10 STEPS TO GDPR COMPLIANCE

1. RETHINK HOW YOU USE PERSONAL DATA. It's not your data, it belongs to the individual. Personal data is a risk and a liability as much as it is an asset. Only use personal data to the extent necessary for specific purposes, all the while making sure it is protected and the individual's rights are respected.

2. HAVE A PLAN. You might not need to necessarily appoint a 'data protection officer', but someone needs to be overseeing your compliance project. Usually a team of 2 or 3 with someone taking the lead is best. Assign roles, responsibilities and decide who's in charge.

3. SORT OUT YOUR SECURITY. There's no excuse for poor security. You can minimise the risk of data loss, theft, malware etc. with some simple steps. Remember you're responsible for any personal data your suppliers process on your behalf, so ask them what they're doing about GDPR. Get copies of their security policies and keep them on file. If a supplier isn't GDPR compliant, find a replacement who is.

4. AUDIT YOUR DATA. If you don't know what personal data you've got, where it is or why you have it, then you won't be compliant. Data mapping can be tedious, but it is an essential part of getting ready for GDPR and a useful way of getting staff involved in your compliance project.

5. CHECK SUPPLIER CONTRACTS. From 25 May it will be unlawful to use a third-party processor without a GDPR compliant contract. This includes payroll processors, cloud storage providers, IT services and confidential waste disposal. You'll also need a processing contract with consultants and agency workers. As a controller, you are responsible for ensuring you have a contract which meets the law's (extensive) requirements. Don't just accept your supplier's word that they are compliant (as many aren't) - instead, get their contract checked out. Alternatively, it's inexpensive, quick and easy to have a lawyer to provide a standard contract you can use with every supplier.

6. UPDATE YOUR WEBSITE PRIVACY POLICY. You can't lawfully use personal data without telling people (amongst other things) who you are, what you're doing with the data, and what their rights are. You need a GDPR compliant website privacy policy which is incorporated into documents, forms, email signatures etc. You might need to reprint and reissue existing materials which don't link to your policy.

7. UPDATE INTERNAL DOCUMENTS. The Information Commissioner's Office (ICO) has highlighted not having an internal data protection policy (relating to how the law applies to a business and explaining how data should be handled) as an area where businesses have failed to meet the law's requirements, stating these policies are 'essential' to compliance. A staff privacy policy is also needed (you can't lawfully process personal data about your own staff if they haven't received the information required by the GDPR). We can provide you with suitable documents, tailored to your business, quickly and inexpensively.

8. GET MARKETING AND CONSENT RIGHT. The rules on marketing are complicated, but the basics are pretty simple. Consent has to be opt-in, and you can't email or text individual recipients who haven't consented (unless the marketing relates to goods or services similar to those the recipient has already purchased or negotiated to purchase, and he or she didn't opt-out at the time despite being given the chance). The rules are slightly more relaxed when communicating with corporate/LLP employees in their professional capacity, or when telephoning people (though make sure you screen against the TPS and Corporate TPS lists), and always link to a privacy policy. Be careful about purchasing marketing lists and beware of activities like profiling or segmentation (if something seems too good to be true, it probably is).

9. TRAIN YOUR STAFF. The ICO has identified a lack of training as a particular failing within many industries. Not training staff could be a breach of the GDPR in itself, and it makes data breaches much more likely. An afternoon's training from a data protection professional, which is then updated every year or so and backed up with policies is all most businesses will need.

10. USE COMMON SENSE (AND DON'T PANIC). GDPR can seem overwhelming, but most of it is about common sense and respect for individuals (for example, keeping personal data safe, only using data for specific purposes and keeping it no longer than necessary). The complex bits are the legal contracts and policies, and implementing the more advanced security measures – all of which can be dealt with by lawyers or IT professionals (respectively). A lot of the basics, such as registration, encryption, passwords, screen locking are DIY jobs. If there's too much to do then prioritise, take a risk-based approach, focus on the most important issues (but also go for the low-hanging fruit/easy wins which keep up the momentum).

For expert advice on GDPR, and support with GPDR compliance, please contact our Data Regulatory Law Partners: Oliver Neil (oliver.neil@lewis-townsend.com) and Nick Mathys (nick.mathys@lewis-townsend.com).