Executive Brief

Cloud, Compliance and the Case for HR Transformation to Support Your HCM Strategy

Sponsored by: ADP

Duncan Brown Alexandros Stratis

November 2016

EXECUTIVE SUMMARY

HR leaders face the challenge of legacy approaches to the handling and processing of employee data. This can differ significantly between headquarters and subsidiaries, through a combination of different software application usage, third-party outsourcing providers and a distributed datacentre footprint. Similarly, the widespread adoption of cloud places even greater pressure on security regulations.

To address these challenges, and the need to become more strategic in the eyes of the business, CHROs are driving HR transformation projects and HR technology investments. A key ingredient in achieving the expected return on these initiatives is working with an HR technology vendor that can ensure that consistent data protection and compliance approaches are built into its services and software offerings as best practice.

HCM is undergoing a rapid transformation that is reshaping the management of the workforce. This is being driven by the evaluation of performance based on projects, collaboration and results, the overall engagement with employees, and how they can plan their paths and futures. The HR department, which has historically been a keeper of employee records, an administrator of training and a processor of HR transactions, is now evolving into a strategic partner for the growth of the organisation.

HCM is undergoing a rapid transformation that is reshaping the management of the workforce.

A key part of this HCM transformation involves proprietary solutions and manual processes rapidly giving way to packaged solutions and public cloud services. Adopting cloud solutions is likely to deliver increased functional user scope for customers, as well as delivering the efficiencies and flexibilities of cloud architectures.

But security concerns persist. Trusting sensitive information to a third party is a major step in any event, but putting employee data into the cloud, to an unknown location protected by vague assurances of security, is insufficient for most HR executives. How can employer organisations be certain that their employees' data is safe?

The game is about to get much more serious, in terms of both obligations and consequences. The General Data Protection Regulation (GDPR) will apply from May 25, 2018, and it increases the requirements on security and other personal data processing activities that seem to compound the risk. Importantly, GDPR is a regulation, not a directive, which means that it applies equally to all 28 member states with no need for transposition into national law.

In light of GDPR, companies are finding it difficult to understand and respond to regulatory changes as they take place. Non-compliance costs and risks can be significant.

Cloud – if done properly – can mitigate risks of non-compliance with GDPR and local employment laws. IDC believes that many companies will choose to outsource HR data processing in order to *reduce* their risk and compliance obligations. But an HRO provider must have a strong action plan, data flow maps, data retention plans, robust security platforms and data transfer programmes, all under the auspices of a data protection office (DPO).

This paper explains the impact of GDPR and shows how cloud can enable, rather than inhibit, compliance while enhancing your digital HCM strategy.

Cloud — if done properly — can mitigate risks of non-compliance with GDPR and local employment laws.

THE CHANGING REGULATORY ENVIRONMENT FOR HR DATA

GDPR is the biggest change to data protection law in three decades. It both refreshes the existing law that predates the emergence of Facebook, LinkedIn and the cloud, and unifies data protection legislation across all 28 member states.

GDPR is the biggest change to data protection law in three decades.

The existing Data Protection Directive was agreed in 1995 and is not fit to protect the personal data of individuals in a world where we habitually store and exchange personal information online. The directive was also implemented by each individual member state according to its business customs and cultures, resulting in a disparity of data protection regimes across the union. GDPR is therefore a substantial step forward in the homogenisation and modernisation of data protection law in Europe.

The definition of personal data is very broad: it includes any information that does or could identify – directly or indirectly – an individual. This includes the obvious identifiers such as name or identification number, but it also includes location data or IP address as well as biometric and genetic information. Importantly, personal data includes that of employees of a company as well as that company's clients or customers.

The main implication of GDPR on HR data is perhaps obvious, but worth stating. Employee data is granted identical rights under GDPR as client or customer data. This means the obligations of the company to protect its HR data are increased, the rights of employees to access, update and erase data are enforced, and the consequences of non-compliance are severe (as we shall see).

Employee data is granted identical rights under GDPR as client or customer data.

However, HR departments are not limited to the regulatory environment surrounding GDPR and data privacy; the number of rules and country-specific regulations that organisations must remain compliant with is a challenge in itself. There are five distinct areas where HR must ensure that it remains compliant: benefits and insurance, recruiting, work safety and hazard, payroll accounting, and employee life-cycle management.

Organisations are increasingly asking their HR departments to be proactive and engage with all sorts of "people risks" related to the five areas above. The challenge is more intricate for those organisations that operate in different jurisdictions, with subsidiaries or parent companies in different locations. What is of importance here is to understand that compliance within HR should be seen as a rounded risk management function that also advances the human capital agenda.

In addition, compliance helps elevate the role of HR from a system of records with minimal strategic function to a key strategic partner that can reduce risk-related costs for the organisation, and at the same time increases productivity and employee engagement.

Examples of compliance requirements for HR departments, which require the constant monitoring and management of their parameters, can range from payroll and taxation contributions (the PAYE system in the UK versus "impôt sur le revenu" in France, etc.), training (onboarding, fraud detection, etc.) and professional development requirements (monitoring of Credits of Professional Development/CPDs or other metrics used by professional associations and boards to ensure membership) or due diligence in the recruiting and termination process.

KEY FEATURES OF GDPR

As discussed, GDPR's definition of personal data is very broad. From an HR perspective, any information that relates to an employee is protected, and indeed some categories of data are forbidden to be collected. This includes so-called "special categories" of data, often also called sensitive data. Such data categories include genetic, biometric and health data as well as sexual preference or orientation. However, an important caveat to this prohibition is the processing of information for the purposes of preventative or occupational medicine or for the assessment of the working capacity of an employee (GDPR Article 9).

GDPR also introduces a joint responsibility and liability between data controllers (typically, in the context of HR data, the employer) and data processors (third parties processing data on behalf of the employer) in some instances. This is important to any employer using or considering the use of outsourced HR processing.

In terms of security requirements, GDPR is deliberately vague. Of the 99 articles in the final text of GDPR, only one (Article 32) specifically relates to security provision and it is short on detail. The main direction of the regulation is that organisations should take into account "state-of-the-art" technology, as well as cost, risk and the business context. Organisations therefore need to decide what state of the art means for their organisation: not a straightforward task. The article also strongly encourages (though does not mandate) encryption and pseudonymisation (broadly equivalent to tokenisation).

Note, however, that security is a fundamental part of the principles relating to the processing of personal data (Article 5). In particular, GDPR mandates that data must be processed in a manner that "ensures appropriate security of the personal data". So although GDPR is imprecise on the measures taken to deliver security, it is unambiguous in the importance of security.

GDPR is imprecise on the measures taken to deliver security, but is explicit in the importance of security.

From an HCM perspective, GDPR points CHROs to a number of key technological decisions. Although not required, many CHROs will conclude that encrypting all employee data is desirable, at rest, in transit and in backup. GDPR does mandate the keeping of records of data processing and the ability to facilitate audits, for both compliance and forensic purposes.

GDPR: More Than Security

A common misperception of GDPR is that it is essentially a data security regulation. While data security, as we say above, is an important aspect of GDPR, it is a mistake to consider security as the fundamental technology at play. There are other requirements that involve a variety of technologies beyond security.

For example, the data portability requirement (Article 20) creates the right of an individual to demand personal data from the controller, in a machine readable format where possible, when the processing is based on the individual's consent or on contract. The right to erasure (often known as the right to be forgotten, Article 17) enables an individual to require a controller to delete personal

data (under specific circumstances and with several exceptions). And the rules for consent — notably gathering parental consent over children's data (Article 8) — are severely tightened.

One of the main concerns of GDPR, as exemplified by the seven articles covering the subject, is data transfers (Articles 44 to 50). Data transfers involve the movement of data to a so-called third country. A third country is that which is not a member of the EU. The concern is to ensure that data controllers adequately protect the data even if it is moved outside its jurisdiction. The EU has two mechanisms to contain this threat: the control of data transfers beyond the EU and an extra-territoriality clause extending the scope of GDPR to any data regarding a person in the EU (irrespective of the location of that data, see Article 3).

Data transfers are important in the context of HR data where employers are using cloud-based services or HR outsourcing providers. It is a legal requirement for employers to know where their HR data resides physically, and specifically whether it is held outside the EU. It is perfectly legal to export data outside the EU: however, this must be done under one of several mechanisms of regulatory oversight. These include:

- Transfers on the basis of adequacy: the EU maintains a list of countries with data protection laws that are deemed adequate (or equivalent) to GDPR. There are only 12 countries on this list and (importantly for many) this does not include the US.
- Binding corporate rules (BCRs): this is an official commitment by a data processor to implement a data protection programme providing a high level of data protection in accordance with GDPR, which has been approved by EU Data Protection Authorities. It is not a trivial undertaking, and demonstrates a lasting and legally binding commitment to the EU's privacy principles.
- Standard model clauses inserted on a per-contract basis.
- Consent from the data subjects to transfer their data beyond the EU.
- Adherence to an approved code of conduct or certification mechanism. Both of these structures are enacted in GDPR but are yet to be implemented.

The other main mechanism for conducting lawful data transfers is where a specific agreement between the EU and the third country exists. This approach is typically used where an adequacy decision was not granted. The best example of this situation is Privacy Shield, a bilateral agreement between the US and the EU that allows data transfers to processors adhering to the terms of the agreement. However, Privacy Shield is likely to be tested in court, as was its predecessor Safe Harbor. IDC thinks that US-headquartered firms that want to demonstrate long-term commitment to GDPR principles should follow the BCR route.

A timely illustration of the data transfer regime is, of course, Brexit. As far as data protection law is concerned, Brexit is largely irrelevant. This is because of the data transfer rules in GDPR: if any UK company wishes to trade with an EU partner, or process EU personal data, then it will have to adhere to data transfer rules in GDPR. Given the scale of business between the UK and the EU today, it is likely that the UK will adopt a GDPR-like law when it leaves the EU (and the ICO has already indicated this position).

As far as data protection law is concerned, Brexit is largely irrelevant.

Penalties for Non-Compliance

Much headline space has been given to the "effective, proportionate and dissuasive" administrative fines potentially imposed by regulators. In particular, much attention has been directed towards the maximum fines of up to 4% of total worldwide annual revenue or €20 million, whichever is the higher. It is worth noting that this level of fines is applicable only to infringements that relate to the principles of GDPR (Article 5), fundamental data subject rights such as consent

and erasure, and data transfer violations. Data breaches themselves, resulting for example from security weaknesses, attract a lower level of fine of up to 2% of total worldwide annual revenue or €10 million. Employers may be more worried about mandatory breach notifications. Data controllers are required to notify their supervisory authority in the event of a personal data breach that results in a "risk to the rights and freedoms of individuals" (Article 33). In these cases, they must also communicate the event to individuals themselves (Article 34). This may then lead to negative publicity which may subsequently damage brand and reputation.

Ultimately, a supervisory authority has the power to order the suspension of data processing (Article 58). This could mean effectively an order to cease trading, or running a payroll cycle, if the data processing in question underpins a core business process.

It is no surprise, given these sanctions, that GDPR is getting the attention of the board-level executives at companies across the EU (and beyond, due to extra-territoriality). However, it is important to understand that sanctions (such as fines) are likely to be imposed where there is a lack of evidence of effort to comply. There is a strong emphasis in GDPR on evidence compliance, including the creation and maintenance of records of data processing. Auditability is critical, and the ability to demonstrate compliance (accountability) is a fundamental tenet of GDPR.

THE CASE FOR CLOUD: WHY CLOUD HELPS, NOT HINDERS, HR OPERATIONS

In essence, cloud services are a form of outsourcing. As with any outsourcing activity, due diligence must be undertaken on the provider. Cloud-based HR processing must therefore undergo the same level of contractual due diligence.

However, cloud is different because of the multiplicity of processing facilities it involves. Companies need to address practical due diligence by asking different questions about the level of security and data protection processes in place and by analysing audit reports, including independent third-party reports possibly made available by the cloud provider. For example, understanding the physical security of the datacentre in which personal data is hosted is critical. A credible supplier will have at least as good a security capability as the largest enterprise firm, and most probably considerably better than the average employer organisation. This is likely to include certification to ISO 27001 and (increasingly) 27018, which focuses on personal data in public clouds.

There is no legal or technical impediment to storing HR data in the cloud.

There is therefore no legal or technical impediment to storing HR data in the cloud. Some companies may opt for a configuration with an EU-based datacentre, including proven physical and logical security certifications. Further, access to that EU data should be only from within the EU: access from outside the EU would constitute a data transfer (effected by data in transit) and diminish the efficacy of EU-based datacentres.

Most cloud-based solutions will require data transfers outside the EU to a small or large extent. Suppliers have developed solutions to protect the personal data including model contract clauses. But binding corporate rules are emerging as the most robust form of legal assurance to address data transfers.

Binding corporate rules are emerging as the most robust form of legal assurance to address data transfers.

Many companies will choose to outsource HR data processing in order to reduce their risk and compliance obligations. Employers cannot eliminate risk, but choosing a credible provider is an appropriate action to take.

TECHNOLOGY VENDORS AND THEIR ROLE IN HR TRANSFORMATION AND COMPLIANCE

It is often said that enterprises can outsource processing but never responsibility. In terms of GDPR this is still true, but the broadening in liability to include processors means that at least some of the responsibility for compliance can move to a third-party data processing provider.

To be clear, the controller remains responsible for, and must be able to demonstrate compliance with, the core principles of GDPR (Article 5). But the prime requirement of a data processor is that it is able to implement the technical and organisational measures agreed with the controller. It also faces the same sanctions for non-compliance. This begs the question: how can a controller tell whether a processor is able to meet this requirement?

With the clock already ticking towards May 25, 2018, employer organisations mustn't ignore GDPR, or the substantial changes it brings.

Codes of conduct and certifications are established in law under GDPR, but to date neither mechanism exists in practice. So processors may convince employer organisations of their credentials by other complementary means, such as ISO 27001 (information security management), 27018 (protection of personal data in public clouds) or 29100 (privacy framework) certifications, independent audit reports and BCRs for processors demonstrating long-term and organisational commitment to adhering to the principles of GDPR. BCRs are considered the gold standard for data protection by EU Data Protection Authorities.

A challenge for HRO providers is to achieve efficiencies across multiple employer organisations by operating at scale, while exhibiting knowledge of local employment laws and practices. Thus they must be both international in operation but local in implementation: IDC thinks that few HRO providers will be able to deliver this combination of capabilities.

An important aspect for the HR professional is the fact that the modern business sees, wants and expects more from the HR department. The HR systems of the past were systems of record with limited added strategic value for the organisation and focused solely on the management of the simplest aspects surrounding the employee life cycle.

An important aspect for the HR professional is the fact that the modern business sees, wants and expects more from the HR department.

Over time, with the change in capabilities, regulations and most importantly in the role HR is expected to play, the HR professional aspires to be more strategic, more insightful and more valuable to the entire organisation. Under this lens, compliance cannot be underestimated; on the contrary, managing the compliance aspect from an HR perspective becomes a key risk mitigating factor for the business and has the potential to reduce costs and protect from litigation, despite the increase in complexity and the scope of the HR department's role.

KEY RECOMMENDATIONS

Don't Ignore GDPR

With the clock already ticking towards May 25, 2018, it is important that employer organisations do not ignore GDPR, or the substantial changes it brings. The legal and technical school of GDPR is vast and most organisations will struggle to implement it in full by the date of application. If employer organisations have not yet started to examine the impact of GDPR, then they should do so immediately.

GDPR is an Opportunity

It is easy to see GDPR, with its raft of changes, as a major obstacle to negotiate, and a distraction from normal business activities. In fact, IDC believes that GDPR presents substantial opportunities for employer organisations. It creates a clear and even regulatory environment for data transfers that underpin cloud-based HRO services. With the appropriate insurances in terms of security from a provider, companies can securely and legally use cloud-based HRO as part of their HCM strategy.

Compliance is a Partnership

In August 2016 IDC completed its *Human Capital Management Survey* in Western Europe, with more than 250 responses from HR decision makers and managers. In our survey the issues of data privacy and changes in legislation (GDPR) were seen as a key concern for one in three of the respondents, while a mere 23% appeared to be slightly concerned to not at all. The majority of respondents (76%) still sees data privacy and compliance (to GDPR and other legislation) as a factor influencing the purchasing decision for an HCM solution.

It is crucial for vendors to provide HR with the required tools and insights, along with the assurance that the solutions in their portfolio are both compliant and secure because then they can help HR departments achieve more of their long-term goals, namely their transformation from a back-office function to a valued partner to the board.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC U.K.

IDC UK
5th Floor, Ealing Cross
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Copyright and Restrictions