify sensitive data across any system, map it back to data handling obligations, identify violations, and automate actions.



The current regulatory environment is driving urgency to meet modern enterprise data handling challenges

At their core, data privacy regulations like GDPR and the California Consumer Privacy Act (CCPA) require good data handling practices. Continuous defensibility to meet compliance requirements boils down to doing two things well:

1 Understanding where sensitive data resides across all data sources.

This should include structured, unstructured, semi-structured, data in motion, at rest, on premise or in the cloud. The ability to scale up and down is critical.

2 Mapping data back to existing data handling obligations.

Not just regulations, but also contracts and internal policies, as well as the ability to take action within your data ecosystem, such as encrypting files, or processing a consumer's data access request.

Seven data handling best practices

Having visibility into where sensitive data resides and tying it back to obligations is critical to enabling these seven data handling best practices:

1 Implement data security controls

Documenting policies are important, but to be defensible you need to be able to show that you can identify different types of sensitive data across your enterprise, and that you have compensating controls in place to keep it encrypted, hashed, or masked.

Be cautious about solutions that simply map IDs to pre-existing metadata. You'll run the risk of creating a false sense of security about the data you have, which security parameters are being applied, and whether they're in compliance with regulatory mandates.

> Metadata can be misleading. Integris operates at the data element level to inform you exactly what personal information is in your dataset, not just what the metadata implies. By using a combination of contextual awareness, natural language processing, and machine learning, Integris maps all sensitive data elements so as to assess privacy, integrity, and handling violations.

2 Establish and enforce a data retention policy

You probably have different retention policies for different types of data. Make sure you're calculating retention in a consistent way such as creation data, date of last transaction or other metric.

Of course, to be defensible, you'll need to be able to identify your sensitive data, and show that you're adhering to your own retention policy.

3 Identify mislabeled data

Data handling policies only work if your data has the right labels. For example, it's not uncommon to find databases backing webforms to have mislabeled data. For instance, a customer accidentally typing in their credit card number in a phone number field could put you in violation of a regulation, because you're not encrypting the phone number column in your database.

4 Identify misclassified data

Much like mislabeled data, misclassified data poses significant risk. For example, SSN's found in a phone number column will not have a high enough classification tied to the data set. Don't rely on manual data mapping efforts, which can be riddled with errors.

Integris automates the identification of misclassified and mislabeled data, then surfaces issues for human intervention or kicks off automated remediations.

5 Tackle data proliferation, including data in-motion

You probably have data handling policies that restrict where sensitive data resides. For example, it must sit in Oracle or Hadoop, but not in network file storage or Dropbox. For data streaming into an organization from places like Facebook, Instagram, or business partners, data in motion can be a big blind spot. Identify and monitor your data streams to ensure you know what is entering and leaving your organization and that you are adhering to all data handling policies.

Integris' ability to handle data in motion is key to helping you understand which data is entering or leaving your organization via data sharing agreements, and the streams and feeds your company relies on for continuous innovation.

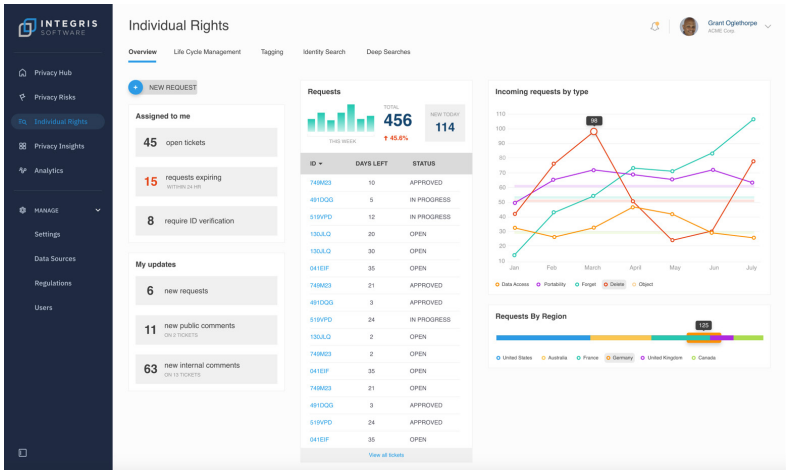
6 Residency-based policy-making

Both GDPR and the California Consumer Privacy Act (CCPA) indicate that data handling policies apply differently depending on a person's residency or citizenship. Track data against residency policies to ensure effectiveness.

Integris can infer residency from geospatial data, a country code, or phone number.

7 Handle what GDPR calls data subject access requests (DSAR)

Under both GDPR and CCPA, individuals have the right to enquire about their personal data, what data companies collect about them, how it's being used or shared, and to exercise their right to "be forgotten." In order to address DSAR, you must understand where all personal data resides and be able to map it back to your users.



Integris provides workflow and issue handling capabilities to manage the data subject request process, and keep track of progress, owners, and communication.

How Integris Enables Data Handling Best Practices

Use Integris to discover and classify sensitive data across any system, apply data handling policies, assess risk, and take action. Our extensible platform helps you manage your most important data and automate actions to protect your company and customers.

You can even extend your data protection strategy beyond privacy.

Integris gives you the ability to add sensitive terms specific to your company, such as intellectual property, or other areas critical to the management of your business.

Modern reporting makes it easy to have fact-based discussions with colleagues, customers, regulators, internal auditors, and partners.

Deeper discovery and classification of sensitive data

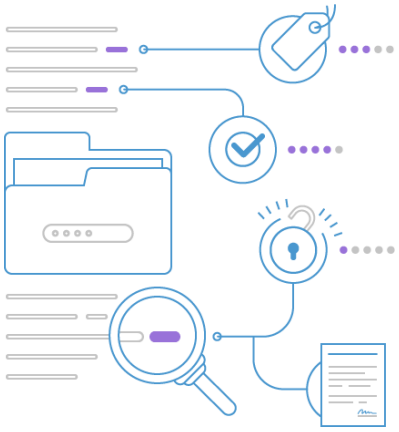
Our deeper inspection down to the data element level informs you exactly what's in the dataset, not just what the metadata implies.

- Not dependent on user IDs-- combines contextual awareness, natural language processing and machine learning to map all sensitive data elements.
- Honors existing data classification and sensitivity policies. You can even assign different classifications by data source.
- Machine learning is tuned to personal information, making it more accurate than broad-based data mapping tools.
- Ability to classify not only labeled, but inferred, derived, and behavioral-based sensitive data.
- 250 pre-built sensitive data labels and the flexibility to create your own unique definitions.
- Multi-label classification identifies combinations of data that alone are benign but together become highly sensitive.
- Extensible machine learning allows you to to add sensitive terms specific to your company, such as intellectual property, or other key business terms.

Connect to any structured or unstructured data source, at rest or in motion, in the cloud or on-premise.

- Connect into any repository or location (via JDBC, ODBC, Kafka) -- file storage, structured databases, SaaS applications, Hadoop data lakes, and streaming data.
- Ability to handle semi-structured data like MongoDB, JSON, and XML documents. Create schemas/metadata from anything with key-value pairs.
- Real-time scanning and classification of streaming data as it enters and exits the organization.
- Integrates into popular streaming analytics tools such as Apache Kafka, AWS Kinesis*, and more.
- Flexibility to have Integris build custom connectors.

Wider control to support your entire enterprise control framework regulations, policies, and contracts



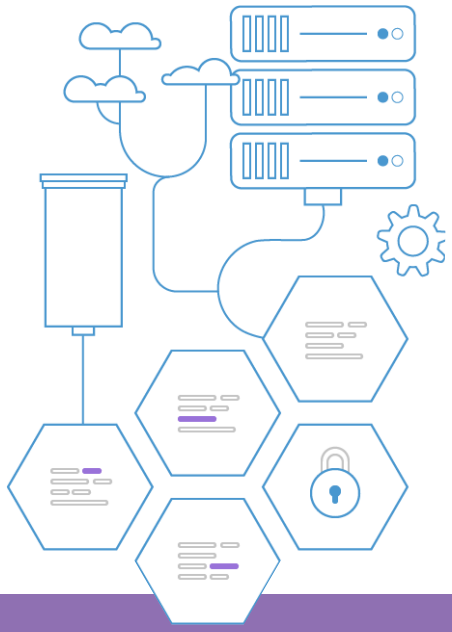
Operationalize and automate the enforcement of policies that incorporate security, privacy, and data governance.

- Sensitive data is continuously classified, labeled, and mapped to regulations, data sharing agreements, and internal use policies.
- Flag data handling issues related to data residency, retention, proliferation, misclassification, and mislabeling.
- Flag security issues, such as lack of encryption and masking on highly sensitive data.
- Provide auditors and 3rd parties evidence of your data logic, policies, and enforcement.
- Kick off workflows with existing ticketing systems to remediate issues.
- Quickly respond in the event of a breach, audit or lawsuit.
- Ensure that data governance and data management systems are accurate and current.

Secure, scalable, architecture meets the demands of petabyte—scale processing

Flexible, hybrid deployments go where your data resides, minimizing costs and deployment friction, while maximizing processing power efficiencies.

- Self-healing, microservices-based architecture built using Kubernetes and Docker.
- Equally capable in your on-premise virtual environment as well as any private or public cloud platform.
- Polymorphic processing engine runs workloads on existing computing power, wherever your data resides.
- Advanced tokenization improves regex performance by over 100x.
- Hadoop Connection Engine sits as an adjacent edge node inside existing Hadoop clusters utilizing existing compute power.



ABOUT INTEGRIS SOFTWARE

Integris Software, the global leader in data privacy automation, helps enterprises discover and control the use of sensitive data in a way that protects privacy and fuels innovation.

Privacy is now critical to an effective data protection strategy. By sitting upstream from security, Integris tells you what data is important ans why so you can be precise in your InfoSec Control.

Integris works securely, at scale, no matter where sensitive data resides. You get a live map of your sensitive data where you can apply policies, surface issues, and automate remediations via your broader ticketing and InfoSec ecosystem.

Regulations like GDPR and the California Consumer Privacy Act (CCPA) are triggering knee-jerk reactions as companies lock down their data for fear of misuse. With Integris, there is finally a way to use your data without fear.

1525 4th Avenue, 5th floor Seattle, WA 98101-1607 USA +1 (206) 539.2145 sales@integris.io @integrisio integris.io