In partnership with

The Pelicam (oh no, not another) GDPR Briefing

For more information, please contact:

Helen Morgan (Business Manager)
Tel: +44(0)7811 404 127
Email: helen.morgan@pelicam.com

www.pelicam.com

pelicam ASSURED DELIVERY

In partnership with

Create & Comply CUTTING EDGE CITY SOLUTIONS

Oh no, not another GDPR Briefing?

At the risk of irritation, many GDPR briefings are heavy in frequency, but perhaps light on clarity and usefulness. So, together with our friends at Create and Comply, we venture a little warily into the GDPR den and offer a view and a few pragmatic recommendations that we hope will be well-received by our community of Intelligent Project experts.

Business context

The facts are straightforward. By May 2018, all organisations are required to demonstrate compliance with the General Data Protection Regulations (GDPR). Failure to comply can – in the most serious cases – lead to the risk of fines of up to €20m or 4% of global revenues, whichever is greater.

So, no wonder many organisations have tasked project teams to scope, prepare and ensure all reasonable steps are being taken to comply. While many businesses can demonstrate this commitment, a good deal more may not be adequately prepared. Indeed, feedback from the expert Pelicam team of practitioners across our client base, indicates that boards are asking tough questions and not always receiving satisfactory answers.

In mitigation, any organisation that can show that serious steps are being taken in terms of documentation, processes and practice, then the Information Commissioners Office (the ICO) will likely take a more lenient view in the event of any breach. However, woe betide any business that is seen to contravene good practice. Check out the ICO website for just some of the latest breaches and heavy fines that have been levied in recent times. Link here.

GDPR Obligations

So, what are the obligations? Simply put, every organisation that holds or processes EU citizen's personal data, must be able to demonstrate compliance with the legislation. In practice this means:

- Appointing a Data Protection Officer
- Notifying the ICO of any breaches within 72 hours
- Design and implement processes that safeguard subject's rights AND only hold personal data that is necessary
- Being able to identify and document risks connected with data processing (including sharing data with partners and third parties)

Some implications

Alongside the ***substantial fines*** that the ICO may levy in the event of a serious breach, major organisations in Financial Services, Commercial and related sectors can of course, suffer ***severe reputational damage***. Yahoo, eBay, Equifax, JP Morgan, Sony PlayStation, Adobe, TalkTalk, have all been the 'victim' of attacks and serious data breaches in the last four years.

In fact, recent news regarding Uber may well have serious consequences, perhaps more down to the way they responded (and failed to alert relevant authorities) than the data breach itself.

How should organisations respond?

While bad people can do bad things, a (weak) response from an organisation can have just as serious a consequence as the attack and breach itself. ***Reputational damage*** can adversely affect consumer confidence to consider or stay with an organisation and this may effect revenues and profits for years to come.

That is aside from of course ***the cost of repairing a data breach*** and the allocation of resources to resolve and ensure adequate protection is taken to prevent future breaches. All in all, a scary proposition that is beginning to exercise the minds of board members alongside the usual in-house functions spanning IT, operations, finance, marketing, sales, HR and legal teams.

For many, the ***cost is less of compliance*** and more on assuring sufficient protections and defence for the organisation and its partners who also are involved in managing customer data. In fact, assurance on the supply chain of partners is just as important as from within the organisation.

That said, another view is to take a more positive view of preparing the organisation for growth and many clients have created cross-functional project teams to do exactly that. Other substantial transformation programmes may not have a GDPR name or focus - but you can be sure that the 'implications' of GDPR compliance are – or should be – uppermost in the project sponsor's minds. And it is this aspect that may benefit from an expert eye.

Some pragmatic suggestions

The Pelicam team have seen smart organisations benefit from some expert help that can include:

- Commission an independent project and assurance audit

  The Programme sponsor can ascertain that all the project attributes are defined, managed and under control. This involves a short, sharp piece of work with clear insight and pragmatic recommendations

- Attain control and visibility of transformation programmes

  Provide convincing and credible objective oversight to reassure Boards that key projects are on track, on time and budget

- Performing a front to back review and health check

  Assurance and compliance focus of your third parties and outsourced service providers for GDPR in the specific context of your business model

- Overview of GDPR in the context of Change projects

  For programmes already in flight or planned, ensure cross reference is in place, share best practice and leverage cost saving opportunities

Conclusion

In today's digital-led landscape, it's imperative to ensure change initiatives are mobilised quickly and effectively aligned for success and that your teams are resourced with the right mix of leaders, shapers and followers. The Pelicam team of expert practitioners and our partners at Create and Comply can assist you to explore how best to accelerate delivery and defend your timescales and costs, and continually seek to build intelligence and capability within your teams. Or, as we often say, deliver control, certainty and compliance in corporate project & programme transformations.

For more information, visit www.pelicam.com or www.createcomply.com