The perfect storm: GDPR, BREXIT and corporate governance in the UK
Introduction

As the amount of data we create increases, so does the amount of regulations enforced to deal with data handling and security. The personal nature of most of the data that is collected relies on these regulations and laws being enforced for our own security and the reputational and financial damages that can occur as a result of not meeting these regulations can be substantial.

This is certainly the case with the EU General Data Protection Regulation (GDPR) that is coming into force as of the 25th May 2018, and will remain law, even after we leave the European Union in 2019 (at the time of writing).

Under current UK data protection laws, whilst the threat of public scrutiny and damage to the brand’s reputation is heavy enough to deter most, the Information Commissioners Office has had very little success in imposing fines, which were limited to £400,000. Under the new GDPR, non-compliance has serious consequences of up to €20,000,000 or 4% of annual global turnover, whichever is greater.

Organisations have enough to deal with, ensuring compliance with the GDPR, along with other compliance regulations, without the added complications of BREXIT thrown into the mix. The climate of uncertainty caused by BREXIT is not the backdrop you want to have for the forthcoming year.

In this whitepaper, we will look in-depth at the new regulations coming into place for organisations in the UK as well as the GDPR and the tools to help you set up a compliance framework for operating in this shifting sand.
A three-pronged attack

The current geo-political and financial climate means that most organisations are finding it tough to do business, but then add on top of that the impending compliance deadlines for GDPR, the UK Corporate Governance Code and Brexit, not even knowing what this one will look like, and you will find most businesses struggling under the weight.

The timing of these three new regulatory codes could not be worse for Company Secretaries. The role was already a high-pressure job, a senior role traditionally responsible for filing of annual returns and maintaining the company’s existence as a legal entity, the focus on the role has intensified in the last decade or so with the responsibility of the organisation’s corporate governance thrusting the role into spotlight.

This increase in focus on governance has also spread to the public consciousness, and news of corporate scandals and failings are now commonplace across the media, meaning that the awareness of any failing is now much greater than it ever has been. The governance scandals that gather the most attention from the press are usually concerned with executive pay. This is a contentious subject for all concerned as it is one of the key areas covered in the new Corporate Governance reform introduced by the UK government in August 2017.

Government response

A greater worldwide focus on governance came at the right time for the UK government, as it gave them an opportunity to consolidate and update its already robust stance on good corporate governance and re-confirm the UK as a prime destination for business in the light of the leave vote following the EU referendum held in 2016.

Whilst it is unclear exactly what the exit bill will contain, the UK needed to reaffirm its position as a global force for
business to ensure against a mass exodus, financially crippling the country. The governance code already in place, the Companies Act 2006, was already one of the most thorough in the world, defining fiduciary duties for directors, along with the ‘Combined Code’ which provided general principles for organisations to follow under the ‘comply or explain’ basis. This principle allows companies to not comply with the code, so long as they can provide an adequate reason as to not following it.

The decision to make major changes to the corporate governance system shortly before the release of its green paper on the subject in November 2016, taking much that is in the voluntary code and putting it into enforceable laws and regulations.

A survey by accounting and consulting firm Grant Thornton in December 2015 showed that only 57 percent of the FTSE 350 companies fully complied with the Code. This, along with the increase in public interest in executive pay and employee rights has prompted this change.

Compliance with the code has always been limited to public companies, whilst private companies can voluntarily choose to adhere if they wish, but that is changing with large privately held companies now being required to comply with the new code as part of its reform.

The government’s response to the green paper focuses on three main areas; executive pay, employee rights and engagement and corporate governance in large privately-held businesses. The highest-profile item here for sure is executive pay, which attracts controversy from both sides of the fence.

When the reforms were announced, all of the headlines were grabbed by the inclusion of the required legislation that companies are to report annually on the ratio of CEO pay to the average pay of its UK workforce along with a narrative explaining changes to that ratio from year to year as well as putting it in context with pay and conditions across the organisation.
There are other reforms to executive pay outlined in the report, but the other main change lies in handing broader responsibility to remuneration committee to oversee pay and incentives across the whole company and requiring them to engage with the wider workforce to explain how executive remuneration aligns with wider company pay policies, creating greater transparency over pay ratios across the organisation.

Section 2 of the report outlines ways in which the code can be used to strengthen the employee voice and create greater engagement with stakeholders. The main change here is the introduction of secondary legislature that requires all large companies, both private and public, to explain how their directors regard their responsibilities towards their employees, shareholders, customers and wider society. The increase in accountability and transparency here is something that the general public has been crying out for since the financial crisis of 2008, but it will be interesting to see how willing some organisations are to make this change.

Overall, the response and new reforms refocuses the director’s attention to prove that the salary and incentives they are receiving are commensurate with their performance and in turn, placing extra responsibilities on them to help ensure this. This is certainly the case with the GDPR, under which Directors have extensive responsibilities with potentially life changing consequences.

 Keeping organisations in check with the advancement of technology

The advancement of technology since the turn of the century is nothing short of remarkable, and whilst it has revolutionised every aspect of our day-to-day lives, however the amount that we rely on technology to facilitate our business decisions and communications, the likeliness of a data breach is greatly increased. This has led
to some very high profile hacks, leaks and security breaches in recent years concerning a lot of personal data, and this is the purpose of the GDPR, to better protect personal data.

The EU General Data Protection Regulation was adopted in April 2016, and comes into full effect on 25 May 2018, when it supersedes the Data Protection Directive (DPD). The new regulation doesn’t fundamentally change any of the core rules in the DPD, rather it extends the directive’s requirements significantly by introducing a range of new obligations. The GDPR heralds the most significant change to data protection law in the EU for some time.

Introduced to keep pace with technological advancements, the regulation’s purpose is to improve consumer confidence in organisations that hold personal data by reinforcing their privacy and security rights, and also to simplify the free flow of personal data in the EU in a coherent framework across all member states.

The UK has recognised the value that the new regulation brings to protecting consumers rights, and has confirmed that the GDPR will continue to apply to UK companies, even after the UK leaves the European Union.

The biggest change comes in the way that records must now be kept and maintained detailing how the data is both stored and used. Furthermore, under the new regulations, it is outlined that the onus is on the data controllers, or the company that will be using and manipulating the data, to ensure that the data processors or collectors are fully compliant with GDPR. This extra step will help to further protect the consumer’s data, however will also add significantly to the burden of the IT department and the CIO when performing due diligence on any potential new contractor.

In a recent survey of 500 IT executives across different industries for Varonis Systems, 75% companies believe they face serious challenges in becoming compliant with GDPR. At financial services firms, executives seem to be taking these challenges more seriously than most. Only 33% of IT executives in the financial services sector say
their company has not made it a priority to comply with the law by the deadline. That compares with an average of 42 per cent across all sectors. Over 25% of all IT executives surveyed agreed that banking would be the sector most likely to be made an example of.

In an FT article of May 2017, highlighting the insurmountable task that the banking sector faces, Chris McMillan, a partner at Oliver Wyman, a consultancy outlined the problems faced by banks, “From our discussions with chief technology officers at banks, they are concerned the technical challenge may be impossible given there is only a year to go.”

“Banks are struggling with legacy systems,” says Chris McMillan, a partner at Oliver Wyman, a consultancy “From our discussions with chief technology officers at banks, they are concerned the technical challenge may be impossible given there is only a year to go.” Banks may have up to 100 different systems with different piece of data for each client stored on each one, a joined up approach is a huge task. However there are some other small ways which show that perhaps some of the biggest organisations haven’t even started to make changes.

RiskIQ reviewed the public websites of FTSE 30 organisations and found that some of the most basic changes haven’t been made. Most websites use data capture forms, which fall within the scope of GDPR as they collect personal data. The regulation emphasises that provisions should be in place to ensure that PII is securely captured and processed. In the UK, the Information Commissioner has provided guidance that, in the case of data loss where encryption software has not been used to protect the data, regulatory action may be pursued.

The RiskIQ research on the public facing websites of FTSE 30 organisations revealed that there are 99,467 live websites in total, an average of 3,315 websites per organisation. Of these, 13,194 pages collect PII (personal information), an average of 440 pages per organisation. Crucially, 34% of pages that collect PII are doing so insecurely, with 29% are not using encryption.
Many organisations are beginning to panic over the short timeframe before they need to demonstrate GDPR compliance particularly around the stringency of compliance standards and the recording of data processing in the event of an audit.

The Regulation now places the onus on organisations and data processors to keep their own records of data processing activities and make these available to the supervisory authority on request. This record needs to contain a specific set of information so that it is clear what, where, how and why data is processed.

Where the compliance standards are concerned, the GDPR actively encourages the adoption of certification schemes as a means to demonstrate compliance. Compliance with, or partnering data hosts that have complied with, the international information security standard ISO 27001 – the only independent, internationally recognised data security standard – will help organisations demonstrate that they have endeavoured to comply with the data security requirements of the GDPR.

Breach of any of these duties, or failing to ensure compliance, can lead to direct legal action being taken against the directors by prosecutors, or even shareholders. Even without this extra element of personal jeopardy, the increased scrutiny that would come with any claims of data misuse or failings would draw significant attention to the directors in question and their suitability.

Further legislative change may also be on the horizon in the UK. In a meeting to discuss the UK’s draft Digital Economy Bill in October 2016, the Information Commissioner recommended imposing personal liability and accountability on directors of companies that violate data protection laws.

What is clear is that accountability and transparency are again key to the success of any organisation in dealing with the new regulations coming into place. Clear and concise planning is needed to ensure that every aspect of these new regulations are complied with, or at least explained why compliance is not an option as is the case with the
new UK code, but how do you plan for something without knowing the exact details of what you’re planning for? That is the difficult position that organisations currently find themselves regarding Brexit.

The uncertainty around BREXIT

There is a growing concern around what will be included in the Exit Bill, if there will even be one agreed upon, and the length of time this gives organisations to comply with the, as yet, unknown regulations.

Chris Bates, Head of Financial Regulatory Practices for Clifford Chance, speaking at the European Compliance and Legal Conference run by AFME earlier this month was keen to press home just how little amount of time there is before the deadline of March 2019 for the exit bill, and how tricky this is for businesses especially if you’re waiting until an exit bill is agreed upon before making any business critical decisions. “The uncertainty around Brexit can paralyse your organisation, you have to press forward with your plans as the timeline is simply too short to wait and see.”

Panellists at the AFME conference all agreed that the amount of paperwork and admin that will be needed for dealing with clients the other side of the Brexit deadline in the wake of the, as-yet, unknown new regulations that will come into play was also a point of contention amongst many of the delegates.

The final part of this hellish jigsaw is what Scott Vincent, managing partner at consultancy Parker Fitzgerald, described at the AFME conference as the alphabet soup of other financial regulations coming into force soon. Companies face “an enormous challenge” in complying with the EU’s General Data Protection Regulation alongside other new regulations — including MiFid 2, PSD2 and IFRS 9 coming into play, both known and unknown. He describes a growing sense of “industry panic” around compliance.

“Most issues can be avoided by the implementation of strict laws and by rigorously enforcing those laws.

This may sound scary, but is the only way to ensure a smooth Brexit transition”

– Barnabas Reynolds- Shearman & Sterling
The ramifications of Brexit do not just affect how we deal with the EU as a third-party, but also has implications on the UK’s trading with other countries as new trade deals, as well as yet more regulations, will have to come into play to enable and secure this after the deadline in 2019.

The advice from all industry experts is to begin your preparations now, if you haven’t done already. In a recent survey at FundForum 2017, eShare discovered that 40% of the organisations in attendance had not yet begun setting aside resources, time money and people, to deal with the potential fallout and repercussions of Brexit.

Transparency at the forefront

A paper published by Deloitte said: “The sheer complexity of governance and the huge number of related procedures and other mechanisms in a global financial institution may indicate a need for a governance operating model. The elements of such a model may exist within many large FSI companies. However, those elements may not have been connected, rationalized, and organized to provide the consistent guidance and incentives that executives, risk managers, and business unit leaders require. A governance operating model has the potential to address this need and thus enhance management’s ability to implement governance and the board’s ability to exercise proper oversight”

Whilst this feature focuses on the financial services industry, it rings true for all industries and businesses. One thing is certain though, it’s a big subject and you cannot tackle everything at once. By focusing your efforts initially on improving your transparency when making decisions as well as proving accountability, you have put in place the building blocks for addressing all of the three hurdles mentioned above.
Whilst many of the new regulations under the UK Corporate Governance reforms focus on the use of technology, it can also be the answer to achieving this first step towards addressing these hurdles.

By utilising a fully secure and compliant governance platform, your board of directors can be safe that their meetings are captured in a fully transparent way as well as allowing for a traceable and auditable actions and decisions system to capture a complete picture of the business critical meetings and discussions being held. Since ultimate responsibility lies with the board of directors this transparency around their meetings and the decisions they make can help to foster a culture of transparency.

**Improved governance**

Failure to comply with the new regulations, particularly GDPR, could have disastrous personal and professional consequences, but there are tools available to help with this. Online board portals are growing in use with many organisations, enabling enhanced board communication and collaboration, document review and annotation, and a host of other features that make board meetings more efficient and effective.

There is also a real need to push the use of portals down into the subsidiary governance layer, particularly for regulated entities. Traditionally, software has only been used at the plc level, but risk is present in operating entities throughout the entire corporate structure.

Online board portals make it easier for board members to demonstrate accountability, compliance and transparency, supporting the information sharing, decision making and risk management that comes with good governance. They provide an overview of governance throughout the organisation, helping identify issues and drive improvement.
Conclusion

The spotlight of world media is now fully on organisations when it comes to compliance and the consumers have never had a greater understanding or power when it comes to where they take their business.

Non-compliance with the new regulations coming into place is not an option, but it is clear that organisations need help when it comes to focussing the mind and knowing where to begin. Technology could be the key to unlocking this puzzle, and with the right tools in place, the burden of proof could be eased considerably.

eShare works with hundreds of organisations and their company secretaries all over the world and we understand the demands and challenges of the role. To hear more about how we can help address some of the issues outlined in this paper, please get in touch via email on info@eshare.net, or call us on +44 (0) 845 200 7829.