5 Oracle Perspectives on GDPR

ORACLE

Contents

What is GDPR? The EU General Data Protection Regulation Explained

By Alessandro Vallega, Security and GDPR Business Development Director, Oracle EMEA

The EU General Data Protection Regulation (GDPR) came into effect on 25 May 2018. For those still getting to grips with what it means, let me answer some frequently asked questions.

What is GDPR?

The EU General Data Protection Regulation (GDPR) came into effect on 25 May 2018. It applies to all organizations inside the EU and any outside who handle and process data of EU residents. It is intended to strengthen data protection and give people greater control over how their personal information is used, stored and shared by organizations who have access to it, from employers to companies whose products and services they buy or use. GDPR also requires organizations to have in place technical and organizational security controls designed to prevent data loss, information leaks, or other unauthorized use of data.

Why is GDPR being introduced?

The EU has had data protection laws in place for over 20 years. However, in that time, the level of personal information in circulation has grown dramatically, and so have the different channels through which personal information is being collected, shared and handled. As the volume and potential value of data has increased, so has the risk of it falling into the wrong hands, or being used in ways the user hasn't consented to. GDPR is intended to bring fresh rigour to the way organizations protect the data of EU citizens, while giving citizens greater control over how companies use their data.

What should organizations do to comply with GDPR?

GDPR does not come with a checklist of actions businesses must take, or specific measures or technologies they must have in place. It takes a "what," not "how" approach, setting out standards of data handling, security and use that organizations must be able to demonstrate compliance with. Given the operational and legal complexities involved, organizations may want to consult with their legal adviser to develop and implement a compliance plan.

For example, while GDPR strictly speaking does not mandate any specific security controls, it does encourage business to consider practices such as data encryption, and more generally requires businesses to have in place appropriate controls regarding who can access the data and be able to provide assurances that data is adequately protected. It also states businesses must be able to comply with requests from individuals to remove or amend data. But it is up to organizations how they meet these requirements and ultimately it is up to them to determine the most appropriate level of security required for their data operations.

What are the penalties for not being compliant with GDPR?

If organizations are found to be in breach of GDPR, fines of up to 4% of global annual revenue or €20 million (whichever figure is highest) could potentially be imposed. Furthermore, given how critical personal data is to a great many businesses, the reputational damage could be even more significant, if the public believes an organization is unfit to control or process personal information.

Who needs to prepare for GDPR?

Any organization based inside or outside the EU that uses personal data from EU citizens, whether as the controller of that data (such as a bank or retailer with customer data) or a third party company handling data in the service of a data controller (such as a technology company hosting customer data in a data centre), depending on their respective roles and control over the data they handle.

What personal information is covered by GDPR?

GDPR is designed to give people greater control over personal information which may include direct or "real world" identifiers, such as name and address or employment details, but may also include indirect or less obvious geolocation data or IP address data which could make a person identifiable.

Is GDPR bad for businesses?

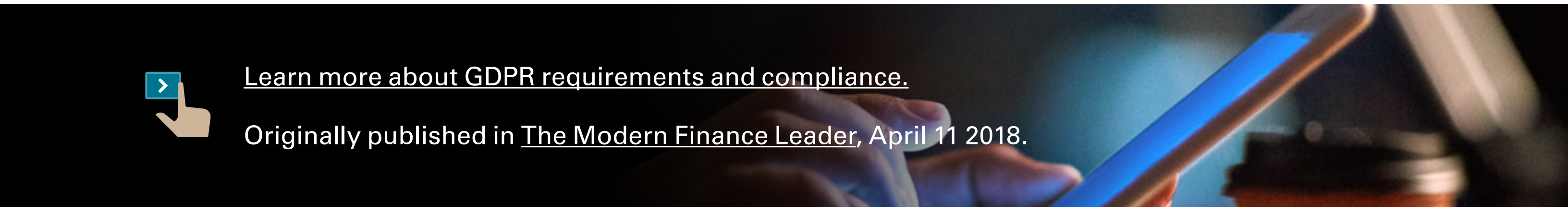
Complying with any new regulation may bring additional work and expense, but GDPR also gives organisations an opportunity to improve the way they handle data and bring their processes up to speed for new digital ways of working. We are living in a data-driven economy. Organizations need to give consumers the confidence to share data and engage with more online services. Following the requirements of GDPR can help in that regard.

Who should be in charge of GDPR?

GDPR compliance must be a team effort. It is not something that can be achieved in, or by, one part of the organization. Ultimately, its importance is such that CEOs should be pushing their teams and appointed owners across the business to ensure compliance. Almost every part of a business uses and holds data and it only takes one part of the business to be out of alignment for compliance efforts to fail.

How can Oracle help with GDPR compliance?

Oracle has always been a data company and takes very seriously our role in helping organizations use their data in more effective, more secure ways. We have more than 40 years of experience in the design and development of secure database management, data protection, and security solutions. Oracle Cloud solutions are used by leading businesses in 175 countries and we already work with customers in many heavily regulated industries. We can help customers better manage, secure and share their data with confidence.



Learn more about GDPR requirements and compliance.

Originally published in The Modern Finance Leader, April 11 2018.

GDPR: What should CFOs be doing about new compliance rules?

By Dee Houchen, Senior Marketing Director, ERP/EPM, Oracle

If there's one aspect of GDPR that is likely to grab the attention of any CFO it is the potentially eye-watering fines organizations could be hit with if they are found to have breached the new data protection regulation.

As the gatekeepers for the company finances, and often the boardroom owner of risk management, what CFO isn't going to sit up and take notice when the sums involved could be up to €20 million or four per cent of annual revenue (whichever is larger)?

However, CFOs shouldn't just be sitting in fear, hoping the day never comes when they have to pay out such a fine. There is much they should be doing to ensure their organization is prepared, starting with participation in cross-organization planning and an audit to ensure they understand the types of personal data that is being processed within their organization, where it resides, who has and needs access to it, and how their processing activities are affected by GDPR.

For CFOs this process should include reviewing what data they hold, create, and preside over with finance. That could include employee information such as payroll or salary data, as well as data held by suppliers, contractors, and outsourcers who may report into the CFO. CFOs should be reviewing the contracts they have in place with those supplies to ensure they are fit for GDPR.

Another key role of the CFO is ensuring the organization's compliance efforts are properly funded and resourced. In order to do that, the CFO must understand the cost of compliance and where investment needs to be made in order to ensure it. This may well involve additional budgets for teams such as IT, which will certainly be at the sharp end of GDPR compliance, ensuring data is protected and structured in such a way that the organization can respond to requests from data subjects to provide, modify or delete data.

However, to prevent the cost of compliance spiralling, CFOs will also need to ensure they understand which measures are essential and should maintain a cautious cynicism towards some of the requests for additional budget that may cross their desk. "This is needed for GDPR compliance" could be used to push through any number of purchases that may not be essential. This is all the more reason why the CFO needs to ensure they are on top of GDPR and what it means.

There are clear opportunities which can arise in a data-driven economy for any organization that improves its data handling and usage practises. CFOs should therefore be weighing the potential upside of GDPR and the way it could help them unlock valuable insights, improve operations, know their customers better, and become more responsive to risks and opportunities.

However, as a final consideration, CFOs may also choose to plan for the potential downside. For all the planning there may be some organizations who are caught out and hit with fines—or potentially lawsuits. While they should of course do all they can to ensure that is not their organization, some CFOs may still choose to plan for the worst and put aside funding as an insurance policy against those eye-watering fines.

Learn more about how to comply with GDPR regulations.

Originally published in The Modern Finance Leader, April 30, 2018.

Life After GDPR: Why CEOs Need to Lead from the Top Down

By Alessandro Vallega, Security and GDPR Business Development Director, Oracle EMEA

GDPR is now in effect, but companies across every industry have been under pressure to become compliant since the law was introduced in 2016. Some responded by changing their IT processes, others placed the burden on their legal team, but others only began to adapt in earnest once the 25th May deadline was just around the corner.

Data protection must be treated with the right level of gravitas. It might be tempting to think you can steer clear of regulatory issues as long as you are not doing anything untoward with people's personal data, but this is short-term thinking. GDPR may only mark the beginning of a global regulatory push to improve data protection, and regulation will only become more demanding.

Real change requires a shift in culture. The way companies govern data has not yet caught up to the way employees use technology, which is why we still see staff taking a lackadaisical approach in many organisations. They save company information to personal devices, use (and sometimes lose) business laptops on the train, and turn to file sharing sites to share sensitive information. All these practices pose a security risk, and they are all too common.

The cost of not complying with GDPR can be significant. Business leaders will be aware of the potential risk of non-compliance (up to 20 million euros or 4% of the company's global turnover) but there are less obvious consequences too. Data breaches must be made public to the supervisory authority within 72 hours once a company becomes aware of them, and the reputational damage that comes with these if the company does not have a good handle on security, has its own cost.

In addition, a supervisory authority has the power to impose a temporary or definitive limitation including a ban on processing, and data subjects have the right to bring claims for compensation.

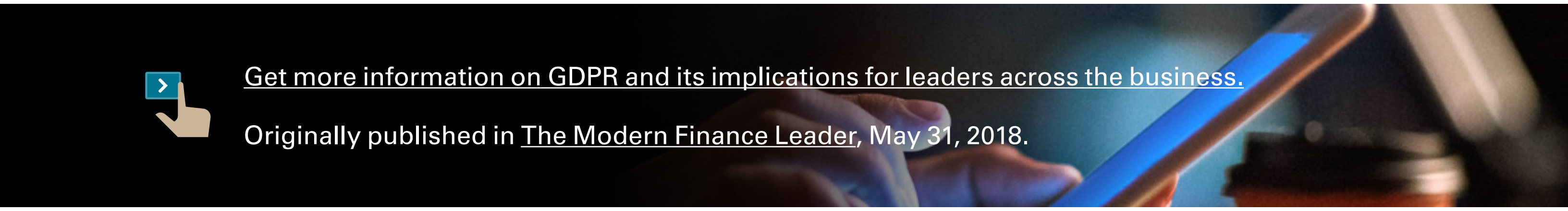
GDPR is a boardroom issue

This makes GDPR a boardroom issue, but this does not mean companies can just appoint someone to take charge of compliance and let them run with it. With an imperative this important, the bucks stops with the CEO.

Business leaders must be figureheads for data protection. For an organisation to manage data more responsibly and stay on top of its data in the long term, it needs buy-in from all staff. Each individual must be accountable for their actions and play their part in compliance, and this understanding must be driven from the top down.

How can business leaders help achieve this? The first step is to make training compulsory. This could include anything from data management training, to workshops on protecting data or even running phish-baiting tests to help employees identify suspicious emails.

Incentives also help drive change. Data protection needs to be as much a part of someone's job as doing their timesheets, so why not reward team leaders who have ensured all their staff have taken the appropriate training, or include security training as part of employee performance objectives? It will ultimately come down to HR, IT or legal teams to develop these initiatives, but the imperative must come from a company's leadership.



Get more information on GDPR and its implications for leaders across the business.

Originally published in The Modern Finance Leader, May 31, 2018.

GDPR: Time to See It as an Opportunity, Not a Chore

By Dee Houchen, Senior Marketing Director, ERP/EPM, Oracle

When many people think of data-driven businesses, the temptation may be to think of major consumer facing websites, online retailers or social media companies. But the reality is, organisations of all sizes, across all sectors are getting closer to their data in order to improve and personalise the customer experience or the way they work, or to transform whole industries or create new opportunities.

The UK's NHS Business Services Authority (NHSBSA) recently uncovered insights in its data that have helped it improve patient care and uncover nearly £600 million in savings. In India, a new crop of financial institutions have reimagined credit checks for the country's unbanked population, assessing people for small business loans based on an analysis of their social media data.

General data protection regulation (GDPR)

But while the rise of data-driven business models and organisations has made life better for many people it has also raised concerns about how our data is collected, used and managed. This is the major motivation behind the EU's General Data Protection Regulation (GDPR), which aims to raise the standard of data protection in modern businesses and provide consumers with greater transparency and control over how their personal details are used.

New regulation can feel like a burden, but organisations should see GDPR as an opportunity to put in place processes and protections that them the ability to make the most of their data, and give consumers the confidence to keep sharing their data with the organisation.

To paraphrase TechUK's Sue Daly, who joined a panel of data experts to discuss GDPR on the Oracle Business Podcast, we are moving to a world driven by connected devices, the Internet of Things, and new forms of artificial intelligence, and to succeed with these technologies businesses will need the public to trust their approach to managing data.

Using transparency to differentiate your business

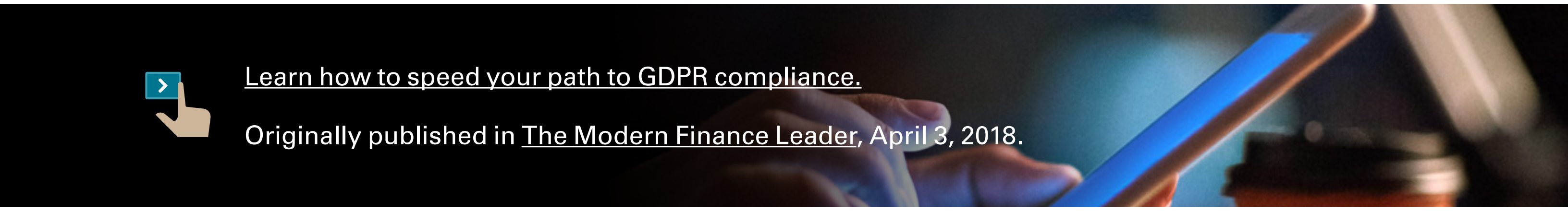
Transparency can also be a valuable differentiator. Telefónica, one of Spain's largest telecoms operators, provides advertisers and content providers with anonymous audience insights so they can better tailor their content to individual users. In the interest of transparency, the company publishes the customer data it sends to third parties and gives people the option to opt out of sharing their personal details. Telefónica's data-driven approach has taken it from strength to strength. Despite currency pressures and a difficult market, the company posted a 23% rise in profits at the end of February 2018.

The exchange is mutually beneficial, as it allows the operator to curate the right content for its own customers and provide them with a better user experience. Telefonica has now captured 40% of Spain's lucrative digital media and advertising market. By comparison, most telcos only contribute to roughly 2% of the advertising value chain, according to Analysys Mason.

This perfectly illustrates why businesses should not just wait for GDPR to arrive and do the minimum required in the name of compliance. With major changes come major opportunities, but only for organisations that are proactive and look beyond the short-term regulatory burden.

Nina Monckton, Chief Insight Officer at the NHSBSA, who also joined the Oracle Business Podcast panel to discuss GDPR, had this to say: "The trick is to help people see how their data helps your business improve their quality of life. For example, when you explain that their anonymised details can help researchers find cures to serious illnesses, the benefits become much more tangible."

By acting now, companies will guarantee their approach to data is compliant and gain the confidence to continue delighting customers with better, more personalised services.



Learn how to speed your path to GDPR compliance.

Originally published in The Modern Finance Leader, April 3, 2018.

GDPR Compliance and the Cloud: Help or Hindrance?

By Paul Flannery, Senior Director, EMEA Business Development, Oracle

Organisations are currently faced with the question of how to approach the General Data Protection Regulation (GDPR), the new legislation which sets out to harmonise data protection across the European Union. Rather than be seen as a compliance burden, GDPR should be seen as one of the best opportunities to deploy long term technology investment to unlock true digital transformation.

Whilst the regulation itself is limited to the processing of personal data, the EU's interpretation of what that actually constitutes is broad. Essentially, any data relates to an identifiable living human, including something as disconnected as an IP address that can identify a specific user's device, is regarded as within the scope.

The extended scope of the legislation doesn't end there. For example, organisations are obliged to take into account the "state of the art" in cybersecurity—yet specific technologies, controls or processes beyond that phrase remain unmentioned, leaving a high degree of risk assessment and subsequent judgement to be applied by the organisation itself.

The timescale for addressing compliance is tight too, and any organisation of sizable scale will find it difficult to even understand what data they have in the first place and assess its sensitivity.

The cost of non-compliance is what has brought GDPR to the attention of boardrooms not just in the EU, but globally. The potential magnitude of fines are significant (4% of an organisation's global revenue, or €20 million, whichever is greater), as well as the potential reputation damage that may result from non-compliance with the new mandatory breach notification requirements.

The inevitability of cloud computing

The cloud, whether it's public or private, Software-, Infrastructure- or Platform-as-a-Service, can mean different things to different people. The overall understanding across the majority of industries is somewhat immature, specifically with regards to compliance and security. Yet the journey to the cloud is happening regardless, and without proper security in place, that inevitable shift will arrive in the form of shadow IT, bringing with it unnecessary risk exposure.

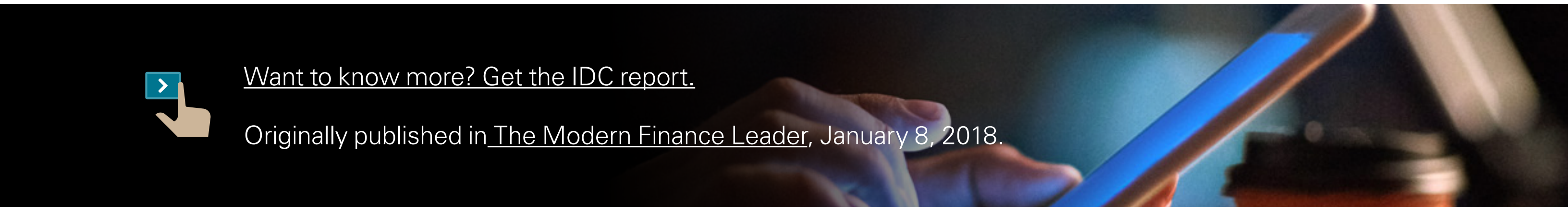
Generally speaking, there are substantial benefits in moving to the cloud, such as enhanced security capabilities that go beyond what would be affordable for most organisations in an on-premises environment. However any move to the cloud needs to be carefully planned and architected properly; with the new legislation approaching, the consequences of getting it wrong are significantly increasing.

GDPR compliance is a long term commitment, and investment in implementing a cost-effective supporting infrastructure will prove to be valuable in the years ahead. It might even represent one of the biggest opportunities to accelerate digital transformation in recent years.

It places focus on good data management, with benefits to organisations ranging from increased security and operational efficiency, to improved customer service and corporate reputation. For example, one of the key legislative requirements is to be able to provide any individual with every piece of data an organisation holds on them, including all data records and any activity logs that may be stored.

On the one hand, this places significant technology requirements that would only be possible with the simplification and standardisation of complex IT environments. Yet on the other, the potential for converged data of that quality from a business or marketing perspective is substantial, and brings with it a wealth of possibilities.

Earlier this year, IDC gathered CIOs and CSIOs from enterprises across EMEA, to gain insight into how they are approaching GDPR in light of current cloud adoption and security requirements. Their resulting report, "Does Cloud Help or Hinder GDPR Compliance?" summarises discussions from events in France, Italy, Morocco, Spain, South Africa, Sweden and Switzerland. It not only flags the many potential benefits of compliance, but also sets out IDC's simple but effective technology framework to help organisations focus on the particular requirements of GDPR, and select the right technology for the job.



Want to know more? Get the IDC report.

Originally published in The Modern Finance Leader, January 8, 2018.

ORACLE CORPORATION

Worldwide Headquarters

500 Oracle Parkway, Redwood Shores, CA 94065 USA

Worldwide Inquiries

TELE + 1.650.506.7000 + 1.800.ORACLE1
FAX + 1.650.506.7200
oracle.com

CONNECT WITH US

facebook.com/oracle youtube.com/oracle linkedin.com/company/oracle twitter.com/oracle

Integrated Cloud Applications & Platform Services

Oracle is committed to developing practices and products that help protect the environment

ORACLE®