workday
Built for the future®

CRITICAL FUTURE

The Impact of GDPR on HR

Report by Critical Future for Workday

Dear colleagues,

We are delighted to sponsor this independent research on the impact of the General Data Protection Regulation (GDPR) on HR by Critical Future. As a part of their research, Critical Future interviewed a number of HR leaders at organisations across Europe and as you will see from their feedback, while GDPR compliance will require time and effort, it will also deliver a number of benefits.

As May 25th, 2018 approaches, many of the organisations that I speak to are choosing to modernise their HR systems to help with their compliance efforts. In particular, where organisations have a complicated mix of different HR systems and spreadsheets, with employee data spread across different databases managed by multiple security models, GDPR compliance will be more difficult. Contrast such a complicated mix of HR systems with Workday's unified, single system approach to HR, with a single source of HR data and a single security model, and you can see why organisations are choosing to move to Workday as they work to both modernise their HR systems and move towards GDPR compliance.

We hope you find this research an interesting and useful aide for your GDPR compliance journey.

Barbara Cosgrove
Chief Privacy Officer
Workday

CRITICAL FUTURE

www.criticalfuture.co.uk

THE PUBLISHER

Critical Future is the market leader in providing white papers written by highly influential global academics on the most important management topics of today. Critical Future's white papers combine expertise, research, and industry insight to inform government, the media, and the business community.

THE AUTHORS

Jeremy Baker is an Affiliate Professor at ESCP Europe, ranked as the 11th best business school in Europe by the Financial Times. He is also a Lecturer at Tongji University Shanghai and Visiting Lecturer at Grenoble Graduate. He earned his MBA from Stanford University and is expert in business strategy including big data, and is regularly featured on the BBC, Sky News, and other leading news sources.

Dr. Antonia Lampaki, earned an MBA and a PhD in Business Strategy from the University of Athens. Dr. Lampaki has professional experience as a consultant at PwC, and has achieved several academic publications in leading management journals and conference proceedings on topics from leadership and organisational behaviour to human capital.

workday
Built for the future®

THE COMMISSIONER

Workday is a leading provider of enterprise cloud applications for finance and human resources. Founded in 2005, Workday delivers financial management, human capital management, and analytics applications designed for the world's largest companies, educational institutions, and government agencies. Organisations ranging from medium-sized businesses to Fortune 50 enterprises have selected Workday.

THE CONTRIBUTORS

This report is based on comprehensive research on the GDPR, combined with in-depth interviews with HR directors from Europe's leading companies and major employers. The cross-sector interviews included Financial Services, FMCG, Construction, Business Services, Broadcasting, Energy, and Automotive. This has provided first-hand direct insight into the GDPR from HR leaders at important European companies. We would like to thank all the HR directors for their participation in this research.

THE IMPACT OF THE GDPR ON HR

Valid and reliable employee data brings value to the organisation 6

Awareness of the GDPR 7

Significant changes the GDPR brings 8

The cost of non-compliance 9

The cost of compliance 9

Major concerns of HR managers related to the GDPR 10

The people concerns 10

The technology concerns 11

The communication concerns 12

Best practices for becoming a GDPR compliant-ready organisation 13

GDPR is an opportunity for HR 14

Key takeaway 16

VALID AND RELIABLE EMPLOYEE DATA BRINGS VALUE TO THE ORGANISATION

Employees are a source of competitive advantage and a strategic asset worthy of investment. Human resource (HR) managers have a crucial role in ensuring that this investment yields high returns through increased employee satisfaction, high retention rates, and enhanced workforce productivity and efficiency. Effective analysis of employee data has been a primary concern for many businesses for quite some time now. Based on Deloitte's 2016 report on global human capital trends[i], 77 percent of executives consider people analytics as a key priority, while 44 percent use employee data to predict business performance (representing an increase of 52 percent compared to 2015). To do so, HR managers need to make effective use of technology and make timely decisions based on valid and reliable employee data.

As technology makes tremendous leaps forward, companies can quickly collect a deluge of employee data. This data can, in turn, provide in-depth analysis and insights for business gains. However, often this data is scattered across many different HR and non-HR systems. These systems may be redundant and ineffective when dealing with such high volumes of data. As such, many HR professionals may feel overwhelmed and fall prey to the "analysis-paralysis trap". Additionally, if access to data is not securely managed, the risk of a data breach increases.

To respond to the pressing need to protect the privacy rights of individuals and for increased data security and transparency, the European Union decided to enact a new law that will change the way organisations handle personal data. This new law, the GDPR, is the most prominent change to the EU data privacy laws in the last 20 years.

This report aims to raise HR managers' awareness about the GDPR and the pressing need to take action. It will inform HR managers about the types of organisational change required to effectively implement the GDPR mandate related to employee data, and highlight the potential benefits that this new regulation may bring. To provide insight and practical advice to managers that ensure full and timely compliance with the GDPR, we interviewed seven HR directors from leading European companies across different industries (including financial services, personal services, non-alcoholic beverages, broadcasting, auto manufacturing and technology). Specifically, we asked them to assess their companies in relation to the GDPR and:

- ***Pinpoint any major concerns.***
- ***Describe the preparatory steps taken so far.***
- ***Identify the resources required to be compliant.***
- ***Explain how they plan to address challenges related to some of the new rights introduced by the regulation (for example, the right to be forgotten, the right of access).***
- ***Suggest ways to engage employees to adopt and remain compliant.***
- ***Discuss the changes in their data systems.***
- ***Identify potential benefits as a result of the GDPR.***
- ***Assess whether the benefits of GDPR compliance outweigh the costs in the long run.***

[i] Schwartz, J., Bohdal-Speingelhoff, U., Gretczko, M. and Sloan, N. (2016). Global human capital trends 2016. Deloitte University Press. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/HumanCapital/gx-dup-global-human-capital-trends-2016.pdf. Accessed on 16/11/2017.

AWARENESS OF THE GDPR

Ever since the initial preparatory discussions back in 2012, the GDPR has attracted a lot of attention. It covers the processing, storage, and management of personal data for customers, employees, and other individuals, to ensure that their privacy rights are respected. The EU Parliament approved the new regulation in April 2016 allowing a two-year transition period before it is fully effective on 25th May 2018. Personal data refers to any information that can be used to directly or indirectly identify an individual, such as basic identity information, racial or ethnic origin, web data, genetic and biometric data, philosophical/ religious beliefs, and political opinions.

This new regulation introduces a handful of employee rights that significantly impact organisations' compliance strategies. It pushes them to redefine systems and processes. Organisations that collect personal data on citizens in the European Union are required to review the data they hold, deploy several control mechanisms to protect this data, and appoint an independent Data Protection Officer (DPO) to ensure compliance and provide accountability. To this end, HR departments need to decide how to process and store the personal data of their employees, keep employees up to date with such changes, inform employees how and who will have access to that information, and how the data is handled when providing people analytics.

The HR directors that we interviewed raised concerns about the applicability of these new rights, such as the right of the employee to be forgotten. For instance, a HR director, who works at a world-leading company in the beverages sector, said:

"It is still unclear how HR will handle employee data if employees exercise their right to be forgotten. For example, we hold applicant data or sick leaves for six months. Should we delete them earlier in case someone exercises their right to be forgotten? We are still in consultation with our legal department and external consultants about this, but there is still a lot of ambiguity."

SIGNIFICANT CHANGES THE GDPR BRINGS

Motivated by the GDPR, HR departments need to complete a full audit of the employee data they store, log what it is, where it is and who can access it. To this end, they need to design new policies or update existing ones and train the entire workforce to ensure compliance. As a HR director from a multinational financial institution noted:

"All new joiners already participate in training on data protection. But, we now need to update this training in the context of the new law."

In addition, some companies will have to hire or assign someone who will be responsible for compliance with the GDPR. For example, companies with 250 or more employees, public organisations, companies that regularly monitor individuals on a large scale, or organisations that process special categories of data on a large scale, such as health data, must hire one or more Data Protection Officers (DPOs).

"We already have a DPO in Germany, Berlin. But maybe we will strengthen his role. We need to hire more as we have 25,000 employees" noted a HR director from a leading company in the beverages industry. When a DPO is not required by law, compliance monitoring could become the responsibility of an existing employee.

According to the new law, a DPO should be a person with expert knowledge of the data protection laws and practices. There is still some debate as to whether a DPO should be a lawyer with the necessary knowledge and experience of the laws and regulations, or an individual with an IT background. Succinctly put, a DPO should:

1. ***Inform and advise the company and its staff on the GDPR requirements.***
2. ***Raise the awareness of all employees and train those who will be involved in processing operations and related audits.***
3. ***Collaborate with the existing management and act as a consultant on issues surrounding the implementation procedure.***
4. ***Monitor the internal policies and procedures of the company associated with the protection of personal data and take corrective action.***

On the other hand, a DPO:

1. ***Should not influence the purpose and the means how personal data is managed. Hence, a DPO should not have a senior management position such as Chief Operating Officer, Chief Financial Officer or Head of Marketing, HR or IT, for example.***
2. ***Should be independent and report directly to senior-level management.***

THE COST OF NON-COMPLIANCE

Non-compliance with the GDPR could result in a penalty that may reach up to 4% of a company's annual revenue or €20 million; whichever amount is the highest. Interestingly, Ovum's survey[ii] revealed that 52% of companies expect to be fined for non-compliance. In addition to any financial losses, non-compliance with the new mandate may cause various problems for the company, jeopardising its brand and reputation. Alternatively, GDPR compliance may result in high-quality employee data that HR can analyse to predict business performance. Therefore, the incentives for compliance are there, but companies need to be agile in order to be ready on time.

THE COST OF COMPLIANCE

According to a recent (December 2016) PwC pulse survey related to the GDPR preparedness of US multinationals[iii], more than half of them (54%) considered the GDPR as their top data protection priority and another 38% said it was one of their priorities. To this end, 71% had already started to prepare for the GDPR, but only 6% had completed this work. Interestingly, 77% of the participating companies reported that they plan to spend more than $1 million on GDPR preparations and compliance efforts. Specifically, 68% of the companies said that they are willing to spend between $1 million and $10 million, while 9% stated that they plan to invest more than $10 million to ensure GDPR compliance. Therefore, meeting the privacy-centred requirements of the GDPR should not be taken lightly. Companies need to immediately start their implementation efforts, rather than reacting in haste and suffering the costs associated with non-compliance.

[ii] https://www.ovum.com/analyst-opinion-gdpr-will-force-changes-in-strategy/
[iii] https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html

MAJOR CONCERNS OF HR MANAGERS RELATED TO THE GDPR

The people concerns

Most of the HR directors we interviewed fear that the workload of employees will increase as companies act to be compliant. A HR director from a multinational financial institution underlined:

"We now have to review all employment contracts with third parties and imagine that we are a multinational firm; moreover, we do not know exactly who has the ownership of these contracts".

Likewise, another director, who works at a world leading company in the beverages industry, mentioned that:

"We have subsidiaries in many countries and this makes it difficult to review health insurance employee contracts with third parties. We now have to review all contracts from a GDPR perspective".

We expect that data audits will help companies to evaluate the quantity and quality of employee data that they store in various HR and non-HR systems. As a HR director from a personal services company stressed:

"We have undergone a data mapping exercise to find out where personal data is kept within our organisation and to ensure that we are compliant with the GDPR, at the least to a large extent. For example, we decided that for legal reasons we need to keep some personal data for some time".

Hence, companies will have to find out what kind of employee data they possess and where this data is stored, discuss strategies with employees or third parties that use that data and eventually evaluate the data and the value it brings to the organisation.

In a similar vein, other interviewees are concerned that the new legislation forces them to maintain less data. For instance, a director from a broadcast company noted:

"If a large amount of people exercise their right to be forgotten, we will have to delete a large portion of valuable data!".

In fact, five sections in the GDPR explicitly refer to data minimisation, considering it as an essential principle of data protection. According to the new law, personal data of employees must be ***"collected for specified, explicit and legitimate purposes"*** and must be ***"adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed".***

Practically, HR departments will need to minimise the amount of personal information they collect and maintain this data only for as long as the company needs it. This concept may sound paradoxical but, to reap the benefits of people analytics, companies need to apply the rule 'less is more'. Some organisations may prefer to keep a great deal of employee data for future use, but this costs time and money, and runs afoul of the GDPR's data minimisation principle. Therefore, companies need to keep only data that is relevant and necessary.

The technology concerns

The technical changes needed for GDPR compliance add another dimension to the management of personal data. The HR directors that we interviewed were also ambivalent about what compliance with the GDPR will require in terms of technology. For example, a HR director of a business standards company noted:

"I do not know the exact requirements of the new law, but we have cloud-based systems and a good company who provides it to us; they have a good understanding of the GDPR, so I feel confident that we will do alright".

But, where can we attribute this confidence? Article 4 of the GDPR differentiates between data controllers and data processors. The former includes those entities that are responsible for determining the purpose and the method for processing personal data. The latter contains those responsible for managing and processing personal data on behalf of the controller. The GDPR provides that data controllers and data processors share compliance obligations to a greater extent than under existing law. Together, they need to take the appropriate technical and organisational measures to ensure that any data processing is performed in compliance with the GDPR. This implies that data controllers need to entrust and collaborate with processors to help them to comply with the GDPR. Such collaboration will alleviate companies from considerable angst in the pre- and post-GDPR era.

Another director from a well-known UK broadcasting company said that:

"Most people around the company are concerned about the changes in the processes. But I am also worried about the changes in our data management system. We need to look at both processes and systems in our effort to comply."

Managers need to do their research and figure out which HR system meets their needs more efficiently. Key considerations include how to adopt such a system without interrupting daily operations, what it will cost and what changes it will require to the infrastructure and to other installed systems, and how to ensure that the company will remain secure from failures, attacks, or other contingencies. In case the company decides to store personal data of its employees in the cloud using external providers, the cloud provider should guarantee support in case of incidents and the company should be able to recover the data and delete it at the end of the contract.

The communication concerns

Echoing the sentiments of many of our interviewees, one HR director from a multinational beverages company stated:

"We need more details and guidelines about the new regulation. Some requirements lack clarity and create confusion".

She added:

"We need to find ways to ensure that management and employees understand that importance of balance between using and protecting their personal data and that they will exercise their rights in good faith. Otherwise, the price that we will have to pay might be heavy."

To successfully shift to a GDPR-ready organisation, HR needs to communicate to all employees the rationale behind these changes and why these changes are an opportunity for competitive advantage, as we discuss in the next section, rather than a necessary evil. In this respect, companies may need to send out communications to explain the new rules and the changes necessary in their daily work routine in simple terms. They may also want to upload all relevant material online for easy reference by staff. Finally, cultivating a learning mindset may be the key to help employees understand the changes that the GDPR brings. Hence, companies need to train employees on the requirements of this new law (for example, what is personal data, which procedures need to be followed, how to use the new or updated systems, and so on).

MAJOR CONCERNS OF HR DIRECTORS

People concerns

- Work overload from having to review employee contracts with third parties and from dealing with requests to be forgotten.
- Companies need to find ways to engage their employees and minimise the problems associated with resistance to change; those companies without good HR systems will suffer.

Technology concerns

- Worries about the cost of updating or acquiring and maintaining a data management system.
- HR professionals are not IT experts, and they may have difficulties in assessing the right data management system. Good collaboration with IT is a prerequisite.
- The fear of making a mistake and the time loss when attempting to prevent those errors.

Communication/Training concerns

- Most HR professionals need more details and guidelines about the new regulation; some requirements lack clarity and create confusion.
- Need to find ways to ensure that all employees understand their new rights and obligations towards the company.

BEST PRACTICES FOR BECOMING A GDPR COMPLIANT-READY ORGANISATION

Interviewees shared some advice about best practices that organisations may follow in the process of becoming compliant in the most cost-effective way and in the hope of turning these costs into a fruitful investment. Below, we present an action plan that outlines these best practices. The key takeaway here is to execute the plan as smoothly and efficiently as possible and to establish quality control mechanisms to ensure compliance at all the stages of the process.

STEP	BEST PRACTICES
1	• Verify that the company needs to abide by the GDPR.
2	• Develop an action plan.
3	• Perform a gap analysis to identify where the company is and where it should be, including an internal audit review of your readiness and a data mapping exercise.
4	• Create an organisational chart with key roles and responsibilities. • Hire a DPO or assign an employee to entrust compliance.
5	• GDPR team and HR professionals should know where personal data of employees is held and for what reason. Create an updated inventory of personal data that the company handles; this will help identify and classify data.
6	• GDPR team and HR professionals should delete the data they do not need.
7	• Decide on whether to retain the HR system that the company uses or make the necessary arrangements for a shift in technology. • Prepare contingency plans.
8	• Review current controls, policies, and processes to assess whether they meet the requirements of the GDPR, and build a plan to address any gaps. Processes and procedures should be updated to ensure that the company is ready.
9	• Communicate the changes that the new regulation brings to employees using briefs and memos. Update the company's website. • Set up training (online and face-to-face) to inform employees about their new rights but also about the importance of maintaining valid and reliable data.

GDPR IS AN OPPORTUNITY FOR HR

There is no doubt that aligning the company's infrastructure, and organising procedures to comply with the GDPR will require considerable investment in effort and resources, but it may also prove beneficial to the company in the long run.

PRACTICAL BENEFITS FOR HR

Improved data management:	• Urges HR to organise and filter employee data.
Improved data insights:	• Challenges HR to look at their processes and revise how they acquire, store, and maintain data.
Compliance Pays Off:	• Minimises the risk of data losses due to unauthorised access. This will also reduce the likelihood of financial losses. • Keeping all data in one place (for example, a cloud-based system) will allow companies to free up resources that could be used in other activities. • Information will be more reliable, valid and up-to-date, which minimises the likelihood of poor decisions. • GDPR gives HR the opportunity to modernise its HR systems and make cost-effective managerial decisions. • Employees are more engaged if they know that their company protects personal data, is accountable and transparent.

This new regulation will urge HR departments to look at their processes and revise how they organise personal data of existing and future employees. This is an opportunity to organise the data chaos and to improve the efficiency of their HR systems. Companies will have to screen all employee data that they already possess, reliably store it in as small a number of different repositories as possible, and assign various permission rights to access the data. As a HR director from a large broadcasting company argued:

"GDPR challenges your company to look at its processes and revise how you acquire, store, and maintain employee data; employee data is a goldmine that you need to discover",

and added that they

"use correlations of the data to understand employees' high performance capability, and understand the quality of the performance."

Because of this transformation process, companies will only retain employee data that is valid and up to date, the flow of information will speed up, more efficient procedures will be established which, in turn, will increase productivity. Most companies have the basic technical capability to work with data. However, because of the GDPR, they now must do a more thoughtful data collection. As a senior talent acquisition director of a multinational infrastructure and technology leading company aptly put it:

"This new law will simplify the handling of country data for the company. It will be one rule across the borders".

Having reliable data may help companies to better analyse and understand their employees.

"Benefits include the opportunity to put our data into the spotlight and to do the right thing for our employees",

said a director from a large personal services company. Indeed, for some, clean data is considered the new oil. Accurate, relevant and up-to-date data will most likely help HR to gain insight into the capabilities and performance of their employees.

On top of the benefits of improving data management and data insights, employees may become more engaged. Employees feel secure if they feel their data is secure. Existing and future employees entrust their employers with their personal data and appreciate transparency in how this data is processed. A HR director from the beverages company mentioned that:

"To comply is a benefit for our company. It shows that we take the personal data of our employees seriously. In other words, it shows that we care about our employees".

Another HR director from a broadcasting company highlighted:

"Employees feel secure when they know that their data is secure; this increases their trust in the company and makes them more engaged employees."

Hence, building a more trusting relationship will increase the chances of positive reciprocation. Employees may manifest such reciprocation through increased engagement.

KEY TAKEAWAY

Overall, we expect that companies who drive towards compliance will soon observe positive changes in employee productivity and performance. Similar to what happened after the introduction of the Sarbanes-Oxley Act of 2002 that obliged companies to organise their financial data, management will eventually look back and say:

"Well, compliance was a nightmare, but it was all worth it!".

As with most changes, the road will be bumpy, but this is an opportunity for HR to embrace. In the long run, if HR systems and processes are set up properly, it could put HR teams on the front foot with real confidence in the efficacy of their data in the modern, data-driven business world. Therefore, the GDPR may provide the opportunity for HR to take a leading role in the big data revolution, offering substantial benefits for organisational performance.

PRODUCTIVITY

Data will be more valid and up-to-date, the flow of information will speed up, more efficient procedures will be established, all of which will increase productivity.

PERFORMANCE

Reliable data may help companies to get more insight and understand their employees better.

TRUST

Employees will recognise that their organisation is accountable and transparent, and this will increase employees' trust and engagement.

BRAND

Compliance with the GDPR will help reduce data-breach incidents and mitigate the associated costs in reputation.

REFERENCES

1. *http://ec.europa.eu/justice/data-protection/*
2. *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf*
3. *http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN*
4. *http://europa.eu/rapid/press-release_IP-15-6321_en.htm*
5. *http://www.amcham.be/publications/amcham-connect/2016/march/fieldfisher-gdpr-data-protection-human-resources-hr-perspective*
6. *http://www.eugdpr.org/*
7. *http://www.eugdpr.org/key-changes.html*
8. *http://www.fieldfisher.com/publications/2016/03/the-new-eu-data-protection-regime-from-an-hr-perspective#sthash.TbUgiz91.dpbs*
9. *http://www.hrreview.co.uk/analysis/impact-will-gdpr-employers/105990*
10. *https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf*
11. *https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf*
12. *https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf*
13. *https://www.cipd.ie/knowledge/emp-law/data-protection-technology/general-data-protection-regulation*
14. *https://www.complianceweek.com/system/files/resources/gdpr-ebook.pdf*
15. *https://www.hrsolutions-uk.com/impact-gdpr-hr-personal-data/*
16. *https://www.mckinsey.com/business-functions/risk/our-insights/tackling-gdpr-compliance-before-time-runs-out*
17. *https://www.mckinsey.com/business-functions/risk/our-insights/the-eu-data-protection-regulation-compliance-burden-or-foundation-for-digitization*
18. *https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html*
19. *https://www.taylorwessing.com/globaldatahub/article-changes-to-employee-data-management-under-the-gdpr.html*
20. *https://www.taylorwessing.com/globaldatahub/article-processing-of-hr-data-under-the-gdpr.html*