7 GDPR TIPS HR NEED TO KNOW

by Anna Flanagan, Pinsent Masons

1. Identify the lawful basis for processing personal data and keep a record of this

You should bear in mind the record-keeping obligations under the GDPR and start keeping a record of the lawful basis for processing personal data.
- The conditions for processing have slightly changed – review the changes and ensure your organisation can use one of the conditions before processing data.
- Try to avoid consent as it is unlikely to be valid in an employer/employee relationship.
- Update your privacy notice to include the reason for processing personal data, which is a new requirement under GDPR.

2. Train staff

- Roll out a training programme for staff on the new GDPR implications ensuring they are aware of the relevant policies and changes.
- Given that organisations are increasingly vulnerable to the risk of loss, damage or destruction of their data and the new requirement to notify the ICO within 72 hours of a breach, particularly ensure that staff are trained on how to keep data secure.

Join the many organisations who now do this training online. Not only do they find it more convenient and cost effective but it also generates a real time record of all training activity completed by staff.

3. Update"right to be forgotten/erasure"policy

- There are new data subject rights including the "right to be forgotten" or right to erasure (Article 17) which are building on current rights confirmed in case-law, and additionally, right to "data portability" (Article 20).
- Ensure you have the appropriate policy and technology in place to recognise and comply with any of these requests within the relevant time.

4. Examine retention periods for personal data

- Look at how long your organisation holds onto to personal data, (E.g. for ex-employees or unsuccessful applicants for job vacancies.)
- Think about whether you have a logical reason for your current retention periods (if there are such periods). Does this reason apply to all the personal data you hold, or could some be deleted?
- The GDPR does not specify particular retention periods, but the general principle not to hold on to data longer than necessary remains.

5. Update subject access request policy

There is now a shorter timeframe for response (one month) and no fee payable, make sure your policy reflects this.

6. Workout the transfer of data

- Examine where Personal Data is transferred, including to Cloud/Storage providers.
- Look at all Personal Data outsourcing which could include long-term storage/archiving (where appropriate), payroll etc.
- Work out where the Personal Data is held and whether that is inside or outside of the EEA.
- Find out if there are appropriate contracts in place and if not consider or take advice on what mechanisms can be used to regularise transfers under the GDPR.

7. Consider special categories of data

Your organisation is very likely to hold "Sensitive Personal Data" for example relating to data subjects disability, ethnicity, religion or health. Consider whether your organisation has any special security measures in place for the processing and transfer of this type of information.