rowlands

General Data Protection Regulation (GDPR), Candidates Rights and the Recruitment Process

What is GDPR and why you should care

GDPR is a Europe-wide set of data protection laws designed to harmonise data privacy practice across Europe. The emphasis is on protecting citizens and their data, and giving users more information about control over how it's used. The States of Jersey and States of Guernsey are implementing an equivalent law and it is likely that these local laws will be similar to GDPR with the aim to be ready for implementation in May 2018, in line with the EU legislative timetable. These draft laws were unanimously agreed by the States Assembly on the 18th January.

GDPR will drastically change the way businesses of all sizes collect, store and protect personal information, bringing significant changes to existing data protection regulations, introducing new requirements for businesses to adhere to.

Key changes/new rules

The main purpose of GDPR is to ensure that individuals have more control over their data and that clients are more accountable. Employers will need to be very clear on what data they are keeping, for how long and ensure they remove it when it is no longer needed. Ensuring they have a lawful basis for using personal data, which could include consent by the individual for storing and processing data or for the fulfilment of a contractual obligation.

Although most HR Professionals and Recruitment Consultants will be working their way through the exact requirements and changes to current processes, we have provided a brief summary of some of the rules that will apply:

Obtaining consent from individuals

- **Multiple levels of consent** - You cannot assume that because a candidate has given you consent to send their details for a specific role, that they are also happy for their personal data to be sent to other similar organisations or added to mailing lists, without permission.
- **Explicit, affirmative consent** - from your candidates, either active or passive, is essential to demonstrate your commitment to GDPR compliance. You can no longer use terms such as 'If you would not like to receive our messages, please confirm your acceptance of not agreeing with our terms by unchecking the box."
- **Clear purpose** – Clarify what the candidate is consenting to and how it will be used and retained i.e. consent for application, consent to be sent job alerts, consent to receive newsletters, consent to join talent pools etc. The 'legal basis' for capturing and processing candidate information must be clearly distinguishable.
- **Providing greater transparency** - Be clear about the data you are collecting, at the time of collection and how that data will be used.
- **Time limit on consent** - candidates should be able to withdraw consent without detriment.

Personal/sensitive data

During the recruitment process employers collect a large amount of data about your candidates – but how do you know which information will be deemed as 'personal' or 'sensitive'? GDPR expands the definition of sensitive personal data an specifically identifies new categories of data beyond names, addresses etc. (such as cookie ID's and IP addresses) that will be subject to regulation.

Storage

In addition to candidates having additional rights regarding how you store and process their individual data; such as the right to be informed and transparency over how their personal data is used, employers should only keep data for as long as necessary for the purposes for which it is processed. They will no longer be able to capture data once and keep it indefinitely.

Security

The security of the personal data employers work with will need to be 'appropriate to the risk'. Employers will need to ensure they have the appropriate security measures in place i.e. if you use a cloud based ATS/CRM do you have the option for Data Encryption at Rest? Does your ATS/CRM provider have a security management system in place?

Don't leave it to chance

The above list of changes are only a snapshot of a few of the changes to existing data protection regulations that employers will have the responsibility to demonstrate they are compliant with. It is recommended that organisations seek legal advice to ensure that their recruitment processes are compliant and ready for the introduction of GDPR in May 2018.

Consequences of ignoring GDPR

Be prepared for heavy penalties for failure to comply with the new regulations. In the UK, the Information Commissioner's Office (ICO) will be able to impose fines and penalties with a maximum upper limit of €20 million or 4 per cent of annual turnover, whichever is higher.

Preparing for GDPR (Steps to take now - don't leave your preparations until the last minute!)

1. **Conduct a data audit** - To gain a good understanding of the data you currently hold, where it is stored, whether it is shared with third parties and whether it is actually needed. Ensure you document this as GDPR will require you to maintain records of your processing activities to show how you comply with data protection principles by having effective policies and procedures in place. Identify areas that could cause compliance problems.
2. **Identify the lawful basis for your processing activity** - Document this in your privacy notices.
3. **Review all your existing recruitment data processes** - Evaluate how they fit against the new legal requirements. Ensure reporting of any data breaches is included in your recruitment process. Review how you seek, record and manage consent to decide if you need to make any changes. Refresh existing consents now if they don't meet GDPR standards.
4. **Review your current privacy notices** - Put a plan in place to make any necessary changes in time for the implementation of GDPR. You will no longer be able to have a catch-all policy, you will need to be a lot more explicit about what you're doing with the data.
5. **Check your procedures cover all rights of an individual** - Including how you will delete personal data or provide data electronically. Ensure procedures are in place to detect, report and investigate personal data breaches.
6. **Plan how you will handle requests** - Within the new timescale and provide any additional information.
7. **Designate someone to take responsibility for data protection compliance** - Assess where this role will sit within your organisation's structure and governance arrangements. Consider whether it is required to formally designate a Data Protection Officer (this person should not be the MD of the company).
8. **Review arrangements with third parties** - You will need to demonstrate that their systems are secure and that they have taken steps to prevent a breach. Review how these arrangements might change in light of GDPR: for example, setting up a virtual private network with partners to share data.

Sources and further information:

https://www.fsb.org.uk/first-voice/this-is-your-wake-up-call-prepare-now-for-gdpr

https://www.recruitmentgrapevine.com/content/article/insight-2017-11-17-recruiterspreparing-for-gdpr?utm_medium=email&utm_campaign=RG%20061217&utm_content=RG%2061217+CID_38758c2251ce59532e8f3aa8a9f37dbe&utm_source=RG%20Campaigns&utm_term=The%20GDPR%20and%20your%20candidates%20rights

https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf