computing research

RESEARCH PAPER

GDPR – this time it's personal

Imminent EU data privacy and protection legislation has major implications for both the business and supporting IT systems - are you ready to comply?

July 2017

Sponsored by IBM

CONTENTS

Executive summary

The EU General Data Protection Regulation (GDPR) has strict requirements when it comes to what qualifies as personal information and how that data should be collected, stored, protected and managed, with implications for both data governance specialists and wider IT and storage management teams in organisations across the board.

In this research paper we look at how aware of impending GDPR legislation enterprise IT professionals are, the scope of the regulation and how it applies to the management and operation of their IT systems and data storage platforms. We also look at how prepared those teams are to cope with GDPR, their confidence levels, how the process is being managed and practical steps that organisations can, and should, be taking to ensure GDPR compliance in the few short months left before it comes into force.

Hailed as "the most important change in data privacy legislation in 20 years", the General Data Protection Regulation (GDPR) is an EU initiative which, from the 25th May 2018, will harmonise data privacy and protection laws across Europe. It will also extend the reach of those rules to any business wanting to trade with companies and private consumers within the EU - so no Brexit loophole for those in UK! Moreover, GDPR introduces measures designed to protect privacy in data-driven global markets where personal data has become a highly valuable commodity, and it's the implications of these which are of most concern to companies and their customers everywhere.

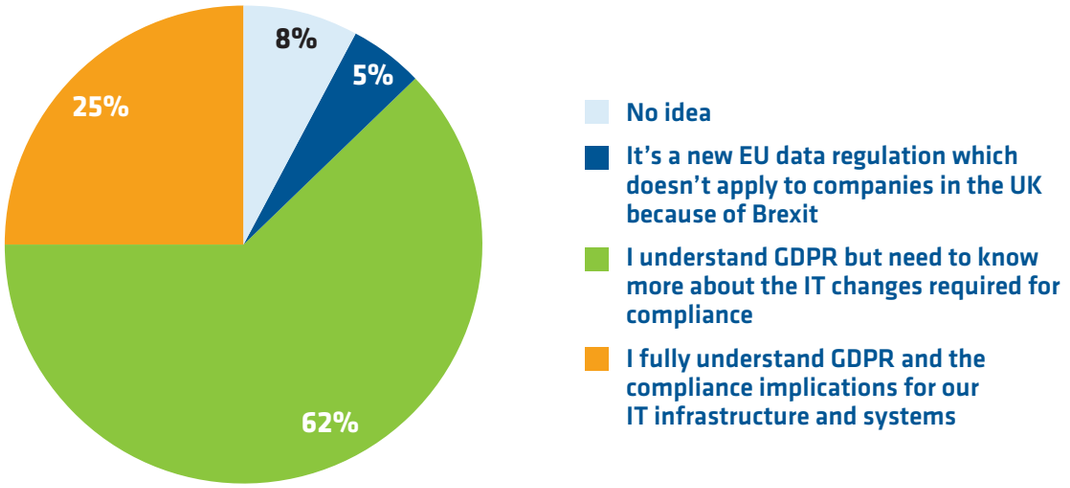
On your marks, set...

Much of the publicity and discussion in the run up to GDPR has been around the threat of huge fines for non-compliance which can be up to 4% of global turnover or €20 million, whichever is greater. However, rather than incentivise those responsible for data privacy and security to find out more about what GDPR entails and do something about it, many appear to be in denial about compliance and its implications for IT in their organisations, as illustrated by the results of a recent online survey of Computing subscribers.

Conducted less than 12 months ahead of the date on which GDPR comes into force, respondents to the Computing poll were selected for their involvement in IT infrastructure planning, management and governance across a broad range of industries. When asked about their understanding of GDPR and its implications for enterprise IT, however, barely a quarter (25%) claimed to be fully up to speed with the impending legislation, while 5 percent thought (wrongly) that it didn't apply to them because of the Brexit vote.

A worrying, 8 percent admitted to having no idea as to what GDPR was all about (Fig. 1).

Fig. 1 : What is your understanding of GDPR and its implications for enterprise IT?



On a more positive note, the majority of respondents (62%) claimed to understand GDPR but felt they needed to know more about the IT changes required for compliance. Given its complexity this is understandable but still of concern given the short run up to implementation in May 2018 which leaves little time for planning, let alone action to change business processes and supporting IT systems. All the more so given that those changes have the potential to be considerable and far reaching.

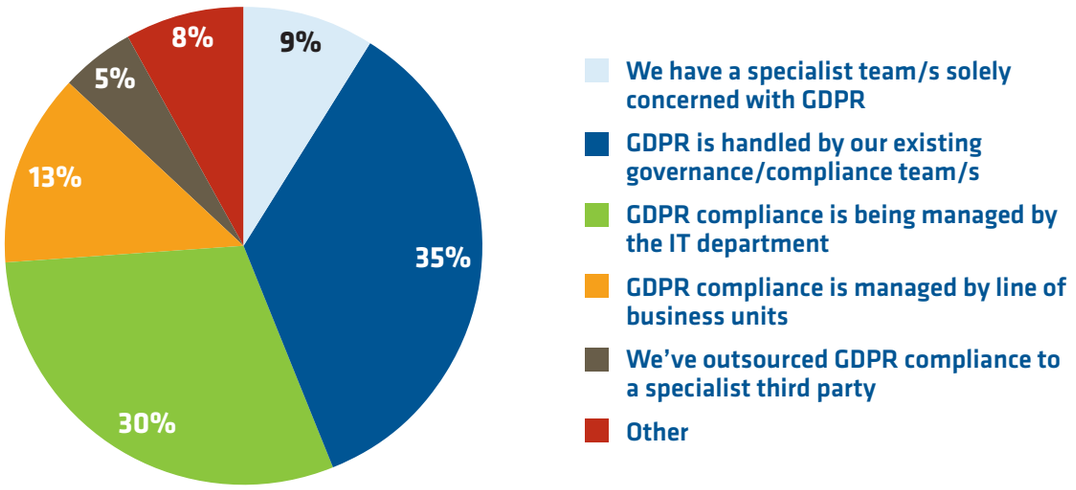
Look beyond the eye-watering fines for noncompliance, for example, and you discover that GDPR requires organisations to be much more transparent about the personal information they collect plus a lot clearer when asking for consent as well as stricter when it comes to what can and can't be stored. Data protection by design is a key tenet of the new regulation and few systems are likely to meet the requirements without at least some reworking. In some cases starting over may be the best way forward but time is short and that may not be a practical option.

Planning to fail

Some of the requirements of GDPR can be met quite easily, such as updating wording on websites and in contracts and terms and conditions although, given the scope of GDPR, this could still take a lot of time and manpower to complete. Moreover, companies should not assume that they will somehow comply just by making their terms and conditions easier to understand as existing privacy measures for compliance with the Data Protection Act (1998) in the UK or the existing EU Data Protection Directive are unlikely to cover every aspect of GDPR and will still need to be thoroughly reviewed.

A great deal of planning is, therefore, required together with continued oversight of the implementation processes all the way up to the cut-off date for GDPR and beyond. At the very least companies should be in the planning phase and, as can be seen in Fig. 2, it certainly looks as though the majority are, at least, taking the task seriously

Fig. 2 : How is GDPR compliance being managed within your organisation?



Some 9 percent of respondents to the poll said they had formed a specialist team solely to handle GDPR compliance with just over a third (35%) handing the task over to established governance/compliance teams well placed to understand and manage the process.

A large number (30%) of those companies surveyed, however, were leaving it to the IT department which, given the need to look at business procedures, staff training and other measures beyond IT, could still lead to compliance problems. Likewise, 13 percent were charging line of business managers with GDPR management where those involved may not appreciate the extent of the IT changes involved or the timescales required to implement them.

There were also some interesting remarks made by the 8 percent ticking 'Other' in answer to this question. Most of these confirmed that nothing much was being done about GDPR compliance in their organisations while others merely assumed it was being addressed in some manner or another. One, clearly overworked, respondent claimed it was all down to them, typing 'Just me' in the comment box!

Personal by any name

In terms of the practical steps needed to get ready for GDPR, one of the most fundamental will be to investigate the way in which applications collect and process personal data and, in all probability, modify the procedures involved to respect the new rules. That, in turn, will require interfaces to be re-designed and processing logic to be restructured to make sure users understand what personal data is being collected and for what purpose.

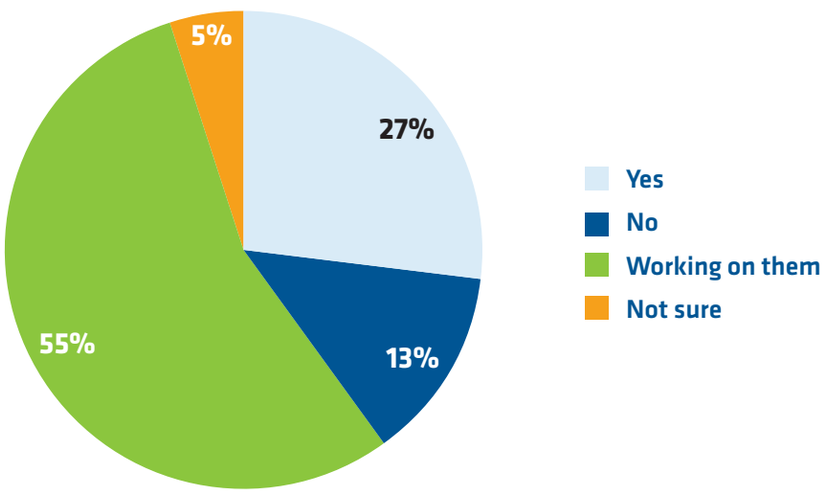
Additional controls to insure consent is explicit rather than just assumed will also be required and not just across in-house developments, but packaged software and hosted services where the necessary updates may have to come from the providers involved. A requirement that not only adds to the complexity of managing GDPR compliance but leaves organisations dependent on those service providers to deliver the goods and do so before the May 2018 deadline.

Some of the organisations polled claimed to be exempt because they didn't process personal data at all, but the definition of personal data is also being widened by GDPR and some care is needed. Things like IP addresses, for example, are now included as they can, in theory, be associated with an individual. Only two survey respondents were aware of this with general confusion as to what is and isn't personal as far as GDPR is concerned. In particular so-called pseudonymized data, a new concept in European data protection law where identifying information is removed and stored separately.

Different to anonymization - where personal information is stripped out and discarded - pseudonymization is an attractive option as, in some situations, it allows organisations to process data for a purpose other than that for which it was collected. However, care is again needed as it doesn't remove the need to protect the identifying information itself, which is still subject to GDPR rules. Plus it gives rise to a number of other very specific requirements, further muddying the data protection waters.

The amount of work needed simply to comply with these and other rules around the new personal data definitions of GDPR is likely to be huge. Added to which time is running out with barely more than a quarter of respondents (27%) confident that they have the necessary policies and processes in place to both identify personal data as defined by GDPR and control when and how it should be collected, protected and stored (Fig. 4)

Fig. 3 : Do you have policies and processes in place to identify personal data as defined by GDPR and when and how it should be collected, protected and stored?



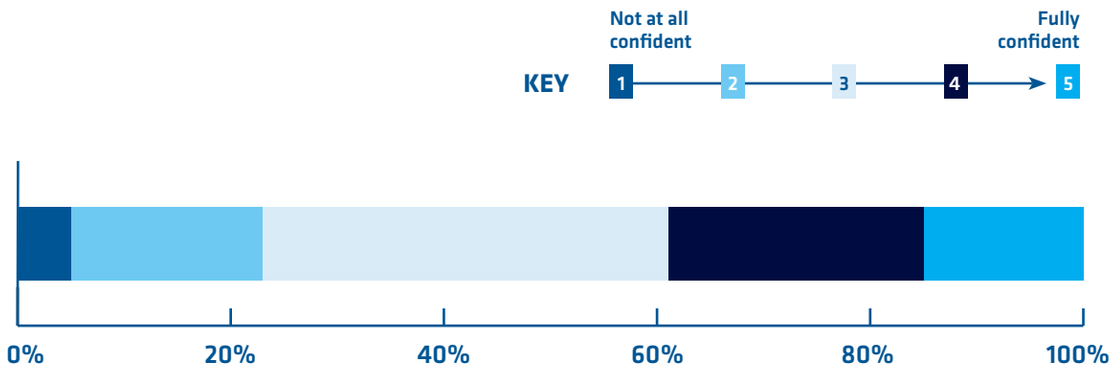
The bulk of respondents said they were working on it (55%) but that still leaves 13 percent apparently with no GDPR compliant policies and processes at all and a further 5 percent not sure which, in all probability, puts them in the same boat. Plus there's no guarantee that those working on GDPR measures now will be ready in time.

The data sprawl effect

Compliance with new privacy rules when collecting and processing data is far from the only headache to come from GDPR. At the other end of the pipeline the ability to fully delete personal data and expunge every possible copy when required takes on a whole new level of importance thanks to the 'right to be forgotten' soon to be enshrined in EU data law.

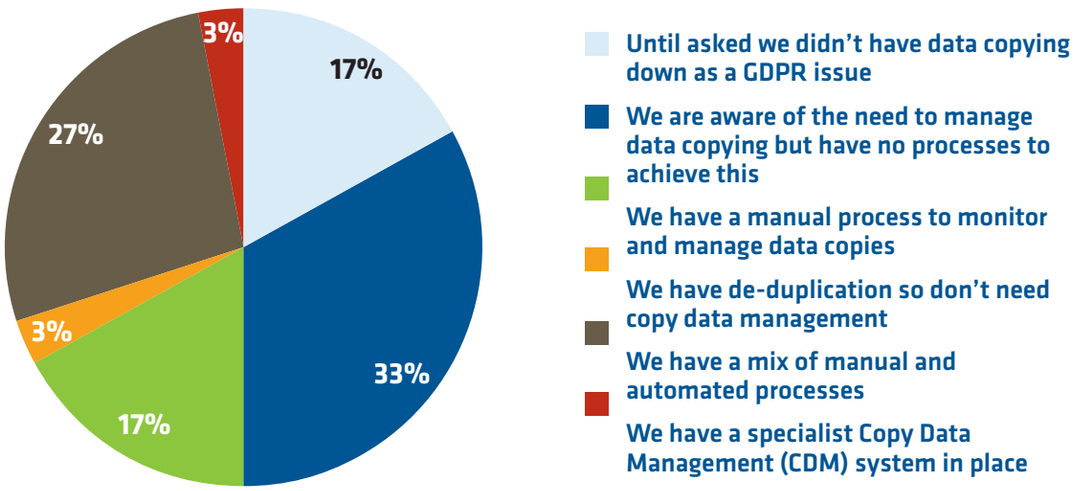
Not only does this call for new interfaces and processing rules to seek out and delete personal data on demand, but for a long hard look at how data and data copying in particular, is managed within an organisation. That's because most will routinely copy and move data around their infrastructure and do so for a variety of valid reasons, such as to archive old files or provide disaster recovery backups, for example, or to allow applications to be developed and tested without compromising production systems. Whatever the reason, however, this kind of data sprawl can cause real problems when it comes to ensuring proper deletion of data for GDPR compliance. Indeed, just tracking down and identifying data copies, could well be an issue for many, as the graph in Fig. 5, below, confirms.

Fig. 4 : How confident are you of the whereabouts of every copy of every bit of data in your organisation?



Asked to rate their ability to locate every copy of a particular piece of data in their organisation just 15 percent of respondents were confident that this would be possible. At the other end of the scale only a tiny 1 percent indicated no confidence at all in their ability to locate copies, leaving the majority more or less equally spread between the two extremes and all likely to struggle when it comes to this aspect of GDPR compliance. All the more so in the light of the low priority, seemingly, afforded to copy data management (CDM) and the use of specialist tools to help support this function within the organisations surveyed (Fig. 5).

Fig. 5 : Which of the following describes the approach taken by your organisation to copy data management?



Asked specifically about their approach to the management of data copies, 17 percent of companies said they didn't have it down as a GDPR issue while a further third (33%) knew they should be doing something about it, but hadn't. Just over a quarter (27%) had at least a mix of manual and automated processes but, given the need to manage copies across unstructured as well as conventional structured data sources, on premise and in the cloud there's a high probability of these failing to provide the comprehensive cover GDPR requires.

Only 3 percent said they employed specialist CDM tools and it was a similar picture, again, when it came to copying data for backup, archiving and disaster recovery. Indeed two thirds (6%) of those asked about this had done little or nothing to review or modify backup, archiving and DR provision in light of GDPR.

A belt and two braces

Given the general lack of preparedness for GDPR highlighted by the Computing poll, non-compliance and breaches would seem inevitable, giving rise to final thoughts as to what the consequences might be and the best way to mitigate against them.

The general consensus amongst industry experts is that large fines are unlikely to be handed down straight away. Especially for simple non-compliance episodes, for example as a result of complaints being made by individuals or failures being reported as part of audit procedures. The bad news is that where personal data is lost or compromised, exemplary action will almost certainly be taken which, in the light of a growing number of cyber-attacks involving the misappropriation of personal data, makes encryption very much a necessity. Moreover, organisations should seriously consider applying encryption both at the application level, where data is collected, and at the hardware level where it's stored.

Only 18 percent of companies polled said they did both, leaving no room for complacency when it comes to providing this kind of belt and braces protection. Moreover, while the majority of companies will have a mixed vendor storage estate with varying capabilities when it comes to encryption, that's not a particularly difficult problem to surmount given the advent of Software Defined Storage (SDS) solutions able to apply uniform encryption policies across heterogeneous storage platforms and technologies.

The same technology can also be used to enforce policy-driven data placement with the most sensitive data, for example, directed to the most heavily protected storage platforms.

Bear in mind too that while encryption everywhere and policy-driven data placement are unlikely to stop the EU authorities taking action when serious GDPR breaches occur, they will help prevent personal data being compromised and minimise consequential loss in the event of a related cyber-attack. Added to which evidence of having implemented such measures could, in turn, go some way to avoiding the really punitive fines threatened by the new regulation.

Conclusion

GDPR is coming and coming all too soon but, as the survey behind this research paper shows, levels of preparedness vary enormously. Less than a year away from the new EU regulation becoming law some organisations have quite clearly failed to give the matter any thought while others have stalled at the planning stage. On the plus side a good number have made changes and are confident of compliance by the due date but, for most, it's a work in progress and a race against the clock.

For those still working towards compliance a clear strategy for managing the collection, storage and protection of personal data as defined by GDPR is needed both at the business level and across the entire supporting IT infrastructure. Moreover, companies need to pay close attention to the wider definition of personal data along with the need for explicit consent to collect it and the entitlement enforced by GDPR to have that data deleted under the right to be forgotten.

Copy data management, in particular needs to be reviewed and better managed as do backup, archiving and disaster recovery systems. Wider use of data encryption and enforcement across heterogeneous storage networks should also be considered if only to provide a safety net when data breaches occur, as they inevitably will.

About the sponsor, IBM

IBM offers comprehensive solutions, services and expertise to help support your journey to GDPR readiness.

Two aspects of GDPR legislation directly touch storage systems and data management software:

1) Encryption of processed personal data, which calls for media-level encryption of data at rest, besides application-level encryption
2) Controlled data placement and tracking of physical copies in a central repository, or copy data management

IBM has always been a front-runner in encryption, leading the field long before GDPR and now applying mature technology and solutions to tackle this new requirement.

IBM's Copy Data Management solution manages the creation and use of copy data across your local datacentre storage infrastructure, hybrid cloud and off-site cloud infrastructure. Copy creation (snapshots and replication) is automated and application-aware; data consumers can use the self-service portal to create the copies they need; copy processes and work flows are automated to ensure consistency and reduce complexity.

IBM's Copy Data Management solution rapidly deploys uniquely as an agentless VM for faster time to value.

Both are served by IBM's Spectrum Storage Software.

For more information:

Visit: www.ibm.com