The race is on to get ready for GDPR next year. In this 16-page buyer’s guide, Computer Weekly looks at how to deal with data under the regulation, how compliance will affect businesses, and what organisations should do to prepare.
Most organisations will now be aware that the EU’s General Data Protection Regulation (GDPR) is already law and will be enforced from 25 May 2018. All businesses that currently process and store data regarding EU citizens should review the need to continue doing so. Where the activity is to be carried on, then the processes and applications involved should be checked for GDPR compliance.

Perhaps the most important thing to note is that GDPR is as much about process administration as it is about data security. The mass of organisations that process some personal data are still considering how to respond to the regulations.

The primary target of GDPR is undertakings; the processing of personal data relating to EU consumers as part of an economic activity. An undertaking may not be your organisation’s primary activity, but a worthwhile one that you want, and as such must continue compliantly.

**Brexit will make no difference**

The UK aims to cease being an EU member on 29 March 2019. UK-based organisations will therefore face a 10-month period of compliance enforced by the EU itself. However, the terms of the General Data Protection Regulation will pass into UK law unless the government specifically repeals it.

GDPR enables data subjects to take back control of their data, so it would be hypocritical of Brexit advocates, who used the same slogan, to suggest UK citizens should have less control of
their own data than their EU counterparts. Furthermore, the UK’s Information Commissioner’s Office took a lead in defining GDPR and, as it stands, supports its core principles.

**Tool up for GDPR**

With enforcement of GDPR looming, almost every IT supplier has something to say about it. This ranges from the highly relevant, such as data processors stating that their services and applications are compliant, to vague buy-me-too claims from suppliers with only peripheral relevance. The lists are long, so we have only included a few examples in this buyer’s guide, mainly suppliers that provided input. The first stop should be to consult the suppliers your organisation already works with. Few organisations will be starting from scratch.

Data protection laws have been in force in most EU countries for about 20 years. Many will have the basics in place. Many will also be complying with other regulations and standards which overlap with GDPR, for example the Payment Card Industry Data Security Standard (**PCI DSS**). For some, this will amount to what Quocirca terms a compliance-oriented architecture (COA). If this is the case, your organisation has a good starting point, and may not need many adjustments to comply with GDPR.

Standards organisations are also providing guidance. The ISO27000 forum provides a mapping of GDPR to the ISO27001 data protection standard. In the UK, the British Standards Institute (BSI) has a new edition of BS-10012, a framework for a personal information management system that is GDPR compliant.

Privacy by design and by default has a concept of minimisation at its core. This is that only the minimum amount of data is held to complete the task at hand. The first activity should be to identify all the undertakings an organisation has that involve the processing of personal data regarding EU citizens, and assess whether that data really needs collecting, storing and processing in the first place.

Where the processing of personal data is deemed unnecessary, it can be stopped altogether – and historic data deleted. For example, market research data may include the names of individuals where their company name will suffice, or home IP addresses may be collected unnecessarily by an internet of things (IoT) application. Stop the collection of personal data and the applications and processes become out of scope for GDPR compliance.

If it is concluded that the data processing must continue, the risk may be such that a data protection impact assessment (DPIA) needs to be conducted.

There are consultancies that specialise in data security, protection and compliance. For example, the
NCC Group and Coalfire both help with DPIAs and provide virtual chief information security officers that can act as data protection officers if your organisation requires one but lacks the in-house skills. Storage suppliers have also geared up. Veritas, for example, offers a GDPR Readiness Assessment.

**Outsource data processing**
Relevant data functions can be outsourced to data processors that will ensure GDPR administrative and data security compliance. For many organisations that have cobbled together in-house systems, now may be the time to bite the bullet and move processing to a third party.

The terms and conditions of agreements should be scrutinised to ensure that, should a data leak or administrative shortfall occur due to the processor’s negligence, then the processor will be liable for the penalties imposed. However, there is a caveat, where access to the processor’s system is required, if there is unauthorised access the fault will probably lie with your organisation (see Access Management, p5).

Many undertakings are all about maintaining a relationship with consumers via email, social media and smartphones. There are
plenty of third-party processors that will take on the task of collecting, storing and processing your data.

Some third-party service providers that don’t sound like IT companies provide relevant services. For example, Just Eat brokers the relationships between restaurants and consumers primarily to collect payments. It can also handle ongoing communication with existing customers, providing information about new dishes, for example. The restaurants do not even need to access the personal data stored by Just Eat’s system, and are therefore out of scope for GDPR compliance – unless they have some other process that collects relevant data.

Online retail involves processing personal data. Again, the whole process can be outsourced. For example, Actinic, one of the suppliers covered in a previous buyer’s guide on e-retail, says its on-demand platform is now fully GDPR compliant for both data security and administration. It also provides a continuous audit trail, including who has access to the system, so in the event of unauthorised access, information is available to support an investigation. In the UK, Sage’s e-commerce platform is based on Actinic.

Direct marketing can also be outsourced to compliant data processors. For example, Marketo’s on-demand platform ensures the safe storage of personal data and enables the compliant administration of campaigns. Customers can use the platform directly or work with Marketo partners, such as UK-based Verticurl, Clevertouch and Bluprint, to run campaigns for them. Marketo provides a full audit trail of who has been accessing the system.

**Access management**

Controlling and auditing who has access to the applications that process personal data is essential. Administrators must be accountable for their actions, and one way cyber criminals gain illicit access to systems is via compromised access credentials. If all processing is outsourced to a single third party then its monitoring of access may be sufficient. However, if you use multiple systems, or run your own, it may be time to use a single sign-on system that enables one-stop provisioning and de-provisioning to multiple applications and maintains audit trails. Identity and access management systems were covered in a previous buyer’s guide.

**Breach detection**

If you have a single undertaking outsourced to a data processor, it should inform you about any data breaches it is responsible for. However, breaches that are due to vulnerabilities of an on-demand service supplier’s platform are rare compared with...
those of in-house systems. If you have monitored access management, unusual activity should be audited and detectable. If you choose to process data in-house, you will need to think about data loss prevention (DLP) systems, to detect and prevent potential breaches.

However, it must be accepted that however systems are run, a breach is always possible. So, for those that consider their undertakings to be high risk, it may be worth considering post-breach detection services from companies such as Recorded Future, Digital Shadows and the emerging UK-based supplier RepKnight.

**Keeping it all in-house**

Some organisations may conclude that the processing of personal data is so core to their business that they want to run the systems themselves. They are then tending to the first extreme described at the start of this article: plans for GDPR should be well underway and an architecture that ensures compliance should be in place.

This will involve technologies such as encryption, tokenisation and DLP. The broad-scope security providers such as Symantec, Trend Micro, McAfee and Forcepoint all provide guidance as to how their product portfolios can support many of the requirements that in-house GDPR compliance requires.

Enforcement of GDPR is little over a year away. However your organisation intends to address the requirements in the interests of your business and its customers, the time to act is now.

Bob Tarzey is an analyst and director at Quocirca.
With just a year until the European Union’s (EU’s) General Data Protection Regulation (GDPR) is enforced, preparations should be at the top of any IT leader’s agenda.

The regulation, which includes mandatory data breach notification, as well as eye-watering penalties for non-compliance, means it is essential to ensure your organisation is compliant, but this is not an easy feat.

At the latest Computer Weekly CW500 Club event, data protection experts shared their knowledge and advice on what the regulation will mean for businesses and how to prepare.

Despite Brexit looming, the UK has committed to implementing the GDPR by 25 May 2018, leaving organisations with little over 12 months to make sure they are compliant.

Those who aren’t yet sufficiently worried about GDPR had better start now, according to Chiara Rustici, an independent GDPR analyst. “You have to own this from the start. Don’t let it hit you when it’s too late,” she said.

Rustici’s key advice for CIOs was to “be in the room from the start”, because every choice that’s made around GDPR affects the IT architecture. “Never let a legal decision be made about the business without you in the room. Please take that seriously,” she said.

Her second message was that GDPR is not an IT governance issue. “If you take it that way, you have to do everything again,” she added. According to Rustici, it’s a three-variable equation. First, you have to understand the business monetisation rules for personal data. “Do we want to own it because we want to sell it
or because we want to license it? Do we need it to optimise our processes, or do we just want to do profiling because we then sell products on the basis of profiling? You need to understand that it is a variable and you need to work out the dependencies,” she said.

The second variable is legal choices. While the regulation doesn’t tell you there’s one specific way of doing things, some choices “have certain effects on what automatic rights the consumer has”.

“Every legal choice that’s made up-front at the start of a journey has an effect on the IT architecture,” said Rustici, which means you need to figure out what the best data infrastructure is as an IT leader. “You have to model the equation so you can feed back the cost to the board. If one legal choice has such a big effect on the IT infrastructure that it makes the product no longer profitable, the board gets a ‘no’ and you need to have that dollar amount of the impact that one legal and business choice has on the IT architecture. Nobody else can do that in the business,” she said.

“You’re not there to tell your legal team what to do, you’re not there to tell the business what to do, but you’re there to show them the dependencies and how much it costs,” she said.

### Like changing a tyre on a speeding truck

Getting to grips with the regulation is key, particularly if you’re a global business, said Monica Cardoso Salgado, senior manager for data privacy and governance at the John Lewis Partnership.

Key questions you have to answer, she said, are around what data GDPR covers. The regulation not only covers organisations located in the EU, but the use of personal data about EU citizens by anyone in the world. If your organisation stores information about an EU citizen, you need to comply, regardless of local laws, or you risk being prevented from trading with the EU.

“Does it cover the data of my EU customers and EU clients? Does it cover the data of the EU citizens that I’ve recruited to work with me in Mexico? Does it cover the data when my Mexican workers are travelling to the EU and use my human resources management tool outside of Mexico?” said Salgado. “The output you can get out of this discussion is infinite, so the extra-territoriality in itself is something massive that needs to be tackled head-on from a strategic standpoint. It’s very easy to go into rabbit holes of discussions that you’re analysing every particular set of data, but it’s more relevant to get a strategic decision about that from the get-go,” said Salgado.

### If your organisation stores information about an EU citizen, you need to comply, regardless of local laws, or you risk being prevented from trading with the EU

If your organisation stores information about an EU citizen, you need to comply, regardless of local laws, or you risk being prevented from trading with the EU.
The regulation, she added, encompasses every part of the business and therefore adds another issue – the change of mentality. “We don’t own the data, we have it on loan. So the idea that we don’t own data is, in itself, a change in mentality,” she said. “How do we put individuals and data first in a world that is evolving with the speed that is unprecedented in terms of data processing, data collection and data management? Where what is common and usual in a year’s time, we haven’t even thought about yet. How do you change a tyre on a speeding truck?”

**The role of the ICO**

However, while it’s a complex issue and one that rightly should be on everyone’s agenda, it is important to place the General Data Protection Regulation into context.

Technology lawyer Dai Davis from Percy, Crow, Davis & Co said while GDPR is an enormous change, with “a hundred times more obligations you have to think about”, the budget of the Information Commissioner Office (ICO) hasn’t increased.

The amount of money information commissioner Elizabeth Denham has to spend on **policing GDPR compliance** has not “in any way, shape or form increased with the amounts of potential wrongs she has to police”, said Davis.

“I’m not saying you can ignore the legislation. However, you have to put it into the context of what you can practically do to comply,” he said.

According to the legislation, a company in breach may be liable for a large fine of up to €20m or 4% of annual worldwide turnover, whichever is larger.
Davis said the reality is that large international companies would probably get away with extraterritorial breaches, despite GDPR being very clear on this. If a company such as Google or Twitter is caught, for instance, is the ICO likely to police it? “How many assets does Twitter have in the UK or the EU? How can [the ICO] possibly enforce any judgement against Twitter?” asked Davis.

However, Rustici said while she doesn’t envision the ICO flying over to the US to do “dawn raids” on Twitter headquarters, for example, the regulation does have implications even for large companies. Not only does she expect class action-style law suits to grow, but the market itself will act as a regulator.

“In many ways, it’s true that the regulator can only do so much and the consumer will be more powerful, but the real clinch and sledgehammer for enforcement is the market,” she said.

**Dealing with suppliers and outsourcing**

Under GDPR, as a company holding personal data on an individual, you as a data controller are liable for any breaches relating to that data. This means it’s your responsibility to ensure that any datacentre or cloud provider you use is adhering to the regulation.

“Essentially, the controller has an obligation to only do business with processors that demonstrate they’re GDPR compliant, which effectively puts the controller in the position where it has to demonstrate compliance to do business,” said Rustici. “You’re only as GDPR compliant as the weakest link in your supply chain.”

While she expects that seals of trust will become the norm in the future, the best you can currently do as a processor is to demonstrate GDPR compliance across the board.

Under the regulation, you have to inform the ICO in 72 hours if you have a data breach. While a supplier or a processor of the data you hold has to assist you in finding out about the data breach, it’s the responsibility of the controller to report it.

Davis said the existing regulation, which was originally written in 1991 by the European Union commissioners, stems from a time when there was less outsourcing, meaning that the GDPR makes it easier. However, he added: “There are some circumstances in which you can rely on the safeness of compliance from compliance outsourcers, which just didn’t exist in the old legislation to a real degree, but there are still issues of non-compliant circumstances.”

From a supplier’s perspective, he said, the legislation can be used to an advantage. “Looking at the question of justification in the legislation, you have to justify GDPR compliance - you can do that through a supplier. A clever supplier can come on and say, ‘This system is GDPR compliant’, and we’re going to use that external third-party compliance as part of the law.”
**AUTOMATED DECISION MAKING AND CONSENT**

The GDPR strengthens the rights and the rules around obtaining consent to gather and use personal data.

The ICO has produced *Preparing for the GDPR: 12 steps to take now* to give organisations a list of the key issues they need to address in their preparations, but for organisations – some of which may have never have had to deal with the issue of data protection legislation – it can be something of a minefield.

By May 2018, businesses will be required to make it easy for individuals to exercise the right of subject access to their data, the right to object to direct marketing and profiling, and to move their data from one supplier to another.

Ideally, individuals should have self-access to the data you keep on them, such as a dashboard where an individual can look up what data the company has about them and what data is transferred to third parties. However, this only applies to raw data.

Another worry is around automated processing – something insurance companies in particular have been very concerned with. But they do not need to worry as much as they have. There is no outright ban on automated decision making, said Rustici.

“The General Data Protection Regulation is not saying you cannot do automated decision making, it’s saying there has to be a human element at some point. Whether that means you have blended automated algorithmic decision making mixed with human, or whether that means you have an appeal system whereby a consumer can say ‘you made this decision about my right to have an insurance policy, I want to contest it’, the choice is yours,” she said.
On your marks, get ready for GDPR

With barely a year until the European Union fires the starting gun on the General Data Protection Regulation, Jim Mortleman looks at what UK organisations should be doing to prepare

On 28 May 2018 the EU’s ambitious General Data Protection Regulation (GDPR) comes into force, with the aim of strengthening data privacy and protection for all EU citizens. The regulation puts individuals firmly back in charge of their personal information and what happens to it. It will fundamentally affect any organisation that stores, processes or handles the personal data of EU citizens – irrespective of that organisation’s size or where in the world it’s based. From sole traders working at home to giant multinational corporations, no one (except law enforcement and intelligence agencies) is exempt. But how well-prepared is the UK?

The regulation is the most far-reaching change to data protection in a generation. It places significant new strictures upon organisations, including having to build privacy into systems by design (and switched on by default); conduct regular privacy impact assessments; implement stronger consent mechanisms (particularly when processing data pertaining to minors); follow stricter procedures for reporting data breaches; and document any use of personal data in far more detail than previously. Organisations failing to comply could face fines of up to €20m or 4% of annual turnover (whichever is greater).

UK firms unprepared for GDPR

There’s little reliable data on UK firms’ level of preparedness for GDPR, but anecdotal evidence suggests it’s nowhere near where it should be, with lack of awareness particularly acute among smaller businesses.
Hazel Grant, a partner specialising in data protection issues at European law firm Fieldfisher, says: “We see a wide spectrum of levels of compliance. If an organisation has been following not only the law but also best practice over the years, GDPR will be less of a shock to the system.

“However, a lot of organisations haven’t really dealt with data protection to date because the risks have been relatively low. Fines have tended to be imposed only for significant data breaches, not for things like failing to do what you say in your privacy notices or not responding to requests as promptly as you’re meant to.

“I couldn’t venture a percentage, but I suspect a huge proportion of UK business is not ready. And if they’re not already complying with data protection law, they’re certainly nowhere near where they need to be.”

Chris Weston, a leading CIO turned independent digital technology adviser, has recently been working mainly with small and medium-sized enterprises (SMEs) in business-to-business sectors. He says among this type of organisation, levels of GDPR awareness, let alone compliance, is woefully low. “Most of the companies I speak to are compliant with the Data Protection Act (DPA), but it comes as a shock when they learn they’re going to have to address data protection issues again in a way that significantly affects not just their technology but their business processes,” says Weston.

**GREATER AWARENESS ESSENTIAL**

While he says IT professionals, particularly those in larger companies, seem to be on top of the issue, Weston believes there needs to be a concerted effort to raise GDPR awareness among the general business community, and especially SMEs. “It’s urgent. I think we should be seeing a campaign of a similar scale to Y2K,” he says.

The reason we’re not, he says, is that the Information Commissioner’s Office (ICO) – which will be responsible for enforcing the GDPR in the UK – simply doesn’t have the resources to mount an awareness campaign of the size and scope needed. “It already seems to be doing a great deal with not very much money, but the government and others should be doing more,” says Weston.

Security expert Brian Honan, who has long advised organisations on data protection issues,
agrees that more effort is needed to raise awareness of GDPR requirements. “Although the ICO has a lot of good material on its website, there’s a lack of education from the government, and that vacuum is being filled by messages that aren’t always particularly helpful,” he says. “In many ways, GDPR in 2017 is what Y2K was in 1999 – not just in terms of urgency and scope, but also in the way everybody is claiming to be GDPR experts overnight, trying to sell technical solutions to what are actually strategic business issues. There’s a lot of scaremongering and FUD [fear, uncertainty and doubt] from IT and consulting firms, talking up the €20m fine and implying it can be avoided if you buy their solution.”

A summary of the Information Commissioner’s Office’s 12-point GDPR checklist

- Ensure senior/key people are aware of GDPR and appreciate its impact.
- Document any personal data you hold, where it came from and who you share it with. Conduct an information audit if needed.
- Review your privacy notices and plan for necessary changes before GDPR comes into force.
- Check your procedures cover all individuals’ rights under the legislation – for example, how you would delete personal data or provide data electronically in a commonly used format.
- Plan how you will handle subject access requests within the new timescales and provide any additional information.
- Identify and document your legal basis for the various types of personal data processing you do.
- Review how you seek, obtain and record consent. Do you need to make any changes?
- Put systems in place to verify individuals’ ages and, if users are children (likely to be defined in the UK as those under 13), gather parental consent for data processing activity.
- Make sure you have the right procedures in place to detect, report and investigate a personal data breach.
- Adopt a “privacy by design” and “data minimisation” approach, as part of which you’ll need to understand how and when to implement Privacy Impact Assessments.
- Designate a Data Protection Officer or someone responsible for data protection compliance; assess where this role will sit within your organisation’s structure/governance arrangements.
- If you operate internationally, determine which data protection supervisory authority you come under.

For more detail on each of these 12 steps, refer to the ICO guidelines here.
Honan adds that the EU General Data Protection Regulation is not primarily an IT project. “It’s a business project. IT can help implement controls and systems to **protect privacy and ensure the security of data**, but there are business processes that need to be put in place regarding subject access requests, ensuring privacy by design in all systems and services, privacy impact assessments, and so on. Businesses have to understand this can’t just be left to the CIO or IT director,” he says.

**Brexit offers no GDPR get-out**

Honan is also concerned that a number of the smaller businesses he’s spoken to believe Brexit means they no longer have to worry about the regulation. This seems to be confirmed by a recent survey conducted by Crown Records Management, which suggested a quarter of UK businesses had cancelled GDPR preparation following the vote to leave the EU.

In fact, Brexit is likely to make little difference to the need for GDPR compliance among UK organisations. The UK will be a full EU member for at least 10 months following its introduction so therefore firms still need to be fully compliant by the deadline. In addition, the legislation is likely to be adopted wholesale when we leave. Even if it’s not, any company with EU-based customers will have to remain fully compliant.

As Fieldfisher’s Grant notes: “Post-Brexit, the UK will still want the rest of the world to consider it has an adequate data protection regime. It will be far easier for us to do that if we implement the GDPR as originally drafted and don’t relax any of its provisions.”
Compliance as a business differentiator

Rather than viewing the General Data Protection Regulation as another compliance burden, smart organisations should see it as an opportunity. First, people are increasingly likely to choose businesses that can show they take their customers’ data privacy seriously.

And as Chris Weston points out: “Businesses that look at their data model, understand where that data is and put measures in place to find and manage information more effectively to comply with GDPR will reap significant benefits and value in terms of being able to process that data more efficiently in their day-to-day business.”

CIO view: SThree’s Lance Fisher has confidence in the firm’s compliance strategy

Recruitment company SThree started preparing for the European Union’s General Data Protection Regulation (GDPR) in earnest 18 months ago, and CIO Lance Fisher (pictured) is confident the company will be compliant.

“We’ve brought all the people responsible for areas touched by GDPR – such as cybersecurity, insurance, data protection and so on – under a single group which I head up,” he says.

“We’ve studied ICO guidance, brought in consultants and audited ourselves. We’ve automated core processes such as giving people the ability to opt in or be forgotten, verified our key technology partners are compliant and have even helped some smaller partners get up to speed.”

But there are still uncertainties. “For example, we don’t yet know how many subject access requests to expect. We’re also having to rethink how we market to candidates. Mass mail-outs will no longer be viable, and even targeting people via LinkedIn may fall foul of the legislation. LinkedIn claims it’s compliant, but that could be challenged once the legislation is in force,” says Fisher.

He also believes we could see an army of ambulance-chasing insurers emerge (as with PPI), helping individuals challenge companies on GDPR failings in a bid to earn a percentage of any compensation won.

Fisher says the best advice he can give to CIOs not yet up to speed with GDPR is to accept they no longer own people’s data. “We used to take the view it was ours, but you must now accept it’s theirs. Since that realisation hit us, it’s helped keep us on the right course,” he says.