SUPERCHARGING HR DATA MANAGEMENT
FROM REGULATORY REQUISITES TO STRATEGIC OPPORTUNITY

accenture
Human resources (HR) functions in financial services (FS) organizations have historically under-invested in their data capabilities and infrastructure. The result? Many of them are not driving the full value they could from their vast reservoirs of data. Perhaps even more importantly, they are not well prepared for the ever-stricter data privacy regulations and growing cyber-security risks they face as stewards of some of the organization’s most sensitive information.

This paper explores the challenges HR faces around improving data quality, integration and governance; why data is ultimately a people and business concern rather than a technology issue; HR’s role in creating a cyber-secure workforce; and how new data privacy regulations are turning data protection into an imperative for FS HR functions.
PREPARING HR FOR A DATA-DRIVEN FUTURE

Marketing, sales and other enterprise functions in FS organizations understand that data drives the digital economy. HR, too, is looking for ways to leverage this valuable resource to enhance business performance, optimize workforce costs, improve employee engagement through personalization of the workplace experience, and unlock the potential of tomorrow’s adaptive workforce.

Some leading FS organizations are already seeing impressive returns on their investments in using HR data and advanced people analytics to drive better decision-making and workforce performance. For example:

- Accenture is working with an Asian life insurance firm that harnessed analytics insights to reduce attrition among managers by 50 percent in six months.

- A global asset management firm—an Accenture client—boosted the productivity of its operational workforce by 25 percent by benchmarking internal and external productivity, analyzing service maturity and cost to serve, modelling an improved distribution of workload, and identifying productivity-boosting factors.

However, data analytics and digital HR platforms are only as good as the data that feeds them, and all too many HR functions in FS have not historically treated data quality, ingestion, integration and governance as a priority. As a result, HR lags other corporate functions in its ability to drive value from data and lacks confidence in the accuracy and relevance of its analytics insights.

Much of the data HR collects continues to be used primarily for retrospective, operational purposes, or simply remains fallow. Just 8 percent of senior HR leaders believe they are using HR data in an effective manner that generates material returns.

Some reasons that HR functions in FS organizations are not yet getting the optimal value from data and analytics include:

- HR departments have not invested aggressively enough in their data skills, capabilities and governance structures.

- HR IT landscapes are often complex due to a lack of investment, legacy systems, and organic growth without long term strategic planning. Therefore, data is scattered across fragmented business systems and processes. Quality is inconsistent, compatibility is limited, and access is hampered.

- HR often sees data management as an IT issue rather than a business concern and does not assume sufficient accountability for its data.

- Some organizations lack the basics of data hygiene—for example, consistent definitions of data entities such as a full-time employee versus a contractor or part-time worker across all countries and business units.

As FS HR functions strive to become more data-driven they will encounter significant data quality and integration challenges in every HR activity and process. Taking accountability for data will empower HR to drive more accurate insights from analytics, reduce operational errors and increase confidence in its service among employees and the business.
DIGITAL TRUST AND DATA PRIVACY
MOVE UP THE AGENDA

Sound data quality, processes, systems, controls and governance are not only key to releasing the trapped value in HR data. They are also central in managing the reputational and regulatory risks attached to managing personal workforce data in a world where employees, regulators and other interested parties have put digital trust and data privacy firmly on the agenda.

HR manages an array of sensitive data such as employees’ national identification numbers, social security numbers, bank account details, addresses, salaries, disciplinary histories, and family details. A data breach could harm the employer brand, undermine trust in the HR function and its data among employees and business leaders, and open the organization to sanctions from regulators.

Three out of four employees say they would not trust their company again if their information was leaked. What’s more, countries worldwide are enshrining data privacy rights for employees in stringent data protection laws and regulations such as Europe’s General Data Protection Regulation (GDPR).

GDPR raises the stakes

The GDPR, which came into effect on 25 May 2018, prescribes the data rights of European citizens such as the right to be forgotten and a requirement for unambiguous consent for their data to be used. It covers employee and customer data alike. The GDPR affects all firms, employers and vendors who are based in or operate across Europe, or who store or share European citizens’ data, regardless of where this data is processed.

Those who fail to comply face fines of up to the greater of €20 million (US$24.5 million) or 4 percent of annual worldwide turnover. If a company does not report the scale and impact of a data breach within 72 hours, it can be prevented from processing personal data under the GDPR, effectively shutting down the business.

The HR function should not regard regulations such as the GDPR as a burden, but as a stimulus to grow the strategic value of its data. Accenture sees several opportunities for HR in complying with stricter data privacy laws and regulations, including:

- Raising the quality and value of HR data, in turn delivering more accurate insights and fewer operational errors.
- Reducing the effort of reconciling and manipulating data.
- Winning the trust of the C-suite by demonstrating the material benefits of using HR data and analytics for human capital management.
- Leveraging analytics to enhance workforce performance and enable forward-looking insights that inform leadership decision-making.
- Building a well-informed, cyber-secure workforce, in turn reducing the risk of a data breach and ensuring the organization can respond quickly to a breach.
- Preparing for the future by putting in place the right protocols and processes to support a digital, data-driven business.
GDPR is just the beginning of a worldwide shift to tighter regulation of how organizations manage and protect the personal data they gather. China, for example, has issued the Personal Information Security Specification effective 1 May 2018. This framework, which aims to regulate the use of “personal information” by data controllers, is largely aligned to the strict conceptualizations under the EU’s GDPR.

It is expected that China will introduce a more comprehensive Personal Information Protection Law within the next two to five years. Other examples of countries that are tightening “personal data” privacy laws and regulations include New Zealand with its new Privacy Bill and South Africa with the Protection of Personal Information Act.

The landscape is also changing in the US, where government traditionally allowed the private sector to lead the way in data protection and relied on a combination of self-regulation and legislation rather than on government oversight alone. Look at California, which may place a Consumer Right to Privacy Act initiative on the November 2018 ballot. If it passes, it will bring more onerous data protection regulation to the state, including stricter disclosure and opt-out requirements.
HR organizations that start to adapt today to the right behaviors and that implement the right systems and processes for compliance will be better prepared for the stricter data protection laws and regulations likely to emerge in the future.

**Managing the data lifecycle**

To meet the demands and opportunities of regulations such as the GDPR, HR organizations need an approach that covers the acquisition, management, storage, transmission, usage, retention and deletion of information or data from employees, job candidates, former employees and other stakeholders.

HR needs to decide:

- Which data scattered across its fragmented systems it should retain;
- For which purposes it can reasonably and legitimately use this data; and
- Which steps it needs to take to comply with data protection regulations as well as to inspire confidence among its employees and in the wider business.

Under the GDPR, an organization will be held responsible for a data breach or leak whether the fault lies with its own systems and employees or with those of a third-party supplier. HR functions should ensure that any vendor—be it a training company, third-party recruitment firm or a cloud software provider—that will process their candidate or employee data meets the stringent requirements of the GDPR. They should also ensure that everyone who accesses this data has a business need to do so.

This may demand a mindset and cultural change, since HR functions and HR IT departments in FS have often taken a relaxed approach to sharing data, reports and integration with other parts of the business. Data stewards and security teams will need to learn to stop saying yes by default to requests for access to HR data.

HR needs to work closely with IT to understand the data architecture of the organization before it can tighten controls over who can access data, which data they can access and when, and for what purpose they may use it. It needs a clear picture of which external and internal parties access data via integrations or reports, so that it can put a stop to unjustifiable third-party use and storage of data mastered by or sourced from HR.

Compliance is complicated by the fact that not all data is equally sensitive. Some types of data, like medical details, salary information, and whistleblowing cases need to be managed and secured with tighter controls than others. In addition, regulations differ across countries regarding the consent organizations need to collect data, how they may use it and how they should store it. For example, some territories have laws that restrict the movement of personal data outside the country.

---

**SUPERCHARGING HR DATA MANAGEMENT**

59% of senior executives anticipate that the GDPR will have a business impact or even be a global game changer.

£50m Estimated cost for a large company to comply with the GDPR (US$69m).

£1m/year Estimated cost for a large company to maintain compliance with the GDPR (US$1.4m).

45% of companies do not currently have the tools to ensure compliance with the GDPR.

45% of senior executives anticipate that the GDPR will have a business impact or even be a global game changer.
HR AND THE GDPR –
THE COMPLIANCE CHALLENGE

1. GDPR implications for your organization’s talent strategy
   - Data privacy and GDPR talent (high priority)
     Hire and retain data privacy skills.
   - Equip leaders with the right skills (high priority)
     Senior management will need to be aware of the key principles and requirements of GDPR.

2. HR’s role in embedding the principles of GDPR across your organization
   - Data governance (high priority)
     HR needs a clear data management strategy.
   - GDPR requires a mindset change
     Day 1
     On-going awareness campaigns to ensure compliance with GDPR.
     Day 2
     Culture and behavior change interventions to ensure people take responsibility for data handling and help to identify and respond to risks.

3. GDPR requires changes to HR processes, policies and procedures
   - Build a robust data dictionary with data sourced from HR (high priority)
     The data dictionary will be the master record for answering any queries.
   - Next steps (Day 1 and 2)
     Build a master data dictionary encompassing all HR data elements—talent, workforce admin, risk and compliance etc. Identify personal data and sensitive personal data. Identify where, how and with whom these data elements are shared.
     Challenge if sensitive data elements are business-critical for down-stream users. Remediate where necessary.

4. Align with new employee data privacy rights
   - New data subject rights (high priority)
     Realign HR processes with past, present and prospective employees’ new rights with respect to their personal data, such as the right to be informed, portability and objection at any time in the employee lifecycle.
   - New data privacy statement (Day 1)
     Articulate changes to the way your organization uses employee personal data, as well as employees’ new rights in a new data privacy statement.
HR CAN HELP DRIVE BETTER DATA SECURITY ACROSS THE BUSINESS

Not only does the HR function need to sharpen its own ability to manage data (and keep it clean), it should also play an enlarged role in building a cyber-secure workforce ready for the digital future. In so doing, it can help address one of the major challenges an FS business faces as the volume and velocity of data moving through the enterprise grows.

The people in the workforce are, after all, one of the major vulnerabilities in an organization’s defenses against cyber-threats. Employee negligence and misconduct remain among the biggest causes of enterprise data breaches and leaks.

Accenture research shows that half of security violations are caused by human behavior and 93 percent of workers are engaging in at least one form of behavior that puts data security at risk.8

Since HR sets the agenda for workforce planning, learning and development, and organizational change, it is well positioned to help the wider organization to implement appropriate data security policies as well as to embed a cyber-secure culture. What’s more, employees are looking to HR to provide leadership. Three quarters of employees see information security as an HR issue and want their companies to develop better personnel policies to help safeguard private company data.9

In addition to concerning itself with the security behaviors of the workforce, HR needs to regard the vulnerability of its HR systems and data to breaches and leakages as a people risk. Employees expect their personal data to be securely stored and properly managed. Cloud-based solutions and machine learning can support the rollout of comprehensive data protection policies and systems that boost productivity while ensuring sensitive data remains secure.

Three steps to a data-fit HR organization

HR organizations need to look at data protection and cyber-security as important components in their portfolio. Accenture identifies three considerations for FS firms as they seek to optimize the management of their data, while mitigating data protection risks.

1. Get your data under control

• **Engage with IT but take accountability:** The CHRO should engage with the CIO and Chief Data Officer (CDO) to ensure appropriate data management and controls are in place. However, HR should assume accountability for its data rather than continue to treat it as an IT issue.

• **Evaluate how your data is currently managed, stored and provisioned through the organization:** Look at HR data across its lifecycle, including creation, storage, usage, sharing, archiving and destruction. Each stage of the lifecycle carries different risks to be addressed through a combination of policy, people and technology. Whether the organization is retaining data in on-premises HR systems or in the cloud, you should ensure access rights and delegation permissions are appropriate to the role of each employee. When embarking on technology transformation, ensure your data and data management strategy are key considerations in defining the target state.
An FS organization should address inconsistencies in and fragmentation of its HR data before moving onto cloud-based solutions such as Workday, SAP Success Factors or Oracle HCM. It should aim to achieve a consistent data management approach between legacy and target applications before converting legacy HR systems to the new platform. Addressing and improving the quality of HR data in legacy systems can help reduce the time that it takes to move to the cloud.

Since the data models are different and there is limited support for custom data sets in cloud platforms, this is a complex process requiring tough decisions on simplifying the data architecture. This approach can, however, create lasting benefit if data quality levels are maintained after going live on the cloud platform. The solution architecture is key in building a consistent and integrated enterprise systems and data environment.

- **Create a data governance committee:** This body should drive HR data governance standards and tasks for data of varying sensitivity and utility. It should include data owners from HR, key vendors, a data steward in HR who is responsible for the content held within the data, and a data custodian who is responsible for the technical environment and controls around your data.

- **Enhance data management:** Build a data model based on an understanding of the critical data and who owns it. Ensure that your data model is aligned with the information relating to your legal entity, company structure and financial structure. Consider implementing data quality tools to automate the process of improving data quality at source, especially in recruitment and onboarding. One example of such a solution is Accenture’s HR Audit and Compliance tool, which enables users to set up rules to monitor data, use a dashboard to review exceptions, and maintain an audit trail of exceptions.

- **Establish employee and manager ownership of data:** Ensure that the people with the greatest level of interaction with the data are assigned as its owners and define their roles and responsibilities from the outset. Encourage stakeholders to take ownership of their data by implementing self-service tools; for example, managers should have insight into and control over data about their teams, while employees should be able to update their own personal data and the permissions they give their employer to use it.

- **Invest in data skills:** Build data skills and confidence in the HR workforce by upskilling colleagues and hiring data specialists.

2. **Gear up for more regulation**

- **Assess regulations across your markets:** Evaluate your cyber-security and data privacy maturity against the regulatory demands of the jurisdictions in which your
organization operates. In some cases, there may be conflicts or gray areas between the GDPR and local regulations in other markets. These laws and regulations need to be carefully navigated.

- **Ensure the right processes are in place:** Implement data storage policies and processes that take account of the regulations impacting the different types of data your organization holds. Ensure GDPR controls are built into the management of your HR systems; the transfer of data to external suppliers and vendors; and the management of hard- and soft-copy documents.

- **Be transparent:** Be open with your workforce about the type of employee data HR collects and retains. Create policies and controls that allow the business to gather and analyze data to drive better outcomes, while giving due consideration to the need to get consent to collect or use certain data, as well as to employees’ privacy concerns and their rights under laws such as the GDPR.

3. **Build a cyber-secure workforce**

- **Educate the workforce:** To protect the organization and the employee, adopt advanced training methods that raise employee awareness and shift behaviors.

- **Change the culture:** Build a culture of cyber-defense that develops and rewards good habits to ensure your workforce can identify the risks and respond appropriately.

- **Assess cyber-security maturity:** Determine how deeply cyber-safe behaviors and policies are embedded in the firm’s culture. Do leaders and managers know how to nurture cyber-security in their teams and spot unusual behaviors that may indicate an employee who is a malicious actor? Do employees and contingent workers know what to look out for and how to react?

---

**ENTRENCHING SAFE BEHAVIOR**

HR could use innovative learning methods and engaging campaigns—for example, provocative videos, fake attacks, and 30-day challenges—to instill cyber-secure behaviors and habits in the workforce. Accenture used this approach at a global oil & gas company to reach more than 90,000 employees in over 50 countries. Following the campaign:

- **89%** of employees took action;
- **87%** felt they had high awareness; and...

...the organization reduced its phishing vulnerability from **36%** to **8%**
CONCLUSION:
BECOMING A TRUSTED PARTNER IN CYBER-SECURITY AND DATA MANAGEMENT

FS HR functions can drive huge value out of the data they collect and manage. However, they can no longer take a back seat when it comes to data governance, quality and protection. To maximize the potential value of its data, the HR function must recognize that data is not simply a technology concern, but an amalgamation of people, process and business.

HR leaders should focus on partnering with the CDO and the CIO to improve data governance and protection, but they must also take accountability for the quality and security of their data. They and their teams cannot ignore the ethical, privacy, regulatory and technical dimensions of data protection and quality, and how these impact on the workforce.

The potential benefits to HR of using data more effectively are enormous: transforming HR services, managing workforce cost, enabling greater workforce agility and improving business performance. This is especially true in financial services, given its high-cost, highly complicated and highly regulated workforce. Yet unlocking this value demands effort and investment in ensuring data is accurate, secure and trusted.

Is your HR function ready to tap into the value of your data?
REFERENCES


CONTACT THE AUTHORS

Andy Young
Agile Organization Lead, Accenture
Financial Services Talent & Organization
andrew.s.young@accenture.com

Yorrick Bakker
Technology Consulting Manager,
Accenture Financial Services Talent & Organization
yorrick.bakker@accenture.com

Marc Le Claire
Management Consultant, Accenture Financial Services Talent & Organization
marc.le.claire@accenture.com

Susan Rice
Management Consultant, Accenture Financial Services Talent & Organization
susan.rice@accenture.com

David Boyd
Management Consultant, Accenture Financial Services Talent & Organization
david.boyd@accenture.com

Thomas Goodacre
Managing Director, Technology Consulting, Accenture Financial Services Talent & Organization
thomas.w.goodacre@accenture.com

Mel Lee
Managing Director, Accenture Financial Services Talent & Organization
melanie.lee@accenture.com

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world’s largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 442,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com

This document is produced by consultants at Accenture as general guidance. It is not intended to provide specific advice on your circumstances. If you require advice or further details on any matters referred to, please contact your Accenture representative.