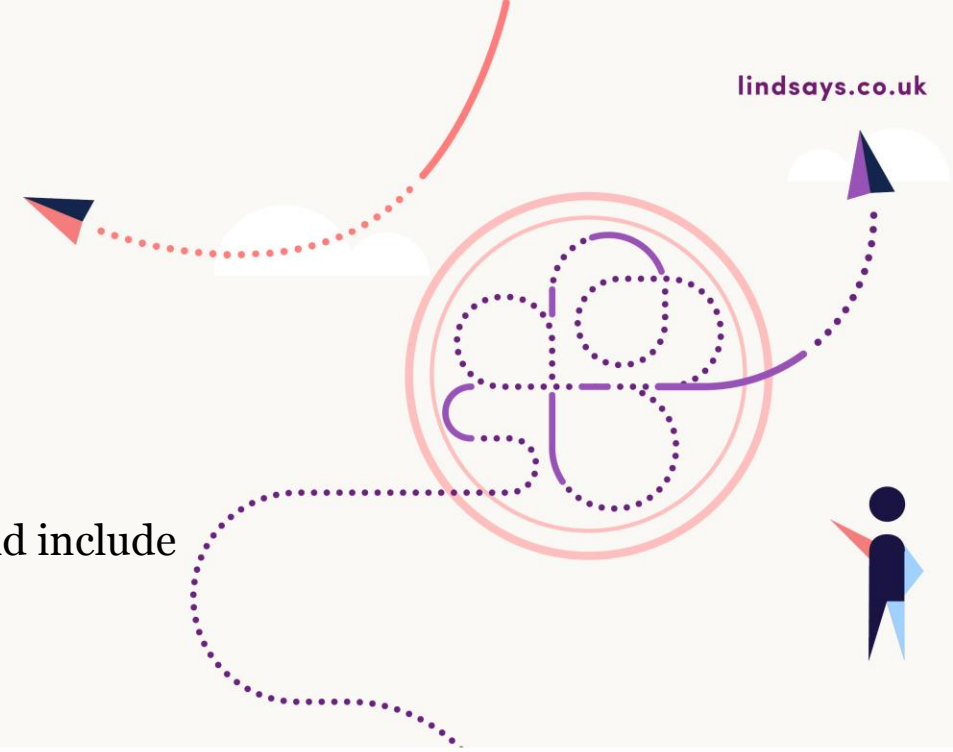

INSIGHT

GDPR preparations should include looking for weak links in operations

The new data protection regulations come into force on 25 May and businesses whose preparations focus on marketing and employee data could leave themselves exposed to breaches in other areas

With much of the advice around the General Data Protection Regulation (or GDPR) focusing on ensuring that marketing and HR practices are compliant with the new rules, we're seeing many businesses and other types of organisations including charities and social enterprises make good progress on this. Many are auditing the data they hold on employees, volunteers and service users and are taking steps towards compliance.

It's not just marketing and HR

But organisations are still at risk of failing to comply with the new rules in respect of other data they hold – such as personal data relating to customers, clients, contractors, and other business contacts. This data will also need to be audited and acted upon before the GDPR takes effect.

Unlike employee data and marketing activities which are usually clear and defined, the difficulty with this other data is that it's likely to be spread across a number of different departments or teams. Yet every organisation, however large or small, needs to review what information it holds on suppliers, contractors, customers and other contacts. Businesses need to consider where that data came from; how it is used; and how and where it is stored.

Organisations will also need to be clear about their 'lawful basis' under the GDPR for holding and processing personal data and this should be made clear to the relevant individuals up-front.

GDPR preparations should include looking for weak links in operations

For most companies, this will mean reviewing – and probably tweaking – contracts (especially any data sharing or data processing contracts), terms of business, and privacy notices.

Going beyond a data audit

The other issue many businesses face is not having sufficient administrative processes in place to be able to deal with their increased obligations under the GDPR – for example, dealing with requests to view, update, move or delete data; and monitoring for breaches.

Again, since HR and marketing teams have been the focus of many organisations' GDPR preparations to date, most are making good progress on developing pro forma responses to requests from individuals, and designing new processes for monitoring compliance with the new requirements for obtaining consent.

But compliance must be organisation-wide, reaching teams that may hold personal data in other contexts. Since these teams are less likely to systemise the way they process and hold personal data, they may not yet have audited their data or reviewed their administrative processes.

Updating your action plan

There's much written about the GDPR, especially information about reviewing your marketing and HR procedures to prepare for the new rules. But there are three points you should keep in mind to ensure there are no weak links in your plans.

Firstly, you must be careful not to focus solely on data relating to employees, volunteers and other workers and overlook personal data in other contexts, such as data relating to customers, clients, contractors, and other business contacts.

Secondly, much of the information around is excellent, but when looking at contracts, terms of business and privacy notices, and updating these to comply with the new rules, you'll probably need to take advice tailored to how organisations operate.

Thirdly, 25 May is not just the starting-point for the new rules, it should also be viewed as the target date for you to have all your preparations completed. This means considering and putting new compliance arrangements into effect as soon as possible.

Any organisation or charity that hasn't already conducted a full audit of personal data it holds and processes and considered the administrative processes it has in place should do so now without delay.

May 2018