GDPR

Detailed Board Action Plan

There are now just six months to go until the new GDPR regulations come into force.

We've all heard the headlines:

- the new rules will apply to all businesses regardless of size
- GDPR is significantly more demanding than existing rules
- fines for non-compliance will be up to 20M Euros or 4% of turnover

GDPR is an opportunity to streamline your business processes:

- Reduce your costs
- Reduce risk
- Improve customer service

© Freeman and Clarke Limited 2017

GDPR

FREEMAN CLARKE

Detailed Board Action Plan

Set GDPR compliance in the context of a growth roadmap:

- **Innovation and Digital**
- **IT Roadmap for growth**
- **Efficient, effective processes & systems**
- **Risk & compliance management**

Our clients are companies who want to expand and seize opportunities and, to this end, GDPR compliance should be seen as a badge for a well-run organisation with slick, secure, integrated processes and systems.

Well organised companies are efficient, provide good service, expand without fear, and innovate using digital technologies. For these companies, achieving GDPR compliance is not a great challenge.

GDPR is a far greater challenge when systems are not integrated, processes are manual and ad-hoc, and data is out of control. Addressing GDPR without addressing the underlying weaknesses is a missed opportunity, and in all likelihood will not fully address existing risks.

So when we work with companies on GDPR compliance we see this as part of a journey to implement IT that will drive their growth.

So how can you approach this in a way that's sensible and commercial? How do we go about this in a reasonable and lawful way?

The approach has six phases

- Awareness
- GAP analysis
- Implementation
- Ownership & discovery
- Planning
- Monitoring

© Freeman and Clarke Limited 2017

GDPR

FREEMAN CLARKE

Detailed Board Action Plan

Awareness

- **Presentations/workshops**
  Start by educating staff about the issue through simple presentations and/or discussions
- **Leadership team reviews**
  The Board and senior managers need to have a more in depth understanding of the regulations and to start to consider how this affects the business

Ownership & Discovery

- **Define Board owner, roles & governance**
  Who is accountable and how will the compliance project be overseen?
- **Appoint a Project Manager and team**
  Who will actually manage the detailed project and who else will need to be specifically involved?
- **Identify affected internal processes**
  List all the internal activities that involve collection, handling and deletion of personal data in organised, centralised or ad-hoc ways, both deliberately and inadvertently!
- **Identify affected external suppliers**
  List all suppliers who have a role in collection, handling and deletion of personal data in connection with your activities.

For larger companies:

- **Appoint a Data Protection Officer** – if necessary, someone will have to formally take on the role of Data Protection Officer.
- **Appoint legal advisors** – if necessary, appoint expert lawyers.
- **Use external tools** – if necessary, use external questionnaires and diagnostics to assist with the analysis.
- **Use IT discovery tools** – if necessary, use IT tools to help locate and categorise data and equipment.
- **Backfill project staff** – if necessary, bring on additional staff to free up those staff allocated to the GDPR project.

© Freeman and Clarke Limited 2017

GDPR

FREEMAN CLARKE

Detailed Board Action Plan

Gap Analysis

- **Review all data acquisition**
  Review compliance of all personal data acquisition.
- **Review all data processing & deletion**
  Review compliance of all personal data processing and deletion.
- **Create a RAG Health Check report**
  Create a simple report showing compliance of all the data handling categorised into Red, Amber and Green.
- **Business risk assessment**
  Consider the commercial risk and appropriate actions.

For larger companies:

- **Review with legal advisors** – if necessary, retain legal advisors through this phase.
- **Review business value of data activities** – if necessary consider whether the personal data activities are actually adding value or whether they can/should be stopped.

Planning

- **Prioritise changes**
  Based on RAG and risk assessment, prioritise the necessary changes.
- **Create costed project plan(s)**
  The prioritised list needs to be turned into a simple, but fully costed project plan.
- **Review plans and agree**
  The plans need to be reviewed and properly agreed with full support of the Board.

For larger companies

- **Consult with IT suppliers** – if necessary, involve IT suppliers who might need to make tech changes.
- **Review with cybersecurity experts** – if necessary, involve cybersecurity advisors where there are complex issues or if penetration tests are necessary.
- **Create overall programme plan** – if necessary a more substantial programme plan might be needed.

© Freeman and Clarke Limited 2017

Implementation

- **Deliver systems and tech changes**
  Make whatever changes are needed to infrastructure, line-of-business systems or online activities.
- **Amend processes and documents**
  Agree changes to ways of working, contracts, policies, job descriptions, notices or anything else relevant (including new processes for handling subject access requests).
- **Communicate with and train staff**
  There needs to be an organised engagement with staff to explain the changes in detail and to ensure they are fully engaged. Crucially, they will need to know how and where to report any potential breaches or potential non-compliance they may see.
- **Communicate externally**
  Communication may be necessary with suppliers, partners and customers.

For larger companies

- **Engage suppliers for IT projects** – if necessary, IT suppliers will need to be involved, there may be a process of RFP, quotes and full scale projects.
- **Consider systems/process redesigns** – where processes or systems are fundamentally non-compliant then ground-up redesign might be necessary.

Monitoring

- **Define frequency/approach**
  How will compliance be monitored and how often?
- **Add to monitoring processes**
  Record the new monitoring arrangements within existing processes.

For larger companies

- **Add to Board schedule** – if necessary then organise formal Board reviews on a regular basis.
- **Add to strategic Risks Log** – if there is a strategic Risk Log then GDPR compliance should be added as an ongoing item.

© Freeman and Clarke Limited 2017

GDPR

FREEMAN CLARKE

Detailed Board Action Plan

In our experience, these phases and steps provide a simple framework for GDPR compliance.

Although achieving GDPR compliance will consume effort, it really should be seen as an opportunity to reorganise, to streamline and integrate activities.

Companies that are able to manage data well are also able to work efficiently and to provide good service, and a strong commitment to data safeguarding will increasingly be a **marketing advantage**.

GDPR is an opportunity to streamline your business processes – reduce costs, reduce risk and improve customer service.

One of our IT Directors will get you on track. Get in touch today.

Phone
0203 020 1864

Email
contact@freemanclarke.co.uk

More content on...

- **Solving Integration Problems**
- **IT Risks, Compliance & Security**
- **IT Roadmap for Growth**

Click the images to go directly to the documents

© Freeman and Clarke Limited 2017