General Data Protection Regulation
GDPR framework
second opinion

January 2018
The GDPR gave organisations a two year grace period during which it is expected that they have been preparing for May 2018. Some businesses have been on a long journey whilst others are just starting out. In each case programme design and delivery is either solely managed internally, in the hands of a third party or is a hybrid of both.

The GDPR will automatically come into effect in all EU Member States on 25th May 2018. From that point on ‘data controllers’ and ‘data processors’ will be exposed to the full effect of the law, which includes the risk of regulatory action (enforcement notices and fines), the risk of compensation claims brought by data subjects and business interference.

Does our GDPR programme have a clear vision and end state?

The programme team/DPO has decided what the scope of the programme is, however this has not been discussed or agreed with senior leadership. What are the implications? The programme is clearly focussed on the GDPR but does it also consider the objectives of the overall business strategy and other existing positions such as our organisational ethics policy?

Will we be compliant by 25th May 2018? What happens if we are not?

Our business expects to be compliant by May 2018 although we haven’t specifically discussed what it means to be in a state of non-compliance. How would our position be scrutinised if our programme does not deliver compliance by the deadline?

How do we know that our programme is addressing all the key priorities, in the right order and at the right pace?

We know that a number of workstreams are underway but we are not clear on the purpose or priority of each activity. Do the workstreams involve all relevant functions and consider their priorities and risks? Overall what risks are we concerned with and how have we assessed what matters most? How are we confident that the required change will take place in good time for the May 2018 deadline?

Do we have adequate funding for the GDPR?

Budget has been allocated for the programme but the coverage isn’t organisation wide and functions such as HR and Technology are unsure where the funding for their areas is coming from. The funding is limited and there is no way of understanding how the programme is ensuring that the investment is being directed at the areas considered to be high risk. Has a decision been made in relation to the post May 2018 programme budget and does it extend to cover culture and technology change?

Have we got the appropriate Governance model and skill-set to deliver?

We have allocated the GDPR to our compliance department however we have limited skill in the business in relation to data protection and heavily rely on external law firms and other single service advisors. Have we assembled a multidisciplinary team to ensure our programme covers all relevant areas or have we simply focussed on legal and compliance expertise? Does our GDPR governance framework involve the appropriate level of senior management and are they getting meaningful and comprehensive reporting on risk?

Does the programme cover operational change, including culture and the Technology stack?

There is activity underway that focuses on updating policies and procedures but to what extent does the programme extend in to directing and managing operational change? Does our Technology department understand the impact to our IT environment and do they appreciate that the business will they be able to demonstrate that the GDPR does not simply live in paper in our business? How much about the GDPR does our workforce understand and have we identified if our culture presents a risk to compliance.
Our point of view

For many organisations the transition from the Data Protection Act (1998) to the GDPR requires significant investment and change to be made and there is often indecision around where to start and what the programme vision, end state and priorities should be. This has resulted in a number of programmes encountering delays, going off track and undertaking activity that serves little purpose. Few programmes consider the ‘Special Characteristics’ of the organisation in their design (the operational and environmental features that make a business unique) and have been built as traditional compliance programmes, which do not reduce real risk, i.e., litigation or other enforcement action, consumer/employee complaint, failure to deliver operational change and missed commercial opportunity to monetise data.

Taking stock for rising anxiety
All these factors have resulted in a growing concern, across sectors, in how likely it is that what has been built and delivered so far is fit to meet the May 2018 deadline for GDPR compliance. Every business should now pause and take stock of what has been achieved and what is yet to be done in order to gain confidence that their efforts around the GDPR have been purposeful and will deliver real risk reduction alongside legislative compliance.

Ignorance is no defence
The Regulation was conceived in 2012 and the full text announced in April 2016 and as such it would be indefensible to suggest that your programme was immature or tackling the wrong priorities due to a lack of awareness.

A very long history of relevant jurisprudence under data protection law will carry over into the GDPR. This alongside the text of the regulation itself and European Data Protection Authorities (including the UK Information Commissioner) frequently publishing blogs and guidance on the GDPR provides a wealth of advice. Although there are still a number of areas that remain unclear, there is enough guidance for businesses to have used the two year grace period to have begun making the changes required.

The penalties for getting this wrong can be severe not only financially but, in terms in the degree of scrutiny your business will be subjected to.

Today and tomorrow
To date most organisations have not been fully compliant with existing data protection laws and this position is increasingly becoming more unforgiving. With only a matter of months remaining in the grace period there is a clear need to gain confidence that your organisational plan for the GDPR has been clearly defined and agreed with its risks understood. It is also necessary that assurance is sought in relation to the appropriateness of where investment has been made, that the programme supports the objectives of the overall business strategy, compliance obligations and that your plan is comprehensive enough to take your organisation beyond May 2018 into BAU.

Keep your confidence fresh
As with any form of business change, regulatory focused programmes are susceptible to stalling and run the risk of failing to deliver what is required. Not only is the business environment ever changing, but the regulatory guidance for the GDPR is frequently updated, often providing additional instruction and interpretation of the requirements. This can result in the unpicking of what has already been implemented.

For many GDPR programmes KPI’s and appropriate MI have not been established and as a result progress and risk is not being adequately tracked. This has led to a number of Executives not truly understanding what is and is not being covered/achieved by their GDPR programmes and as such large volumes of legacy risk is being increased.

The programme needs Board level ownership
You need someone on the Board to be ultimately accountable for the GDPR. Typically, the Data Protection Officer or the legal department is cited as the de-facto accountable owner of GDPR programmes, but this is the wrong answer. They should have a key role in advising and leading aspects of the programme but if your focus is on taking the GDPR seriously and ensuring your organisation is doing the right thing for your data subjects, the Board need to take proactive ownership roles.
What good looks like

- You have an Enterprise wide vision and strategy for the GDPR which reflects the ‘Special Characteristics’ of your organisation.
- You have considered your programme from a risk management perspective and have not simply followed the legislative compliance route.
- You have assembled a multidisciplinary team to support your transition to the GDPR.
- The implications of the GDPR are well understood by those who need to know.
- You have assessed the budgetary and resource requirements to make the necessary changes required under the GDPR and funding and staff have been secured.
- Your programme is not just concerned with updating policies and procedures but has been designed to embed the requirements of the GDPR in to your technology and culture.
- You have metrics and reporting which allow you to confirm the progress and effectiveness of your GDPR programme.
- You have ensured that your GDPR programme reflects the need to evidence compliance and generate the necessary artefacts within the appropriate timelines.
- You are tracking the development of regulatory guidance and enforcement cases.

How we can help?

Using our global multi-disciplinary data protection team, deep understanding of the GDPR and our insight gained from practical experience in supporting organisations who are suffering the consequences of failing GDPR programmes, we can help you understand if your programme is on the right track to deliver real risk reduction, meaningful and measurable operational change along with the necessary compliance obligations in time for May 2018.

Programme design and set-up
We will consider if your programme design and set-up has covered all the necessary components for success such as smart financing, sponsorship and stakeholder engagement and assess if it is delivering as intended to. We will also critique the level of skill you have within your organisation to deliver, along with evaluating how governance and reporting has been implemented.

Vision and strategy
We will assess the extent to which you do or do not have an adequate vision and strategy for the GDPR. Without these guiding principles it is likely that your programme will not have been built to reflect the unique characteristics of your business and risk profile.

The risk of what?
We will consider your business in light of your ‘Special Characteristics’, the sector with which you are most closely associated with and your major data processing operations. We will combine this insight with our insight on regulatory hot topics, the aspects of data protection that tend to aggravate data subjects and review if your programme has prioritised the reduction of risks in these areas.

Paper shield
How you have described your approach to the GDPR is a fundamental requirement of the GDPR. With the introduction of the ‘Accountability’ principle we will assess the extent to which any updates to your paperwork and policy framework are appropriate for compliance.

Technology and operational change
Our experts will consider your organisational cultural and the technology and business process related requirements contained within the GDPR have been understood and considered within your programme.
When to act

The following are triggers should get you thinking about a second opinion on your GDPR programme:

- You are yet to scrutinise your programme.
- You have outsourced the design and build to a third Party.
- Your programme is being managed by a single function team with limited or no input from the broader business.
- You have an upcoming Executive forum where an update on your organisations GDPR journey would be beneficial.
- Your enterprise strategy contains initiatives or aspirations that will require you to have built an agile approach to the GDPR.
- You or your sector are under scrutiny by the press, your customers/employees or the regulator.
- New A29 WP/ICO guidance is published.
- Privacy leadership leaves the business.

What you gain

- **A multidisciplinary approach** – Your review team will comprise of data protection legal experts, risk and control advisors and programme management consultants. All with deep subject matter expertise.
- **A friendly challenge** – An opportunity to defend your programme in a safe environment, allowing you to reflect on decision making and investment.
- **Confidence** – Our second opinion will either give you confidence that you are in a strong position or it will provide you with the support and guidance you will need to adjust your approach to achieve your desired outcome.
Contacts

Jane Wainwright
GDPR Strategy, Law and Compliance
Director, PwC UK
E: jane.a.wainwright@pwc.com

Stewart Room
GDPR Strategy, Law and Compliance
Partner, PwC UK
E: stewart.room@pwc.com