Brought to you by the publishers of COMPLIANCE WEEK

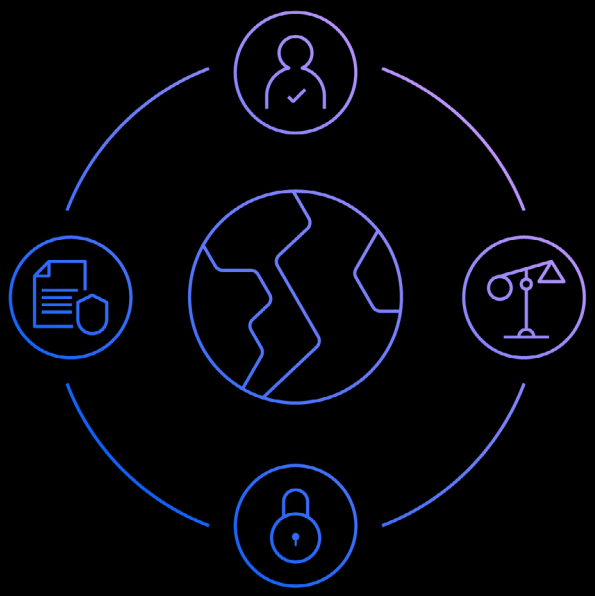
INSIDE THIS PUBLICATION:

The current state of GLOBAL PRIVACY REGULATION

An e-Book publication sponsored by IBM

Global privacy compliance is more demanding than ever

IBM OpenPages Data Privacy Management gives you oversight of your organization's private data and eliminates compliance blind spots



Our risk and compliance experts are here to help you:

- Get up-to-date, quality data for AI and analytics
- Automatically classify and inventory all information assets containing sensitive data
- Run privacy compliance assessments on every information asset using private data
- Do more with data while maintaining compliance
- Automate workflows for privacy monitoring
- Improve visibility of privacy programs to strengthen brand trust and meet regulatory privacy concerns

Learn more at:
ibm.biz/op-data-privacy

Watson

IBM

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is a business intelligence and information service on corporate governance, risk, and compliance that features a daily e-mail newsletter, a bimonthly print magazine, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for chief compliance officers and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance practitioners. www.complianceweek.com

IBM

IBM OpenPages with Watson transforms the way risk and compliance professionals work. By providing core services and functional components on a scalable platform that spans operational risk, regulatory compliance, IT governance, internal audit, business continuity, model risk, third-party risk, policy, financial controls and data privacy management, IBM OpenPages with Watson delivers a holistic view of risk and regulatory responsibilities across the enterprise. It delivers on the marketplace demand for an integrated end-to-end solution that enables organizations to connect internal GRC policies and practices to the external regulatory environment.

Click here to learn more about IBM OpenPages.

Inside this e-Book

Private right of action a problem for state privacy laws

An enforcement provision allowing customers to sue firms that misuse their data is a stumbling point for state data privacy regs, writes **Aaron Nicodemus**.

With the prospect of a federal data privacy law still remote, state legislatures have moved forward with their own versions of California's Consumer Privacy Act (CCPA).

Ten states were considering data privacy legislation as of May 5: Alabama, Alaska, Colorado, Connecticut, Illinois, Massachusetts, Minnesota, New Jersey, New York, and Texas, according to a tracker from the International Association of Privacy Professionals (IAPP).

Legislation in several states where a privacy law had strong support—Florida, Oklahoma, and Washington—failed to pass because lawmakers disagreed on enforcement.

The Florida bill, HB 969, would have imposed new disclosure requirements on companies that collect information on customers who use the company's app or Website. Customers would have the right to access the personal data collected on

"It has become clear that the main gate to passage of any data privacy bill is not going to be substance; it is going to be how the bill is enforced, and, in particular, whether a bill includes a private right of action."

Nathan Taylor, Partner, Morrison & Foerster

them, the right to correct that data if it contained errors, the right to delete it, and the right to opt out.

But the sticking point in Florida was the bill's private right of action, which would allow customers to sue businesses that violated any provision of the law. The bill died April 30 because its supporters could not overcome business opposition to private right of action, the *Miami Herald* reported.

For the third consecutive year, a data privacy bill failed to pass in the state of Washington in April, primarily because of opposition to the bill's private right of action, the National Law Review reported.

A bill in Oklahoma also died in April because of opposition to a requirement allowing consumers to proactively consent for businesses to collect their data, known as an opt-in provision, the National Law Review said.

"It has become clear that the main gate to passage of any data privacy bill is not going to be substance; it is going to be how the bill is enforced, and, in particular, whether a bill includes a private right of action," said Nathan Taylor, partner at law firm Morrison & Foerster.

For many businesses, private right of action poses the potential for significant legal exposure through consumer class-action lawsuits, said Vivek Mohan, partner in Mayer Brown's Cyber-Security and Data Privacy practice.

Private right of action also presents concerns for compliance specifically, he said. If a state data privacy law is enforced by the state attorney general, businesses seeking in good faith to comply with the law can have a conversation with the regulatory body. Regulators can offer guidance and interpretation of the law, helping a company adjust its efforts toward more substantial compliance.

Private right of action, conversely, can appear to businesses to be "an opportunistic gotcha game," where the guidance changes as lawsuits are resolved, Mohan said.

Of the states with pending data privacy legislation listed earlier, only Massachusetts, Minnesota (one of two bills), and New York (all three bills) contain private right of action provisions, according to the IAPP.

The only state data privacy bill currently in force, the CCPA (effective as of Jan. 1, 2020), offers a limited private right of action that consumers can invoke only if their personally identifiable information was lost in a hack or breach.

Nearly 50 class-action lawsuits were filed through Jan. 1, 2021, seeking damages related to CCPA-related violations, according to Morrison & Foerster. Children's clothing retailer Hanna Anderson paid $400,000 to settle a CCPA-related lawsuit in November.

Other lawsuits pending include class actions against Walmart, Zoom, and Houseparty, in which consumers alleged the companies mishandled their personal information.

Two other state data privacy laws have passed since the CCPA took effect. Both will be enacted in January 2023. Neither change the state of play on private right of action.

The California Privacy Rights Act (CPRA) ladles additional responsibilities onto businesses on how they should handle private data such as: prohibiting companies from sharing sensitive information about customers' health, finances, race, ethnicity, and precise location; tripling fines for violations related to children's data; and putting new limits on how companies can collect, share, and sell customers' personal data.

The private right of action provision remains unchanged from the CCPA.

Virginia legislators recently passed the Consumer Data Protection Act (CDPA), which mandates companies publish privacy policy notices that describe how they use, collect, and share personal data.

The CDPA does not contain a private right of action, giving the Virginia attorney general the sole power to enforce the law.

Had Florida's bill passed, its private right of action would have resulted in a significant widening of the legal basis to sue when compared to the private right of action contained in the CCPA.

Consumers could have sued for any violation of the law, not just when a breach or hack occurred.

Florida's bill "would have created a lot of headwind for the business community's legislative efforts in other states," Taylor said. ■

Key regulators: GDPR one-stop shop unsustainable

Ireland and Europe data protection chiefs among those who believe the GDPR one-stop shop provision needs reform. **Neil Hodge** reports.

The mechanism that determines which EU data protection authority (DPA) should lead investigations and enforcement actions against companies for data breaches and abuses is "slow" and "unsustainable," says the head of the regulator that oversees most Big Tech firms.

Helen Dixon of Ireland's Data Protection Commission (DPC) believes the "one-stop shop" provision under the General Data Protection Regulation (GDPR) is not fit for purpose in the long term.

Dixon spoke as part of a panel discussion on April 26 at an International Association of Privacy Professionals-organized event. She noted the one-stop shop "slows the enforcement process down" and "drains resources."

Part of the reason for the slow turnaround is because different EU member states take very different views on what constitutes a GDPR infringement, she said. They are also divided over how punitively the legislation should be enforced.

"A DPA reaches a decision, tries to defend it against a lot of arguments from 26 other national DPAs under Article 60 [of the GDPR], and then tries to defend a revised version again under Article 65 that attempts to take into account their concerns before the European Data Protection Board (the EU's umbrella data regulator) steps in to give a final verdict," said Dixon. "That is unsustainable."

Dixon added the Irish DPC is being "drowned" by "scattergun demands" from other DPAs for mutual assistance requests, which are slowing down its work.

The Irish DPC is working on more cross-border investigations than any other EU country. It has 28 ongoing cross-border inquiries into Big Tech firms, with Facebook and its associated companies accounting for 15.

In the nearly three years the GDPR has been in force, Ireland has faced fierce criticism over the slow progress the authority has made in trying to investigate Google, Facebook, and others. With a budget of just €16.9 million (U.S. $20.4 million) this year—and a staff of 145—the Irish DPC's resources pale in comparison to those of the companies it is meant to regulate.

European Data Protection Supervisor Wojciech Wiewiórowski said at the same event he would like to see the one-stop shop reformed in the long term because there is a "danger" the lack of consensus leads to DPAs "disowning decisions they don't like" in the way some regulators—namely, Austria, Germany, Hungary, and Italy—did with the Twitter GDPR decision in December.

Wiewiórowski, who is in charge of overseeing data protection in the EU's institutions, thinks there is a risk one-stop shop binding decisions taken by the EDPB "may become orphans" because a majority of DPAs "will all say in the end that, 'We would've done it better only if it was our own decision.'"

He warned trying to achieve consensus among the EU's 27 members could result in "a national DPA pushing through a decision it does not agree with."

Wiewiórowski added some of the problems relating to the one-stop shop are because the mechanism was agreed in haste after the rest of the GDPR's articles and details had been signed off. Several DPAs objected to it as unworkable. ■

"A DPA reaches a decision, tries to defend it against a lot of arguments from 26 other national DPAs under Article 60 [of the GDPR], and then tries to defend a revised version again under Article 65 that attempts to take into account their concerns before the European Data Protection Board (the EU's umbrella data regulator) steps in to give a final verdict. That is unsustainable."

Helen Dixon, Ireland's Data Protection Commissioner

ICO head: Fines key attention to data privacy from boards

Neil Hodge has more on the U.K. information commissioner's thoughts on why the threat of fines goads executives to take privacy seriously.

The threat of fines has done more to focus boardroom attention on data privacy and effective cyber-security than any other measure, says the head of the U.K.'s data regulator.

Elizabeth Denham, the U.K.'s information commissioner and chair of the Global Privacy Assembly, a body that aims to coordinate best practice and enforcement among data regulators worldwide, believes without the threat of significant fines, executives would simply not bother thinking of privacy—and particularly cyber-security—as a risk issue boards should be concerned about.

"Fines get directors' attention, drive better behavior, and are an invaluable tool for any regulator," Denham told attendees at a recent Webinar on the need for privacy regulation that was organized by the International Association of Privacy Professionals. "How can you regulate without fines?"

Under the U.K.'s previous Data Protection Act 1998, maximum fines were capped at £500,000 (U.S. $700,000)—a figure few believed changed the behavior of many major companies toward better data protection.

But in the run-up to the EU's General Data Protection Regulation (GDPR) coming into effect at the end of May 2018, companies complained compliance costs in preparation had rocketed, "as if there hadn't been any national legislation in place beforehand." said Denham.

The Information Commissioner's Office (ICO) issued 17 penalties totaling approximately £42.4 million (U.S. $59.2 million) just last year. Significantly, three GDPR fines against British Airways, Marriott International, and Ticketmaster accounted for £39.65 million (U.S. $55.4 million) of that total.

Denham believes there is "no doubt" increased awareness of the need for better privacy protection is attributable to the GDPR's ability to hit companies with a maximum penalty of up to 4 percent of global turnover for serious non-compliance.

While a more tangible threat of meaningful enforcement has pushed data privacy onto a board's risk agenda, Denham also pointed out there are still significant barriers to achieving the level of data protection and best practice regulators want to see.

One of the key problems, she said, is that some concepts around data privacy are either not well-defined, not understood, or not practicable.

For example, said Denham, there is a challenge globally about what constitutes—or should constitute—"consent." The term "lacks meaning and is not scalable," she said, citing as a notable example cookie consent (where users give a Website their permission to track and process their personal data, ostensibly to improve the service—though, not necessarily).

Denham suggested there needs to be a push globally by data regulators toward establishing what "consent" actually means, what it involves, and how it can be enforced. She added that a certification process to ensure compliance might be more appropriate as a way forward.

More generally, Denham is in favor of better coordination among data protection authorities to achieve a globally similar view of privacy; consent; and enforcement, possibly through standards. She hopes the Global Privacy Assembly will do more to push for this.

She also highlighted new challenges data regulators face in the aftermath of the pandemic.

Denham added that there is a "very real danger" organizations that have been given "privileged" access to sensitive data, particularly health and medical records, are going to be reluctant to face any kind of data restrictions or attempts to scale back access over fears doing so prevents innovation.

Consequently, the ICO—and other EU data authorities, she suggested—will need to have "deep conversations" about the "beneficial" uses of peoples' data during future national or global crises. ■

Facebook facing 10th GDPR probe over data leak

Neil Hodge reports on Facebook's historic data leak and where the company has failed in terms of disclosure.

The Irish Data Protection Commission (DPC) has launched an inquiry into Facebook over concerns the social media giant may not have properly disclosed the full extent of a historic data leak and that it failed to report a subsequent breach within the necessary 72-hour timeframe.

Scrutiny from the data regulator came after a dataset containing 533 million users' personal details recently resurfaced on a hacking forum.

Facebook said the data had been recycled from hacks that had already been publicly disclosed after occurring between June 2017 and April 2018—prior to when the General Data Protection Regulation (GDPR) came into force.

The company added, however, that hackers had been scraping data from people's Facebook profiles "prior to September 2019" through its "contact importer," a feature designed to help users find friends to connect with using their Facebook contact lists.

"When we became aware of how malicious actors were using this feature in 2019, we made changes to the contact importer," said Mike Clark, Facebook's product management director, in an April 6 blog post.

Under the GDPR, companies have a requirement to inform regulators of a breach within 72 hours.

In April, the Irish DPC launched an own-volition inquiry under the GDPR, as well as under Section 110 of the (Irish) Data Protection Act 2018 for any infringement of users' data prior to the GDPR coming into force.

In a statement, the regulator said: "The DPC, having considered the information provided by Facebook Ireland regarding this matter to date, is of the opinion that one or more provisions of the GDPR and/or the Data Protection Act 2018 may have been, and/or are being, infringed in relation to Facebook Users' personal data."

This latest GDPR inquiry is the 10th Facebook faces in Ireland. Lawyers have suggested given the number of users involved in the possible breach, a fine—if applicable—could be sizeable. Several experts also believe the company could face multiple class actions.

A Facebook spokesperson said the company is "cooperating fully" with the investigation: "These features are common to many apps, and we look forward to explaining them and the protections we have put in place." ■

New chief compliance officer, same old Facebook

Kyle Brasseur explores how Facebook is seemingly unchanged, despite the hiring of its first chief compliance officer.

It isn't surprising to see Facebook think it doesn't have an ethical obligation to alert users to its latest data leak, but this time there's an extra level of disappointment.

The social media giant has been relatively mum on the publication of a data set that contained the personal information of over 533 million of its users on a hacking forum in April. Facebook released a blog post explaining how the data was scraped prior to a platform update in September 2019 and assuring the vulnerability no longer exists, but that has been the extent of its customer-facing communication thus far.

No notifications on its app. No efforts to e-mail users. Just a blog post wedged in an online newsroom full of promotional posts that leaves to chance whether those affected will know their names, locations, birthdays, e-mail addresses, and phone numbers were potentially made available for free to anyone looking to find them.

Meanwhile, LinkedIn, put in a similar situation after reports surfaced of data scraped from its site being made available on hacking forums days after the Facebook leak, issued a statement that it promoted prominently in its LinkedIn News section of users' feeds for multiple days.

Facebook is no stranger to these kinds of ethical dilemmas, but one might have hoped the company's appointment of its first chief compliance officer earlier this year would change the way it does business.

Henry Moniz got his start in the position in February after a lengthy run as compliance chief at Viacom/ViacomCBS. His role at Facebook was billed as being empowered to enhance the legal and ethical standards of the company, with direct report to General Counsel Jennifer Newstead and a board committee overseeing audit and risk.

It sounded great on paper—perhaps even too good to be true. The fact Facebook named its first chief compliance officer in 2021 despite going public in 2012 and all the regulatory scrutiny it has faced since is all you need to know about how the company views compliance. A big factor in whether Moniz can succeed in his position will be buy-in from CEO Mark Zuckerberg, and whether that comes to fruition remains to be seen.

What we know now is he isn't off to the best start. Not only is Facebook's handling of the leak ripe for ethical criticism, it could also lead the company to pay a fine under the EU's General Data Protection Regulation (GDPR). The Irish Data Protection Commission announced it has launched an inquiry into whether Facebook did not properly disclose the full extent of the leak and failed to report the breach within the necessary 72-hour timeframe. The GDPR probe is the company's 10th it faces in Ireland.

The problems don't end there: Facebook is also facing a potential "mass action" lawsuit under the GDPR on behalf of users in response to the leak.

Facebook maintains the data made available in the leak is old and the issue behind it resolved. It surely knows better than we do. But if that's the case, why not make some effort to let users know everything is under control? The way things stand now, it sure doesn't feel that way. ■

The fact Facebook named its first chief compliance officer in 2021 despite going public in 2012 and all the regulatory scrutiny it has faced since is all you need to know about how the company views compliance. A big factor in whether Moniz can succeed in his position will be buy-in from CEO Mark Zuckerberg, and whether that comes to fruition remains to be seen.

Italian DPA fines Fastweb $5.3M under GDPR

Kyle Brasseur reports on Italy's fifth-largest fine handed down recently to telecom firm Fastweb for misusing customer data with telemarketing.

The Italian Data Protection Authority ("Garante") on April 2 announced a fine of €4.5 million (U.S. $5.3 million) against telecommunications company Fastweb for misusing customer data for telemarketing purposes.

The fine is Italy's fifth-largest handed down under the EU's General Data Protection Regulation (GDPR). Three others in that group have targeted telecommunication companies for similar violations of the 2018 legislation.

In a translated press release, Garante noted an investigation into Fastweb was launched following hundreds of complaints from users regarding unwanted promotional calls received without their consent. The calls appeared to originate from unregistered numbers, and in some cases, customers also complained of receiving calls not meant for them. The scope of the problem was viewed as affecting Fastweb's entire customer base.

"The security measures of the customer management systems were … inadequate," Garante said. The regulator further criticized the maintenance of contact lists provided to Fastweb by external partners that did not acquire user consent to share such data.

Fastweb was viewed as a repeat offender in Garante's judgment after being sanctioned under laws other than the GDPR in 2012 and 2018 for similar telemarketing violations. Another aggravating factor listed is the continued presence of the vulnerabilities in the customer database.

Garante has ordered Fastweb to strengthen security measures to prevent unauthorized access to its databases, overhaul its telemarketing practices to include enrolled customers only, and discontinue use of data obtained by third parties that did not first gain user consent.

Mitigating factors in the case included Fastweb's cooperation in the investigation, stated intention to further improve its control systems, and participation in roundtables focused on combating the phenomenon of aggressive telemarketing. ■

IBM **OpenPages with Watson**

Navigate Data Privacy in an Uncertain World

Navigate Data Privacy in an Uncertain World

We live in a business environment of unprecedented change. Business conditions and regulatory environments can change in a matter of hours. Fines from regulatory bodies across the globe have nearly quadrupled in the last two years.

To keep pace with rapid change, enterprises need a proactive approach to risk and regulatory compliance. They need to recognize new or emerging risks and respond quickly to regulatory change in order to protect and secure the business.

Many businesses' approach to governance, risk and compliance (GRC) is siloed, spread out across a dozen or more risk management systems. Data and workflows are trapped in legacy applications and isolated databases that don't talk to each other. This means that GRC professionals lack visibility into the company's risk exposure across domains.

From reactive to predictive
Introducing IBM OpenPages with Watson, a more holistic, modern approach. OpenPages is a fully integrated, flexible enterprise risk platform that breaks down silos and opens up GRC capabilities to leaders across the organization. It gives you total visibility of your company's risk position from one integrated point of view. With better access to your data, you can establish a more predictive approach to GRC. Author and deploy GRC workflows on any cloud or on prem environment in 15 minutes.

OpenPages supports ten risk domains, including:

- Operational risk
- Regulatory compliance
- Third-party risk
- Financial controls
- Policy
- Business continuity
- Internal audit
- Data privacy
- IT governance
- Model risk governance

Powered by AI for smarter workflows
There's no training required, and with an intuitive interface and 24/7 support from a Watson-powered virtual assistant, you don't need to be a risk expert to get started. In addition to the virtual assistant, OpenPages is equipped with other advanced AI capabilities. With natural language processing (NLP), you can achieve data accuracy in risk reporting, as the platform makes data categorization and mapping suggestions to the user, further reducing training times. You can also perform natural language translations to detect and translate over 50 languages selected within OpenPages.

With IBM Cognos Analytics embedded, OpenPages allows you to reduce reporting time from 30 days to three hours. You'll have faster access to better data, resulting in both cost savings and risk reduction.

Approachable UI
Created with IBM Design Thinking principles, OpenPages was made to be approachable to different types of users from across the organization. Dynamic dashboard capabilities support improved productivity and risk management, with customized views, visualizations, widgets, task tabs, and personalized landing page options based on user profile. Task views streamline complex processes and give users the ability to add favorites, heat maps, sibling relationships and more.

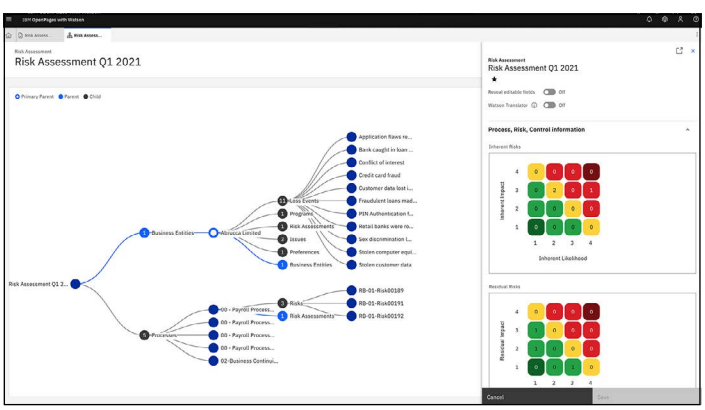


Figure 1.
IBM OpenPages with Watson provides holistic data needed to perform a GRC task

IBM OpenPages Data Privacy Management

By 2023, more than 80% of companies worldwide will face at least one privacy-focused data protection regulation. Today, individuals are more aware of their data privacy rights, with three out of four consumers saying that they won't buy from companies they don't trust to protect their privacy, no matter how great their product is. As of January 2021, $331 million in fines have been issued for violations of GDPR alone across its lifespan. It's clearer than ever that ensuring privacy is non-negotiable.

In today's regulatory environment, you must bring risk and compliance together with your data governance strategy. GDPR, CCPA, and other regulatory frameworks around the world virtually demand that organizations integrate these functions to safeguard the organization and its stakeholders. CDOs, CPOs, CROs, CCOs and other leaders must have a holistic view of all sensitive data that lives throughout the organization's information architecture and understand how that data is being used, where it's being used, by whom, and for what purpose. Leaders must be able to readily turn that information into demonstrable proof of compliance that can be presented to regulators.

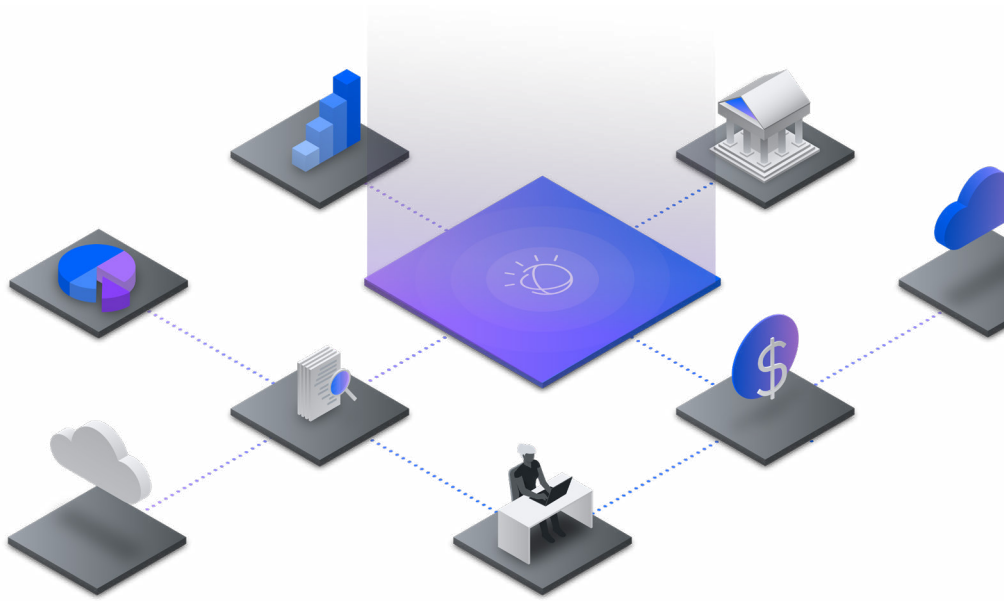
Running data GRC efforts as distinct functions is a recipe for violations, which can lead to hefty fines or a catastrophic loss of consumer trust. You need a solution that can embed GRC management across the entire organization. This democratizes the GRC function, so that line-of-business leaders can partake in ownership of the GRC effort and contribute their unique understanding of and proximity to their domains.

A new solution for total data visibility
IBM OpenPages is now equipped with Data Privacy Management, a new module within the OpenPages platform that enables organizations to meet new data privacy challenges head-on.

Automate privacy monitoring
IBM OpenPages Data Privacy Management automates private data reporting to improve accuracy, reduce audit time and accelerate initiatives across the organization. It enables model builders and data scientists to maintain trust in compliance efforts relative to specific regulatory frameworks.

This module will give users a unified view of all of the private data assets being stored across their organization, and it will enable users to run privacy assessments and reporting on them. To assist with this, OpenPages has built an integration with IBM Watson Knowledge Catalog, a cloud-based data catalog and data governance platform, to enable the loading of asset metadata into OpenPages. Working together, both products cover the spectrum of discovery and usage scanning to identify sensitive and private data. Users can also manage private data to build AI models without sacrificing privacy compliance.

Ultimately, OpenPages Data Privacy Management brings a compliance focus to data governance, helping organizations take a proactive approach to risk and privacy by embedding GRC management across all teams.



OpenPages Data Privacy Management provides a configurable and customizable solution with key features that include:

Real-time view of private data
Create and maintain a complete inventory of sensitive or private data across your organization. Integrates with IBM Watson Knowledge Catalog's asset repository to maintain an up-to-date view of data assets using private data.

Privacy assessments
Use the questionnaire assessment feature to build and deploy privacy assessments for all of the relevant jurisdictions where private data resides in your organization.

Workflow management
Conduct automated workflow management of the privacy assessment process for data assets and applications using private data.

Demonstrable compliance
Maintain a record of completed privacy assessments performed on data assets that can be used to demonstrate compliance to auditors.

Issue management
Any issues discovered based on privacy assessment results can be created, logged and assigned to the appropriate stakeholder and linked to appropriate risks and controls.

Why OpenPages with Watson?
IBM OpenPages with Watson transforms the way risk and compliance professionals work. By providing core services and functional components on a scalable platform that spans operational risk, model risk, third party risk, regulatory compliance, IT governance, business continuity, internal audit, policy, data privacy and financial controls management, IBM OpenPages with Watson delivers a holistic view of risk and regulatory responsibilities across the enterprise. IBM OpenPages with Watson merges Watson's AI capabilities and the expertise of our extensive partner network to help risk and compliance professionals make more informed decisions to manage risk and compliance processes. It delivers on the marketplace demand for an integrated end-to-end solution that enables organizations to connect internal GRC policies and practices to the external regulatory environment. To learn more, visit our product page at ibm.com/openpages

For more information
To learn more about IBM OpenPages Data Privacy Management visit: ibm.biz/op-data-privacy

IBM Corporation
Software Group (or appropriate division, or no division)
Route 100
Somers, NY 10589

Produced in the United States of America
Month 2020

1 Technology CEO Council Report, One Trillion Reasons, October 2010 (www.greenbiz.com/research/report/2010/10/25/one-trillion-reasons)

XXXOOO-USEN-01