hollaroo reach people

Checklist

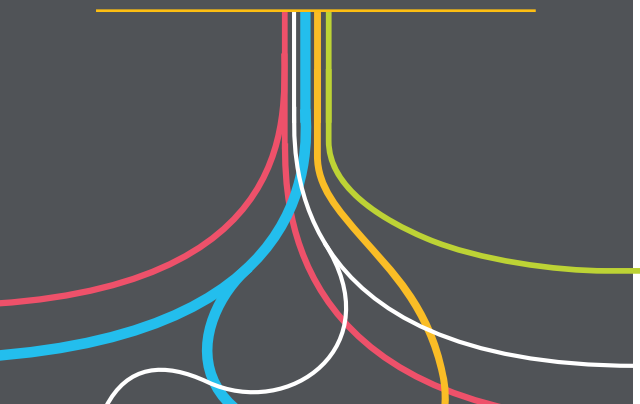
With time racing on and GDPR taking effect on the 25th May 2018 (only just over a month away) it's the right time to check you've got your 'house in order'.

The Information Commissioners Office have confirmed there will be no "grace" period before the law is set, and there's much ruminating about the organisation or group who'll be the first to hit the headlines... Will it be another Facebook expose or will they head for a big Corporate or Government department.

"there has been two years to prepare and we will be regulating from this date" - **ICO blog**

The good news is that the ICO prides themselves on being "fair and proportionate". So as long as you can show you are putting in place the "key building blocks" for compliance this will be taken into account.

The bigger risk is actually from the wider public - particularly disgruntled job-seekers who might be tempted to seek compensation when they've been rejected from their dream job - so our advice is to focus on the most visible parts of your processes and make sure those are compliant first, whilst putting the building blocks in place for your broader compliance over the next few months.



Here is a suggested list:

Things to do by the 25th May

Ensure that your organisation understands the implications

We all know that the biggest risks are often caused by non-compliant activities by hiring managers and rogue agents (and often not the recruiters themselves). By May 25th there needs to be very clear communication to the whole organisation, ideally from a very senior stakeholder, outlining the risks that this is placing on the organisation and the potential implications.

Things that need to stop; storing candidate data in spreadsheets, email inboxes and desktop folders. Dealing with agencies that have not been through a GDPR audit process with you. Retaining any sort of candidate data without being transparent with them about what you are doing and their individual rights.

Make sure your application process is compliant

This will be the first port of call for most people and the place people will look for signs of non-compliance - so this needs to be rock solid. We have covered the issues around **consent** and the broader treatment of **applicants** in more detail elsewhere. People are still tying themselves up in knots about what basis to use, how to handle the user rights and what to do if someone wants to withdraw mid-process. Our advice is to keep this very simple and just cover processing that person's data for the job they are applying for.

The messaging then becomes very simple - "We will process your data for the purpose of evaluating your application for this role. At the end of the process we will retain your data for as long as required by employment regulations but only for this purpose," These two activities are covered by the "performance of contract" and "legal obligation" bases under GDPR so relatively simple to manage.

Sort out your third-party relationships

Where you have started to process a candidate's data without their knowledge or via a third-party there are some very clear steps you need to take to acknowledge the basic GDPR requirements for transparency and user control. This covers candidates submitted as employee referrals, found on public sources such as Linkedin or submitted to you by an agency.

In all these cases you need to inform the candidate that you are now processing their data, explain what for and for how long, and give them the opportunity to refuse. In the case of an agency submission control is passing from the agency to you, so you need to work with your suppliers to manage that in a way that works for both sides.

Get in touch

To discuss how to mitigate the challenges that GDPR will bring to your organisation, contact Hugh Fordham on **01727 298081**

Ongoing Processes - start now but continue after May

Establish policies for data retention

Typically, you will be required to retain an applicant's data for a period of time after it is no longer being considered for selection. In some countries this is mandated by law, in others there is an accepted practice to retain records in case of challenge by unsuccessful applicants. For each case, once the policy is established this can be added to the information you give applicants when they start the process.

Where candidate data is being stored for marketing purposes (speculative applicants, recycled applicants, talent pools) the basis for processing will be consent from the candidate. You need to establish a policy for how often this needs to be refreshed - typically a period of time where there has been no interaction with the candidate so you need to check they are still happy for you to continue processing their data.

Decide on a post-selection process for applicants

GDPR means you need to give a candidate the option to opt-in to a marketing relationship after the selection process is complete. This needs to be clearly recorded and the candidate data should not be visible to recruiters until consent has been obtained. Because this is more onerous to manage, and you then need to comply with the rights of the retained candidates, you may want to be more selective in choosing who to take through the process rather than just keeping everyone.

Work out how you will comply with the user-rights requirements

The GDPR gives users many more rights over how their data is managed so you need to have systems in place to support this. The rights most relevant to recruitment are:

Rights of access, rectification and erasure: Letting candidates see what data you are processing and makes changes or delete it if they want. This doesn't override your rights as an employer so, for example, people can't change vital parts of their application in the middle of a selection process. On the other hand, you do need to give candidates full rights if you are just using their data for marketing.

Rights to object or restrict processing: People should be able to withdraw from the process but that doesn't necessarily mean their data being deleted. Employment law may require you to retain it but you need to do it in a way which means it is not used for any other purpose. In an ideal world you might want to offer your candidates the chance to opt-out of marketing, so they don't get approached, but in a way that means they can easily opt back in at a later date.

Rights to data portability: Make it easy for candidates to export their data.

Rights about automated decision-making: If you are using automated tools then candidates need to be able to choose a manual alternative.