CORPORATE DATA GOVERNANCE: CHALLENGES & SOLUTION

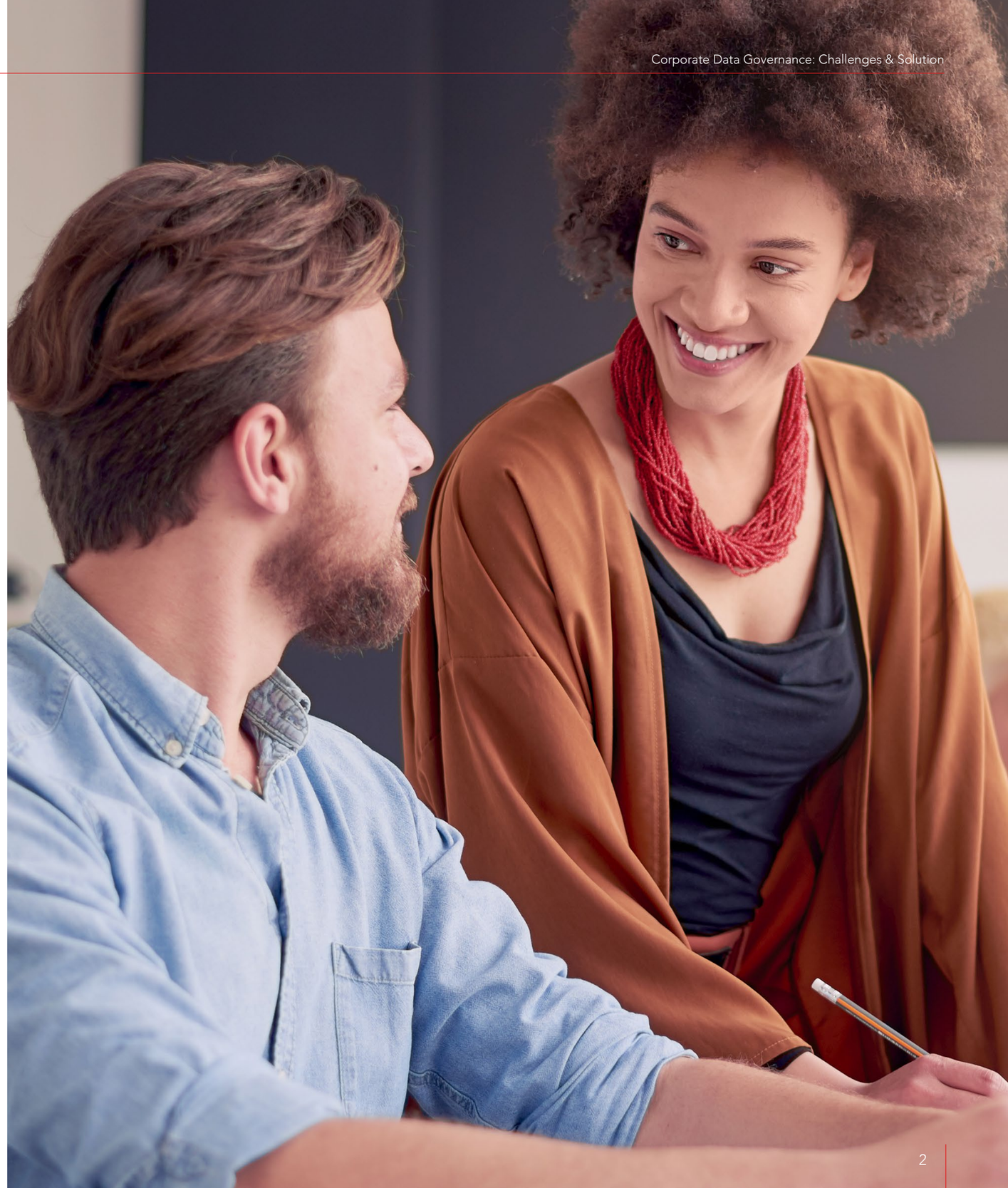
CONTENTS

CORPORATE DATA GOVERNANCE: CHALLENGES & SOLUTION

Within enterprise organizations, millions of electronic messages containing critical business information are exchanged every day. Large volumes of data containing the sensitive personal information of employees and customers are likely being processed and stored as well in various company servers, local computers, and physical media.

Corporate data needs to be managed properly – protected against breaches, monitored for compliance with HR and company policies, and in some cases defensibly retained as evidence for audits, investigations, and litigation. Organizations risk legal, compliance, and security exposure for failing to do so.

In this eBook, we outline the top challenges to corporate data management, and detail how Global Relay's comprehensive data governance solution helps organizations of all sizes, in all industries, effectively address them.



Top Corporate Data Governance Challenges & Risks

TOP CORPORATE DATA GOVERNANCE CHALLENGES & RISKS

Corporate data management is fraught with challenges as many, varied, and interconnected as the types of data and information it seeks to preserve and organize. These challenges include:

HUMAN RESOURCES ISSUES

The U.S. Equal Employment Opportunity Commission estimates there were over 67,000 charges of workplace discrimination in the U.S. in 2020.[1] As well, the Center for American Progress reports that U.S. companies spend $64 billion annually to replace workers who quit their jobs due to bullying, discrimination, and other forms of mistreatment.[2]

The #MeToo movement has only increased awareness of sexual harassment and violence perpetrated against women in the workplace. A survey conducted for the Fondation Jean-Jaures and the Foundation for European Progressive Studies found that six out of every 10 women in the European Union have experienced sexism, harassment, or sexual violence at work.[3]

Racial issues worldwide, recently highlighted by the Black Lives Matter movement, are expected to shine a similar spotlight on racial discrimination within organizations.

HR teams face an enormous challenge uncovering incidents that take place on communication and collaboration platforms due to the sheer volume of messages exchanged every day, and the diversity of the platforms that employees use.

To complicate matters, many of the platforms lack an adequate message retention mechanism, and allow users to edit or delete messages at will. Consequently, it is almost impossible to retrieve and review information – and piece together events – accurately and on time.

It is important for organizations to retain all their employee communications, monitor them for compliance with internal rules, and address violations swiftly. This is a costly, complex, and painstaking undertaking, but companies similarly pay a steep price for failing to perform it.

INSIDER THREATS

Insider threats coming from current and former employees, contractors, and business associates pose some of the greatest risks to organizations. Based on responses from numerous companies it surveyed, Crowd Research Partners lists in descending order data most vulnerable to insider attacks as follows:

- **Confidential business information** (financials, customer data, employee data)
- **Privileged account information** (credentials and passwords)
- **Sensitive personal information** (Personal/Protected Health Information)
- **Intellectual property** (trade secrets, research product designs)
- **Employee data** (Human Resources)
- **Operational/Infrastructure data** (network, infrastructure controls)[4]

[1] Charge Statistics: FY 1997 through FY 2020, U.S. Equal Employment Opportunity Commission

[2] The Costly Business of Discrimination, The Center for American Progress

[3] European Observatory on Sexism & Sexual Harassment at Work, a survey conducted by Ifop for Fondation Jean Jaurès and FEPS using a self-administered online questionnaire from April 11-15, 2019 among a sample of 5,026 females aged from 18 years old and over and resident of Italy, Spain, France, Germany, and the United Kingdom.

[4] Insider Threat: 2018 Report, Crowd Research Partners

HR teams face an enormous challenge uncovering incidents due to the sheer volume of messages exchanged every day – and the diversity of communication and collaboration platforms that employees use.

Organizations need to be able to efficiently monitor employee conduct and business activity across communication platforms – and to swiftly detect and address suspicious behavior.

The Ponemon Institute reports that the average annual cost of insider threats jumped from $8.76 million in 2018 to $11.45 million in 2020 (31%). During this same two-year period, the number of incidents also rose from 3,200 to 4,716 (47%).[5]

To understand insider threats better, a couple of things are worth noting. Incidents are not always due to employees acting with deliberate or malicious intent. In fact, almost two-thirds of the cases are the result of simple employee or contractor negligence.

Communication and collaboration platforms have also made it easier to share sensitive corporate data accidentally with people who shouldn't have access to it, and to steal intellectual property and trade secrets for financial gain. Forty-two per cent of the companies that had experienced an IP leak in the past two years reported it involved trade secrets.[6]

'Flight risk' employees typically are dissatisfied individuals searching for a new job, who may take proprietary company information with them when they depart. Recently, an ex-engineer for Google's self-driving car received an 18-month jail sentence and a $179-million fine for stealing thousands of Google files before leaving Google to lead Uber's robocar project.[7]

The quicker an organization is able to detect and act on a threat, the better. The Ponemon Institute found that incidents that took over 90 days to contain ended up costing $13.71 million (annualized), compared to $7.12 million for those thwarted within 30 days.[8]

The message is clear: It is essential for organizations to monitor employee conduct and business activity efficiently across communication platforms, and to swiftly detect and address suspicious behavior before it creates any lasting damage.

EDISCOVERY & LEGAL HOLD

When organizations are involved in audits, investigations, and litigation, they typically have to produce evidentiary records to prove their case and protect their business.

Recently, the Delaware federal court slapped a U.S. communications equipment manufacturer with a $3-million sanction after one of its high-level executives deleted more than 40% of his emails following his company's receipt of a notice of an antitrust suit.[9]

The case provides a stern warning not to destroy potentially responsive electronically stored information (ESI), but it also underscores the need for:

- A centralized, tamperproof archive that enables companies to effectively supervise all their electronic communications, and securely and defensibly preserve those that serve a legal, regulatory, or business need.

- An eDiscovery solution that allows for efficient data search, case management, and legal hold placement, as well as rapid data production for information requests and legal proceedings.

Many companies continue to store their data in multiple data silos and fragmented backup systems. Not only does this present search, supervision, and retrieval challenges, but it also poses legal and security risks, particularly when data is lost, tampered with, or shared without authorization.

Companies also rely on the retention function of the collaboration platforms they are using, which may not meet regulatory standards. Using Slack's retention tool, for example, will not adequately shelter legal holds, and can increase the disclosure burden for companies if it retains their data longer than necessary.

Once again, these instances underline the essentiality of a centralized, tamperproof archive, where data can be securely retained, supervised, accessed, and retrieved from for various purposes.

[5] 2020 Cost of Insider Threats Global Report, The Ponemon Institute

[6] 2019 Intangible Assets Financial Statement Impact Comparison Report, The Ponemon Institute

[7] Anthony Levandowski: Ex-Google Engineer Sentenced for Theft, BBC News

[8] Cost of Insider Threats, Ponemon

[9] $3 Million Spoliation Sanction Despite Company's Litigation Hold, The National Law Review

DATA PRIVACY RISKS

Privacy regulations aim to strengthen the protection of personal data, and give individuals greater control over the use of their personal information. Recent regulations such as the GDPR and CCPA are putting pressure on companies to enforce stricter personal data processing, storing, and handling policies.

The GDPR and CCPA have many similarities, including their disclosure requirements, exceptions, and private rights of action.[10] Among these requirements is the 'right to be forgotten,' which grants data subjects the right to request companies holding their personal data to delete it.

Under the GDPR, a non-compliance penalty may be up to the higher of €20,000,000 or 4% of a company's worldwide annual revenue. CCPA imposes a maximum fine of $7,500 and $2,500 per intentional and unintentional violation, respectively. With no ceiling on the number of CCPA violations, however, CCPA fines can quickly add up and outweigh those of the GDPR.[11]

According to a DLA Piper report, $193.4 million in GDPR-related fines was issued in 2020. Since GDPR came into effect in May 2018, there have been more than 281,000 data breach notifications, with total reported fines reaching $332 million.[12] (No CCPA data is available yet.)

Non-GDPR/CCPA-related cases further illustrate efforts to crack down on personal data mishandling. In the UK, the Information Commissioner's Office fined British Airways around $230 million for a data breach that affected half a million of its customers.[13] In the U.S., the Federal Trade Commission imposed a staggering $5 billion-penalty for privacy breaches relating to the Cambridge Analytica scandal.[14]

To comply with privacy regulations, organizations must:

- Ensure the security, accuracy, and integrity of personal information in their custody.
- Have retention/deletion policies appropriate to their company and lines of business.
- Be able to find, retrieve, and provide individuals with access to their personal data.

[10] Enforcement is Coming: How CCPA Fines Compare to GDPR, Riskonnect

[11] Ibid.

[12] GDPR: Fines Increased by 40% Last Year, and They're About to Get a Lot Bigger by Daphne Leprince-Ringuet, ZDNet

[13] British Airways Faces Record $230 Million Fine Over Data Theft by Paul Sandle, Reuters

[14] FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, The Federal Trade Commission

Recent regulations such as the GDPR and CCPA are putting pressure on companies to enforce stricter personal data processing, storing, and handling policies, or face hefty penalties.

A Comprehensive Corporate Data Governance Solution

A COMPREHENSIVE CORPORATE DATA GOVERNANCE SOLUTION

Global Relay helps organizations across industries preserve, supervise, and gain critical business intelligence from their communications data – all while meeting their data privacy, security, search, and retrieval requirements.

Global Relay Archive, the company's industry-leading data governance solution, offers a comprehensive suite of tools that address regulatory requirements and the demands of Big Data and today's collaboration platforms.

SECURE & UNIFIED ARCHIVING

No matter an organization's volume and variety of data, Global Relay Archive can support it. Global Relay Archive preserves over 100 data types, including email, IM, text, social media, and enterprise collaboration. Capable of supporting over 400,000 users in a single repository, the platform dynamically scales for growing user counts and data volumes.

Global Relay Archive captures and preserves all company data (including metadata and other related information) in a secure, unified cloud. As an organization's single source of truth for all its business communications, it creates a permanent, tamperproof 'gold' copy of every message, which can be easily searched for and retrieved – even if the original has been deleted.

By eliminating dependency on multiple, fragmented storage systems, Global Relay Archive ensures consistent search results for the purpose of eDiscovery, case management, legal hold placement, and records production. Role-based controls provide users with the appropriate level of access to company data.

Global Relay Archive preserves communications data for the entire length of an organization's specified retention period. This ensures data is not retained longer than necessary, which could put businesses at risk of regulatory breaches or increase their disclosure burden during litigation.

Data stored in Global Relay Archive cannot be deleted before the expiry of its retention term or, in the case of data that could serve as evidence, if it is subject to a legal hold.

POLICY-BASED SUPERVISION

Through policy-based supervision, Global Relay Archive enables HR, compliance, and legal teams to monitor and ensure that employee communications comply with company rules.

Policies are criteria used to flag content – for example, lexicon (keywords and phrases), metadata (sender, recipient, data type), and other operators (exact phrase, word proximity). Global Relay Archive scans every company communication against configured policies, automatically flagging content if there is a match.

For a more detailed evaluation of employee conduct and business activity, Global Relay Archive offers analytics and data visualization.

Analytics empowers users to drill down to relevant communications, examine them within their original contexts, and discover the broader story behind a communication. Analytics can expose 'inside conversations' and anomalies within a message that are often hard to detect.

Data visualization provides valuable supplemental data, such as the top message senders/recipients, communication channels used, and (conversation) topic trends, using diagrams, graphs, and charts.

Global Relay helps organizations preserve, supervise, and gain critical business intelligence from their communications data – all while meeting their data privacy, security, search, and retrieval requirements.

EDISCOVERY & LEGAL HOLD

Global Relay Archive streamlines the eDiscovery and legal hold process by serving as an organization's single source of truth for all its communications data. The 'gold data' set stored in Global Relay Archive is litigation-ready and available for eDiscovery at all times.

With up to 1,000x the speed of competitive systems, Global Relay Archive enables Legal and eDiscovery teams to search across petabytes of data in a matter of seconds (not hours or days) to find that 'needle in a haystack.' AI/Machine Learning capabilities further accelerate searches by recognizing persistent user commands and recurring search patterns to identify data of potential interest.

Global Relay Archive's case management tools allow Legal and eDiscovery staff to segregate, classify, and collaboratively review data. Cases, folders, and tags simplify data organization and prevent important information from getting lost in the noise.

Organizations need to preserve potentially responsive data when they anticipate litigation. Failure to do so can result in hefty fines and a weaker defense. With Global Relay Archive, authorized users can systematically place defensible legal holds on data – no IT assistance or third-party products required.

Holds override corporate retention schedules applicable to the data, protecting it (and all related information) from automatic or manual deletion. Once a legal hold is in place, all currently archived and incoming data meeting the hold criteria is dynamically tagged for preservation. Data placed on hold can't be deleted until an authorized user releases the hold.

By managing all legal holds 'in-place' (within Global Relay Archive), organizations do not have to transfer data between different systems and devices, and can preserve a clean chain of custody.

DATA PRIVACY PROTECTION

Global Relay Archive can help organizations meet their personal data protection requirements under the GDPR and various other privacy laws. Proprietary features that make Global Relay Archive particularly well suited for this purpose include:

- Advanced search and analytics to identify and retrieve communications related to a data subject;
- Case management tools to organize, review, and produce communications related to a data subject;
- Retention, legal hold, and disposition tools to defensibly preserve and delete personal data;
- Role-based access controls to enforce least-privilege and need-to-know policies;
- Unified storage and management of all corporate communications; and
- Professional services to assist with specific requests (e.g. an access request).

Global Relay Archive enables authorized users to systematically place defensible legal holds on potentially responsive data – no IT assistance or third-party products required.

LOOKING FOR A COMPREHENSIVE AND DEPENDABLE CORPORATE DATA GOVERNANCE & MESSAGING SOLUTION?

Global Relay provides cloud-based archiving, information governance, surveillance, eDiscovery, and messaging solutions to over 20,000 organizations in financial services, energy, government, healthcare, retail, media, and more. Global Relay enables you to manage, control, and profit from your electronic communications data.

CONNECT
Connect your electronic communications, voice, social media, trade, and legacy data, and deliver it to your Global Relay Archive or wherever you need it.

COLLABORATE
Chat compliantly with your customers, colleagues, and industry peers via text, voice, WhatsApp, video, or instant message.

Available on iOS, Android, and desktop.

DISCOVER
Enrich, store, manage, and discover your data – all in one system.

- Compliant storage
- Dynamic policies
- Team workspaces
- Real-time AI
- Custom workflows
- Collaboration tools

For more information or a free consultation
email info@globalrelay.net or call 866.484.6630 (North America)
or +44 (0)20 3206 1850 (Europe) today.

For all the latest news, events, and product developments at Global Relay, sign up for our newsletter at **www.globalrelay.com/newsletter**

globalRELAY®

globalrelay.com info@globalrelay.net North America: 866 484 6630 Europe: +44 (0) 203 206 1850

new york chicago vancouver london