The 25 May 2018, when GDPR, and the associated UK Data Protection Act 2018, came into force was a landmark date for data privacy, but fast forward nearly six months, what should you be doing now?

A plan is critical

Doubtless you will have all seen project plans setting out all the things your organisation needs to do to be 'GDPR compliant'. That compliance is however not a single, set, marker - but rather an evolving landscape where what is required for compliance changes, based on your activities, operations and your people. We often get asked 'what do we need to do to be GDPR compliant?' The core parts of the answer are self-evident from the requirements in the GDPR itself and related guidance, and then making those operational. This article focuses on planning and delivering that ongoing change, as well as raising awareness.

A perfect storm

Shoosmiths often works with General Counsels and compliance teams, who are faced with the impossible. The number of reported data incidents increases all the time, as awareness grows within organisations as to what a breach may be, and how to report incidents. Equally, individuals are now more aware of their rights - and they are exercising them in considerably increased numbers. We've seen rises of several hundred percent, placing resourcing issues on those tasked with 'being compliant'. But what does this mean for those teams, and how can they progress data incident management, data subject rights management as well as progressing the ongoing compliance actions?

Focus

For those organisations facing this storm, there needs to be focus on both the compliance obligations as well as the changes and improvements which still need to be delivered. Without achieving both, that Holy Grail of 'GDPR compliance' is further away. Imagine the scenario where you have had a data breach (of any kind) and the ICO is investigating. It may well want to know the steps you've taken (and are still taking) to be compliant. You have to record this as part of your Accountability Principle obligations. But have you? Do you know where it is and who holds it? The Information Commissioner herself said that 25 May was the beginning of an ongoing compliance journey. But as with all good journeys, if you don't have a timetable or map then it will be more difficult.

Many organisations have created repeatable processes - for example breach triage forms, or data subject rights portals - although these add to the challenge, as they create a great deal of work in reviewing the results, particularly when the answers provided are inadequate. And whilst this is a step in the right direction, if wider actions are not
progressed, there's real danger of stagnation - not progressing that compliance. The tight
deadlines for dealing with data subjects' rights requests and breaches contribute to teams
feeling overwrought. A deliverable project plan with a clear focus can help here.

Agile delivery

Adopting elements from agile development methodologies, we've worked with clients to
streamline their approaches to their 'to do' list and use agile-like 'sprints' to focus on
review, delivery and follow up of a clear set of actions, in a risk-based priority order and
including risk mitigations. This creates a focused and deliverable plan to improve
compliance.

Many at the business coalface will think that GDPR has passed and the business can now
focus on the next legal or regulatory change ahead. But [as you and we know,] the reality is
very different - so the plan can include actions to re-engage the business and raise
awareness of the ongoing compliance journey.

Raising awareness, breaking silos and driving business ownership

Many organisations will have rolled out GDPR training, with varying degrees of success.
Perhaps it will have been rolled out from the Group's compliance team overseas, with
language issues, key messages missed out or perhaps very general without any
specialisation or tailoring to the business function. We've seen it all!

One of the things you as GC and/or in the data privacy compliance team will have now, as
part of all this work, is an incredible view of what each part of the business does, and how
it all fits together. In one review we undertook some months ago, the GC said by
undertaking the review, over a couple of weeks she had learned more about the business
and what it does (and the associated risks) than she had done in the last couple of years
of working at that organisation. This insight enables you to move the business from siloed
functions to a lifecycle view of data - representing what is done with data and why (and
future-proofing where possible).

In breaking those silos, and also providing more specific training, an important message
will be to give the business ownership, and explain why it is important for them have this.
We often find after a breach report has been passed to the data team, the business team
won't then answer questions or provide the timeliness of response which is needed to
assess whether a data incident is reportable or not. If that information isn't there, the
wrong answer may be arrived at, and it will be the business's operations, revenue and
reputation which is put at stake. Taking ownership is therefore critical. It's another of
those situations where collaborating will achieve much more, much more quickly. You
could establish a network of champions, from those who are interested in each business
team. These champions can provide additional Q&A level of support for teams, and able to
be familiar with process, so core data privacy teams can focus on adding the most value.

Perhaps if things really need shaking up, a breach role play would be useful. A bit like a fire
alarm test, a mock data breach is rolled out so that processes, personnel and practice are
all tested. It will iron out weaknesses, improve process and bond personnel so that if/
when there is a real breach, the learning will have been done.
Evolving your approach to compliance can mean a significant benefit can be delivered, whilst minimising additional resource needs. We hope some of the things we've seen as a firm can help deliver change in your organisation.