Global Payroll Association

Protecting Personal Data and Payroll Professionals

Has the payroll industry embraced GDPR effectively?

Sponsored by

ADP

A more human resource.℠

Introduction

With the EU GDPR (General Data Protection Regulation) now only a matter of weeks away, earlier this year, GPA surveyed our global membership to understand how the payroll profession is preparing for the new legislation.

We found many competent practitioners that have worked diligently over several years to ensure that they are ready; but we also found widespread confusion and gaps in preparation among many of those that responded.

Although there are good signs of progress, the research highlighted that:

Only 14% of respondents have received GDPR training specific to the payroll industry.

Less than half of payroll and HR functions have fully documented all their policies and procedures; a key first step in ensuring compliance.

Only 39% of payroll professionals have 'every confidence' that their suppliers/partners will be GDPR compliant by the May 25th deadline.

I would like to thank the 200 of our members that responded to the survey and I am grateful for the ongoing support of Human Capital Management provider ADP in our ongoing partnership to help the industry prepare for GDPR.

Melanie Pizzey CEO
globalpayrollassociation.com

Introduction

It is encouraging to see the payroll industry's response to GDPR and the excellent progress that has been made. This complex legislation is a massive upheaval for many companies yet this research has shown that the vast majority of HR and payroll teams (84%) have taken action despite fears that the new law would be met with apathy.

However, there are still concerns to address when considering the lack of employee training that has taken place, which also has repercussions when attempting to ensure compliance. Compliance is one of the more difficult areas of GDPR because it is not just about your own company - organisations will have a duty to ensure that their partners are also fully prepared. Furthermore, whilst it may prove easy for companies to focus on the deadline of May 25th, GDPR must also always be treated as an ongoing process.

While a few companies have made progress in these areas there are further challenges that need to be addressed, such as how to respond in the event of a data breach and around the right to be forgotten' – a particularly tricky area to manage and one that often seems to be overlooked. These areas are where the industry really needs to improve.

Yet despite the challenges that remain, the payroll industry has now built a certain standard and there is positive momentum which companies can look to build on going forward. At ADP, we're passionate about protecting the privacy of our clients and setting an excellent benchmark within the industry, and look forward to ensuring a continual process of developing our products and policies at every step.

Binding Corporate Rules (BCRs) were developed by the European Commission to allow multinational corporations, international organizations, and groups of companies to make intra-organisational transfers of personal data across borders in compliance with EU Data Protection Laws.

Implementing Binding Corporate Rules illustrates our commitment to protect personal data in accordance with the standards required in the EU, regardless of where the European data is processed, accessed or hosted.

Don McGuire
President ADP Europe

Report introduction

Payroll professionals are accountable for some of the most sensitive data in an organisation and with imminent enforcement of GDPR, many payroll functions have been proactively preparing themselves for the change.

The payroll industry has been active in the roll out of GDPR, with major providers, governing bodies and advisory groups pulling together to develop best practices and incorporating recommendations from the national regulators and EU authorities as they are announced.

As the various regulatory bodies continue to issue guidance approaching GDPR enforcement, a strong understanding of data protection principles will help to guide payroll professionals through the changing landscape. Access to information, support and training will be central to successfully implementing data protection strategies that fulfil the six principles, and the principle of accountability.

Article 5 of the GDPR requires that personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Source: ICO

The positive attitude towards GDPR shown in the survey is a testament to the payroll profession and the willingness to embrace change. However, the research also identified a lack of support and training being offered by organisations and some areas where more work may be required for organisations to truly thrive in a GDPR world.

High Priority but Gaps in Knowledge and Understanding

GDPR is undoubtedly a priority for many of the organisations where survey respondents work, scoring an average of 73 on a 100 point scale.

Although just over half of organisations have or are currently developing and distributing a statement on how they will approach GDPR in relation to HR and payroll data, the evidence suggests that many payroll professionals are already making strides in GDPR adherence.

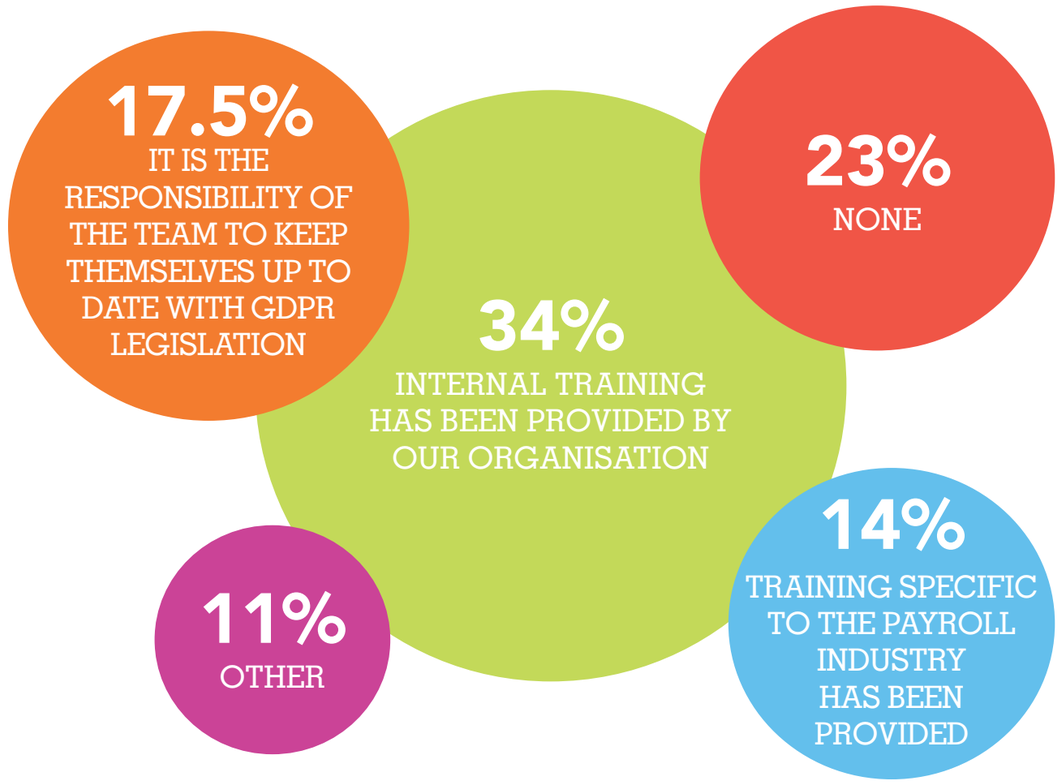
Has the organisation developed a statement about how it intends to approach GDPR in relation to HR and payroll data and distributed it to all employees?

An overwhelming majority of HR and payroll teams (86%) have taken action, from creating a GDPR taskforce to conducting risk assessments. There were concerns in the payroll industry that GDPR would be approached with some degree of apathy; the results of steps already taken clearly show that this is not the case.

However, despite compliance being seen as an organisational priority, only 14% of payroll professionals have received specialist training relating to payroll, with 34% receiving generalist internal training from their organisation. A surprising 23% have not received any training at all. It is therefore perhaps unsurprising that challenges remain in ensuring compliance.

Whilst we recognise the efforts and determination of those who are self-educating, this could lead to organisations unwittingly falling foul of GDPR requirements. Not only will organisations need to invest in education for their employees in order to ensure accurate knowledge of the regulation, payroll specific training regarding data privacy and protection principle will give payroll professionals the information they need to be able to make well-informed decisions.

What GDPR training is your company providing?

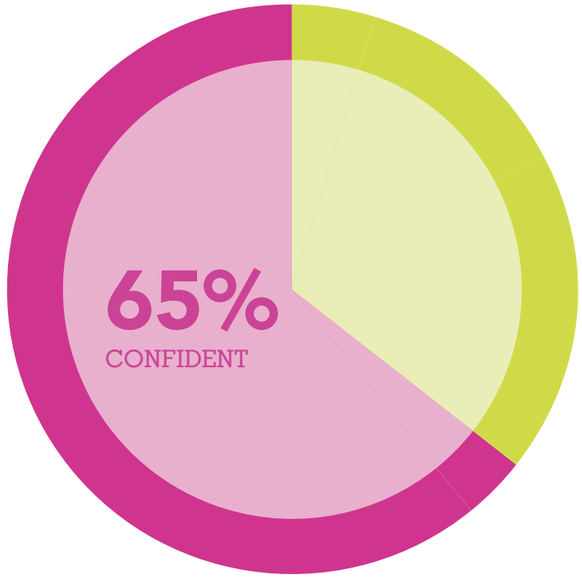


Confidence in success. Confidence in suppliers

One of the most significant changes that GDPR will bring is in the principle of accountability, where "the controller shall be responsible for, and be able to demonstrate, compliance with the principles". This extends the data controllers' obligations across the full spectrum of data processing regardless of whether some of those elements are outsourced or managed by other Data Processors.

In the world of payroll, this means that software and service providers are part of the compliance story and organisations should be taking steps to ensure that their chosen partners are ready for GDPR. Indeed, as the deadline looms it is concerning to see that 19% of respondents do not know where their suppliers and partners stand on GDPR or if they will be ready.

Furthermore, as much of the legislation itself will be subject to interpretation after May 25th, it's important that compliance is not viewed as a one-time event but rather an ongoing process of improvement. It is therefore perhaps unsurprising that 26% of respondents report being worried about this area of compliance.



Has the organisation developed a statement about how it intends to approach GDPR in relation to HR and payroll data and distributed it to all employees?

Payroll professionals are showing a positive outlook on the upcoming enforcement of GDPR, as 65% reported that they are confident that their organisation is ready for GDPR with regards to employee data. To support this further 40% of organisations have already sought and received confirmation of compliance from their specific suppliers.

While the majority of respondents have confidence that their suppliers and partners are either already compliant or well on their way, it is incumbent on the payroll professional to ensure compliance for their organisation. A disconcerting 9% of respondents have yet to realise that they are responsible for the full impact of GDPR regardless of their operating model. Payroll professionals are encouraged to engage with their suppliers to understand how they are applying data protection policies and procedures to the services provided. This will help payroll to continue to provide a continuous and robust service to their employees.

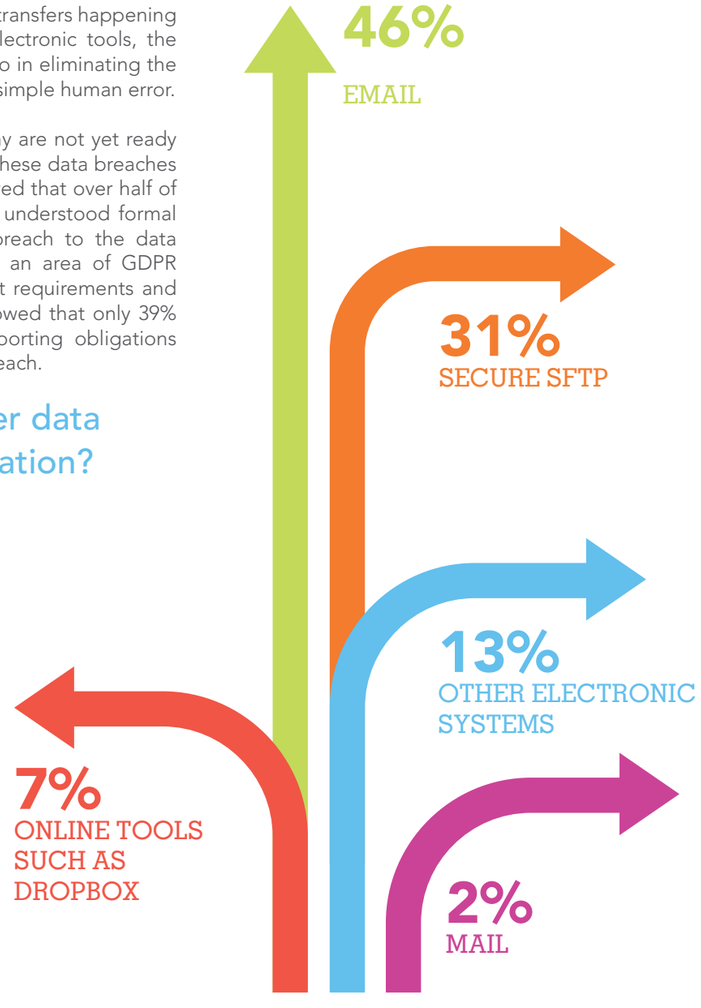
Devil is in the detail

Despite an overall positive trend in the research findings, it appears that the GDPR impact on data security and the implications of 'right to be forgotten' may be being overlooked by the payroll profession.

With almost 50% of payroll data transfers happening via email and other insecure electronic tools, the industry still has a long way to go in eliminating the risk of data breaches caused by simple human error.

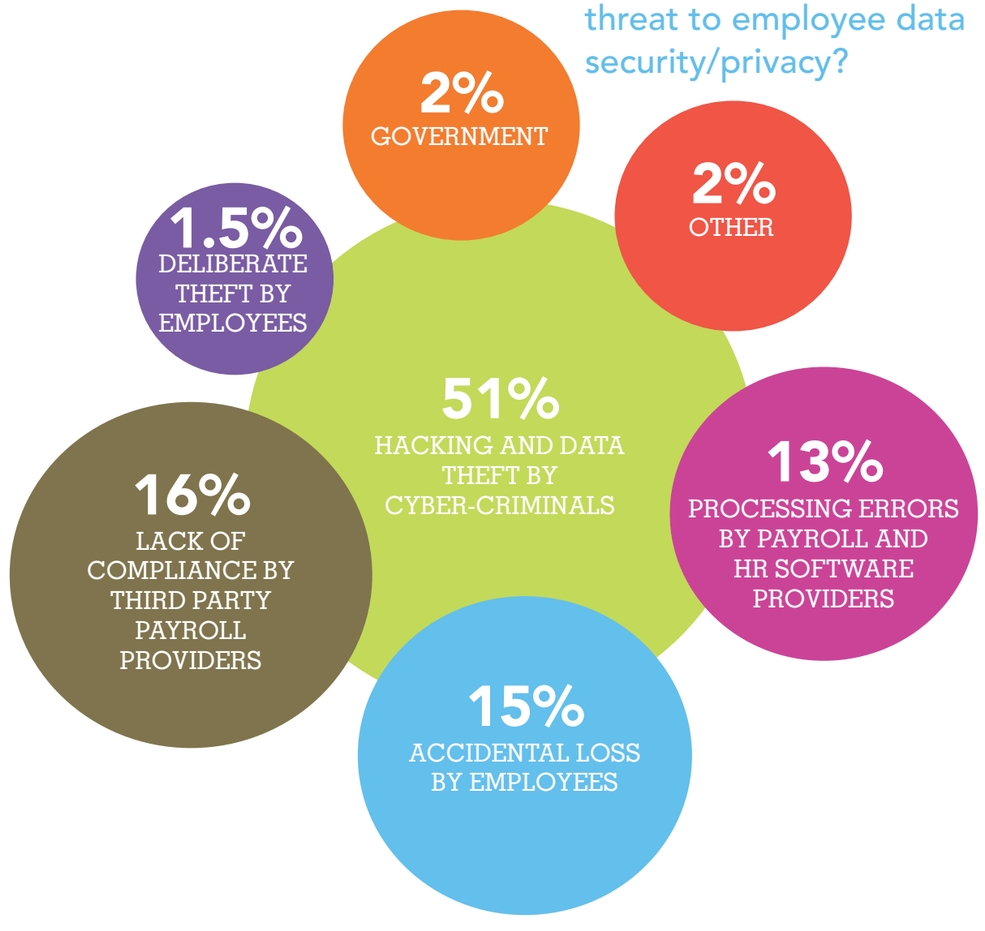
Furthermore, it is clear that many are not yet ready to deal with the implications of these data breaches under GDPR. The research showed that over half of organisations don't have a well understood formal process for reporting a data breach to the data protection authority, yet this is an area of GDPR with some of the most stringent requirements and penalties. The research also showed that only 39% accurately understood their reporting obligations and timeline in the event of a breach.

How do you transfer data within your organisation?



As with previous studies of this kind, respondents tend to worry most about the external threats and are perhaps under prepared for the simpler elements of human error.

Which of the following do you see as being the biggest threat to employee data security/privacy?

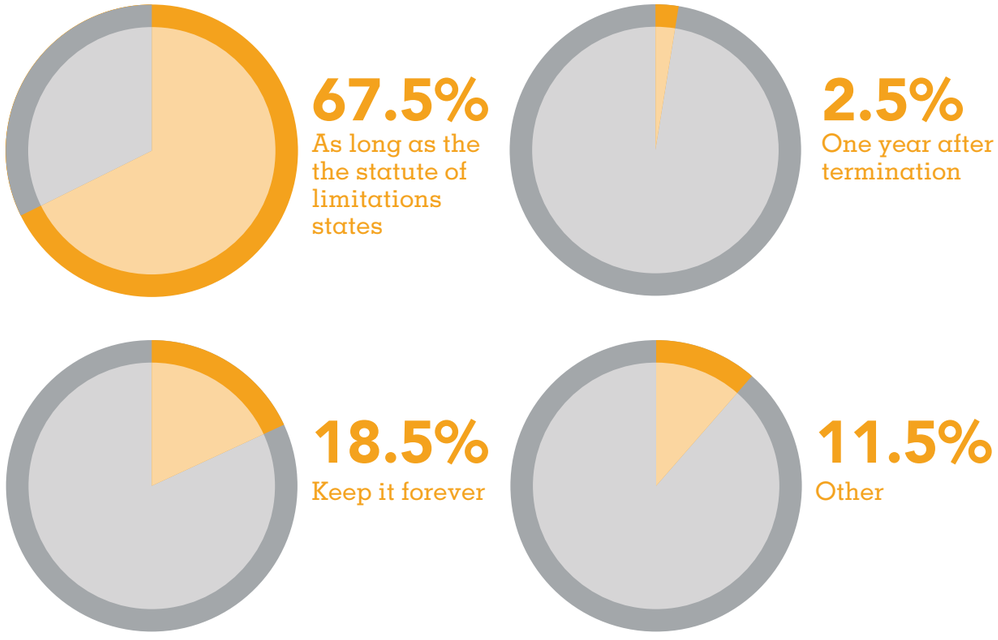


The ‘right to be forgotten’, or to have personal data deleted, is formally introduced into GDPR as the right to erasure. It is important to note that this right is not absolute, and local statutory obligations will take priority.

Although the majority of respondents will have a clear process in place by the May deadline, some confusion remains about how long records can be kept and how this data can be managed in a post GDPR world.

Whilst personal data should only be kept for as long as is necessary for the purposes that it was intended however this does not override any statutory requirements to retain records.

How long do you currently retain an employee’s information



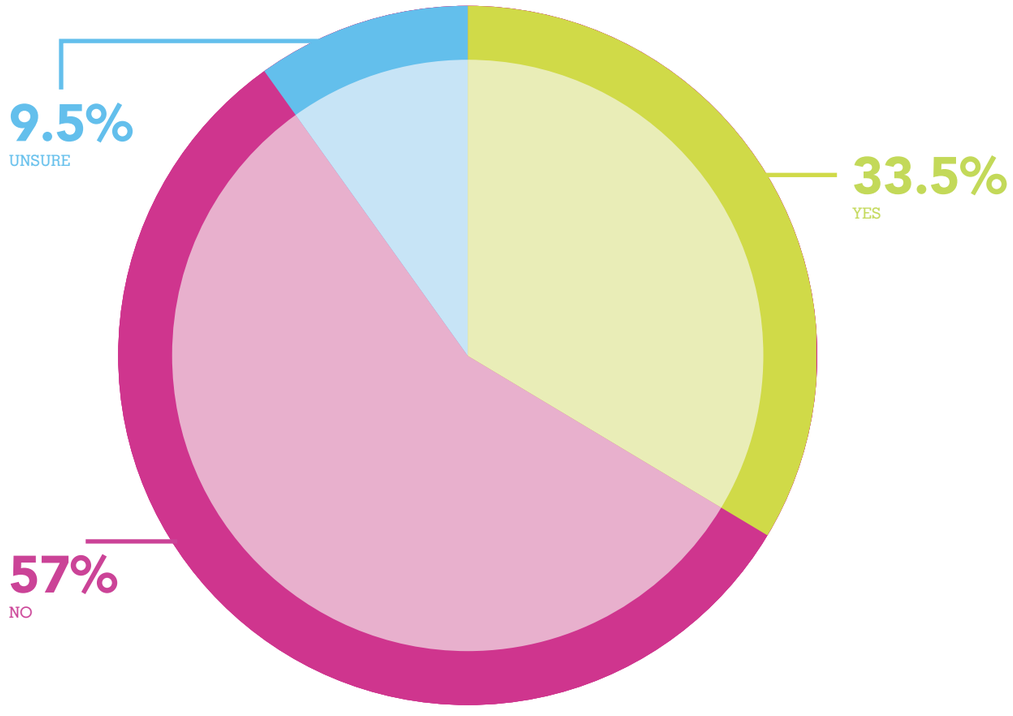
With 1 in 5 organisations currently keep employee data indefinitely once they have left the business, there are significant process changes that must take place to bring these organisations in line with GDPR requirements.

Under GDPR, sensitive personal data will receive additional protection to ensure the rights and freedoms of the individual. Crucially, 82% of payroll professionals are aware of the provisions that extends the definition of ‘special category data’ under the current Data Protection Act 1998, to include new types of data such as biometric and genetic information.

As well as expanding the definition of sensitive data, employers must also ensure that this data is processed in accordance to at least one of the conditions of processing special category data.

To maintain the levels of protection afforded to individuals under GDPR, restrictions have been placed on ‘the transfer of personal data outside the European Union, to third countries or international organisations’. Affecting a third of organisations, safeguards must be put into place as the conditions and processing requirements of GDPR will remain applicable to the organisation receiving the individual’s data.

Do you share employee information with organisations outside of the EU?

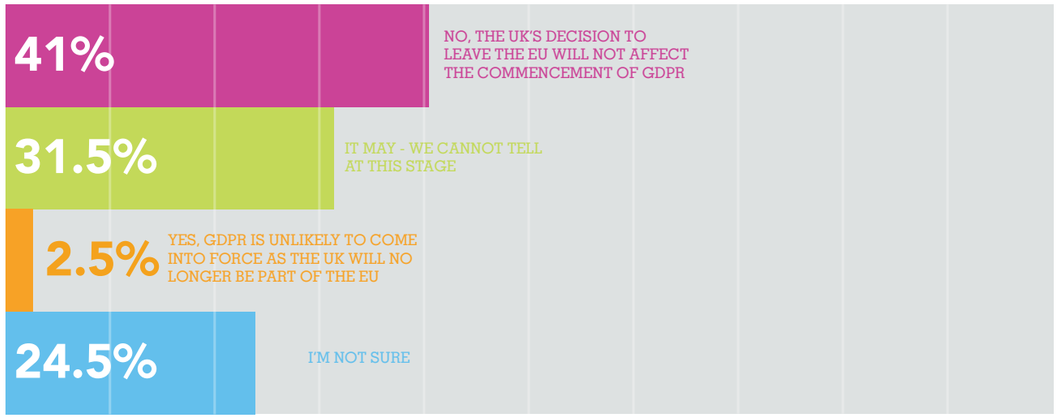


The Ambivalence of Brexit

A key objective of GDPR is to create consistency across the EU to ensure the protection of its citizens' personal data. Whilst the regulation aims to provide a benchmark for member states to work against, provisions have been made to allow local conditions and additions to requirements. This however, has brought into question the extent to which GDPR will affect the UK due to Brexit.

Payroll professionals are confident that the enforcement of GDPR will go ahead despite the political landscape, and 42% are in agreement that the UK's decision to leave the EU will not affect the commencement of GDPR. Most positively, there is hope that there will be 'a trade arrangement where GDPR applies fully to the UK, thereby encourage the industry to follow in the footsteps of EU best practices.

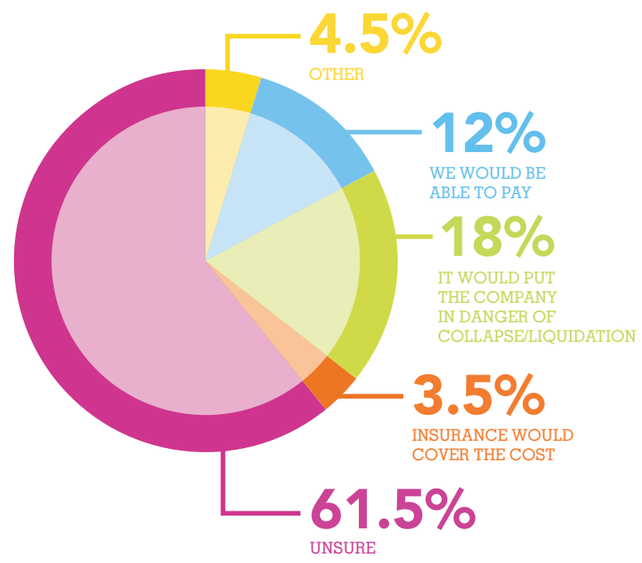
Do you think it likely that Brexit negotiations will impact GDPR in the UK?



This positivity and proactive attitude is reassuring as the UK Government are actively working towards implementing the Data Protection Bill, which will enshrine GDPR into British Law. This is due to come into force at the same time as GDPR and modernise the Data Protection Act 1998.

Conclusion

If your company was forced to pay the maximum fine of either 20 million or 4% of its total worldwide turnover for the preceding financial year, what would be the consequences?



Whilst a breach could result in a significant maximum fine of €20 million fine or 4% of global turnover, previous penalties levied by the ICO leads us to believe that the maximum will only be issued in the event of a serious continued breach and complete disregard for data privacy regulation.

Although this will help to ease the degree of fear across the payroll industry with over 60% of respondents unsure of how this could affect their organisation, it does not give organisations licence to be lackadaisical in their approach to data protection.

Now we are in May with the deadline looming, evidence shows that many payroll functions will adhere to GDPR regulation, however the results suggest that their wider organisations and supplier networks still has much work to do.

Organisations must also take greater ownership of their role to ensure that all functions have adequate training, and to make payroll and HR specific courses available so that they can be confident that the actions taken are correct and will help to protect the business' interests.

With the positive impetus the research has shown, the practical approach payroll professionals have shown towards GDPR and data protection must continue into the future beyond May 2018 to ensure that we continue to lead the industry and embrace change.

Next steps:
With an abundance of confidential personal and financial data, protecting the effectiveness of payroll is central to a business running smoothly. Payroll suppliers following industry best practices should:

- Have an in-house GDPR/data protection champion team to implement existing and new requirements
- Have appropriate information security processes that show commitment to data protection
- Have well documented policies and procedures that are available on request, including what to do in the event of a data breach

Global Payroll Association

Sponsored by

A more human resource.℠