The 10-step GDPR Action Plan

Bite-sized practical guidance on how to meet the requirements of this new regulation.

Produced by LexisNexis Enterprise Solutions in conjunction with Gary Hibberd, Managing Director, Agenci

LexisNexis®

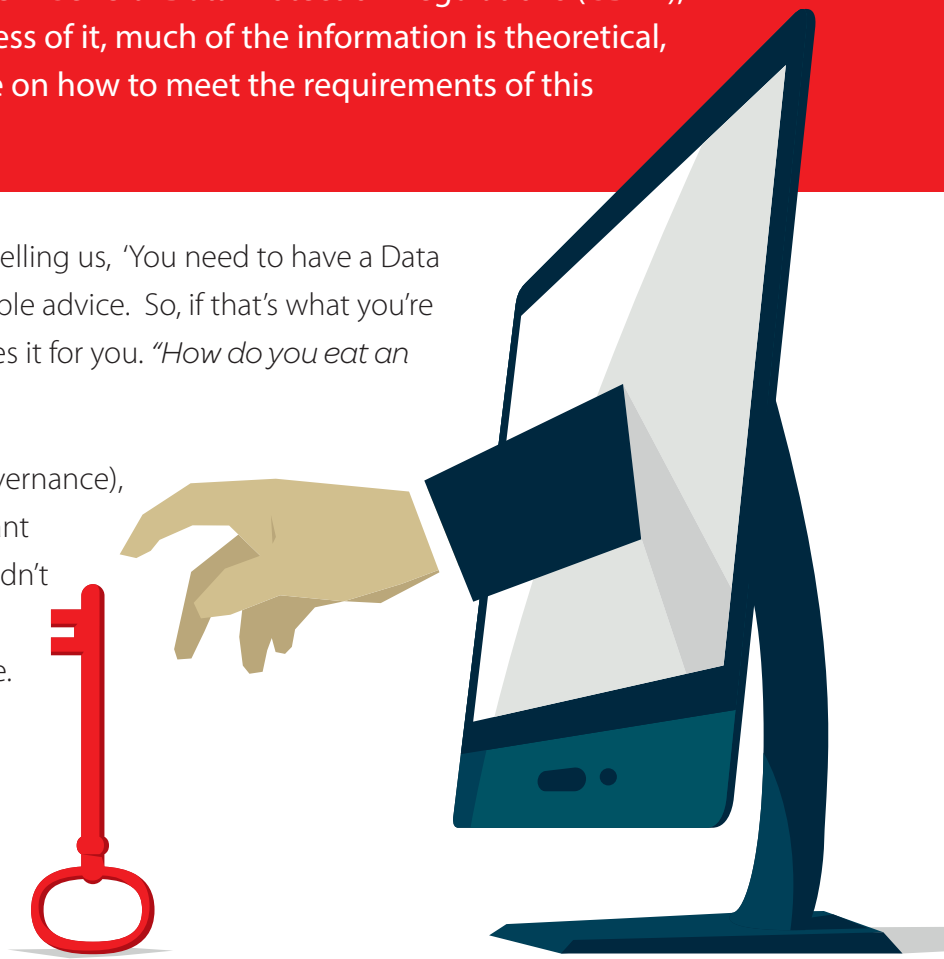
Enterprise Solutions

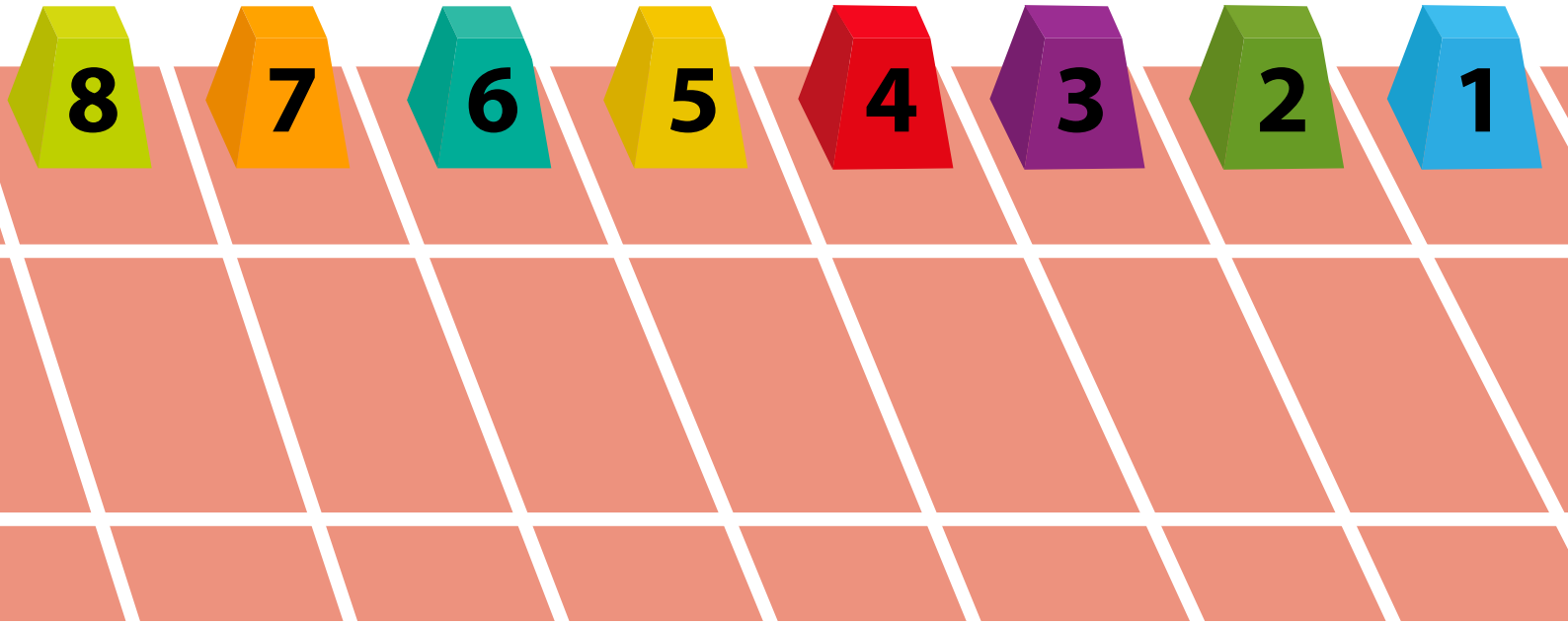
Contents

Much has been written about the new General Data Protection Regulations (GDPR), and whilst it's good to raise awareness of it, much of the information is theoretical, and doesn't offer practical guidance on how to meet the requirements of this new regulation.

What we really need isn't another post telling us, 'You need to have a Data Asset Register', rather a little more tangible advice. So, if that's what you're looking for, I hope the following provides it for you. *"How do you eat an elephant? One bite at a time".*

Yes, GDPR is BIG (Better Information Governance), but the first and probably most important point to note, is that addressing it shouldn't be more complicated than any other major project that you would undertake. Planning is everything.





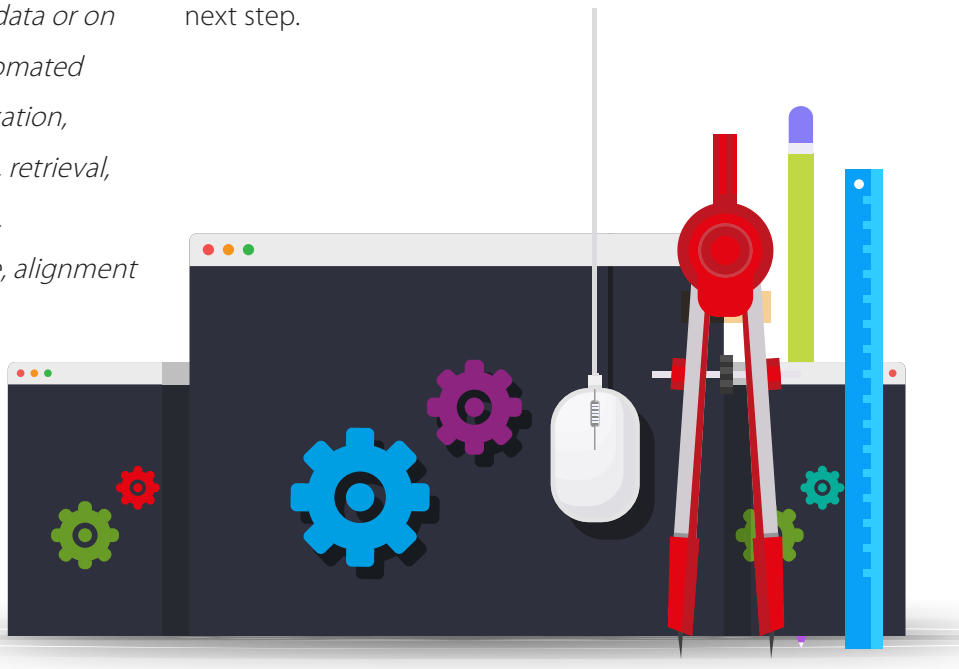
Step 1. Project initiation

Preparation for GDPR should be approached as a project, so establish a team to ensure the entire business is aware of the process. Bring together key people from across your business. This includes HR, Finance, Sales, Marketing, Operations and IT. These are typically the areas that will be involved in processing data.

Remember, processing is "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*". (Article 4.2)

Once the team is assembled you need to define your scope (what needs to be included), your objectives and the timeline for the project, with key milestones.

GDPR should be supported by the business owner/ leader, and therefore if you can't get the above together… the rest is going to be extremely difficult and this project will most likely fail. This brings us to the next step.

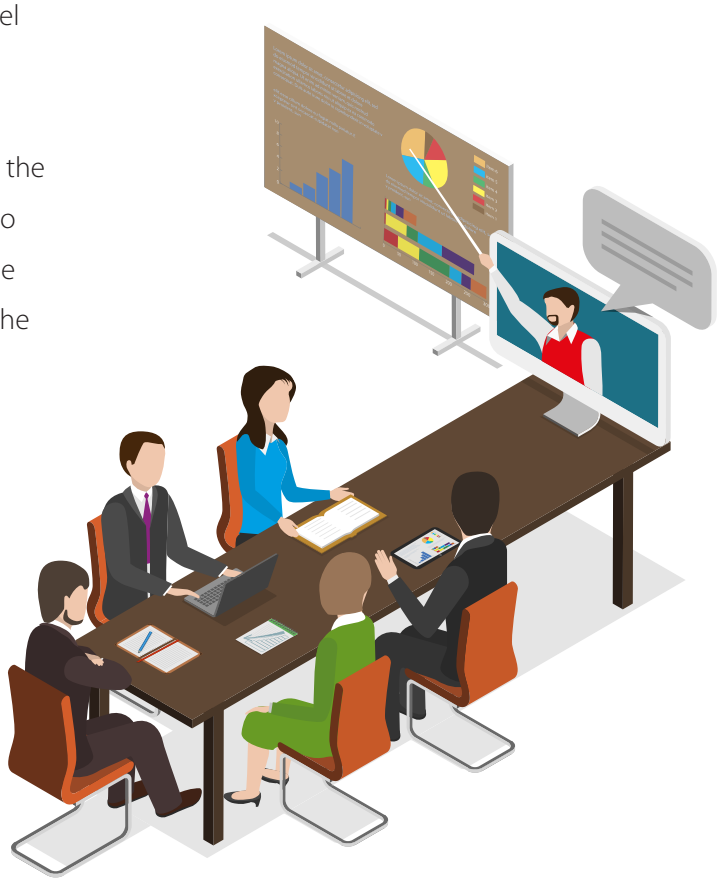


Step 2. Raising awareness

You're going to need the support of 'everyone' in the organisation, as 'everyone' in the organisation will ultimately be impacted by the changes that are coming. So, create an awareness campaign. Don't just send out an email. Think about a time line. What do you want people to know? What is important to each area and each level of the business?

Does the head of the business need as much detail as the frontline or support staff? What do you want people to take away from your messages? Your campaign can be as simple as a series of updates and newsletters over the coming months.

Or it could be a poster campaign, videos and webinars. It can and should include face-to-face briefings with key teams. Frequently Asked Questions - FAQ's on your intranet is a great tool. Create a buzz around GDPR, and take people on the journey with you.

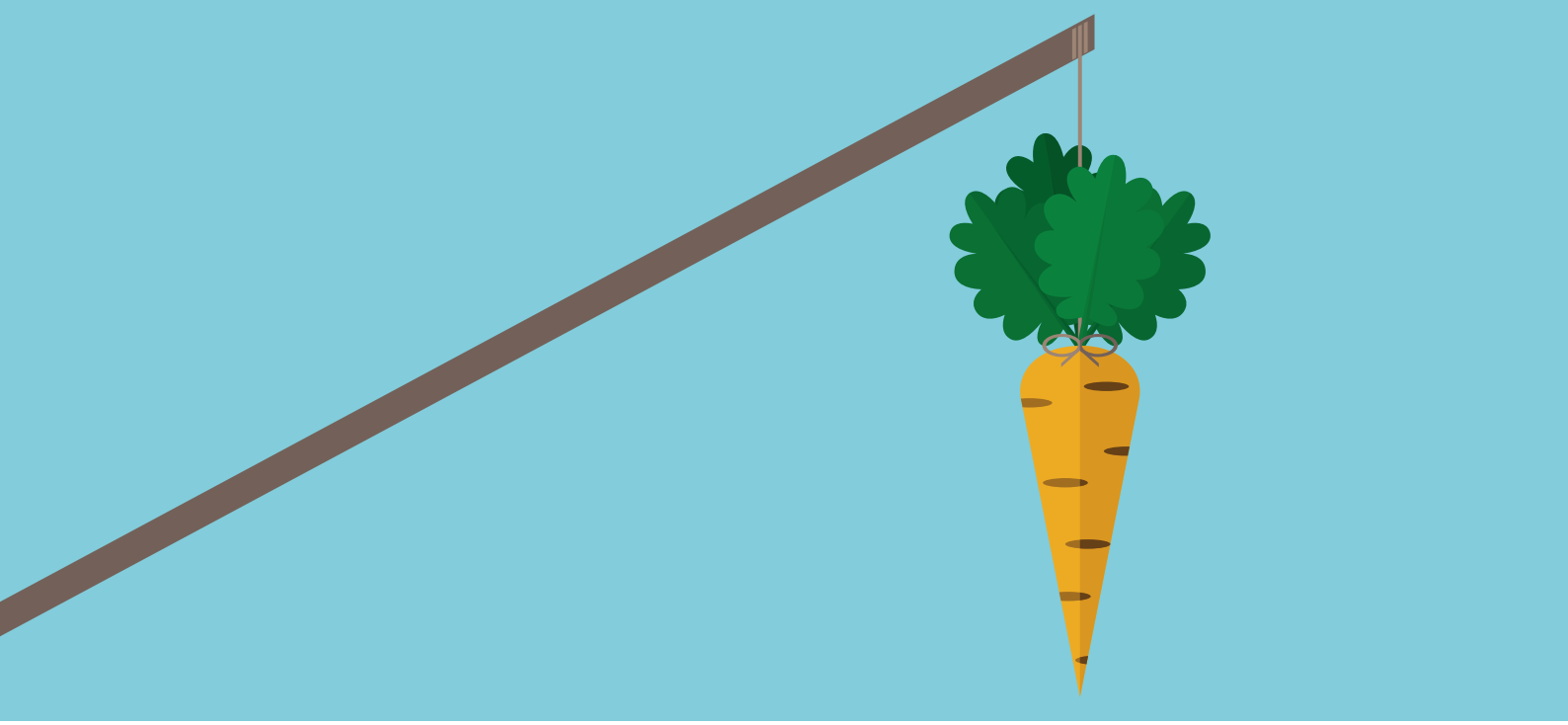


Step 3. Analyse your data

At Agenci, we believe you can't protect what you don't understand. So, it's time to roll-up your sleeves and gather some information. Depending on the size of your business this can take some time, or can be relatively easy. But create a set of questions which you can send to each head of department. The following questions must be included:

- Who is responsible for Data Protection in your department?
- What kinds of personal data e.g. name, date of birth, address do you hold, if any.
- Do you hold any 'sensitive' personal data, if so, please list.
- What is the purpose of processing this data?
- How has this information been obtained? E.g. via third-parties, direct marketing or any other.
- Where and how is this information held? E.g. on the corporate network, 'Cloud', laptops, in the CRM, in spreadsheets or any other.
- Roughly speaking, how much data is held? E.g. 10,000 case files, 100,000 CVs' etc.
- Have you defined a 'data retention' period for this data?
- Do you share this information with third parties or internationally?
- Have you or your team attended any training on Data Protection?

These are some of the basic questions to ask. At Agenci, we have a "39 steps to GDPR Insights". But the level of questioning is down to you. What you're looking to achieve is an understanding of where your risks are.
I would also suggest, that if you have multiple sites and departments, that you use Excel to collate the above. This information needs to be analysed and having 5, 10, 15 or more separate emails or word files will present a siloed view of your data landscape.



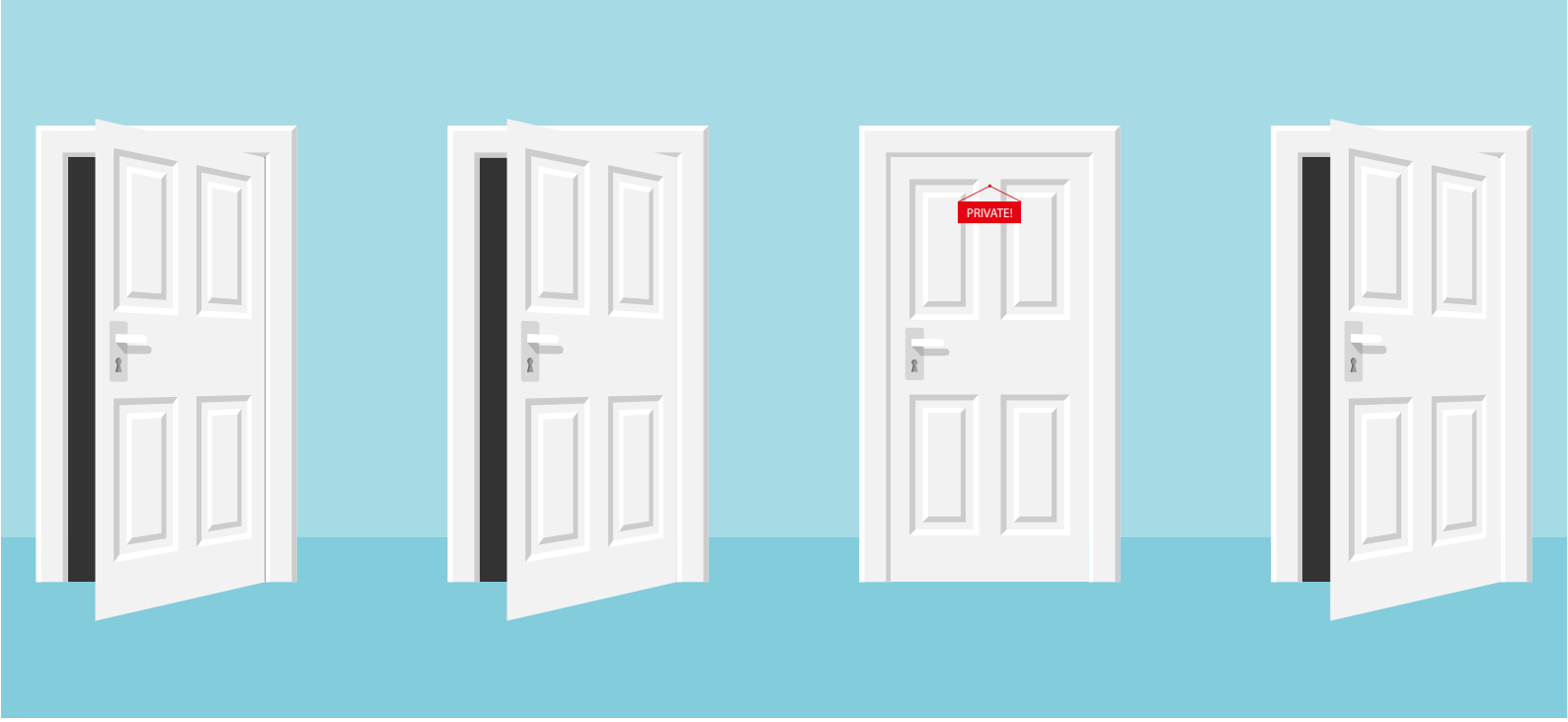
Step 4. What's up Doc?

Now you've got a good view of where your data is, you'll need to understand what documentation you need to put in place to protect it. This again is part of the analysis phase, and involves establishing any gaps in your policies and procedures you need to close. Begin by collating a list of policies, procedures and contracts from each area of the business that have any kind of impact on data protection.

Examples include:

- Data Protection and information security policies
- Employment contracts
- Supplier contracts
- Privacy notices
- Breach notification process
- Data inventory, aka an 'Information Asset Register'
- International organisations process
- Parental consent (and withdrawal) form / process
- Privacy impact assessment template and procedure
- Privacy notice(s), aka 'Fair Processing Notices'
- Subject access request form / process
- Training policy
- Transfer of personal data to third party countries

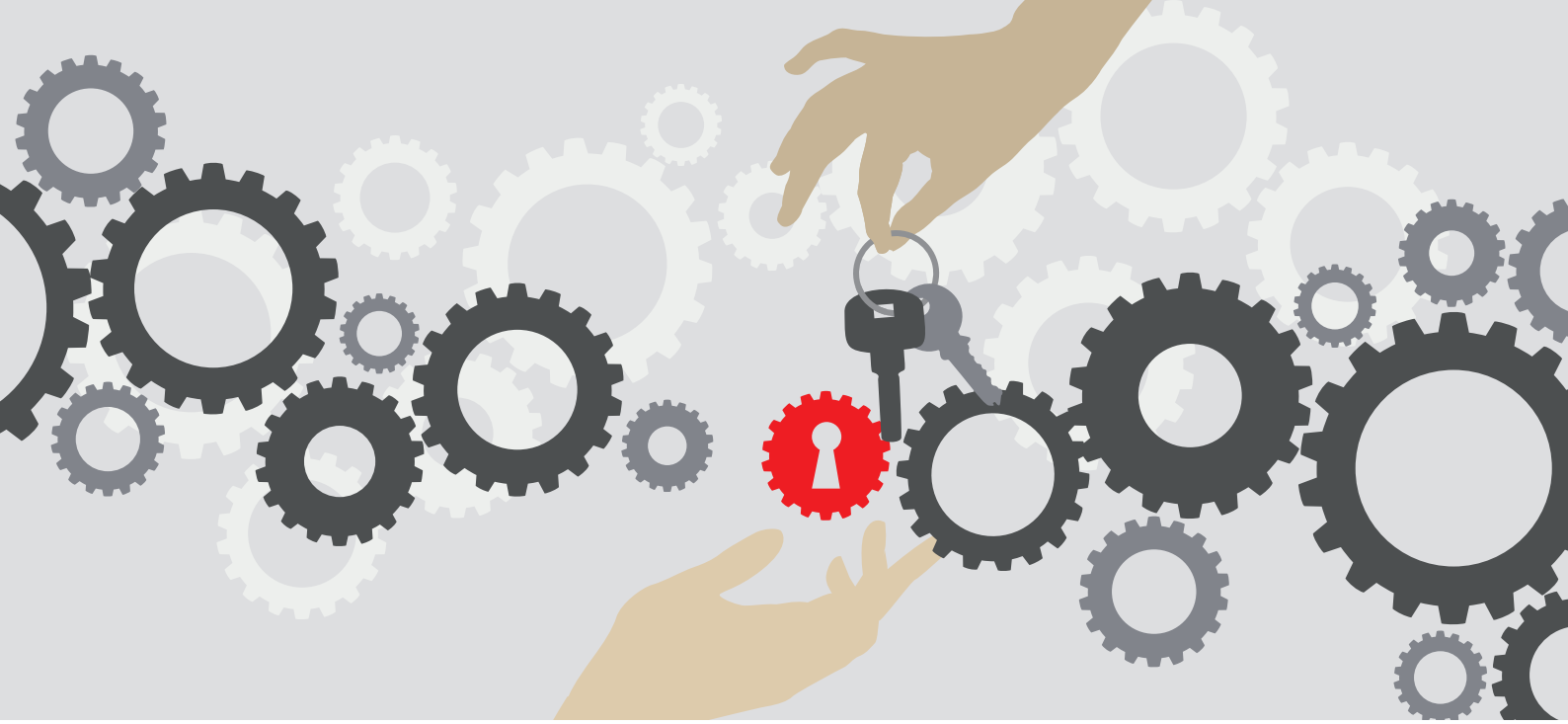
During this process, you'll also need to understand what 'privacy notices' you have and the contracts that are in place. Which brings us to Step 5.



Step 5. Say what you see

You will most likely already have some form of 'privacy notice' in place, possibly on your website, perhaps in other places too. You may not call them by this term, but essentially this is what 'Articles 13 & 14' of the regulation are looking for. Specifically, it is "Information to be provided where personal data are collected from the data subject". They tell the person you're collecting data from, what data you're collecting and what you'll do with it. This now extends to explaining who you'll share the data with, and who to contact if they have any concerns.

The 'privacy notice' can exist in contracts of employment and contracts with suppliers, contractors and of course, the customer. So, take some time to review what contracts you have in place and make any necessary changes.



Step 6. "I have rights," said Fred.

Under the current regulations we have rights, and few people know what they are, but the Information Commissioner's Office ICO has stated that the rights of data subjects should be central to processing of data. These rights are:

- Right to be informed (Article 12 - Article14)
- Right of access (Article 15)
- Right to rectification (Article 16)
- Right to erasure ('right to be forgotten' - article 17)
- Right to restriction of processing (Article 18)
- Right to data portability (Article 20)
- Right to object (Article 21)
- Right not to be subject to automated-decision making (Article 22)

Depending on the legal basis upon which you're processing data, you will need to assess if you can satisfy these rights, and if you can't then you need to explain why. Be aware that it is only if you're processing data based on 'consent' that a data subject has the 'right to be forgotten' and 'right of data portability'.

So, what is the basis on which you're processing this data?

Step 7. Let's keep it legal

The first principal of the GDPR is that personal data shall be… "processed lawfully, fairly and in a transparent manner in relation to the data subject" (Article 5.a). This means you need to establish a lawful basis upon which to process someone's data, and there are six reasons why you can process someone's data. These are detailed in Article 6, and summarised below as:

- The data subject has given consent
- Processing is necessary for the performance of a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary in order to protect the vital interests of the data subject
- Processing is necessary for the performance of a task carried out in the public interest
- Processing is necessary for the purposes of the legitimate interests pursued by the controller

Consider WHY you are processing the data and ask yourself of your business, how can you demonstrate that this is the case? For example, in the case of 'consent' you will need to evidence that you obtained the data subjects 'consent', to process their data (possibly for marketing purposes?). 'Consent' is the most difficult area, currently as the ICO itself is yet to fully define what is and is not acceptable (at the time of writing). However, this will become clearer over time, and I would always advocate looking to the other legal basis for processing, before relying on 'consent'.

Step 8. When it all goes wrong… who are you going to call?!

If you don't know what to do if (when?) you have a data breach, then you could be in for a rough ride with the ICO and your customers. You're probably well aware of the hefty fines, if you 'get things wrong', but you might not be aware that not informing the ICO within 72 hours could land you in hot water.

You might have put in place all the measures in the world to protect the data - trained all your staff, backed-up daily and have fantastic physical security - but someone, unfortunately, will let you down by emailing the wrong information to the wrong place – and then you'll have to explain yourself. And if you don't have a process to explain yourself very quickly to the ICO and to the data subjects in question, you'll possibly be faced with a fine but most certainly find your reputation has taken a strike, possibly even a mortal blow.

So, the first question is: Do you have a business continuity plan or an incident management process? If you do, then you've simply got to review this to ensure it covers not only 'physical' incidents (fire, flood etc.), but also technical ones. The next step is to ensure someone has the role on your 'crisis management team' to review the incident and make an appropriate assessments: - Does the ICO need to be notified? Do the data subjects need to be notified?

There are variables and it is not ALWAYS necessary to inform the ICO, or the data subjects (e.g. if the information has been anonymised or is encrypted). But someone needs to make that assessment. Who will it be? And are they in your plan?

Step 9. The Data Protection Officer

The role of the 'Data Protection Officer' (DPO) in the past has normally 'landed' with someone who didn't really want the role, but seemed to inherit it as part of another role. Compliance officer, legal secretaries, company secretaries, finance and risk leaders all seem to have the role of 'DPO' tagged onto what they do.

But the GDPR has stated that the role of the DPO is very specific, and requires very specific skills and a level of autonomy that currently does not exist. Articles 37 – 39 describe in detail if a DPO is required, what the position is and what their tasks are.

Your first step is to decide if you do indeed need a DPO, as there are only three reasons this is mandated.

These are:

- The processing is carried out by a public authority or body
- The core activities require regular and systematic monitoring of data subjects on a large scale
- The core activities of the controller or the processor consist of processing on a large scale of special categories of data

If you don't need to designate a DPO (which is a role that can be outsourced), you need to document your reasoning. But in any effect, even if you decide you don't need a DPO, you need someone who is designated to consider Data Protection in everything you do, because at some point, someone is going to want to exercise their rights, and when that happens you need a process for dealing with these requests.

Step 10. Your right of access

'Subject Access Requests' (SAR) have been with us for a long time, so most organisations will have a process for managing them. Under the new GDPR however the previous charge that you could levy against an individual to conduct a 'SAR' has been removed. Any form of official request should be treated as serious, meaning that an email stating: "I would like access to my personal data that you hold on me, for the following reasons…", needs to be dealt with swiftly. Even if the request is made on a call, the request should be seen as serious and whilst you may ask for clarification via email, you should know that rather than the current 40 days, you now have 'a month' to comply.

So, review your 'SAR' process and ensure everyone understands the importance of bringing any such requests to the attention of a named individual, possibly the DPO?

Conclusion

There you have it, 10 steps to take right now that will get you closer to being able to say you're ready for the GDPR, come May 25th 2018. Is this an exhaustive list of actions? No. Is this the correct order? Possibly. It has certainly worked for many organisations I have been involved with, but it most certainly generates further steps and actions to take. So, you should see this as being your 'Starter for 10'.

I would add that although 'every great journey starts with a single step', these 10 steps are on a far longer journey than 25th May 2018. We should see the GDPR for what it is: a change to how we treat data; before, on and after the 25th May 2018. So, whilst you're taking your first tentative steps, don't think of this as a journey to a destination. Think of it as a lifestyle change, because at the end of the day, GDPR actually, and simply means "Giving Data Proper Respect".

Contact Us >

LexisNexis®

For more information

To find out more about LexisNexis Enterprise Solutions please visit www.lexisnexis-es.co.uk, email salesinfo@lexisnexis.co.uk or call +44 (0) 113 226 2065 to speak to a LexisNexis Enterprise Solutions consultant.

LexisNexis®

Enterprise Solutions