



Take Steps Now to Avoid Fines of €20m: Overview of the General Data Protection Regulations

The General Data Protection Regulations (GDPR) have been a long time in the making but it has been confirmed that the UK will adopt them prior to Brexit. GDPR will come into force in May 2018 and will replace the 1995 Data Protection Directive. Organisations which do not comply will run the risk of being fined €20m or 4% of global revenue (whichever is greater). In addition to this, they risk the naming and shaming of their organisation.

GDPR is a complex piece of legislation imposing onerous compliance obligations on the Human Resources department of organisations. The purpose is to strengthen and unify data protection for all individuals in the EU. Changes brought about by GDPR include:

1. Expansion of territorial reach to data controllers and processors outside the EU whose processing activities relate to the offering of goods or services to, or monitoring the behaviour of EU data subjects;
2. More stringent controls on what constitutes “consent”;
3. Enhanced rights for data subjects;
4. New accountability measures which may necessitate appointing a data protection officer; and
5. Requirement to inform ICO within 72 hours of a data breach.

The enhanced rights include the right to erasure i.e. the right which data subjects have to be forgotten in the sense that all personal data relating to them is deleted. The right to correction of inaccurate data, removal from digital marketing, the right to request transfer to another service provider and right to be notified of breaches in certain circumstances.

Complying with these rights could lead to foreseeable difficulties. For example there may be difficulties in erasing information where it is held in physical copy or in an un-reportable or un-auditable way. There will be a huge pressure on businesses to take control, ensuring that all data is held in a reportable and auditable way.

There will be specific concerns for HR professionals. Care should further be taken in the hiring of interims, contractors or temps. Whilst these positions may be filled as a result of direct hiring, the vast majority of these staff members are hired via employment businesses which are used to create a disconnect between employer and employee. This is due to the uncertain and changing tax status of the economy. Implementing an Applicant Tracking System which is used comprehensively by every hiring stakeholder in the organisation means there will only be one instance of a CV in each organisation, evidence of where it was sourced, documentation of explicit consent and permission granted, how it was profiled i.e. first screen, telephone interview, video, face-to-face, psychometrics, assessment, reasons for acceptance/rejection, induction and onboarding, as well as who dealt with each step of the process at applicant and successive candidate stages. This will ensure accountability and governance for the employer as well as protection of the rights of individuals.

Advice for organisations would therefore be to implement a GDPR-compliant ATS ensuring that every hiring stakeholder is making use of this system from Chair/Head of Department to HR Recruiter, to further incorporate talent pools, succession and workforce plans into the ATS and automate six monthly permission to erase data. This insures against a mass of claims targeting employers who haven't implemented an ATS and the associated difficulties in proving compliance in the absence of such a system.

This article has been produced for general information purposes and further advice should be sought from a professional advisor.

If you have any queries on the above please contact Michael Black or Aisling Byrne at Cleaver Fulton Rankin Solicitors 02890 243141.