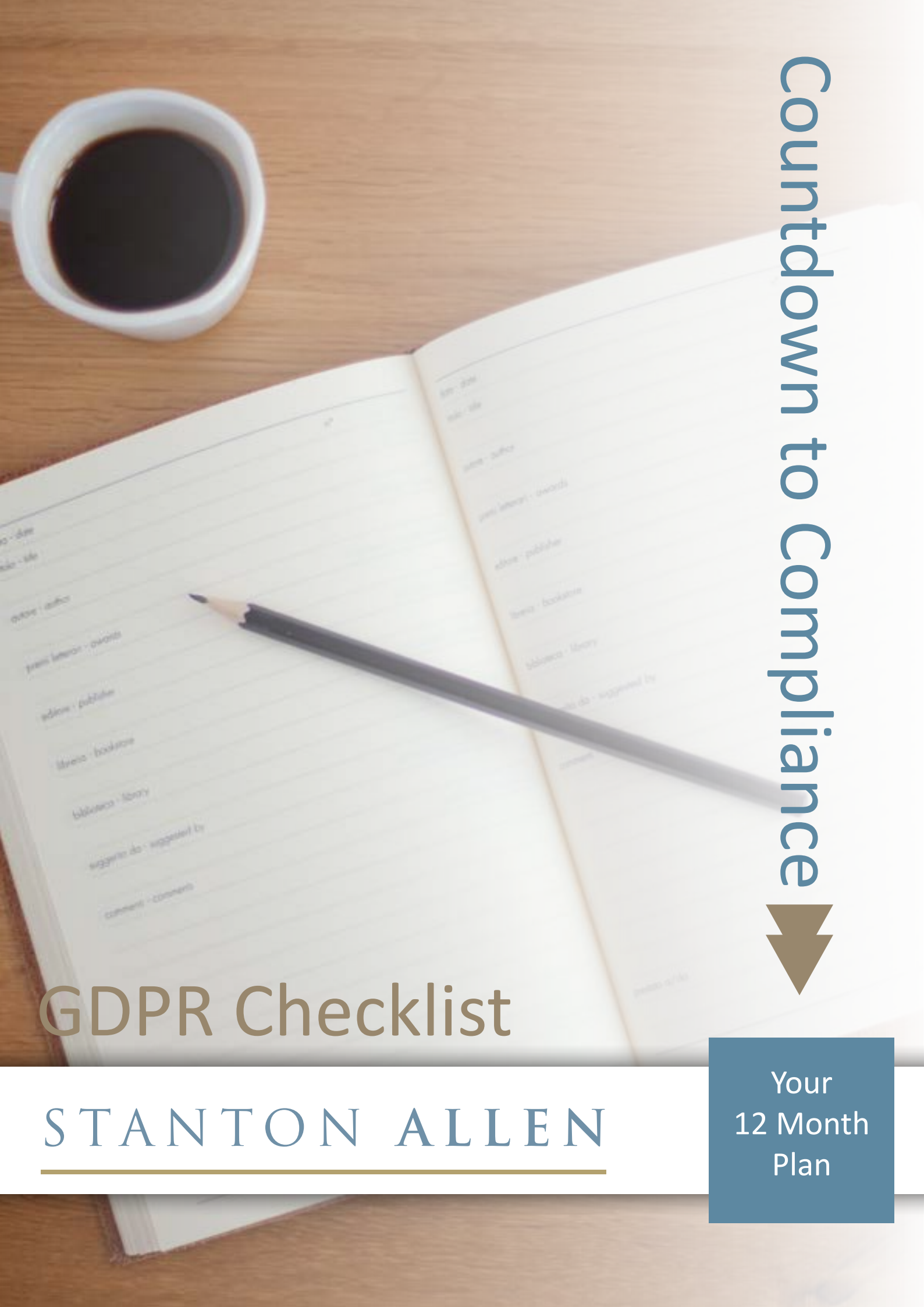

Countdown to Compliance

GDPR Checklist

STANTON ALLEN

Your
12 Month
Plan

10 Key Things you need to know

- You must establish a “legal” basis for processing data the “conditions for processing”
- The principles are similar to previous legislation but specifically of note are:
  - Changes in rules of how to identify a data subject
  - Increased obligations around Data Security & Breach reporting
  - Tightening of Consent definitions and processes
- Accountability is a significant change in emphasis between a “passive” and a “proactive” approach to demonstrating compliance
- Clarification of consent and the need to keep a record of consent.
- Consent must be explicit for sensitive data
- Tightening of subjects’ rights : A.R.E — Access | Rectification | Erasure
- Greater obligations when it comes to processors and sharing data with 3rd parties
- Expansion of territorial reach (those outside EU marketing into the EU are now obliged to comply)
- Obligation to appoint a Data Protection Officer (if the core activities of the controller or processor consist of processing which requires regular and systematic monitoring of data subjects on a large scale)
- **Fines for failure to comply are significant**

Processing Principles

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data is accurate;

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Accountability Principle

- Implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.

- Maintain relevant documentation on processing activities.

- Where appropriate, appoint a Data Protection Officer.

- Implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
  - Data minimisation;
  - Pseudonymisation;
  - Transparency;
  - Allowing individuals to monitor processing; and
  - Creating and improving security features on an ongoing basis.

- Use data protection impact assessments where appropriate.

This month's actions are all about laying the foundations for compliance. This involves checking off some specific actions, but more importantly identifying the stakeholders within the firm that you are going to need to work with.

Notes

MAY

Action

Confirm your legal basis for data processing.

Influence

Identify within leadership the key individuals that you will need to work with to implement the firm's GDPR plan.

Measure

Run a report on your CRM system (and other systems if you have them) that enable you to segment contacts by your confidence in the quality and completeness of their Consent Status e.g. explicit consent, implied consent, no consent.

We now have less than a year to go, so this month there is a need to get some key elements in place in the plan.

Notes

JUNE

Action

GDPR has a requirement to build data security in to your processes by design. So this month's action is to review your existing processes for reporting breaches and to identify specific areas of weakness.

Influence

If you've not already done so you need to identify your Data Protection Officer. You will be working closely with this person over the coming months.

Measure

You need to work with your DP Officer to review your findings from your exciting processes and score them according to their risk.

You might be forgiven for thinking that as we approach the summer you could take your foot off the pedal. However if you are, like most firms, in the position where your existing processes leave somewhat to be desired, you are going to need to work hard to address the issues that your process audit will have uncovered.

Notes

Action

Focus on your areas of greatest vulnerability. Most firms are not likely to be of great interest to hackers (unless you focus specifically on M&A) so whilst data centres and servers are incredibly important, most firms actually have what might be considered fairly mundane points of weakness. For example do staff email unsecured data to 3rd parties? Do they work on Wi-Fi in unsecured locations? These are the sorts of things that can often be overlooked but can be open to interception.

Influence

You're going to need to work with your risk and compliance people to ensure that your policies are up to date and that key areas of weakness are eradicated.

Measure

If you can, with the help of IT, you should be looking at email systems or logs, such as Mimecast, to try and understand how frequently data is emailed outside the firm's firewall

JULY

One of the big changes in the legislation is the increased obligations on data processors, so it's not enough simply to put your own house in order you need to make sure that those processing data on your behalf are in good shape too

Notes

AUGUST

Action

Evaluate your contracts with 3rd parties and determine if you need to speak with your suppliers and/ or review their tighten their contracts.

Influence

You are going to need to involve purchasing (or whoever has responsibility for managing contracts) as you are almost certainly going to need change some of your supplier vetting processes to ensure that they are meeting their obligations.

Measure

Evaluate the number of times that data was processed on your behalf and if you can determine how often that data was taken off-premise or connected to remotely

There is a lot of mythology and misunderstanding on what constitutes compliance. You can take the common sense route, which is that if a person is engaging with your firm then obviously they have given consent for you to contact them. In many cases that's true, but in legal terms it is still only implied consent. This month is all about getting firm-wide agreement on terminology and interpretation

Notes

SEPTEMBER

☐ **Action** Define your Consent statuses.

☐ **Influence** Work with the DP Officer and Risk and compliance on your definitions, where you think you currently stand and what actions you need to take.

☐ **Measure** Re-run your audit of consent and insist that this is discussed at the next board meeting.

Over the last 6 months you've been putting in place the foundations for compliance by looking at policies and processes, suppliers and staff and key areas of concern or weakness. This is all excellent as one of the key changes in the legislation is the fact that you need to prepare for the Accountability principle. What this means is that it's no longer sufficient to be able to defend an accusation of non-compliance but proactively demonstrate everything you do to achieve compliance

Notes

OCTOBER

Action

Start compiling your bible of GDPR with everything you've found so far. The next few months are going to be all about fixing problems, implementation and training.

Influence

Work with your training and HR colleagues as you are going to need their assistance in developing training programmes and building the obligations to follow the firm's processes in to your HR policies.

Measure

Report back to the board on what you have done and your roadmap for the 6 months ahead.

October's actions were all about starting to put together your process bible for GDPR. I discussed the Accountability principle. What this means is that firms must be able to proactively demonstrate that they comply with the Act not just react to breaches or issues. In November your goal is to build the training materials for your firm.

Notes

NOVEMBER

Action

Create the training documentation that will be needed to train your users and to demonstrate that you are including information and data security in all staff training.

Influence

You will need to work closely with the Data Protection Officer and with HR to ensure that your processes and training documentation is included in the induction programme and also in all staff contracts.

Measure

It would be a good exercise to find out from HR is they measure what training people have had and if they are required to sign any statements confirming their acceptance of policies or that they have attended a training course on a specific topic.

Although we might all be thinking of other things in December, we don't want to get complacent. We only have 5 months left until the legislation comes into effect. This month you need to be thinking of the other data subjects' rights, not just consent.

Notes

DECEMBER

Action

Make sure that you and the DP Officer are clear about what the right to Access of information, the right to Rectification of that data and the right of Erasure mean and that you are confident that you have systems and processes in place to manage this. It might be a good time to consider a data amnesty and get people submitting their lists over the Holiday season so that you can evaluate them in the New Year.

Influence

One of the key challenges is that not all the data on individuals may be in the CRM system. Now is the time to make sure that the Directors and Partners of the business are aware that the only way that they can hope to comply is by making their colleagues disclose and share their contact information.

Measure

You should have reports in place that enable you to quantify how much contact data is in the firm's core systems and where else data might be lurking e.g. in spreadsheets or Outlook

Now that you've spent time understanding the rights that data subjects have, you need to put together your policy statements so that they are aware of them. The legislation is very clear about what you have to communicate so it's almost certainly the case that every firm will need to update their information statements.

Notes

JANUARY

Action

Create the necessary policy and privacy statements on your website and on all your outward facing communications.

Influence

You'll need to work closely with marketing communications and also the DP Officer to make sure that your statements are correct and contain all the information that is required by law.

Measure

You should do an audit of the locations where you are required to have policy statements to make sure that you have all your bases covered.

Now that we're getting to the sharp end of the 12 month countdown and by now a lot of what we need is in place, we need to think about the on-going data quality programme. You'll need to build in the necessary processes and measures moving forward beyond May 2018. One of the requirements of the Act is that data is accurate and relevant, so data quality is incredibly important.

Notes

FEBRUARY

Action

Create a data management plan with clear processes for how you deal with adding new contacts to the system, how you maintain and manage data quality and how you are going to deal with archiving and deletion.

Influence

You may find that you need additional budget or resources to ensure that you comply with the requirements of the Act, so it's a good idea to work finance to ensure that sufficient budget is allocated to data management and quality.

Measure

You need to build in detailed audit measures in your system to record data quality. Principally how you validated data and when. It would be a good idea to think about implementing some sort of traffic light system and also give consideration to how your users are going to get involved if contacts don't reply to communications asking them for the express consent, or if their consent status is about to lapse.

Just 2 months to go. In these final weeks it's all about training. Whilst you won't be responsible for training on GDPR specifically, you need to make sure that GDPR training is a critical part of CRM training and that users understand what is expected of them in relation to data that they add to CRM and the use of marketing lists.

Notes

MARCH

Action

Implement a programme of user training on the CRM system with a key focus on consent, marketing lists and data quality.

Influence

You'll need assistance from the board to ensure that users are required to attend training.

Measure

Keep a record of who's been trained and make sure that this is shared with the board so that they can track progress.

So with just one month to go, you should be in pretty good shape. This month is all about making sure that everything is in good shape and preparing a final report for the board.

Notes

APRIL

Action

Create a checklist of all the actions that you've completed over the last 12 months and prepare a report for the board.

Influence

Work with your colleagues in finance, HR and Risk along with the DP Officer to prepare the board report.

Measure

Make sure that the checklist is something that you can use on an on-going basis to ensure that you continue to comply.

So with just one month to go, you should be in pretty good shape. This month is all about making sure that everything is in good shape and preparing a final report for the board.

May 25th

So now it's finally here. All that hard work will be worth it. There will be many others who are probably panicking right now but you can sit back and relax knowing that you've done everything you can to get ready for the legislation.