hollaroo engage hollaroo onboard hollaroo refer

The GDPR legal requirements when processing candidate data

The EU's General Data Protection Regulation (GDPR) comes into force on May 25 2018, enforcing a strict set of new rules concerning privacy and data security and imposing strict penalties on violators - up to 4% of an organisation's annual worldwide turnover or €20 million, whichever is greater.

The severity of the fines going to be imposed mean this is a hot topic for all organisations dealing with personal information, and with less than a year to go before the fines potentially start being applied the time to apply solutions is rapidly running out.

Key Elements of GDPR

The GDPR is wide-ranging and there is a lot of confusion about what is required. In the context of recruitment, and particularly candidate information, employers should check that the key elements listed below are included in their legal documents.

Privacy Policy

This applies between an employer and candidates in relation to the collection and use of personal data collected by an employer from a candidate. The privacy policy should include the types of data being collected and processed, why data is collected and processed, who data is shared with, where data is stored or processed, who data is disclosed to and the rights of the data subject (candidate) to request access to, rectification or deletion of and transfer of any personal data collected.

Data subject requests - Employer's must respond to any data subject request within 30 days, free of charge.

Data Protection Officer - Candidates must be provided with details of any data protection officer appointed by the Employer.

Supervisory Authority - Candidates must be provided with details of the supervisory authority to whom data protection complaints can be made.

Withdraw Consent - Candidates have the right to withdraw their consent to personal data collection and processing at any time.

Automated Data – Candidates must be informed if profiling or any automated decisions are made from personal data collected and have the right to object to this.

Data Retention - Candidates must be informed of how long personal data will be kept and whether there are exceptions to the general rule.

Data Processing Agreement

This applies between the employer (a data controller) and any entity that processes candidate data on behalf of the employer (a processor). The employer's processors will include any group subsidiary or sub-contractor the employer uses to process candidate data. The DPA must be in writing.

The DPA must contain specific mandatory information, which includes the following obligations:

Transfer of personal data outside EEA - Processors may only transfer personal data outside of the EEA to a processor who has provided appropriate safeguards, for example by using EU model clauses or Binding Corporate Rules (BCRs**).**

Sub-Processors - Processors must inform employers of any changes to sub-contractors in advance and inform employers of their right to object. Processors cannot change any sub-contractor used to process candidate data i.e. a data centre or support personnel without first obtaining consent from an Employer.

Breach Notification - Processors must notify employers of any breach of their obligations, without undue delay, after becoming aware of the breach.

Right to Audit - Processors must allow employers to audit compliance with the DPA and its data processing obligations generally.

Data Subject Requests - Processors must assist and permit employers to comply with candidate data subject requests and rights.

Deletion or Return - Processors must allow employers to choose between deletion or return of personal data on termination or expiry of the DPA (unless applicable mandatory law requires storage).

DPO and Supervisory Authority - Processors must notify the employer of the details of any data protection officer appointed or leading supervisory authority to deal with complaints.

Security - Processors must provide detailed security provisions and data processing information to evidence compliance with data processing obligations. Processors must document all processing activities specifying the types of data being processed, in particular whether any sensitive date is processed and the technical and organisational security measures it has in place to protect data

DIPA - Processors must assist the employer in carrying out a data protection impact assessment.

Conclusion

Employers who plan to collect candidate data from individuals located in the EU after the 25th of May 2018, need to take the following action to ensure compliance with the new obligations placed on Employers under the GDPR:

- review and amend existing privacy policies;
- review and amend the terms of existing agreements with sub-contractors who process candidate data;
- enter into a written data processing agreement with all sub-contractors who process candidate data;
- review all internal procedures relating to data protection and security; and
- review insurance cover limits and exclusions;

Contact Us:

If you need any further advice on how to become compliant please call us on +44 (0) 1727 298081 or email us at getintouch@hollaroo.com.