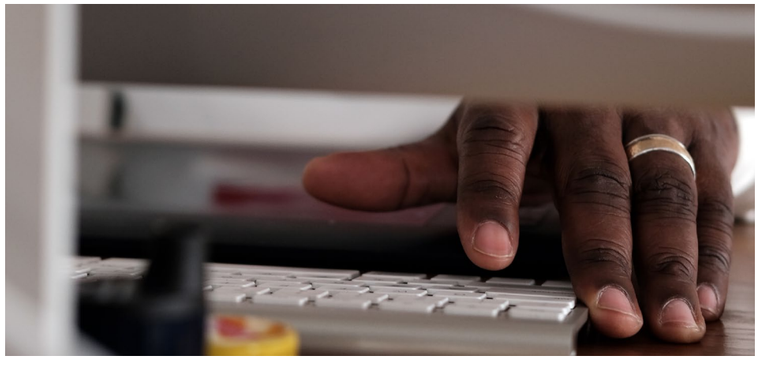
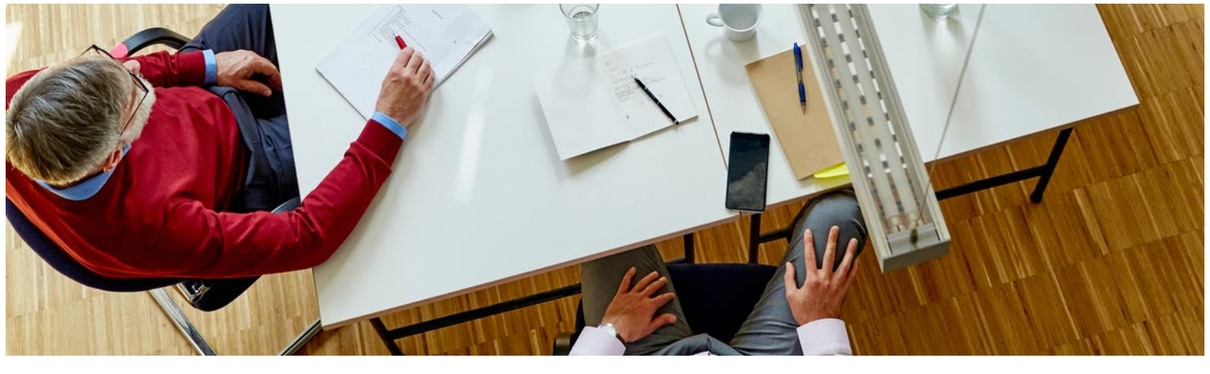
Learning to love GDPR

An opportunity to get your data privacy and cloud content management in order

box

The world is awash with comments about the GDPR…and almost every single one of them focuses on the negative. In this paper, we will look at what the GDPR is, together with how it is likely to be interpreted when it comes into effect in 2018. We'll try to avoid jargon or at least explain that jargon when its use is unavoidable. We'll also outline the salient points, the challenges and the solutions.



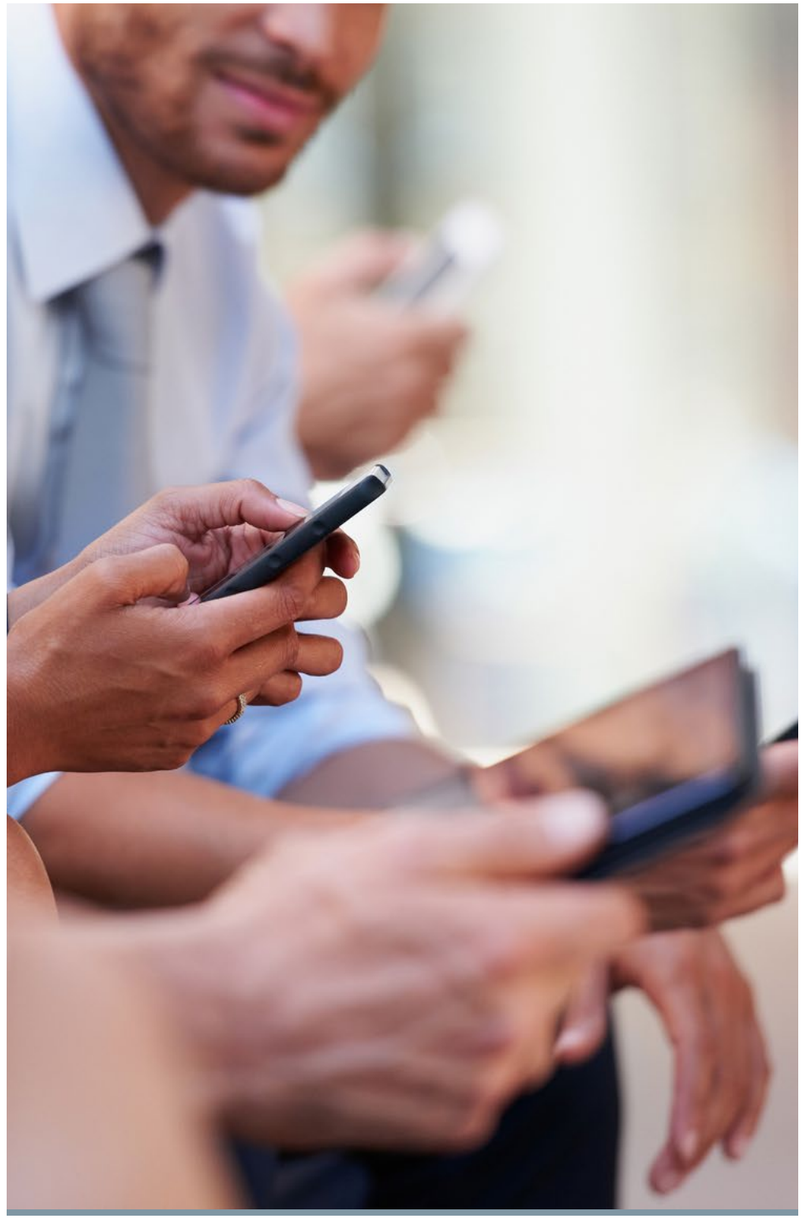


box

The coverage has been negative

Report after report emphasises the downside of the GDPR: huge penalties, shaming by the media and the implicit upheaval in changing the face of how we collect and use personal data. To a certain extent this is understandable: the maximum fines are very large indeed; organisations that are prosecuted are likely to be exposed in public, causing damage to their reputations, creating trust issues, private legal suits and even restricting their ability to trade; and many will need to make substantial changes to processes and working practices. Certainly, to be compliant with the GDPR there will need to be stricter data security, more granular personal data privacy handling obligations, and very likely more investigations and audits.

But rather than fearing and loathing the GDPR it might be wiser to embrace it. The advent of the GDPR heralds a major change in data management and personally identifiable information but it's a change that has been coming for a long time. For too long and too often organisations have not been held accountable for the data under their control when the sensitive materials they hold merit more care and attention. This attitude has enabled organisations to take advantage of the lack of independent oversight which in turn leads to data handling practices and strategies that are inconsistent with the basic concepts of data protection. And this can leave individuals open to scams and abuses of their privacy.



But there’s reason to be positive

Through the lens of embracing change, the GDPR can be seen as an inflexion point that provides an opportunity to make big improvements to data collection, stewardship and sharing. If we make those improvements then we will not only comply with the new rules and minimise our chances of exposure but also keep customers happy, improve our brands and build a platform for business analysis based on accurate, concise, and coherent information assets.

At Box, we will recommend that you tackle the GDPR head on, conducting an audit of data under your control and taking this chance to finally get to that elusive quarry of a “single version of the truth”. We’ll recommend that you ask tough questions of your current vendors/data processors too so that you are fully prepared and cognisant of all relevant risks. We will also point to relevant codes of conduct and approaches as a way to frame and develop your own strategy for GDPR compliance.

Just how big is GDPR?

Some people compare the impact of the GDPR on IT and businesses with the Y2K bug in that it marks a hard stop and demands fast remedial action. But perhaps a more valid point of comparison is the Sarbanes-Oxley Act of 2002. Introduced in the wake of various corporate governance scandals, SOX introduced strict rules on business management, auditing, reporting and accounting transparency. At first it was met with dismay as “more red tape” but many business leaders later considered the journey to compliance as being very good for management and understanding assets and processes that had become fragmented and knotty. And just as with the GDPR, SOX demanded that IT play a key part in unravelling those knots and creating workable new processes.

We won’t pretend to have all of the answers. The GDPR is subject to interpretation and change and it will be incumbent on all of us to pay close attention before and after it comes into effect.

Everything you wanted to know about GDPR but were afraid to ask

There's no shortage of information sources when it comes to the GDPR and it's well worth looking at local guides provided by data protection authorities (DPAs) in your main country of presence in Europe for specific guidance. The following is intended as an easy-to-follow guide to the fundamentals.

box

General Data Protection Regulation

What is it?

The GDPR is an attempt to harmonise rules and boost data protection and security for European Union citizens.

Why should I care?

Because experts believe the GDPR will have a huge impact on how data is collected, processed, used and shared.

So it only applies to Europe?

No. It also affects the export of data outside the EU and of course it affects any organisation that deals with EU citizen data — a vast number of organisations that trade or interact with Europe.

When does the GDPR come into effect?

It is enforceable from 25 May, 2018 and countries affected don't need to pass any domestic legislation beforehand.

box

The penalties surrounding compliance with the GDPR are very big and they constitute a big part of the reason that the GDPR has garnered so much attention. The GDPR provides for fines of up to four per cent of trailing annual gross revenue; for a $1 billion turnover firm, that would equate to a maximum penalty of $40 million. The threat of such large fines means that companies won't easily be able to set aside funds in the event they are found to be incompliant. Nobody can say with confidence that these hefty fines will be applied to anything approaching their fullest extent (and some regulators are providing guidance that smaller fines will be levied except in exceptional circumstances) but nobody wants to find out the hard way.

Seven ways that GDPR will impact your business

The definition of personal data is broad

This covers professional, public life and private life activities and embraces everything from names, postal addresses, images, electronic messaging addresses to IP addresses, posts on social networks, medical information and beyond.

The policy applies to all of the EU

All European Union member states will need to operate under a single rulebook and the EU will try to unite the Supervisory Authority bodies of individual member states.

Consent needs to be explicit.

Citizens will be able to ask tough questions about what is happening with data held on them. This applies to “data controllers” (organisations collecting personal data, for example a retailer, researcher or public-sector agency) and “data processors” (the outfits that process the data on behalf of data controllers, for example cloud service providers).

Systems will need to be retooled

Organisations will need to show that they have built in privacy to workflows and processes – for example by scrambling identity information as it is input to a system – in an approach sometimes known as Privacy by Design.

You will need a go-to person

Organisations of significant size will need to appoint a specialist Data Protection Officer (DPO) who monitors internal compliance and can be called on by DPAs. Depending on the size and type of the organisation, this person could be a part-time consultant.

Any breach will need to be disclosed

Data controllers that experience a breach of personal data privacy will need to report it almost immediately and may also have to notify individuals affected.

Erasure becomes a universal right

Sometimes known under its previous, expanded iteration as “the right to be forgotten”, this allows individuals to request personal data related to them is deleted.

What to do now

(or, *"How I learned to stop worrying and love the GDPR"*)

It's understandable that many of you won't welcome the GDPR with open arms and might view it as yet another layer that sits between tasks you need to be getting on with – creating revenue streams, making profits, battling competitors and other aspects of everyday business.

But as we outlined in our introduction it's far better to tackle the GDPR and see it as an opportunity to create positive outcomes rather than just meet compliance mandates. Put simply, this is a huge opportunity to get your data management house in order. Many of your peers and rivals will be trying to find an easy way out and do the bare minimum so see this as a chance to win a competitive advantage.

Where to start?

Step 1: Audit your data

If you're a sizeable, international organisation you might well have a spaghetti-like array of data types and places where that data is housed. There will be multiple datacentres, databases, applications, operating systems, hardware platforms, desktop and mobile systems. You will probably have some data sitting in private and public clouds or with a co-location hosting provider or disaster recovery partner; there may be rooms full of tapes and disks.

Very likely your company has been part of strategic changes such as mergers, de-mergers and acquisitions and will have seen several new directions, CEOs and CIOs. All of this means that you might well not know where your data sits, where it travels or even what data you're holding. So job one is a voyage of discovery to find out what you have and where it is.

Once you have charted the full extent of your data world you will have a comprehensive overview of what data you hold, the vendors you hold responsible for the stewardship of that data, its physical location and whether that location is liable to change. From there you will be in a strong position to view risks but also rewards and opportunities.

Think of it as a spring clean even if it has been a long time since you last examined your world of data assets. You need a full audit which will help you to prepare for the GDPR and empower you with valuable knowledge. It might well be that you're overpaying for software licences, compute capacity, bandwidth and storage. That data you're sitting on may also be a valuable repository of potential insight so surfacing it is just the beginning.

box

Where to start?

Step 2: Categorise your data

It's well established that certain data categories will be located in different places. However, under the GDPR, customer and employee data will need to be strongly guarded.

The GDPR will also demand a recalibration of the relationship between data controllers and data processors, customers and suppliers. Speak without prejudice to your service providers and demand to know what provisions they have in place to reassure you about risks and compliance. Those providers should be well advanced in becoming GDPR-ready.

At the same time it makes sense to consider the opinion of legal counsel representatives that have studied the rise of the GDPR. Not everyone with legal knowledge will agree with each other and this in part is a result of the challenges of dealing with new laws, interpretation, nuance and a lack of precedent, but many DPAs have been fairly open with guidance and there appears to be a willingness to share views.

Where to start?

Step 3: Rationalise & standardise

For many organisations this will result in a leaner organisation and fewer suppliers, servers, datacentres and data formats. This in turn will provide the opportunity to better analyse data for insights.

So a plan of action might look something like this:

- Analyse the data that you have and determine if any of that data is considered as “personal data” if you are collecting personal data you will need to understand how you process, store and itemise why you need that information, for how long you need to retain it and for what purposes. Try to ensure your data is minimised and accurate, and that the use of this data is limited to specific purposes.
- Draft a Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA) of security policies to determine risk exposure and available protections.
- Try to think in terms of a triangular relationship between your organisation, key suppliers and regulators. Where there is doubt, err on the side of caution and pursue the highest bars of compliance. Outside consultants such as auditors may provide a valuable extra perspective.
- Make changes to technology and processes based on your evaluation of the risks. Data mapping tools and configuration management databases that audit IT systems will be useful here and some vendors are already flagging their GDPR

capabilities. Reviewing your security systems, encryption capabilities and ability to address leaks through data wiping will be necessary.

- Write and circulate appropriate policies on data access, data deletion, how data is required to be handled etc. Create a staff training programme and ensure there is broad awareness of what you are doing and why you are doing it.

Practical steps:
Risks & choices

Having conducted an audit and considered the severe penalties available under the GDPR it might be tempting to be super-conservative and keep all data in your own country. Certainly there is increasing interest in having data reside in earmarked countries or zones: even if the GDPR allows for data to sit outside the EU in certain circumstances, other rules and codes you operate under might demand that data assets stay within a single country of origin or zone. Service providers who can't meet the demands of customers will struggle to compete.

But adopting a belt-and-braces approach where data is locked down and new deployment models are strictly curtailed has a significant downside. For example, public cloud computing delivers an economy of scale by locating data in different parts of the world and many suppliers will have limited local datacentre availability. It's as well to make judgments that strike a balance between strict adherence to laws and codes, business flexibility and cost management.

It's a smart idea to work in concert with your data processing providers, putting the onus on them to be compliant with the GDPR and other rules. Many cloud providers today are rushing to add datacentre facilities and add relevant certifications – seek them out and don't be afraid to ask questions of them. As a data controller you can't push all your obligations onto your vendors but they have a responsibility as the repositories for many customers' data to be well prepared and to show good governance.

box

Use of Binding Corporate Rules, or BCRs, is a positive sign that your service provider understands EU data protection. Companies that have BCR processor packages approved by their local data protection authority have been thoroughly vetted by the DPA and are determined to have the necessary policies and controls in place to handle EU data outside the European Economic Area. Something to keep in mind is that attaining approval for BCR's is not a "one-off" measure, and approved BCR package means that the vendor is subject to ongoing review and potential audits by the DPA. BCRs are important in that they are the only instruments specifically spelled out as a possible way to export personal data outside countries under the GDPR. Another powerful instrument is Privacy Shield, a framework developed by the European Commission and US Department of Commerce. You might think of BCRs, together with Privacy Shield as a sequel to, and replacement for, Safe Harbour which was deemed insufficient by the European Court of Justice in 2015. But for optimal governance look for other factors that augment and strengthen these pillars.

One useful way to learn more about protecting your company is to defer to Germany which has some of the toughest and most comprehensive requirements in Europe. Developed under the auspices of the German Federal Ministry for Economics, the Trusted Cloud Data Protection Profile, or TCDP, incorporates various standards of the International Organisation for Standardisation and certifies cloud service providers that meet privacy compliance and statutory requirements. Another German framework, the Cloud Computing Compliance Controls Catalog, or C5, developed by the German Federal Office of Information Security is another useful tool in the suite of certification available to prove effective data protection to government agencies. And it is typical that where the public sector leads, the private sector will follow.

box

In summary

GDPR is the most high-profile legislation to affect IT and management of personal data in many years. It creates a new line in the sand for data management and gives DPAs powerful new levies. Organisations that don't respect these new powers and react appropriately will only have themselves to blame and the scale of fines is such that we may even see companies fail because of GDPR infractions.

box

Unknown factors remain

We don’t know how hard data protection agencies are going to target organisations found to have fallen foul of the GDPR. It is entirely possible that they will impose larger penalties for the most egregious acts and may be more understanding with companies that have performed due diligence and can show that they took a sober and measured approach to compliance, data management and information security.

Also, we don’t know for sure how well staffed and capable of investigating organisations and making decisions those DPAs will be, although there are signs that they are staffing up.

The impact of the GDPR on the IT department will be significant, notably with relevance to encryption, security, auditing of technology-enabled processes and access management. But, as we have argued, rather than seeing the GDPR as a painful addition to the roster of their chores, organisations will be wiser to look at this as a watershed event that provides a once-in-a-lifetime opportunity to address old issues and build a platform for intelligent insights.

Over the years and decades, organisations have created all sorts of data and that data has been processed, communicated and stored over all sorts of hardware, networks and technology infrastructure.

Data formats have changed over time and never-ending competitive demands mean that companies have leapt on the new systems and technologies to deliver an advantage over rivals. They have rarely been able to review what they have collected and often they will have been unable (or unwilling) to tag content in a meaningful way so that data can be quickly discovered. The result over time is not pretty: unknown assets sitting on old systems and an inability to respond in timely fashion to breaches and requests. The most honest CIOs may even confess to not knowing how many IT systems they have, where those systems are located or what resides on those systems.

To protect their organisations and to be operationally efficient this has to stop. The GDPR offers a break away from the data management merry-go-round, a chance to step off. It provides the impetus to review the way IT has been delivered, to refresh and go again. Forward thinking organisations will take this opportunity to re-platform, effectively creating a new IT that is ready not just for the GDPR – and for potential future changes to the GDPR – but for the broader challenges and opportunities that lie ahead.

box

Find out more from the GDPR experts at Box

Box has worked hard to be GDPR-ready and other laws, rules and codes that pertain to information security and governance. We have a long history of winning certifications including ISO 27001 and 27018, PCI DSS 3.0, HIPAA/HITECH in US healthcare, NIST 800-53 for US federal information under the US Government FedRAMP program, APEC Cross Border Privacy Rules, SEC Rule 17a-4 in US financial securities, SOC 1 and SOC 2 for internal controls, the UK government's G-Cloud Framework and many others.

We have created Box Zones that allow data to remain within countries, we work closely with Europe's DPAs, apply Binding Corporate Rules and comply with Privacy Shield, TCDP and C5. From our position as both processor and controller we hold regular meetings with customers keen to discover more about the unfolding GDPR story.

box

If you haven't already, it's time to take action on GDPR

We're here to help. At Box, we started to think about how new compliance regulations would be measured and tested in 2015. Since then, we've been working on becoming GDPR ready. And today, our industry-leading Cloud Content Management solution powers more than 74,000 businesses globally, including AstraZeneca, General Electric, P&G, and The Gap — along with 74% of the Fortune 500.
Let's work together to make your GDPR journey a successful one.

Find out more at **https://www.box.com/en-gb/security/governance-and-compliance/gdpr**

box