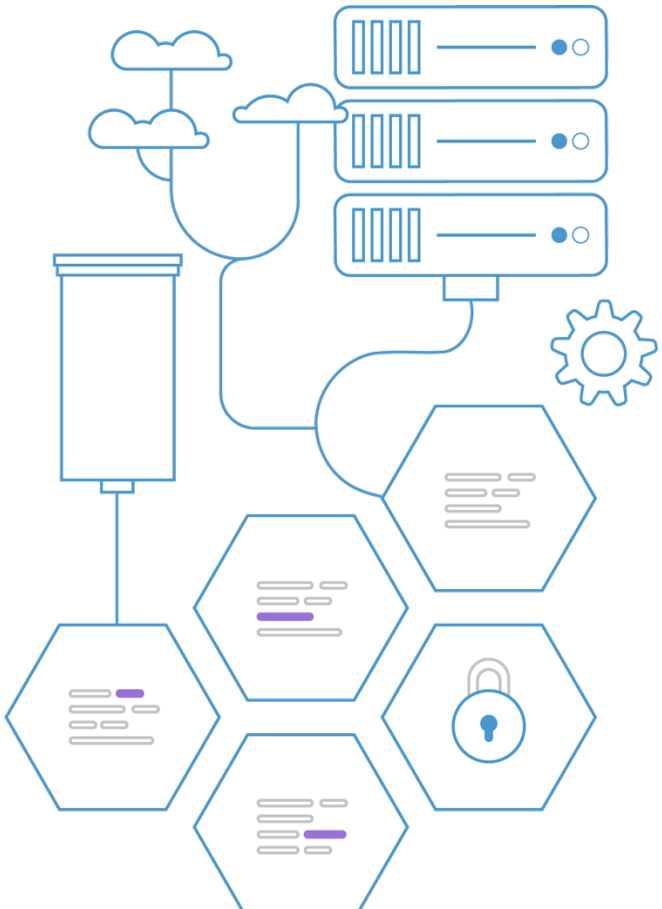
INTEGRIS SOFTWARE

White Paper

Solving DSARs' Big Data Problem

Four recommendations plus the one thing you should never do



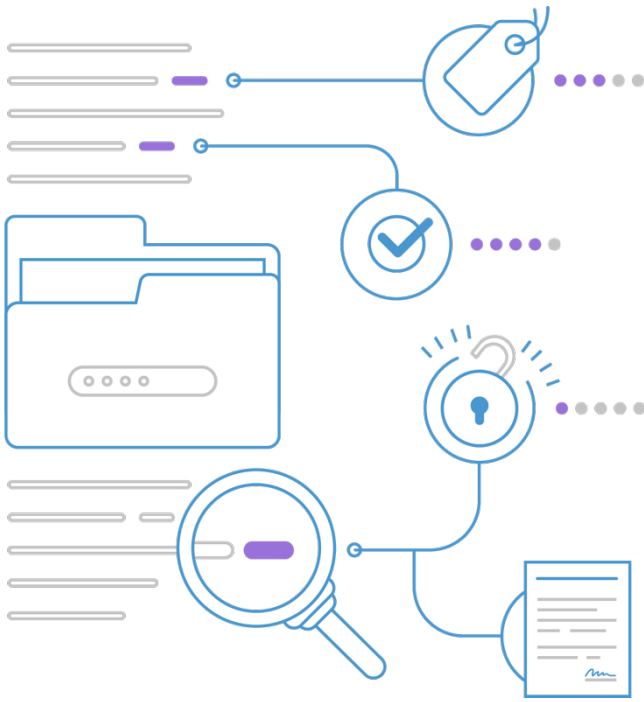


Table of Contents

Addressing Data Subject Rights is a Big Data Problem

Consider the following:

- A single bank transaction may get replicated across 100 systems.
- Storage is so cheap that enterprises collect petabytes of data each year and keep almost all of it.
- Data is routinely propagated across the enterprise to support a wide variety of users and business initiatives.

Unfortunately, the massive growth in data collection and proliferation has not been accompanied by an equally matched effort in data management and governance.

The consequences have been painful. Data breaches. Misuse of private data. Loss of consumer trust. In response, companies have poured resources into implementing security controls to block or restrict access to their data. But whereas Security is focused on *who* is using the data, Privacy is about *how* the data is being used and for *what* purpose.

Meanwhile, regulations like GDPR and CCPA are obligating companies to respect and respond to data subject rights. But achieving basic compliance requires that companies understand what personal information they have, where it's located, and its purpose. Up until now, the basic data inventory process has been a manual one consisting of application data owner surveys and spreadsheets.

DSRs push these manual processes to their breaking point. Not only in people resources required to manually search those 100 systems in the bank example for each DSR, but also in the accuracy and completeness required to be defensible with the regulators. It's a big data problem and a new approach is required to process petabytes of data, extract key data points and derive the relationships between them. Meanwhile, companies have been left scrambling to meet their obligations.

Five Critical Data Subject Request (DSR) Fulfillment Capabilities

The five critical Data Subject Request process and fulfillment capabilities are intake, verify, search, deletion, and response. DSR fulfillment is critical being in compliance with both the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). While CCPA and GDPR have their own unique take on DSR fulfillment, these five critical capabilities are a must:

1. Intake

During intake, a data subject makes a request via email, an online form, or other communiqué. The enterprise then needs to verify the requestor's identity and existence within the data ecosystem and track the request fulfillment through to resolution. All within the required timelines (30-45 days depending on the regulation).

2. Verify

The next step is verification of the identity of the requestor. For companies which provide services online, this step may require customers to login and verify their identity. For regulations like GDPR, which may include employees and vendors, this requires that the enterprise confirm the existence of the data subject anywhere in their ecosystem and then identify corresponding info to include in the response.

3. Search

In order to fulfill the request, the enterprise will need to locate a requestor's personal data by searching across its data ecosystem. The type of information the enterprise will be searching for will differ based on data subject type. For example, is the data subject a current customer or a former employee? CCPA only applies to 'California consumers' whereas GDPR also includes employees and contractors (privacy by design would look to encompass current and potential future scenarios). The search process identifies relevant PI attributes, categories, and the company's purpose for collecting and processing the subject's information. The search then needs to identify the specific systems and locations that contain the data subject's personal data.

4. Deletion

For deletion requests, the enterprise will need to validate which systems the data can be deleted from, based on regulatory or business constraints. An example of a business constraint might be a warranty registration database that contains personal information. The enterprise cannot delete customer information from this database because it impedes the ability to fulfil a legal obligation to provide a customer with, say, an extended warranty on his purchase.

Next, the enterprise will need to initiate a process to delete or obfuscate the customer's data from the relevant systems, as well as request the same from third-party data processors. Lastly, the enterprise will need to audit and confirm the deletions.

5. Response

Templates help ensure an efficient and consistent fulfillment data subject request process. All communications and activities should roll into a reporting dashboard and audit trail to demonstrate accountability, compliance, and progress towards resolving requests.

Which of these five capabilities is the most challenging?

For many organizations, the most complex, tedious, and resource-intensive step in the process is finding PI and tying it back to the data subject.

Why is identifying data subjects and their sensitive data so complex?

Not only has data proliferated, but it's also mutated into derivative forms. Customer data is often collected across multiple channels without being linked to a master identifier. Also, when downstream systems aren't updated there can be discrepancies between primary and secondary systems.

To make matters worse, both the regulatory environment and what's considered sensitive data is changing. CCPA defines personal information that "could reasonably be linked, directly or indirectly, with a particular consumer or household." The word "household" is not found in GDPR. It implies that personal information does not have to be tied to a specific name or individual (think home address, home devices, geolocation data, home network IP addresses, and the like).

Resolving identities across hundreds of sources is a data processing and data quality nightmare. The vast majority of companies simply do not have the tooling in place to access and monitor the volume, variety, and velocity of personal data flowing in, out, and across their organizations.

Master data management to the rescue? Not so much.

Many medium and large enterprises have implemented master data management systems (MDM) to resolve identities and create a golden record for interacting with a customer. MDM and customer data platforms hold the promise of delivering a 360-degree view of the customer to improve sales, service, and growth.

However, "customer" is often defined in different ways across an enterprise and that definition does not always equate to an individual. Also, data subjects can look different across data sources and business scenarios because of:

- Nicknames
- Middle initials and suffixes
- Maiden names
- Different email addresses, phone or postal addresses
- Address changes
- Typos in addresses or abbreviations

Even when companies build master data management processes, they typically identify a few trusted sources from which to provide inputs.

And of course, not all personal data is tied to a user ID. Even without an ID the individual can still be identified in a data set. By simply mapping IDs to pre-existing metadata, the enterprise can run

the risk of creating a false sense of security about the data it has, which security parameters are being applied, and whether it is in compliance with regulatory mandates.

Finally, while CCPA applies to California consumers only, GDPR applies to all data subject types such as customers, employees, vendors, and partners.

Privacy's universal data subject view

MDM and other customer platforms and processes are not tuned to a 'universal data subject' view which includes multiple data subject types.

The result is that companies have to either enhance their mastery of 'the customer' to include other data subject types or build a new identity resolution process. The business case for embarking on such projects has not been compelling up until CCPA and GDPR. Outside of privacy, there aren't any business use cases that require consolidating massive amounts of personal information on different types of data subjects.

Most enterprises simply do not have the intent or willingness to spend valuable resources and embark on an expensive journey to create a master data subject view.

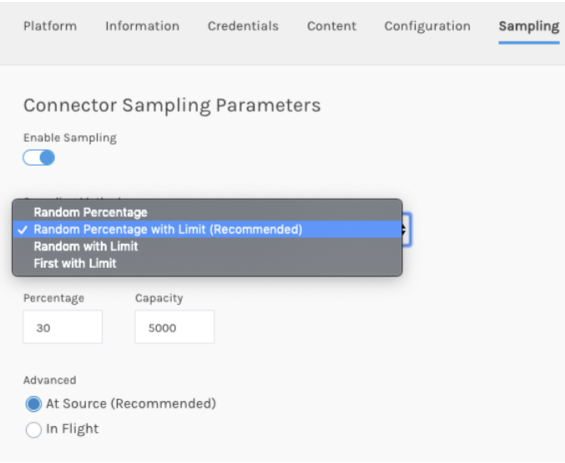
Solving DSARs' Big Data Problem: Four Recommendations, Plus the One Thing You Should Never Do

Reduce Your PI Surface Area: A Three-Step Approach

To help solve the inherent nature of the DSR big data problem we recommend a three-step approach for finding your PI and tying it back to your data subject. The end result of the three steps described below is that you'll dramatically reduce both the surface area for your DSR fulfilment process, as well as what would otherwise have been in scope for CCPA, GDPR, and other regulations.

Step 1: Use sampling scans to discover which systems contain personal information

Solutions that attempt to scan large swaths of your data ecosystem will either keel over or get stuck in a protracted scan. It simply takes too long to do comprehensive data subject searches right out of the gate, especially when you've got 30-day timelines to meet. To solve this bottleneck, reduce your surface area by creating an inventory of personal information, regardless of the data subject. This helps you identify your high-risk systems, locate PI, and detect classification and labeling issues.



There's no need to boil the ocean right out of the gate. Start with a light sampling scan, and based on what you find, you can follow-on with deeper scans.

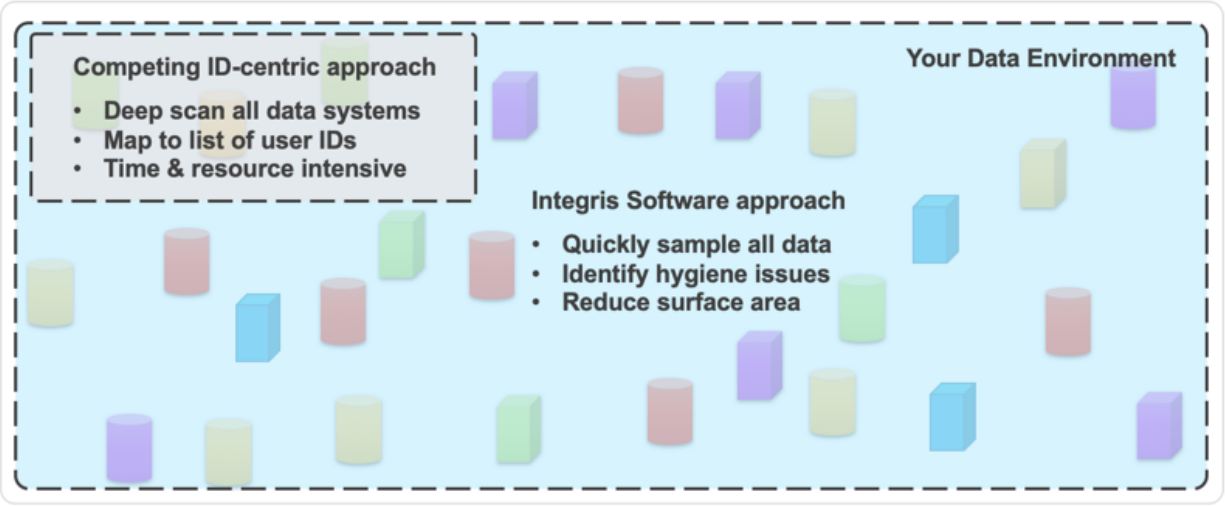
Why sample? Because even with best-in-class architecture, deep scanning takes time. Consider the example below which compares how most vendors handle PI scanning compared to Integris's sample scanning approach.

	Competitor Full Scan	Integris Sampling Scan
Data environment	1 petabyte (1,000 TB)	1 petabyte (1,000 TB)
Type of scan	Identify problem	Describe the solution.
Scan rate per terabyte	Deep crawling	Sampling
Time to scan 1,000 TB	12,000 hours (500 days)	167 hours (7 days)

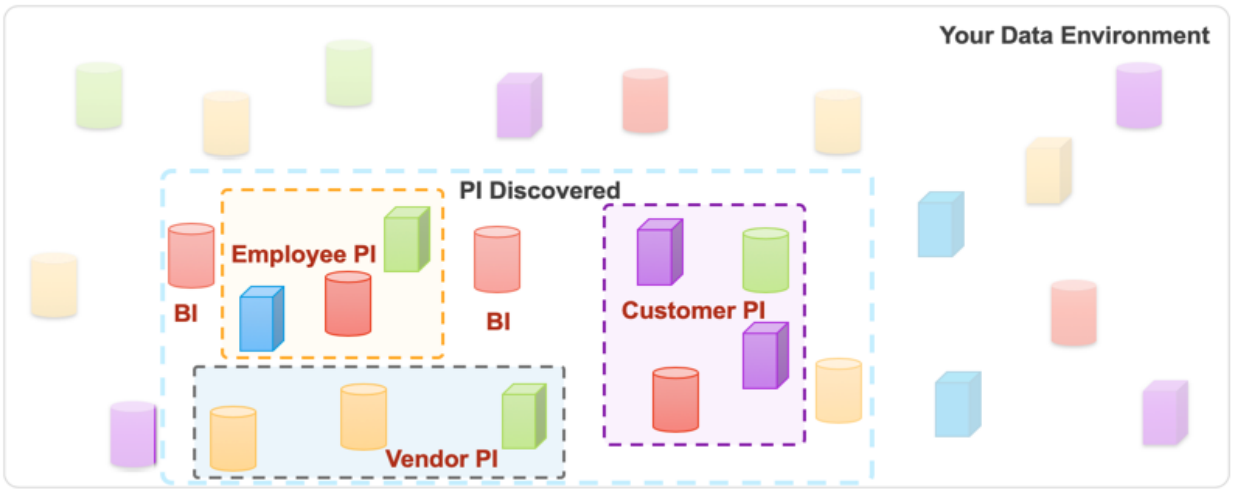
Note: Illustrative and based on structured data sources. YMMV based on number of systems, data volumes, and sampling types selected.

Working 24/7, the competing approach can take 500 days to do a deep scan of one petabyte of enterprise data. With a sampling scan approach, we can finish scanning that same one petabyte in a week.

The competing approach is to do a deep scan to find and map PI back to a set of IDs. In 90 days, the competing approach might only get through a few systems (the small outlined area in the upper left on the graphic below). In that same time period Integris has done a much more complete scan of your data ecosystem.



Next, we reduce the haystack down to the systems where we discovered PI. As illustrated below, we expected to find PI in our customer, vendor, and employee systems. But we also found PI in our Business Intelligence systems.



Step 2: Use deeper scans to identify the tables that contain personal data and any data handling issues

In addition to the timely fulfillment of data subject requests, regulations like GDPR and CCPA also require good data handling practices. Continuous defensibility to meet compliance requirements boils down to understanding where your sensitive data resides across all data sources, and then mapping that data back to your data handling obligations.

To continue with our example, we expect to see CCPA data in our customer, employee, and vendor data systems. But as we dive deeper into these systems, we notice that:

- We've got data that's supposed to be encrypted, but it's in clear text.
- We find a trove of data that's been mislabeled; its sitting in the wrong part of a database.
- Within many of the systems that we know contain CCPA data, we find retention issues.

These data handling issues present a challenge, because when we execute our DSR process, we're going to want to limit the number of tables to those that we know contain sensitive data. We want to make sure the data is where it's supposed to be.

Step 3: Remediate data handling issues

Continuously monitor your sensitive data against your data handling policies and raise these issues so that you can take the appropriate actions. Fixing these issues has the added benefit of further reducing your DSR surface area.

Continue to drill down into your systems to see which attributes, or types of PI elements they contain. And from there, you should drill all the way to the data element level, which allows you to be precise in your remediations.

Ideally, you'll want to tie directly into your broader ticketing and InfoSec ecosystem to tell other tools and/or people where to go to remove, encrypt or minimize a data set.

Prepare for a DSR "Denial of Service Attack"

If you get flooded with thousands of DSRs at once the impact is a denial of service attack that overwhelms your CSR and IT staff. Under this scenario, your manual processes reach the breaking point and you can't respond to requests within the required timelines (usually 30 to 45 days depending on the regulation).

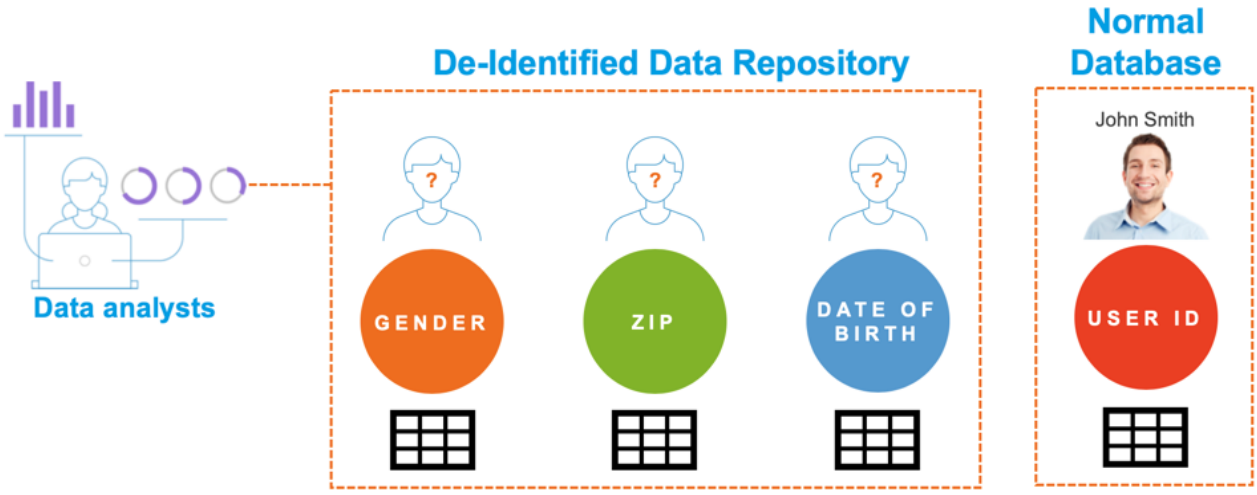
Consider solutions that will allow you to automate your DSR processes so you can fulfill thousands of requests automatically. Today's DSR solutions need to be completely API driven and generate detailed metadata. Detailed metadata like system location, owner, business metadata, and system classification is crucial to support a variety of deletion workflows.

You need to be able to find exactly where the data subject resides within your ecosystem, then trigger deletion and portability workflows. Of course, you'll want an audit trail of all deletion activities including deletion confirmations for internal audits and compliance needs.

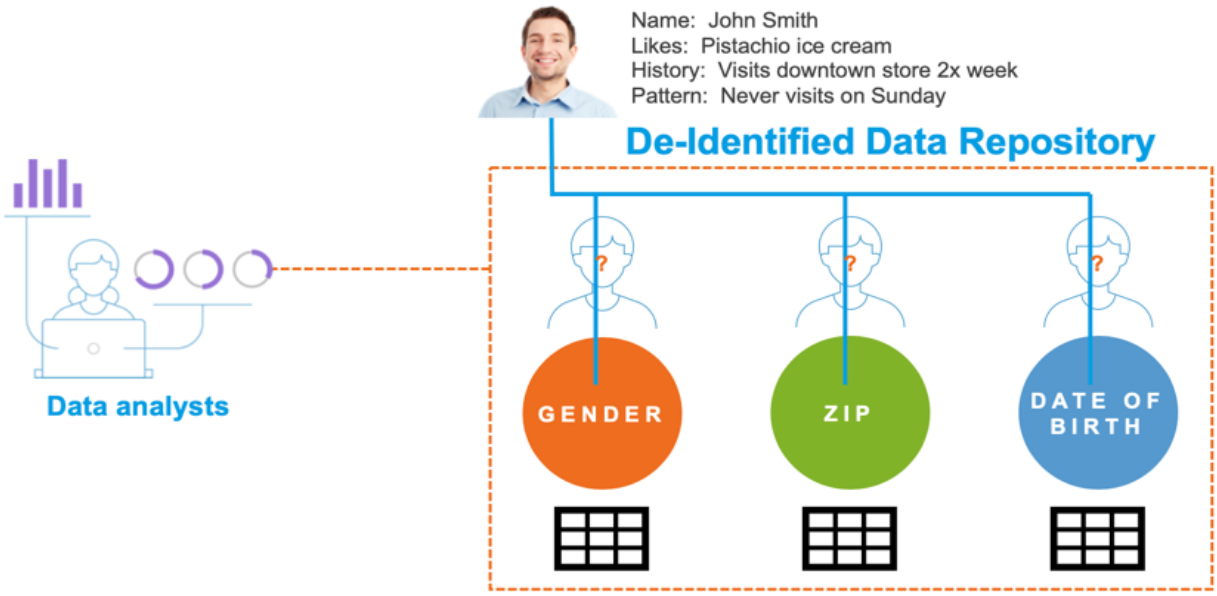
The end goal is to decrease the pressure on IT teams to find data subjects and validate deletions.

Adhere to the Data Handling Best Practice of De-identification

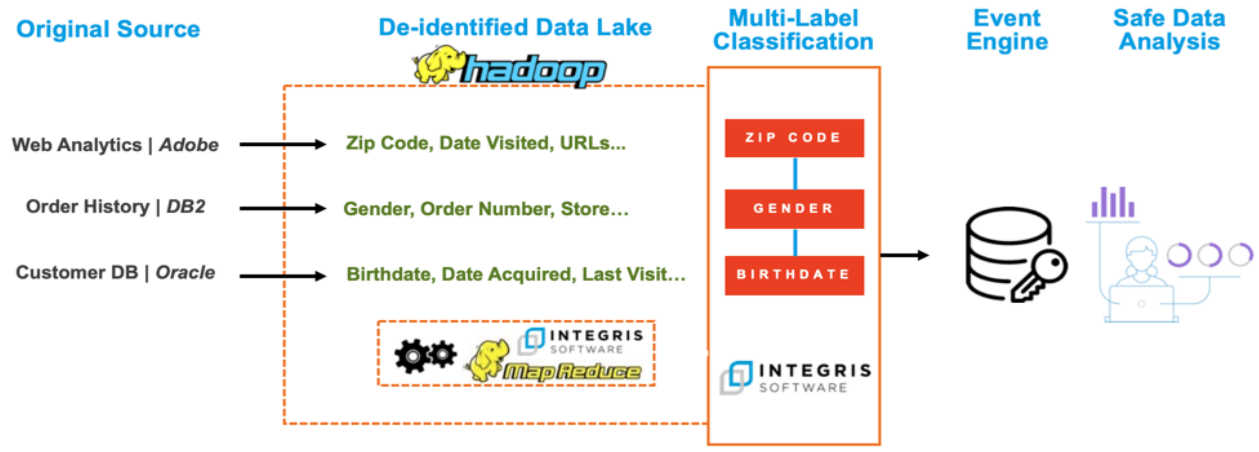
De-identification prevents data analysts from connecting an individual to their personal information. This enables the data analyst to access useful data without compromising customer privacy. Many organizations are de-identifying data for continued analytics after a right-to-forget (as shown in the illustration below).



But not all discoverable sensitive information is linked to an identity. In fact, 87% of the US population can be identified using only their Zip Code, Gender, and Birthdate. Each of these data points is benign on its own, but when combined become toxic. Data lakes, data warehouses and other systems that support data analysis ingest disparate pieces of customer data from a variety of sources. When combined, this data has the potential to reveal customer identities along with highly sensitive personal information (as illustrated below).



That's why it's critical to inspect down to the data element level to inform you exactly what's in your data lake, not just what the metadata implies. When you operate at the data element level you can also identify highly sensitive combinations of data across your data ecosystem. For example, capabilities like multi-label classification (aka correlated labeling) can validate that a dataset can't be used to identify an individual (as illustrated below).



Comply with Privacy and Security by Design Principals

Any DSR fulfillment process and associated systems must comply with privacy and security by design principles.

In August 2019, the BBC reported that a security expert contacted dozens of UK and US-based firms to test how they would handle a "right of access" request made in someone else's name. In each case, he asked for all the data that they held on his fiancée. In one case, the response included the results of a criminal activity check. Other replies included credit card information, travel details, account logins and passwords, and the target's full US social security number.

Annie Bai and Peter Mclaughlin's IAPP article sounded the alarm bell in that "The terrible beauty of the California Consumer Privacy Act is that innumerable companies will soon be required to undertake totally novel consumer-facing responsibilities...It is a new door for improper data access — not a back door, but an actual, legit front door — for fraudsters to obtain all manner of valuable personal information."

Companies in highly regulated industries like financial services already have sophisticated ID verification systems in place. If your firm doesn't have one of these systems in place, then you may want to explore adding this capability into your DSR workflow (Evident ID is one such system).

Another vulnerable area is the personal information that a CSR may have access to when they are responding to a DSR. To protect sensitive information, it's best to obfuscate PI from the UI so CSRs can't see sensitive data as they respond to DSRs.

Apply the Concepts of Identity Resolution to Improve Accuracy

It's also important to apply the concepts of identity resolution to identify your data subjects across multiple data sources. Why? Data subject information changes over time and your data subjects may use different information in their interactions with your company (e.g. nicknames, maiden name, address changes, initials, and Jr./Sr.).

Upon receiving a data subject request, it may be helpful to run a quick data subject search to confirm their existence within your data ecosystem. This helps validate that your data subject exists and also provides instant access to additional attributes that help disambiguate the data subject (e.g. John Smith and John Smith Jr. living in the same household with the same address and family email). This can also tell you if the data subject exists in various data subject types, such as customer, employee, or vendor in your data ecosystem.

For example, when John Smith submits his request you can quickly confirm that he exists, identify John Smith the customer vs John Smith the employee, and look up typical attributes found across your data ecosystem. Based on the privacy by design principles, this information is adequate for most enterprises to respond to access requests.

Never make the problem worse by creating additional copies of customer data

Finally, never make the problem worse by creating additional copies of customer data or violating your own security policies by moving sensitive data between secure network zones. Not only are copies of data inherently outdated, but they exacerbate data sprawl, and open you up to additional security risks. We think Paige Bartley, Senior Analyst at 451 Research said it best:

"Modern data privacy and protection regulations such as GDPR and CCPA have inadvertently created a paradox in which organizational attempts to fulfill data subject requests (DSRs) can occasionally result in the exposure of sensitive data to additional unnecessary parties: particularly when duplicate data is generated.

Integris Software's privacy-by-design DSR methodology minimizes this risk, and provides a highly-defensible approach to meeting data privacy requirements via its ability to pinpoint sensitive data – regardless of whether or not it is tied to a user ID – across data sources both in-motion and at-rest."

Paige Bartley
Senior Analyst, Data, AI & Analytics
451 Research

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 and why so you can be precise in your InfoSec controls.

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, fulfill data subject access requests, 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.

For more information on Integris, visit: www.integris.io or follow @Integrisio on Twitter.

Global HQ in USA
1525 4th Avenue, 5th Floor
Seattle, WA 98101
Phone 1-425-539-2145
info@integris.io

Vancouver, BC Canada Office
450 Southwest Marine Drive
Vancouver, BC
V5X 0C3
Phone 1-425-539-2145
info@integris.io

For an overview of Integris DSR, please see the solution brief that follows

The Only DSR Solution that Doesn't Require Creating Copies of Your Customer Data

Fulfill Data Subject Requests with Unmatched Speed and Accuracy

Integris Software Delivers the Fastest Path to DSR Defensibility

Integris Software tackles the most challenging aspect of data subject requests (DSR) – finding data subjects across your data ecosystem. By automating the discovery and classification of sensitive data, Integris reduces the burden on IT teams and data source owners.

Deep Search and just-in-time identity matching make it easy for your customer service reps (CSRs) to verify and locate data subjects across thousands of systems. CSRs can capture the request, input data into a standard response template, and share it back out with the data subject. They can preview DSR reports, add private notes, and activate the next step in your workflow.

Worried about a flood of DSRs causing a "Denial of Service" on your CSR and IT staff? Integris gives you the ability to automate your DSR processes to fulfill thousands of requests automatically.

Integris DSR Key Capabilities

PI Surface Area Reduction

Our discovery process isolates your systems that contain PI, then maps attributes, categories, purpose, and sources back to each data subject.

DSR Lifecycle Management

DSR intake, workflow management, and response generation, as well as integrations with your existing front-end systems.

Data Subject Validation

On intake, we help you confirm a data subject exists within your ecosystem and identify multiple types like customer, employee, and vendor.

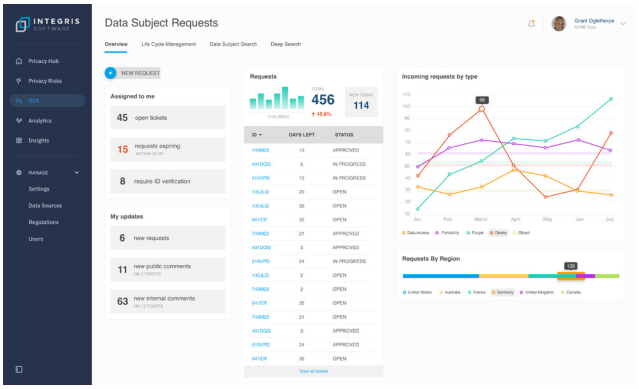
Data Subject Deep Search

We identify the data subject's relevant PI, as well as the specific systems, tables, and files that contain the subject's personal information along with purpose, PI categories, system owner, and related information.

Remediation and Validation

Additional metadata and event orchestration support end-to-end workflows (e.g. deletion), and you get an audit trail with validation to demonstrate compliance.

Integris DSR is fast, accurate, and follows the principles of privacy by design



"Modern data privacy and protection regulations such as GDPR and CCPA have inadvertently created a paradox in which organizational attempts to fulfill data subject requests (DSRs) can occasionally result in the exposure of sensitive data to additional unnecessary parties: particularly when duplicate data is generated.

Integris Software's privacy-by-design DSR methodology minimizes this risk, and provides a highly-defensible approach to meeting data privacy requirements via its ability to pinpoint sensitive data – regardless of whether or not it is tied to a user ID – across data sources both in-motion and at-rest."

Paige Bartley
Senior Analyst, Data, AI & Analytics

451 Research

Fast

Build trust by delivering a rapid response to requests that include up-to-date PI categories and purpose.

Search for data subjects only where you might find them; reducing the PI surface area upfront enables blazing fast, on-demand data subject deep searches.

Future proof your business against DSR "Denial of Service attacks" by automating your end-to-end DSR workflows.

Decrease your dependency on IT teams to find data subjects and validate deletions.

Accurate

Advanced identity matching enables high confidence search and identification of data subjects.

Get up-to-date details on the data subject when you need it; stop relying on historical indexes.

Discover all PI even if its not tied to a user ID; machine learning and contextual awareness operate at the data element level on data anywhere - at rest, in-motion, in the cloud, or on-prem.

Find exactly where the data subject resides within your ecosystem, then trigger deletion and portability workflows.

Privacy by Design

Reduces the DSR data surface area through inventory risk assessment and remediation.

Enterprise ready; multi-zone support with no need to replicate consumer data across network zones.

Reduces exposure to identity thefts; respond to access requests confidently with attribute types, PI categories, and purpose.

By default, obfuscates PI from the UI so customer service reps can't see sensitive data as they respond to DSRs.

REPORT REPRINT

Integris Software's data subject request fulfilment addresses a key privacy catch-22

SEPTEMBER 20 2019

By Paige Bartley

Businesses can inadvertently create a data privacy paradox when they create additional copies of data and expose it to unnecessary parties while fulfilling a data subject request. Integris Software's approach to DSR fulfillment is based on privacy-by-design architecture, eliminating data copies and minimizing data exposure.

Introduction

As well-intentioned as any protective regulation may be, there will always be unintended consequences. In the case of evolving data privacy and protection mandates, the rights bestowed on individuals to access or request their data from organizations have created a paradoxical situation in which simply fulfilling those rights often requires a complex business workflow of data search, access, collection and duplication, potentially further exposing sensitive personal information to parties that may not be fully authorized to process or handle it. With its new data subject request (DSR) capabilities, data privacy specialist Integris Software is aiming to tackle this problem with privacy-by-design architecture that minimizes data exposure while ultimately fulfilling individual rights.

451 TAKE

Because the glacial pace of regulatory reform must employ ambiguous wording to accommodate the comparatively blistering pace of technology evolution, some oddities can arise in functional business execution of compliance. One of these effects is the inadvertent data trail that is often created when a data subject or consumer exercises their right to data access. Data subjects, or consumers, should not have to endure further exposure and unnecessary handling of their data just because they exercise their right to access it. Yet this is often the case.

Many privacy-oriented software platforms on the market are simply concerned with fulfilling these data subject requests in a checkbox manner. Did the consumer/subject receive a functional copy of their data at the end of the process? Then yes, all requirements were technically met. However, with its DSR offering, Integris Software is providing organizations a way to fulfill these requests in a manner that minimizes personal data exposure and duplication throughout the entire workflow, potentially setting a new standard for defensibility.

Details

Integris Software, based in Seattle and cofounded by CEO Kristina Bergman and CTO Raghu Gollamudi, is a member of the new vanguard in sensitive data discovery and privacy orchestration functionality – leaning heavily on machine-learning-driven functionality to accurately identify data types that may potentially be sensitive or protected by various evolving global data-protection regulations. Originally focused on the initial discovery, association and classification process for sensitive data, the vendor helped organizations identify what sensitive information they had and where it resided in the distributed IT ecosystem – typically the biggest challenge in data privacy compliance efforts. Sampling scan methodology, with additional options for deep search, allows organizations to defensibly – yet quickly – assess very high volumes of data so that high-risk systems can be pinpointed for further examination.

While significant, finding sensitive data and associating it with the correct identity or entity is simply the first step. In data privacy and protection compliance use cases, the ultimate goal is to ensure fulfillment of data subject or consumer rights. In many cases, this includes giving individuals access to their personal data, modifying/updating personal data, or deleting personal data from the IT ecosystem upon request.

Integris Software's introduction of data subject request capabilities via Integris DSR aims to address this privacy workflow continuity problem. Numerous problems are endemic to the DSR process that the new capabilities look to address. Regulation-specific time constraints mean that DSRs need to be fulfilled promptly, and the number of stakeholders involved in fulfillment of a single request can create a 'too many cooks in the kitchen' problem. A large batch of DSRs hitting an organization at once can cause a paralyzing denial-of-service effect. Not everyone in the DSR workflow should be able to actually view the personal data being requested. Yet given time pressure and the threat of regulatory enforcement, many organizations have historically done whatever is needed to fulfill the basic requirement of a request, often duplicating data and exposing it to unnecessary parties along the way.

Integris DSR utilizes privacy and security-by-design principles to fulfill requests without data duplication, without copying data across network zones, and without UI exposure of sensitive data – enabling customer service reps or other consumer-facing business personas to deliver data to verified requesters without ever viewing any sensitive data themselves. Data subject validation initially confirms that a DSR's associated data subject indeed exists in the IT ecosystem, and can determine if that data subject is classified in different personas: not only 'customer,' but also classes such as 'employee' or 'vendor.' With DSR lifecycle management capabilities focused on automation, Integris DSR additionally helps organizations scale to large volumes of data subject requests, avoiding human bottlenecks and minimizing human error associated with manual processes. Finally, remediation and validation capabilities help organizations ensure that DSR-resultant tasks (such as deletion) are ultimately completed and documented so that compliance can be demonstrated.

INTEGRIS SOFTWARE

CCPA Compliance

Accurate, continuous defensibility to meet California Consumer Privacy Act compliance requirements

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

CCPA Compliance

Accurate, continuous defensibility to meet California Consumer Privacy Act compliance requirements

- Mantain control over the use and transfer of customer data
- Protect your customers' privacy and your company's reputation

CCPA goes beyond GDPR in its definition of personal information

Requirements for the California Consumer Privacy Act (CCPA) go into effect on January 1, 2020.

Like GDPR, the CCPA is broad in its definition of "personal information".

It defines it as personal information that "could reasonably be linked, directly or indirectly, with a particular consumer or household". You won't find the word "household" in GDPR.

It implies that personal information doesn't have to be tied to a specific name or individual (think home address, home devices, geolocation data, home network IP addresses, and the like).

GDPR lesson learned? Don't do the same work twice

Many companies started preparing for GDPR by hiring lawyers and consultants to do impact assessments, map out workflows, conduct surveys, and introduce internal guidelines.

This documentation is certainly important. But operationalizing GDPR and CCPA requires applying this knowledge to a diverse set of data repositories - in addition to leveraging existing IT security tools, and other IT systems (e.g., SIEM, ticketing, data governance).

In today's world of data-intensive business operations and big data, compliance requires real-time, automated knowledge about your data and data flows. Thus, it's critical to get your CTO, CISO, data governance team, and chief privacy officer together to do it right the first time.

Five things to do to prepare for CCPA

1. Establish a team, define responsibilities, and get your CxOs on the same page (business and technologists).
2. Know which personal data you have and where it resides. Account for all data types — both at rest, and in motion as it enters and leaves the company.
3. Understand why and how you're using your data, and be able to map it back to obligations such as CCPA and GDPR.
4. Assess existing ticketing tools and other applications to help accelerate data subject requests.
5. Operationalize and automate early. Use CCPA as an opportunity to apply data privacy automation to support your GDPR compliance program, third-party data sharing agreements, and internal data use policies - on both personal information and intellectual property.

   Once you have an accurate inventory of your data, you can reallocate scarce resources to better protect your most sensitive assets.

Integris Software delivers accurate, continuous defensibility to meet CCPA compliance requirements

How it works

Map
Data mapping tells you what data you have and where.

Monitor
You apply policies to your sensitive data which we continuously monitor for issues.

Control
We remediate issues by tying into your broader ticketing and InfoSec ecosystem.

Highlights of CCPA requirements, challenges, and how Integris responds

Section	Summary Description of Requirements	Data Privacy Management Challenges	Integris Responds
1798.100 1798.175	**The Right to Access, and Applicability** Consumers have the right to request that a business that collects their personal information disclose the categories and specific pieces of personal information it has collected. Personal information isn't limited to what's collected electronically or over the internet; it also applies to the collection and sale of all personal information collected by a business about a consumer or household. Personal information can also include inferred data used to create a consumer profile.	Not all personal data has an obvious tie back to a user ID (e.g., household data, GPS locations, voice to text, or follower lists on Instagram). Personal data has an evolving nature. What's considered a sensitive category or piece of data today may not be considered sensitive tomorrow, and vice versa. Understanding inferred personal data is important, yet challenging. For example, food choices on an RSVP card can infer religion. The number of sensitive data categories a business needs to track varies widely depending on its industry and specific business type. Categories will often fall into different classifications and schemas (depending on the organization) and have different handling and access restrictions. Companies may need to limit the sale or transfer of personal information based on its classification level.	Integris will never ask you to send us large customer data sets, because we assume all data is identifiable—even if it's not directly tied to user IDs. By using a combination of contextual awareness, natural language processing, and machine learning, we map all sensitive data elements for complete and accurate results. Using machine learning, our deeper inspection identifies data down to the data element level so as to assess privacy, integrity, and handling violations. Your data privacy landscape includes a detailed understanding of personal data categories, classifications, and individual data elements—including derivative personal data. You can even create your own definitions of sensitive data or let our machine learning make suggestions for you. 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 rely on for continuous innovation.
1798.110 1798.135	**Right to Request Disclosure of Information Collected, and Compliance Obligations** A consumer shall have the right to request that a business that collects personal information disclose to the consumer the categories of third parties with which it shares personal information, and the specific pieces of personal information it has collected. For consumers who exercise their right to opt out of the sale of their personal information, businesses must refrain from selling it.	There's often a disconnect between what has been agreed to on paper by lawyers and what's happening with the actual data. Often times, the people who negotiate the contract differ from those shipping the data or there are no controls in place. This can cause public embarrassment and loss of consumer trust. Also, the way contracts are written is not necessarily the way data is represented. The word "location" might appear in a contract, but the data set contains latitude and longitude values. Therefore, businesses must account for how data elements might be combined to fit the legal terms on their data sharing agreements.	Integris continuously monitors your sensitive data against data sharing agreements, and ties relevant information back to contractual obligations. We help you identify data and assign it to categories, giving it classifications such that you have granular control over the use and transfer of customer data. Enterprise multi-tenancy allows you to handle different views of the data. This lets subsidiaries manage their data separately, but still roll up under a master view.

Highlights of CCPA requirements, challenges, and how Integris responds

Section	Summary Description of Requirements	Data Privacy Management Challenges	Integris Responds
1798.105 1798.120 1798.130	**Right to Deletion, Right to Opt Out, and Disclosure Obligations** Consumers have the right to request that a business delete any personal information it has collected about them. Consumers can, at any time, direct a business that sells personal information to third parties to not sell their personal information. This is referred to as the right to opt out. Businesses need to be able to associate information, provided by a consumer in a verifiable request, to any personal information previously collected by the business about that consumer.	Not all personal data is tied to a user ID. Even without an ID the individual can still be identified in a data set. By simply mapping IDs to pre-existing metadata, businesses run the risk of creating a false sense of security about the data they have, which security parameters are being applied, and whether they're in compliance with any regulatory mandate.	Integris operates at the data element level to inform you exactly what's in your data set, not just what the metadata implies. The result? We help you fulfill data subject requests and map and we're able to support your DSAR effort and map data elements back to a specific consumer for complete and accurate results. In addition, we can flag issues relating to data residency and retention, misclassification and mislabeling, and security issues, such as lack of encryption for highly sensitive data. Integris makes it easy to respond to data subject requests (DSR). For example, customer service reps can run an on-demand deep search to locate a customer in your data ecosystem, find requested information, input data, and share it back out with the customer. They can preview data subject request reports, add private notes, and send them to the next step in your workflow. Integris integrates with your existing ticketing system, and provides detailed logs for internal audits and compliance needs.

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 and why so you can be precise in your InfoSec controls.

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.

REPORT REPRINT

The California Consumer Privacy Act: not just 'America's GDPR'

MARCH 1 2019

By Paige Bartley

Going into effect in January 2020, the CCPA has frequently been compared with the EU's GDPR. While the regulations are similar in ethos, they have fundamental differences that reflect subtly divergent cultural attitudes and approaches toward data privacy and consumer rights.

Summary

The California Consumer Privacy Act was passed in June 2018, largely as a legislative compromise. Originally intended to become a ballot measure, the bill was put together in just seven days to avoid a public vote that likely would have resulted in greater restrictions on the processing and analysis of personal data: restrictions that many large, California-based technology companies opposed. The law goes into effect in January 2020, but before then, debate and industry lobbying will likely change some of the details and requirements.

In many ways, CCPA has been compared with the EU's landmark General Data Protection Regulation (GDPR), sharing many of the same principles. What GDPR aimed to achieve with the global economy – setting a gold standard – the CCPA aims to achieve with the US economy, urging other states to adopt similar standards in absence of concrete federal privacy legislation. The differences in the regulations for the enterprise mean that a 'one size fits all' approach will not suffice, necessitating a more nuanced data management strategy.

451 TAKE

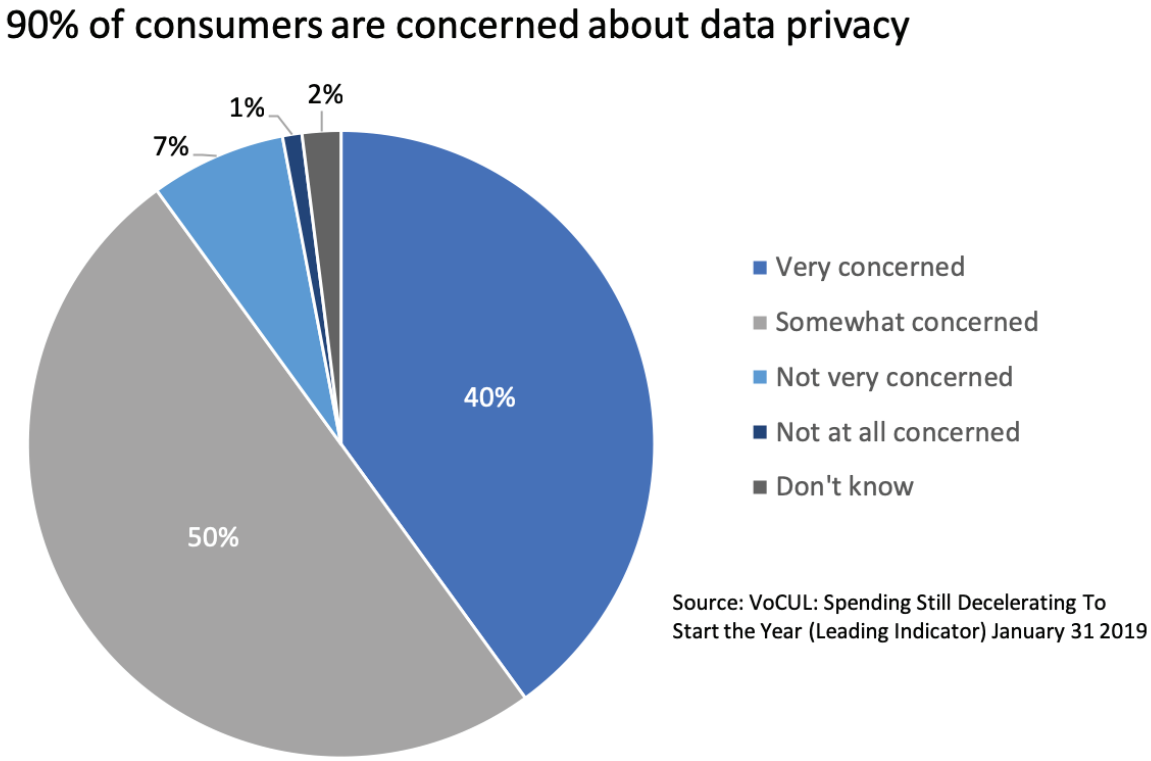
CCPA is trying to forge a de facto standard for data privacy in the US in the absence of federal legislation. With roughly 12% of the US population as its residents, and being the world's fifth largest economy, California has unique heft to enact consumer protection legislation that affects nearly any business with interstate operations in the country. In this sense, CCPA is similar to GDPR in that it uses economic presence to urge other regions – US states – to adopt similarly high standards. But GDPR and CCPA do have their own requirements and nuances, and a compliance program specifically architected to address GDPR will not necessarily translate. Troublingly, CCPA signals the beginning of 'balkanization' of data privacy regulation in the US. Businesses will need to take a more holistic and less regulation-specific approach to data management and compliance to remain competitively viable.

Data privacy and data protection, around the world, has reached a tipping point. The EU's GDPR, which went into effect in May 2018, is largely credited with triggering a domino effect of copycat regulations around the globe, as various countries sought to maintain close economic ties and simple transfer of data with the EU. The pressure to attain an 'adequacy decision' from the EU, deeming regional regulation sufficiently similar to GDPR's standards, was a primary motivating factor in nations closely copying or adapting the requirements set forth in the EU's regulation. The US, with no federal data privacy legislation of its own, started to become an outlier among developed nations.

Consumer awareness, too, has converged with global regulatory patterns to urge the discussion of data privacy in the US. Individuals are becoming more aware and more educated regarding the value and sensitivity of their data, with data breaches at consumer-facing companies now being regular headline news. Perceived privacy violations by major companies, particularly social media companies, receive increasingly vocal public backlash, even when business practices for sharing data with third parties or gaining consent for data collection were ostensibly legal in the US to begin with. 451 Research's Voice of the Connected User Landscape (VoCUL) monthly tracking of consumer trust and confidence in early 2019 shows that 27% total or 26% of US consumers are less trusting of US businesses than they were one year ago. When it comes to data privacy, nine in ten respondents are either very (40% total, 41% US) or somewhat (50%) concerned about the ability of the companies they do business with to adequately protect their personal data.

Figure 1

Source: 451 Research, LLC



With global economic pressure increasing to adopt more standardized data privacy practices and consumers becoming savvier toward violations, the US was lagging in adopting a cohesive national framework for data protection and data privacy. Traditionally in the US, data privacy legislation was very industry-specific. HIPAA, enacted in 1996, forged rules for privacy and portability of healthcare records. The Gramm-Leach-Bliley Act in 1999 created guardrails for the collection, use and disclosure of financial information. But at the federal level, the US was resistant to creating horizontal privacy rules that it perceived might limit broad economic and business opportunity. And as privacy issues came to the forefront with GDPR and increased consumer awareness, the political climate in the US did not facilitate progress. Between the 2016 presidential election and the 2018 midterm elections, gridlock between parties in Congress stalled productive discussions on bipartisan policy.

California saw this as an opportunity. Long known for progressive legislation and for being the most populous state in the nation, laws and rights that apply to California consumers or residents have overarching impact on nearly any organization that does interstate business in the US. The California Consumer Privacy Act in 2018 was a tactical move to advance a de facto national standard for data protection and privacy by establishing high standards that had extraterritorial reach. Most large businesses in the US have California residents as customers, thus pressing adoption of CCPA's standards elsewhere in the nation. But worryingly, California's legislation has spurred other states into action, drafting their own privacy laws. What could result, in absence of a federal standard, is the balkanization of privacy requirements in the US, with each state having different protections for its residents.

Key similarities, but also key differences

CCPA is inevitably compared with GDPR, and it is very similar in its core ethos. At its heart, they are both consumer protection law designed for the digital, data-driven economy. However, the exact mechanisms of how the individual laws function and enforce their requirements differ somewhat. Those distinctions often convey subtle cultural differences between the EU and the US. While detailed legal comparative analysis of the two regulations are well beyond the scope of this report, a high-level overview designed to help organizations craft more defensible data management strategy is within reach.

What they share in common

CCPA and GDPR, as well as most evolving data privacy regulations around the world, are built on core principles that are neither technical nor prescriptive. Common objectives tend to be high level in nature, and it is left to organizations to decide how to implement architectural and technical measures to comply with individual requirements. From this high-level perspective, both CCPA and GDPR are closely aligned in the following shared objectives:

- **The right to know:** Under both regulations, consumers and individuals are given bolstered transparency rights to access and request information regarding how their personal data is being used and processed.
- **The right to say 'no':** Both regulations bestow individual rights to limiting the use and sale of personal data, particularly regarding the systematic sale of personal data to third parties, and for limiting analysis/processing beyond the scope of the originally stated purpose.
- **The right to have data kept securely:** While differing in approach, both regulations give consumers and individuals mechanisms for ensuring their personal data is kept with reasonable security standards by the companies they interact with.
- **The right to data portability:** Both regulations grant consumers rights to have their data transferred in a readily usable format between businesses, such as software services, facilitating consumer choice and helping curb the potential for 'lock-in.'

How and why they differ

The devil is in the details. While CCPA and GDPR share the same broad objectives, their individual rules differ, creating trouble for the enterprise that is striving to comply with both. The US, even California, has traditionally taken a light-touch, free-market approach to business that generally views data privacy regulation as a hindrance to innovation and societal advancement.

Europe, on the other hand, has the historical perspective of WWII to shape its views on the potential systematic abuse of personal information and state surveillance. Regarding data privacy in Europe, consumers generally trust their modern governments more than they trust corporations. In the US, the opposite is true, with consumers having more faith in brands than they do in their own elected leadership. This has shaped the dynamics of the respective regulations.

Significant differences, though not an exhaustive list, include the following:

- **Who is protected by each regulation:** It goes almost without saying that GDPR and CCPA protect distinct audiences of individuals based on geography. GDPR protects identified or identifiable natural persons in the EU, 'data subjects,' whether they are legal citizens or not. CCPA protects 'consumers,' which can be individual California residents either within the state or temporarily traveling out of it.
- **What types of organization are regulated:** GDPR offers certain regulatory exemptions for businesses with fewer than 250 employees. CCPA, in general, is much more protective of small businesses and startups, exempting for-profit ventures with a gross revenue of under $25m, as well as exempting for-profit organizations that handle the personal information of less than 50,000 consumers, households, or devices for commercial purposes.

- **How personal information is defined:** Both regulations focus on data that can be either directly or indirectly linked to a living, breathing individual. However, CCPA specifies that data can also be linked at the household or device level, arguably offering a broader definition. CCPA excludes protection of certain government and public records, while GDPR offers strong protections for special defined classes of data, such as criminal records.
- **Consumer and/or individual consent:** CCPA grants California residents the right to explicitly opt out of the sale of their information to third parties. GDPR, while not giving this specific control, grants rights further upstream: in certain cases requiring explicit opt-in consent for personal data processing or analysis to occur at all. It is important to note that CCPA does not impose consent rules for data collection, only data sales. GDPR has robust rules around data collection and associated consent procedures.
- **Fine structure and civil penalties:** At first glance, GDPR's maximum 4% fine on global revenue (or up to €20m, whichever is greater) may seem to have sharper teeth, but CCPA's 'death by papercuts' approach fines individual violations. A fine of $2,500 per individual violation, or up to $7,500 per violation if intentional, is possible under CCPA.
- **Right to restrict (or object to) personal data processing:** Under many circumstances, GDPR gives individuals the right to restrict the processing and profiling of their personal data. CCPA does not provide for this mechanism; rather, it just allows individuals to opt out of the sale of their information to third parties.
- Right to rectification (correction) of personal data: Under GDPR, individuals may request that incorrect personal information held by a company be rectified, or corrected. Incomplete personal data may be completed. Under CCPA, no such explicit right exists.
- **Automated decision-making:** One very tricky area of regulation is the rules around quickly-evolving AI and ML technologies, which GDPR indirectly addresses with consumer protections and rights to object regarding the use of automated decision-making. CCPA does not address this subject, perhaps because it does not want to hinder the innovation occurring in this space, particularly with California-based technology companies.
- **Children and minors' rights:** The primary similarity between GDPR and CCPA regarding the treatment of minors is age. Both regulations use 16 as a common bar for 'adult' consent, and 13 as a bottom rung for possible independent consent. But GDPR requires adult consent for all data processing consent requests, whereas CCPA invokes adult consent only when the sale of data is involved. However, existing laws such as COPPA in the US provide additional online protection for minors.
- **Data security requirements and breach reporting:** CCPA is not prescriptive with security requirements, but it does establish a right of consumer action for certain data breaches that violate existing California law. GDPR mandates appropriate technical and organizational measures to protect data, and has an onerous 72-hour reporting window for suspected or detected breaches.

Business strategy amid proliferating regulatory requirements

While the list above may suggest there are more differences than commonalities between regulations, their core principles are largely identical. It is key for organizations is to tackle core, shared requirements at the architectural data management level and address individual nuances of each regulation with tools higher in the stack only as necessary. Such an approach allows for flexibility amid evolving regulations, and ultimately, cost savings.

As 451 Research discussed in the report 'Architectural data control: Turning privacy requirements into a blessing, not a curse,' strong, consistent and granular control of enterprise data is a shared requirement across all data-driven regulations. Just as a mother sauce in French cuisine can be adapted to meet the specific requirements of individual dishes, strong enterprise data control can be adapted to meet the individual requirements of individual regulatory requirements. In this sense, a bottom-up approach, focused on architectural control of data, is warranted. No number of custom compliance point solutions, implemented higher in the stack, can address or fix a lack of data control at the repository level.

It is important to note, too, that data privacy and data protection regulations are largely more process-oriented than they are technology-oriented. People, and the workflows they engage in to control data, must be orchestrated. Investment in platforms that help coordinate processes across various data protection and data privacy stakeholders can especially benefit the business, even when these platforms do not exert direct control on data themselves. In these cases, the enterprise must take care to evaluate the breadth and depth of integrations available because these are necessary for ensuring that specific data protection actions, such as encryption, are ultimately executed without disrupting the human workflow. Support for a broad variety of end-user stakeholders ranging from IT to data steward to privacy professionals is also needed.

Finally, enterprise perceptions today are still a hindrance to successful compliance strategy. Most organizations still view compliance as a reactive, costly and burdensome business function. That must change, given the reality of proliferating global requirements. Compliance requirements are an opportunity to reassess and optimize core data management architecture, for the ultimate benefit of all data-driven initiatives within the enterprise. To play Whack-a-Mole with compliance requirements, forging a new task force and new set of tools for each regulation, is not scalable or sustainable. The successful business in the data protection and data privacy era will focus on core competencies that are required and shared by all regulations, and customize only as needed in specific cases.

9 INDUSTRY EXPERTS PROVIDE SAGE ADVICE ON

How to protect your customers' sensitive data in 2019

as well as some things you should **NEVER** do

C-suite execs have a lot on their plates when it comes to protecting their customers' sensitive data in 2019. Please tell us:

1. What's one sage piece of data privacy management advice or tip to help them in 2019?
2. What's one thing they should never do, or a pitfall to try to avoid in 2019?

DAVID HOFFMAN

@hofftechpolicy

Associate General Counsel and Global Privacy Officer

What's one sage piece of data privacy management advice or tip to help them in 2019?

As we move towards a more data-centric economy, understanding what data an organization has, and how it is used, is critical for both shareholder value and protecting privacy.

Organizations need to build the right processes to map where their data is, how they can make innovative use of it, and how they will show they are accountable to the individuals to whom the data pertains.

What's one thing they should never do, or a pitfall to try to avoid in 2019?

An organization should never rely solely upon third parties to have access to data without showing they will be accountable for how it is used. Upstream and downstream data inventory management will be critical in 2019.

CAMERON ETEZADI

@cetezadi

SAP Concur Deputy CTO

What's one sage piece of data privacy management advice or tip to help them in 2019?

Modern enterprises move data through streaming pipelines, where it can be hard to protect provenance and canonicity.

Tracing where the data ends up is as essential as protecting the data itself. Once you publish data internally, it can be very hard to control where it goes or how it's used.

Enterprises should implement strong controls and good hygiene in establishing trust and access – and then verify the results.

What's one thing they should never do, or a pitfall to try to avoid in 2019?

Avoid playing "catch up"; many organizations end up "compliant" at a point in time but gradually fall apart as new software is written or deployed, new people join the organization, etc.

Protection is a process that many organizations fail to bake into the upfront architecture of their projects and then scramble towards when it's too late.

It's too easy to leave holes, pay too much, or find yourself in an impossible situation if privacy is always a bandage applied at the end.

JENNIFER LEGGIO

@mediaphyter

FLASHPOINT Chief Marketing Officer & VP Operations

What's one sage piece of data privacy management advice or tip to help them in 2019?

Engage in external collaboration and information sharing. There are a number of secure, trusted communities that facilitate these activities among security and privacy practitioners, so if your company isn't already a member, join one. These communities range from large and industry-specific, such as the various ISACs, to small and vendor-specific, but all exist for the same reasons: to provide like-minded experts with the means to quickly and easily share relevant information with, and seek guidance from, other like-minded experts. Doing so can expose your company to greater resources and expertise that can help you to better protect your customers' data.

What's one thing they should never do, or a pitfall to try to avoid in 2019?

Never conflate compliance with security. GDPR, for example, has fueled great progress in how companies address the privacy of customer data, but the standards it enforces are by no means sufficient for securing customer data.

This is largely because there are many critical areas of security that GDPR does not regulate, including encryption, security awareness and education, business continuity and penetration testing, and technical and policy controls, to name a few. The same goes for similar compliance bodies such as PCI DSS and HIPAA. Just because a company is deemed compliant does not mean that its customers' data is fully immune to compromise. Compliant businesses can and do experience data breaches, which is why achieving compliance should be never be viewed as an end goal—but rather as one of many essential components of a comprehensive security strategy.

KRISTINA BERGMAN

@KristinaKerr

INTEGRIS SOFTWARE Founder, CEO

What's one sage piece of data privacy management advice or tip to help them in 2019?

Know where your data is.

When I was working in venture capital five years ago and first started researching the data privacy space for investment purposes, I found that the biggest glaring problem was that no one knew what data was where, let alone if they were in compliance with any laws, contracts, or other business obligations.

The foundation to complying with any law, whether it's GDPR or CCPA or any of the other new bills being considered, is to know what data you have.

What's one thing they should never do, or a pitfall to try to avoid in 2019?

Never assume that your work is done just because you've got great policies and procedures in place.

A key component to ensuring compliance, or at least defensibility, is the operationalization of those policies and procedures. Being able to audit your data sources to prove compliance with the law is critical to protecting your brand and reputation.

MARC GROMAN

@MarcGroman

Former Senior Advisor for Privacy in the Obama White House
Former Chief Privacy Officer of the Federal Trade Commission
Principal, Groman Consulting Group LLC
Adjunct Professor, Georgetown University Law Center

What's one sage piece of data privacy management advice or tip to help them in 2019?

Today, data often is a company's most strategic and valuable asset. Companies must treat it that way, by implementing a comprehensive, enterprise-wide, continuous and risk-based privacy and security program. Step one – know what data you have.

What's one thing they should never do, or a pitfall to try to avoid in 2019?

Never make assumptions about the data your organization collects, creates and stores. Rely on facts, evidence, and documentation.

BARBARA COSGROVE

@cosgrove_barb

workday.

Chief Privacy Officer

What's one sage piece of data privacy management advice or tip to help them in 2019?

Privacy will be center stage in 2019, so be proactive and reevaluate your processes to ensure that you not only remain GDPR compliant but also anticipate any future U.S. and global privacy legislation that could be coming in 2019. Start by establishing a cross-functional taskforce to perform an assessment of your current state of compliance. During this process, take the time to understand what's been successful and where there have been challenges from a business perspective prior to introducing new processes. Once you've done that, map new laws and regulations to your existing controls and processes, and determine where you may be required to implement changes. Once implemented, be sure to set a regular cadence for the taskforce to regroup to assess compliance.

What's one thing they should never do, or a pitfall to try to avoid in 2019?

With new regulations like the California Consumer Privacy Act (CCPA) in the pipeline, be sure you don't evaluate them in isolation.
Build a comprehensive privacy governance framework, which enables you to continually re-assess your compliance with existing privacy regulation like GDPR and emerging ones.

MARK KRAYNAK

@AspectVC

Aspect VENTURES Entrepreneur, Venture Partner

What's one sage piece of data privacy management advice or tip to help them in 2019?

Get a handle on employee/contractor off-boarding.
Latent privileges are a big, unnecessary risk. Also, automate your process of understanding what sensitive data you have.

Most organizations have too much data in too many places for human processes to be reliable or consistent enough to be effective.

What's one thing they should never do, or a pitfall to try to avoid in 2019?

Don't stop at Encryption. The most common pitfall I see is when I hear someone's answer about data security is, "We encrypted our data, so we don't need to do anything else." Encryption is good for mostly bulk, mostly static use cases, but tends to fail for data in use.

PAIGE BARTLEY

@451Research

451 Research Senior Analyst – Data, AI & Analytics

What's one sage piece of data privacy management advice or tip to help them in 2019?

View data protection and data privacy as an opportunity, rather than a burden. There's a pervasive enterprise perception that consumer controls for data will result in less analysis and insight, or that privacy controls somehow "lock down" data.

This misses the bigger picture. Data-driven regulation, such as GDPR and similar mandates, all share the same common requirement of strong, granular control of data at the architectural level.

Strong control of data, in turn, has downstream benefits for other proactive data-driven initiatives within the organization.

A robust data protection and privacy program, implemented enterprise-wide, has benefits for data quality, coordination of self-service access rights, and building consumer trust.

At a high level, data privacy and data protection requirements are a golden opportunity to reconsider and optimize data management architecture and practices.

PAIGE BARTLEY

@451Research

451 Research Senior Analyst – Data, AI & Analytics

What's one thing they should never do, or a pitfall to try to avoid in 2019?

We've officially entered the data protection and privacy era, and the enterprise can no longer have a combative attitude towards compliance if it wishes to remain competitively viable.

The biggest pitfall is viewing data privacy or data protection requirements as a list of burdensome technical "checkboxes" that need to be ticked off one by one for each new regulation.

This view of the individual trees misses the broader forest: the core principles that are shared across regulatory frameworks.

Implementing new siloed tools and new processes for each new regulation is not sustainable, economical, or scalable.

Instead, organizations need to focus on optimizing underlying data management architecture and workflows from the ground up.

Focus on the core commonalities, rather than the differences, between regulations. From there, implement highly-specialized point solutions higher in the stack only when necessary.

CRAIG SPEIZLE

@craigspi

agelight Managing Director
OTA Online Trust Alliance Founder & Chairman Emeritus

What's one sage piece of data privacy management advice or tip to help them in 2019?

2018 will likely go down as the year of questionable ethics. From the data sharing and mining practices of Facebook, Google and most recently the Weather Channel's app, to the abuse of social networks, we all need to be concerned.

All too often these entities who were supposedly "stewards of our privacy and trust" appear to have acted unethically.

While executives need to be held accountable, one has to also question employees who failed to come forward and follow their own moral compasses. Our industry is at the center of a seismic change with the convergence of big data and artificial intelligence (AI).

The oceans of digital information and low-cost computing power are providing endless marketing opportunities. At the same time, we are being confronted with ethical dilemmas challenging users' digital dignity and redefining privacy norms.

My big focus for 2019 is Data Ethics: the convergence of big data, AI and Ethics. I have been steadfast on the need to move from compliance to stewardship. Ethics is an extension to this in light of the practices and what I call "data laundering," which is occurring.

The question at hand is:
Can industry and governments be trusted to responsibly regulate AI?
Second, how can ethical guardrails be developed to help prevent abuse?

CRAIG SPEIZLE

@craigspi

agelight
OTA Online Trust Alliance

Managing Director
Founder & Chairman Emeritus

There is no question AI will have a profound effect on how marketers engage consumers.

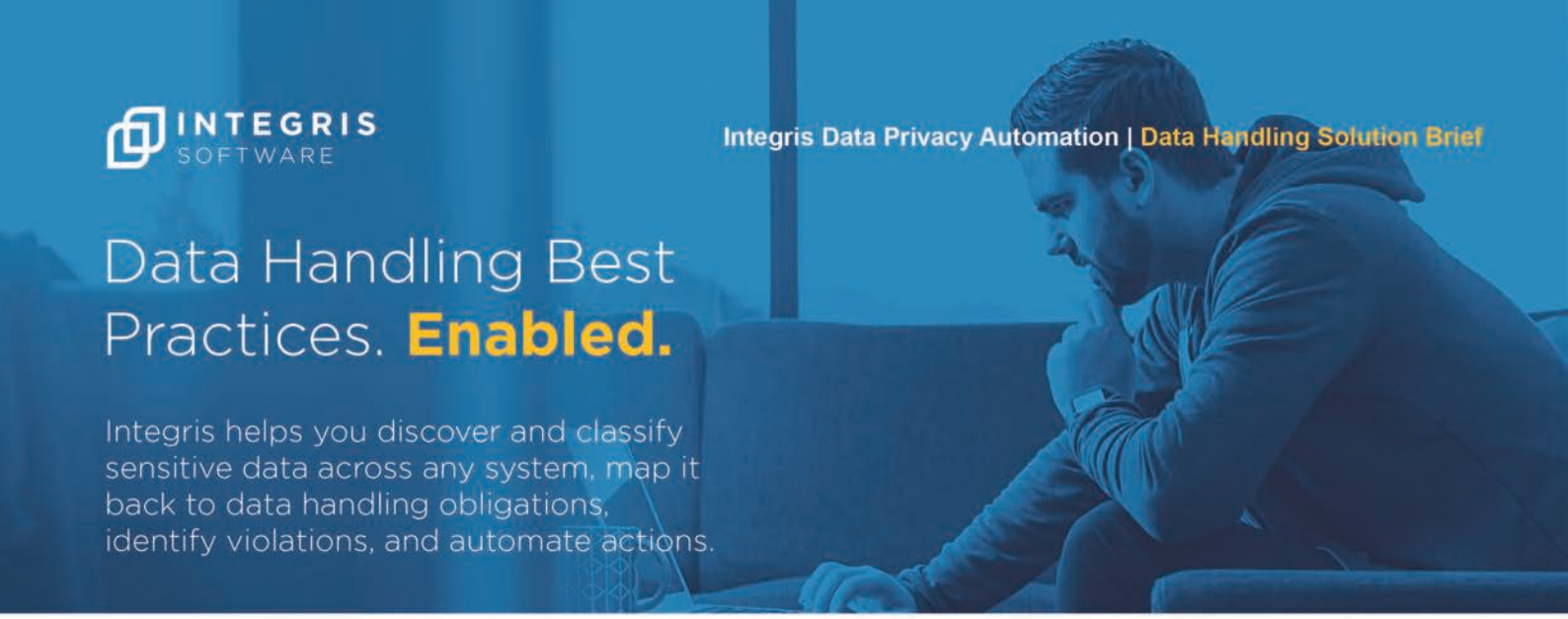
Done right, consumers will get better and more relevant ads, content and services. This can be a win-win, but only if we get it right and address the ethical unintended consequences in advance.

What's one thing they should never do, or a pitfall to try to avoid in 2019?

The one thing executives should avoid is remaining silent.

They need to question their business and data strategy and not fall silent like so many employees at offending companies have.

The question is, are they willing to follow their moral compass and rise above compliance?



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.

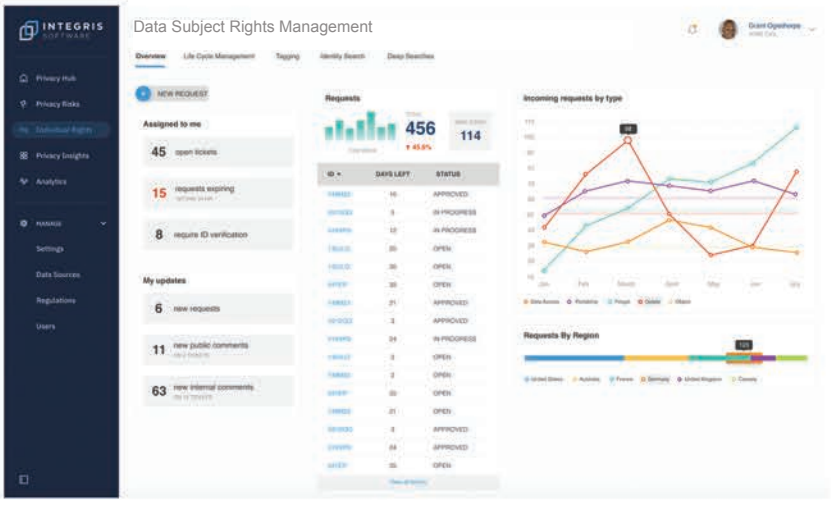
6 Residency-based policy-making

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

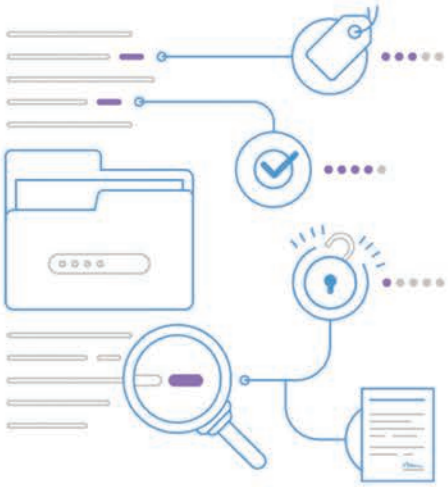
Our deeper inspection down to the data element level informs you exactly what's in the dataset, not just what the metadata implies.

- 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



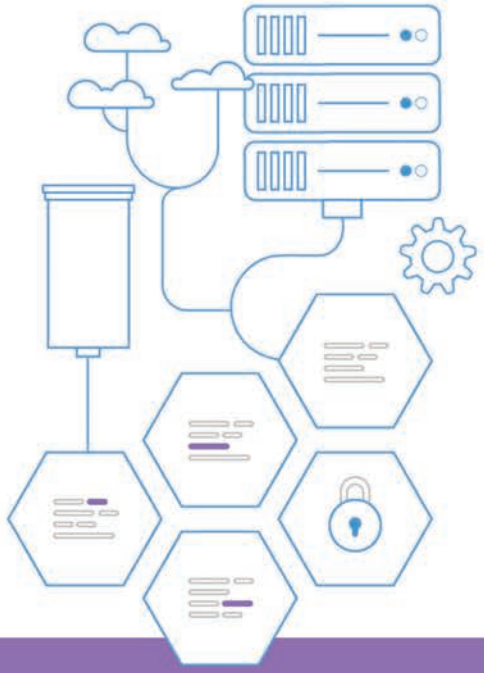
Operationalize and automate the enforcement of policies that incorporate security, privacy, and data governance.

- 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 and why so you can be precise in your InfoSec controls.

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