Grant Thornton

An instinct for growth™

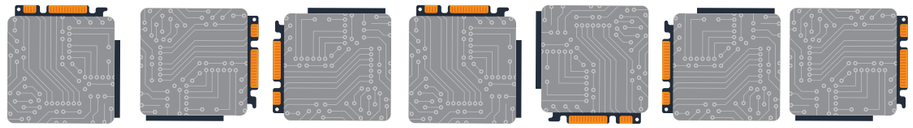
The golden rulebook

Ensuring compliance and data security in a complex and risky world

Extract from technology, media, telecommunication report
Building tomorrow's billion dollar businesses

Ensuring compliance and data security in a complex and risky world

For tech companies, the regulatory environment is tougher now than ever before. As a way to protect the national interest, governments use compliance to restrict companies that could potentially disrupt established industries. The knock-on effect of this is that the tech industry as a whole is coming under extreme scrutiny and is facing a higher level of financial and reputational damage as a result. Rapidly expanding companies also face a wider range of individual regulations as they expand into new territories. Be it employment law, taxation, product safety or licensing.



Today, many of the most pressing compliance issues come down to data anxiety. As citizens become increasingly uncomfortable about threats to their personal data and privacy, governments are cracking down on the companies responsible for hosting that data and keeping it secure.

Worldwide, regulators have made it clear that they are becoming tougher on tech companies. In the summer of 2015, the US Federal Trade Commission (FTC) said it was investigating Airbnb, Uber and other sharing economy pioneers over their use of data and rating systems[1]. Meanwhile, after several global tech companies were criticised for their data use across the continent, all 28 EU states are now working towards a pan-European data protection framework[2]. Key markets such as Australia[3] are also looking to overhaul and strengthen their data privacy regulation.

Taking a positive approach to regulation

Tech companies must build into their products the functionality and capability to comply with a large and diverse set of sometimes conflicting international standards. They must give their customers a high degree of confidence that their services and products are secure, protect their privacy and support compliance with other standards. And, if that isn't enough, tech companies need to protect their own infrastructure and data as much as – if not more than – any other organisation.

Yet expanding tech companies should also remember something very important: approached correctly, regulation needn't be a problem. It can create competitive advantage.

"Regulation is our friend. Governments are saying to telcos, 'You can't treat people in rural areas as second-class citizens. You need to give them fixed wireless rural broadband.' From our point of view, that regulatory overlay is good."

Ken Sheridan
CEO, Netcomm Wireless

1 'Regulator probes pitfalls of sharing economy,' Financial Times, May 2015
2 'EU states agree framework for pan-European data privacy rules,' The Guardian, June 2015
3 'Australia's data privacy laws come into force as providers struggle with data management,' Business cloud news, March 2014

Preparing for complexity

Ensuring data protection is not just about preventing reputation damage. The EU's proposed rules for data privacy could lead to corporate fines of as much as 5% of global revenue for data security breaches[4].
And even if regulators were not focusing on data protection, tech companies would still need to ensure coverage. In 2014, for example, the estimated financial loss from 700 million data breaches was $400 million[5].

The good news for tech companies is that the actions they need to take to secure data from a regulatory standpoint are about the same as the actions they should have taken to ensure adequate protection anyway. This does, however, require different controls depending on a range of variables (see box). As companies grow and rely on expanded networks and supply chains, the risks become more complex. Hackers breached Target's systems, for example, using network credentials stolen from a third-party vendor[6].

All 28 EU states are now working towards a pan-European data protection framework

Without transparency, compliance simply isn't possible

As well as demanding stronger data protection, regulators expect tech companies to be transparent about where, how and why they are storing customer data. In particular, regulators are targeting companies that fail to tell customers exactly what they are using their data for.

Snapchat recently settled FTC charges for deceiving 4.6 million consumers about the 'disappearing' nature of their messages. As a result, an 'independent privacy professional' must now monitor the company for the next 20 years[7, 8.] Facebook has also faced criticism over its face-recognition functionality, with some claiming 'astonishment' that they were not consulted before the firm added it to their privacy policy[9].

Transparency and clear communication is particularly important for companies that provide a B2B service. Bruno De Wolf of BeAligned, a Grant Thornton member firm, thinks many consumers "do not care" where their data is stored. "But in a B2B environment it's completely different," he says. "They are afraid of the cloud, and many IT managers will find any excuse to not put anything on the cloud."

> "But in a B2B environment it's completely different. They are afraid of the cloud, and many IT managers will find any excuse to not put anything on the cloud."
>
> **Bruno De Wolf**
> BeAligned, a Grant Thornton member firm

4 'EU Data Protection Regulation: fines up to 100m proposed,' Computer Weekly, November 2013
5 '2015 data breach investigations report,' Verizon, 2015
6 'Target hackers broke in via HVAC company,' Krebs on Security, February 2015
7 'Snapchat settles FTC charges that promises of disappearing messages were false,' Federal Trade Commission,' May 2014
8 'FTC finalizes privacy settlement with Snapchat over 'deceived' users,' The Verge, December 2014
9 'Facebook's new face recognition policy astonishes German privacy regulator,' PC World, August 2013

Protecting consumer data: beyond the basics

"Most expanding tech companies have smart, savvy employees who have instinctively taken care of a lot of cyber security basics right away," says Mike Harris, cyber security partner at Grant Thornton Ireland. "But often they haven't done so as part of a coherent strategy. Have they considered how they will manage cyber risk in five years' time? Do they understand the cyber risks that their customers – and customers' customers – are facing?

"First, they need to understand the specific threats their business is facing. Each business requires detailed security requirements – and it's expensive to update these at a later date. There are different threats for B2B or B2C providers, for those with a high dependency on IP, for those who plan to host their app on the cloud.

"Tech companies need to think about this from a strategic perspective because investment will be required. They can then ensure their IT systems are configured correctly and that they have the right operational processes.

But Mike warns that the issue is no longer simply about prevention. "What's increasingly important is what happens after you have a breach. The instant response is a growing issue. It's no longer enough to be static in your defences. You need to react quickly. Not only is this more reassuring for customers and the regulator, but it is also essential if you want to stop hackers from breaking their way into the parts of your system that you thought were most secure, such as your IP."

Building relationships on the ground

One of the concerns that regulators have about global tech companies is the relative lack of control they have over them. By their nature, tech companies do not have to keep their servers in every country in which they are selling their services.

For regulators, this can lead to a lack of trust. Tech companies that anticipate and respond to this potential distrust from the outset can avoid excessive regulatory scrutiny. By building stronger relationships with regulators, they will likely find it easier to build their presence overseas.

And, as Simon Coulton, partner, Grant Thornton Australia explains, expanding tech companies need to work with local advisers and experts to get a better understanding of issues and concerns on the ground.

"A lot of it comes down to appreciating that the right locals will know how to handle issues better," he says.

> "Regulation matters because it creates market inefficiencies that didn't exist prior. We've got regulation enabling the re-shaping of whole industries."
>
> **Hussein Kanji**
> Partner, Hoxton Ventures

> "Some of these organisations may need to be more politically aware as they enter new markets."
>
> **Nick Watson**
> Partner, Grant Thornton UK

CASE STUDY

Why Funding Circle welcomes financial services regulation

Funding Circle, which enables peer-to-peer lending between individual savers and small and medium-sized businesses, is one of Europe's fastest growing fintech companies.

Within five years of its launch in summer 2010, Funding Circle had already facilitated around £700 million in loans. In that timescale, however, there was a major upheaval in financial services regulation. "We knew it would be difficult," says James Meekings, CEO, Funding Circle. "But we were confident that our business was going to change the financial landscape. We believed our growth would be really meaningful."

Yet the company is a good example of a tech business that has exploited the market inefficiencies caused by regulation. Clampdowns on capital thresholds for banks, via Basel III regulations that make lending to small businesses more expensive, gave Funding Circle an opportunity to grow their business. "We were told, 'You're the only financial services business that is asking to be regulated'."

The company chose to take a positive attitude to regulation and to be proactive in complying. "If billions of pounds go through this marketplace, it is going to be regulated. Is it not better to take it on our terms rather than have it forced upon us when it's too late? The regulation we are now doing is making our business stronger and more defensible – and protecting customers' money better. Without it, it would have taken us longer, and customers' money wouldn't have been as safe as it will be. We have a growing army of people focused on the regulation process at the moment."

Key questions: ensuring compliance and data security

- How can we ensure our data – and our customers' data – is secure worldwide?
- How will local regulations restrict how and where we use data? And what other local sensitivities should we be aware of?
- What operational changes do we need to make to ensure we can respond to compliance?
- How should we approach our relationship with regulators in each of our markets?
- What should we do when a breach takes place?
- How do we keep track of countless regulations across markets – and across different areas of business – many of which are liable to change?

About Grant Thornton

Grant Thornton is one of the world's leading organisations of independent assurance, tax and advisory firms. These firms help dynamic organisations unlock their potential for growth by providing meaningful, forward looking advice.

Proactive teams, led by approachable partners, use insights, experience and instinct to understand complex issues for privately owned, publicly listed and public sector clients and help them to find solutions. More than 40,000 Grant Thornton people across over 130 countries, are focused on making a difference to the clients, colleagues and the communities in which we live and work.

www.grantthornton.global

Grant Thornton
An instinct for growth™

grantthornton.global