DATA PRIVACY REGULATIONS IN TRANSITION:

ADOPTING A REPEATABLE FRAMEWORK THAT PROTECTS CUSTOMER DATA

Taking an integrated approach to managing customer privacy and complying with privacy regulations can enable companies to rapidly adapt to business, regulatory and technological changes. Having an integrated privacy approach reduces data management and privacy costs and identifies more value in the data by utilizing better data management practices.

A WHITE PAPER FROM

asg technologies®

HMG STRATEGY
Largest Leading Independent Executive Community

EXECUTIVE SUMMARY

The continued escalation of consumer privacy regulations and compliance requirements facing companies is generating heightened focus and concerns among executives.

Data from more than 380,000 customer transactions on the British Airways website were compromised by hackers between late August and early September 2018. Experts have concluded that if the airline didn't do enough to protect consumer information under the rules of the General Protection Data Regulation (GDPR), British Airways could face a fine of more than $639 million, representing up to 4% of its annual revenue. This threat of punitive GDPR fines and penalties is weighing on executives at publicly-held companies, according to multiple studies.

Meanwhile, pressure continues to mount for federal lawmakers in the U.S. to adopt similar consumer privacy protection legislation, as other countries such as China and Brazil have passed consumer privacy laws to simplify organizational adherence to consumer privacy.

The stakes for publicly-held companies – customer and revenue growth, market cap and reputational integrity - are higher than ever. Consumers are aware of the value of their data and fully expect companies to manage and protect their data successfully and ethically.

As the volume of data generated by companies continues to surge, it's evident that companies need a more thorough and integrated approach to data privacy management to retain customer trust and comply with regulations. This helps explain why **35% of U.S. CIOs say their organizations plan to increase investments for both data governance and data provenance in 2019**, according to 'The 2018 ASG CIO Report: The Future of Enterprise Data: Democratized and Optimized.'

To reinforce customer trust, companies need to focus on improving the quality of their data along with better data governance practices. "There's a massive amount of data debt that's costing companies in terms of data integrity and inefficiencies," said Sue Laine, Vice President of Strategic Technologies at ASG Technologies. "Successful data privacy requires effective data management – including data integrity and data governance.

Successful data privacy requires effective data management practices – including data integrity and data governance. Solid data privacy practices can be a competitive differentiator that can enable a company to monetize data in different parts of the organization and to become nimbler with decision-making and business practices.

Sue Laine, Vice President of Strategic Technologies at ASG Technologies

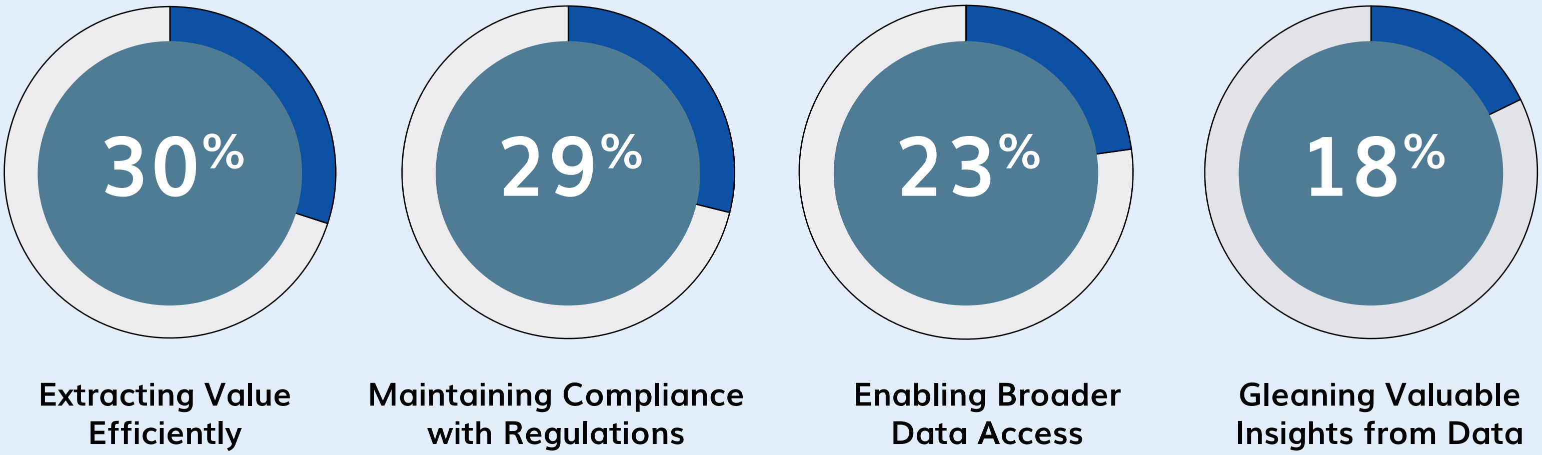
Solid data privacy practices can be a competitive differentiator that can enable a company to monetize data in different parts of the organization and to become nimbler with decision-making and business practices."

In this white paper by **ASG Technologies and HMG Strategy**, you will discover:

- The factors and trends that are shaping consumer privacy protection
- The business and operational benefits of applying an integrated approach to protecting customer data
- Recommendations for decision-makers to become ethical data stewards to strengthen customer trust
- Examples of leading brands that are succeeding with privacy management and how it is enhancing their businesses
- The cost-benefits of establishing a comprehensive data privacy framework

Chart 1: The Top Data Management Challenges Faced by CIOs

ASG ASKED OVER 200 CIOS TO NAME THE TOP DATA MANAGEMENT CHALLENGES THEY FACE



Source: The 2018 ASG CIO Report, 200 CIOs from large U.S.-based organizations across several industries

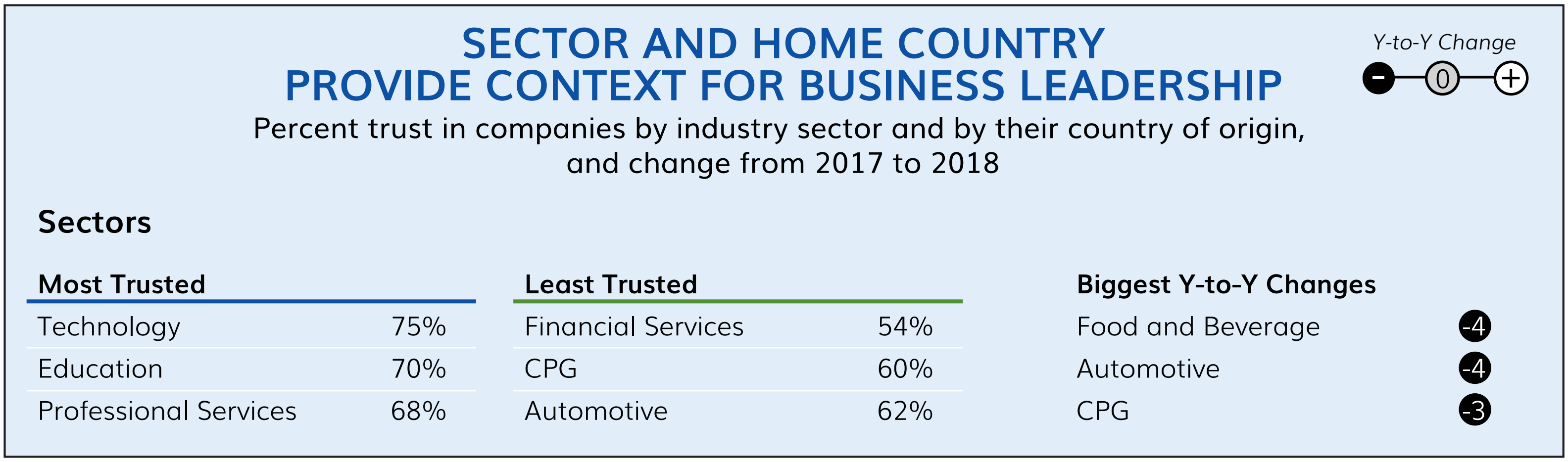
THE BUSINESS BENEFITS OF PROTECTING CUSTOMER DATA

The more data a company has regarding its customers, including their behaviors, preferences, interests and lifestyle changes, the better it can be at catering to those interests and deepening engagement. Protecting this data needs to be a top priority for any organization for a range of financial, operational, reputational and relationship-driven reasons. The task of protecting the brand's reputation among existing and prospective customers is critical.

Customer data – and its protection – can also provide companies with a competitive edge. Personal data that a company has collected on its customers can enable it to create personalized offers and understand its customers' behaviors and preferences better than its competitors.

Without question, the foundational element that unites the business opportunities for protecting customer data with data from employees, suppliers and partners is trust. When a customer trusts how a company manages and uses their data, this strengthens the bond between the customer and the company. It also increases customer loyalty along with the customer's willingness to spend more with that company.

Fostering customer trust is more challenging than ever. Consider the following data points from the 2018 Edelman Trust Barometer:



SECTOR AND HOME COUNTRY PROVIDE CONTEXT FOR BUSINESS LEADERSHIP

Percent trust in companies by industry sector and by their country of origin, and change from 2017 to 2018

Y-to-Y Change

− 0 +

Sectors

Most Trusted		Least Trusted		Biggest Y-to-Y Changes	
Technology	75%	Financial Services	54%	Food and Beverage	-4
Education	70%	CPG	60%	Automotive	-4
Professional Services	68%	Automotive	62%	CPG	-3

While many executives view compliance with the GDPR and other privacy regulations as a burden, research reveals that there are multiple benefits that companies can obtain through more transparent and compliant customer relationships. The top business outcomes for companies that provide clear and understandable GDPR compliance practices are **improved customer satisfaction (35%), increased customer loyalty (34%) and deeper customer engagement (33%),** according to a Forrester Consulting study of 263 data and compliance decision-makers whose companies either operate or do business in Europe.

Applying an integrated approach to safeguarding customer data, in order to comply with a slew of regulations, can also provide numerous operational benefits to organizations. These include the advantages of taking a holistic approach to data integrity and regulatory compliance to streamline operations between organizational functions and in tackling various regulatory requirements. An integrated approach can enable companies to de-duplicate private data and ensure that all data is accurate, while being used with the customer's consent.

"Foundationally, it's important to govern the data that you have and ensure that the controls are in place to effectively protect customer information," said Sam Yoo, Sales – Data Governance at ASG Technologies.

The Cost Benefits of Creating a Far-Reaching Data Privacy Framework

Building a cross-enterprise data privacy template offers companies multiple cost benefits. These include the ability to quickly and cost effectively develop 'what-if' scenarios for addressing new privacy regulations. Creating a data privacy framework can also allow decision-makers to remove unnecessary or inappropriate processes and focus data investments on delivering improved returns for future use cases.

One of the most significant advantages to developing a comprehensive data privacy framework is that it can dramatically consolidate the amount of time and effort that goes into addressing a regulatory audit. "Companies

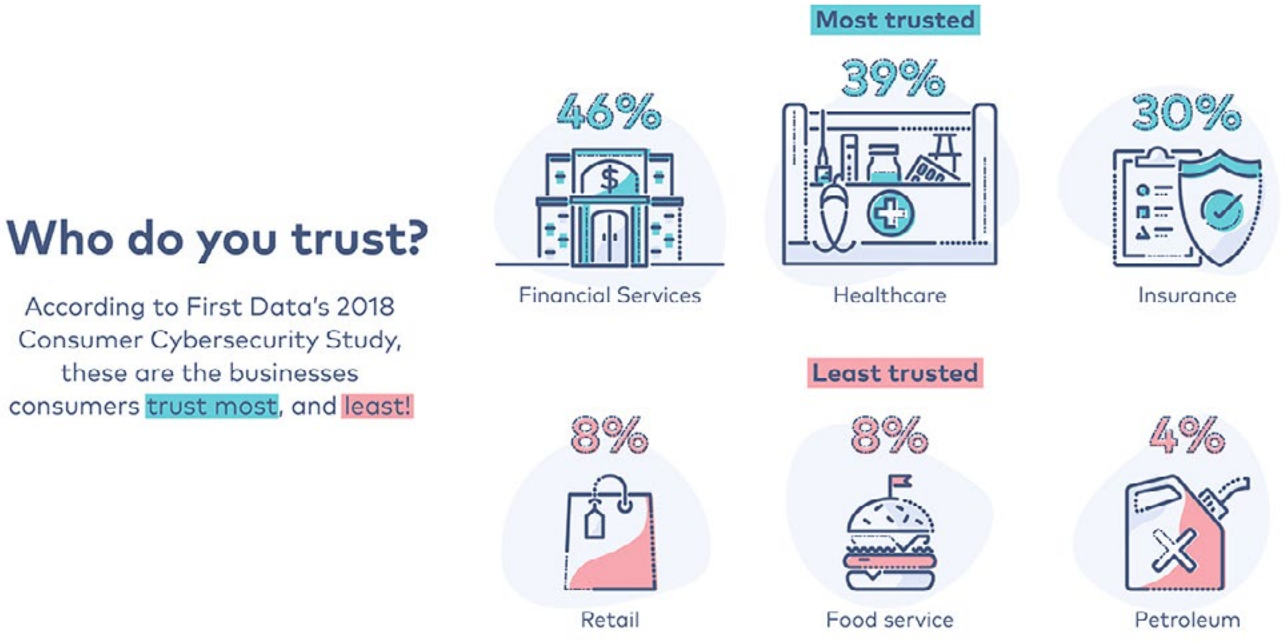
Foundationally, it's important to govern the data that you have and ensure that the controls are in place to effectively protect customer information.

Sam Yoo, Sales – Data Governance, ASG Technologies

benefit from having a template for responding to an audit," said Laine. "Instead of hiring dozens of consultants to map out how to access data, a data privacy framework can allow you to respond more cost-effectively and reliably with automation."

Having accurate and consistent customer data can go a long way towards enabling companies to remain connected with customers on their needs and interests while staying a step ahead of regulatory compliance requirements. In the next section of the white paper, we'll examine why it's so important for companies to be ethical stewards of customer data along with recommendations for delivering on these expectations.

Chart 2: Industries That Consumers Trust Most – and Least
A recent study finds that even the most trusted industries are trusted by fewer than half of their customers.



Source: 2018 Consumer Cybersecurity Study, First Data

BECOMING AN ETHICAL STEWARD OF CUSTOMER DATA

According to BCG, only 20% of consumers say that they trust companies to 'do the right thing' with their personal data, while more than half of respondents believe that companies aren't honest about their data use. This poses a major problem for companies as this level of mistrust can damage a brand's reputation and prompt existing and prospective customers to do business with companies they deem to be more trustworthy.

Under the principles of the GDPR and other consumer data protection regulations, the requirement for companies to practice ethical data management extends beyond brand reputation and profitability. For instance, Recital 4 of the GDPR states "The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."

These are just some of the reasons why it's useful for companies to assign and empower people who can serve as "data stewards". A data steward manages and governs data used throughout the organization. They know how data is collected, how it's being used and are involved in overseeing data policies, data usage and administering the use of data in meeting regulatory requirements.

Prior to selecting and assigning data stewards, obtaining executive commitment to data privacy initiatives is critical. Obtaining this commitment from across the C-suite and business lines can help demonstrate that your company is committed to customer data privacy – including how it supports the operational strategy of the organization.

Executive sponsorship can also aid in obtaining the cultural transformation that's needed for data privacy initiatives to succeed over the long term. This represents a major cultural shift for most companies as few companies are highly transparent about how they use customer data – having executive sponsorship is an important step in setting this transparency.

After acquiring executive sponsorship, data stewards can help create a set of practices which promote collaboration and involvement with key stakeholders. This includes engaging line-of-business leaders for establishing data privacy policies and taking ownership of data assets within their areas of control, as well as the processes used to manage data in those domains. Data 'owners' can also be given the responsibility and authority to ensure that data privacy processes have been established, implemented and maintained. This dovetails with one of the key concepts incorporated into the GDPR - 'Privacy by Design' - whereby companies are now obligated to take a consumer's data privacy into account during the design stages of all projects that utilize customer data.

As the primary responsibility for data privacy falls with the Data Protection Officer (DPO), it makes sense for data stewards to be part of the data protection team and either report to the DPO or have a dotted line connection.

As companies increasingly apply artificial intelligence and machine learning to automate customer-facing processes, data stewards are becoming a vital human element in algorithmic data execution. As part of these efforts, it also becomes incumbent upon data stewards to oversee and execute on ethics guidelines for the trustworthy application of AI.

"There should be a human checkpoint on the algorithms and outcomes that are being generated," said Laine. Additionally, as organizations continue to apply machine learning and cognitive computing to automating business activities, "a data steward can determine whether the data being applied is being used ethically," said Yoo.

Because most line-of-business leaders lack expertise in data management, oversight of data privacy governance should be established through the use of a matrixed organization where ownership is led by business stakeholders. The execution of data management in areas such as data stewardship and distribution should be managed by the IT organization.

Today's savvy customer understands they "own" their data. Coordinating customer feedback groups can help to inform customers how their data is being collected and used and to obtain their reactions in helping to shape privacy policies going forward.

For instance, as BCG reports, Uber took steps to better manage its customer data after it was revealed that Uber employees were able to access customer data and track customers' locations and that the data

There should be a human checkpoint on the algorithms and outcomes that are being generated.

Sue Laine, Vice President of Strategic Technologies at ASG Technologies

was being used for purposes beyond providing car service. To prevent the misuse of customer data in the future, Uber encrypted and password-protected its customer location data. The company also restricted access to customer location data to a small number of employees for legitimate business purposes.

Embedding data privacy policies throughout the enterprise, clearly communicating to employees and other stakeholders the rationale for doing so and making data practices transparent both to customers and regulators is key to successful data stewardship. Regularly measuring and publishing statistics on customer trust with the company's data privacy policies can demonstrate the progress a company is making with its customer data privacy policies while helping to strengthen its reputation in the market and serve as a competitive differentiator.

In the next section of the white paper, we'll explore how one ASG Technologies client – American Fidelity Assurance – has been able to transform its data assets into tangible business value while protecting personal data.

Case Study: Leveraging Data Assets at American Fidelity Assurance

Source: https://content.asg.com/MarketingCollateral/DataIntelligence/Casestudy_AmericanFidelity_Short_EN.pdf

The Challenge:
American Fidelity Assurance Company, founded in 1960, knew they had to become data-centric to be competitive. As a supplemental benefits provider, they serve more than one million customers and are constantly collecting data.

American Fidelity's goal is to provide the most value-added service possible. To do that requires knowing who the customers are, both internally and externally, and knowing what the customers want and need. Data is the best way to get there at scale.

The Approach:
American Fidelity turned to ASG's Enterprise Data Intelligence, the only solution that could work across all the lines of business, departmental systems and environments that the insurer had accumulated over six decades. Working together, they established five critical objectives to ensure success: increase visibility into systems, eliminate redundancy, demonstrate data value, facilitate collaboration and use data to drive success.

Enterprise Data Intelligence provided American Fidelity with a tool-agnostic approach with numerous unique differentiators. Now they had enterprise-wide data lineage insight with coverage of very many data sources. They could perform macroanalysis of data lineage between different data stores and microanalysis of data lineage within the source code. With logical configuration, scheduling and management they were able to see and use their data like never before.

The Results:
ASG Enterprise Data Intelligence quickly revealed that they had more than a dozen different environments, many of which had artifacts that were not known elements and others that had not been retired or fully archived.

The visibility helped to quickly identify both missing modules and redundancies - in one case 464 instances of a single field in 50 different tables and views were reduced to 12. This helped to provide a single, standardized structure to accurately track usage.

Reducing the volume of duplicate data across the network and making the data more traceable across data sources saves ASG customers money in terms of storage costs and backup speeds and enables customers to better manage and protect customer data for improved data privacy.

Data Intelligence programs often drive rapid growth in "Data Literacy" – the key enabler of digital business which is vital for an understanding of Data Privacy. As an example, from just a few data experts, AFA has built a population of 75, including 35 'data navigators' (BI and analytics business users). These experts have built a knowledge base that greatly reduces the risk of Data Privacy failures and makes data more trusted and usable for insight and decision making benefiting the organization.

NEXT STEPS

"A good starting point for moving forward with your data privacy strategy is by first identifying the maturity of your organization's data management practices. By doing so, you can gain insights into your organization's current state and steps that need to be taken to advance to the next level," said Laine.

As we mentioned earlier, data privacy should be a collaborative effort – starting with tight partnerships between the IT organization and the lines of business. "There's so much segregation of data between organizational functions (sales, marketing, customer service) and business units that executives don't know what kind of data is available that can be used to gain a deeper understanding of customers and to strengthen customer relationships," said Laine. "Collaboration should also include other key stakeholders who can help guide data privacy and regulatory compliance efforts, such as the general counsel and the Chief Ethics and Chief Risk Officers for those organizations that have those roles in place. Their involvement can help shape the cultural changes that are needed to foster data privacy efforts across the organization," said Yoo.

From there, once the organization has robust data governance and automation capabilities in place, this will help to simplify data privacy efforts and to make these processes repeatable and scalable.

Said Laine, "Without a methodical approach like this, it's chaos."

ABOUT ASG TECHNOLOGIES AND HMG STRATEGY

ASG Technologies is an award-winning, industry-recognized and analyst-verified global software company providing the only integrated platform and flexible enterprise-wide solution for the information-powered enterprise. ASG's Information Management solutions capture, manage, govern and enable companies to understand and support all types of information assets (structured and unstructured) and stay compliant. ASG's IT Systems Management solutions ensure that the systems and infrastructure supporting that information lifecycle are always available and performing as expected. ASG has over 3,000 customers worldwide in top vertical markets including Financial Services, Healthcare, Insurance and Government. Visit us at ASG.com, LinkedIn, Twitter and Facebook.

HMG Strategy is the world's largest independent and most trusted provider of executive networking events and thought leadership to support the 360-degree needs of technology leaders. Our regional CIO and CISO Executive Leadership Series, newsletters, authored books, and digital Resource Center deliver proprietary research on leadership, innovation, transformation, and career ascent.

The HMG Strategy global network consists of more than 300,000 senior IT executives, industry experts and world-class thought leaders.

To learn more about the 7 Pillars of Trust to HMG Strategy's unique business model, click here.