GDPR: A brief guide for clients

The Basics

Personal data – relates to an identifiable individual

Transparency and Fair Processing – adequate, relevant, accurate, kept for no longer than absolutely necessary, safe and secure

Lawful Reason to Process – consent, in relation to a contract or proposed contract, legitimate business interest, legal obligation

GDPR Consent – freely given, specific, informed, unambiguous, right to withdraw – pre populated opt in boxes are no longer appropriate.

Relationships with your Recruiters

Data Controllers are responsible for deciding how they hold and use personal data

Data Processors process data on behalf of a Data Controller to fulfil the Data Controller's purposes

In most recruitment relationships both parties will be data controllers. A possible exception is a resource processing outsourcing relationship (RP0) Normally, a data processor agreement will not be necessary

The contract between you and a recruiter should specify each controllers' obligations in general terms

An agency worker or a professional contractor will not be your data processor in a standard recruitment business relationship as they are processing your personal data on your systems. You will not transfer data to their systems

Sourcing Candidate Data – Temporary and Permanent Roles

- Direct Application
- CV downloaded from a Job board
- Profile downloaded from LinkedIn or other social media
- From a Recruiter: right to represent
- From a third party

Sourcing Candidate Data – Lawful Processing Grounds

You need to rely on a lawful processing ground for all uses of personal data. The ICO has provided a tool to determine a suitable lawful basis here. The most relevant to the recruitment sector are:

Intention to form a contract: You need to understand whether you have (or are taking steps with a view to entering into) a contract with the particular individual e.g. an application from a candidate following a job advertisement

Legitimate Business Interests: These can include your commercial interests as you require applicants to fill job roles but only rely on this ground to the extent you can justify the impact on individuals and you have completed a Legitimate Interest Assessment

Consent: Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build customer trust and engagement. Avoid making consent to processing a precondition of a service
Avoid over-reliance on consent and if free choice is not possible then another processing ground must be relied on

Consent is generally not suitable for an employer relationship

Use of "Just in time" consent at the point of a particular type of processing is ideal

Recruiters may seek permission to represent prior to introducing

Best practice: Privacy Notice for Candidates

This should be provided at the time a data subject chooses to provide you with personal data (PD);

If data is taken from a publicly available source or obtained from a third party then notice must be provided within a "reasonable time"

This is the earliest of:

- First communication with you;
- Or, if the personal data is to be disclosed to someone else, before it is disclosed;
- Or, one calendar month from the date you obtained the personal data.

What should you include on the Privacy Notice?

Who you are

Type of Information Collected: e.g. CV, application form, interview notes, psychology test results

Special categories of sensitive data – equal opportunities information, disability information, health, criminal convictions

Third parties who supply information: e.g. recruiters, credit reference agencies, DBS, background checkers, referees

How you will use the information

Your lawful processing grounds

Information about Criminal Convictions – why / is it necessary?

Data Security – in particular, special categories of data and highly confidential information

Retention – how long will you keep the data for?

Individual Rights – access, correction, erasure, right to object to processing, right to restrict processing and right to transfer personal data to another party (in certain circumstances)

Individual Rights

The GDPR provides the following rights for individuals:

The right to be informed: about the collection and use of their personal data. This will be via a privacy notice when data is collected

The right of access: they have the right to access their personal data, this is called a Subject Access Request. Post GDPR this must be free of charge and provided within one month of receipt

The right to rectification: individuals are entitled to have personal data corrected if it is inaccurate or incomplete

The right to erasure: individuals request the deletion or removal of personal data where there is no compelling reason for its continued processing however the right to erasure does not provide an absolute 'right to be forgotten'

The right to restrict processing: individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, you can still store the personal data, but not further process it. Again, this is not an absolute right and only applies in certain circumstances

The right to data portability: this allows individuals to obtain and reuse their personal data for their own purposes across different services. This right only applies to processing by automated means

The right to object: individuals can object to processing based on legitimate business interests and marketing. You must deal with an objection to processing for direct marketing at any time at no cost

Rights in relation to automated decision making and profiling: if you undertake automated decision making and/or profiling individuals have the right not to be subject to an automated decision and be able to obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it

On boarding and Vetting

Think before asking for unspent convictions or **Criminal Record Checks** (DBS). Only do so if it is a legal requirement of the role or the role is specified in the Rehabilitation of Offenders Act (SI 1975/1023) or Police Act. Regulations (SI 2002 /233) or the role requires a high degree of trust and integrity e.g. handling client money

Only record result: satisfactory or not satisfactory and not DBS check

Other Vetting: Only do at the appropriate stage, usually prior to start of assignment. Consider whether you should rely on legitimate business interests or consent? Do not make extensive vetting a pre-requisite for all roles unless there is a requirement

Retention and Erasure of Recruitment Data

Data must be accurate, current, necessary and secure

Under the Conduct of Employment Agencies and Employment Businesses Regulations 2003 Recruiters must retain evidence of an introduction or supply for at least one year from the last activity e.g. interview or engagement

The current ICO Employment Practices Code (GDPR version awaited) recommends retention of unsuccessful candidate personal data only for any potential claims periods e.g. individuals have 3 months to bring an employment claim and the ICO mentions retention for 6 months

However, you can choose your own retention periods as long as you justify and document your decision

Consent is needed to retain personal data for roles other than that for which the application was made

Note retaining personal data on your own candidate database may be a breach of the terms you have with your recruiter

Breach and Penalties

Organisations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater)

Breach notification will become mandatory but only where a data breach is likely to "result in a risk for the rights and freedoms of individuals"

Further information is available on the ICO website.

This guidance is for information only, includes our opinion and is not legal advice.

The Association of Professional Staffing Companies Limited
Tel: 08458 997388 Web: www.apsco.org