GDPR checklist for UK small businesses

Remember, your checklist needs to take into account past and present employees and suppliers as well as customers (and anyone else's data you're getting hold of, storing and using).

1. Know your data. You'll need to demonstrate an understanding of the types of personal data (for example name, address, email, bank details, photos, IP addresses) and sensitive (or special category) data (for example health details or religious views) you hold, where they're coming from, where they're going and how you're using that data.

2. Identify whether you're relying on consent to process personal data. If you are (for example, as part of your marketing), these activities will become more difficult under the GDPR because the consent needs to be clear, specific and explicit. For this reason, you should avoid relying on consent unless absolutely necessary.

3. Look hard at your security measures and policies. You'll need to update these to be GDPR-compliant, and if you don't currently have any, get them in place. Broad use of encryption could be a good way to reduce the likelihood of a big penalty in the event of a breach.

4. Prepare to meet access requests within a one-month timeframe. Subject Access Rights are changing, and under the GDPR, citizens have the right to access all of their personal data, rectify anything that's inaccurate and object to processing in certain circumstances, or completely erase all of their personal data that you may hold. Each request carries a timeframe and deadline of one month (which can only be extended in mitigating circumstances), from the original date of request.

5. Train your employees, and report a serious breach within 72 hours. Ensure your employees understand what constitutes a personal data breach and build processes to pick up any red flags. It's also important that everybody involved in your business is aware of a need to report any mistakes to the DPO or the person or team responsible for data protection compliance, as this is the most common cause of a data breach.

6. Conduct due-diligence on your supply chain. You should ensure that all suppliers and contractors are GDPR-compliant to avoid being impacted by any breaches and consequent penalties. You'll also need to ensure you have the right contract terms in place with suppliers (which puts important obligations on them, such as the need to notify you promptly if they have a data breach). See 'How can I check my suppliers are GDPR-compliant?' further down.

7. Create fair processing notices. Under GDPR, you're required to describe to individuals what you're doing with their personal data. See 'Fair processing notices' below for more information.

8. Decide whether you need to employ a Data Protection Officer (DPO). Most small businesses will be exempt. However, if your company's core activities involve 'regular or systematic' monitoring of data subjects on a large scale, or which involve processing large volumes of 'special category data' (see 'Is my data sensitive?' below) you must employ a Data Protection Officer (DPO).