

## Job Applicant Privacy Notice – Guidelines and Points to Note

Before using the template Job Applicant Privacy Note, it is essential that you read these guidelines and points to note and that you have read the overarching document “General Data Protection Regulations - NTF Templates”.

The General Data Protection Regulations come into force on 25<sup>th</sup> May 2018.

### Why do you need this notice?

The General Data Protection Regulations require you to provide job applicants with fair processing information – explaining to them what you do with their personal data.

### What should you do next?

You should read the template privacy notice very carefully and tailor it to suit your own business requirements. It is essential that you customise it to reflect the types of personal data that you hold and how you process. It must reflect reality in your business.

- Criminal Offences/Disclosure and Barring Service checks

Data relating to criminal offences/criminal records is not considered special category data under the new regulations but similar restrictions apply to its processing so it is included in this notice. Disclosure and Barring Service (DBS) checks can only be made by employers for certain jobs which involve working with children, vulnerable adults or healthcare and in most cases it would not be lawful for employers to request these from applicants for jobs in racing.

The BHA as part of its safeguarding requirements advise as good practice that employers ask job applicants if they are known to any local authority as being a risk or potential risk to young people and/or adults and/or if they are the subject of any disciplinary investigation and/or sanction by any organisation due to concerns about their behaviour towards young people or adults at risk. Such information would then be sensitive data.

- Transferring Job Applicant Data outside the EEA

We have not made any reference to transferring data outside of the EEA and if you or a group company do this at a job application stage then again contact the NTF or other adviser for further information.

- Referees

The personal details of referees are personal data and in order to comply with the GDPR you should provide referees with appropriate fair processing information. We have included wording in the Job Applicant Privacy Notice telling job applicants that they must let their referees know what personal data they are providing to you and give their referees your contact details.

However this does not satisfy the requirement for you to provide their processing information to the referees and to be properly compliant you would need to provide referees with further processing information.

To reduce the administrative burden of providing fair processing information to referees, you may wish to consider deleting personal data of any referee you do not intend to request a reference from and any referee data from job applications you receive which you intend to keep on file.

### **Keeping Job Applicant details on file**

It is quite common for employers to wish to keep some job applicant details on file for a future vacancy. You can do that but you need to consider your legal basis for doing it. Asking the employees consent would be an appropriate legal basis in this instance, provided you allow job applicants to apply for a given vacancy without consenting to you keeping the information. That is referred to in the Job Applicant Privacy Notice.

### **When you should use this Job Applicant Privacy Notice and how to issue it**

If you have an online form on your website for job applications, it would be appropriate to have Job Applicant Privacy Notice online and ideally on screen for the applicant to read before sending you the job application.

Otherwise you should issue a copy of the Job Applicant Privacy Notice to all job applicants.

If you receive speculative unsolicited hardcopy applications from potential employees, you must consider whether and how you will provide the Job Applicant Privacy Notice to them. Essentially if it is received looked at and shredded without scanning it filing it or putting into any system, then there is no need to provide a privacy notice.

If you do scan or file the speculative application or if it is sent in electronically then it is personal data and the obligation to provide a privacy notice will apply. There is unfortunately no exception for unsolicited email. Strictly speaking therefore to comply with GDPR requirements you should email or post a copy of your job applicant privacy notice back to the individual – you could do this in conjunction with the communication acknowledging receipt of the application.

Alternatively if you do not want to do that, you could include privacy information about unsolicited applications on your website in the area of the website that covers any job vacancies and applications that is not ideal but it is better to do something than nothing.

You may of course decide to make a risk based decision about compliance and that the risk here is not that high. However if an individual is keen to make trouble and you do not send a privacy notice they can complain to the information Commissioners office. It is likely the ICO would tell you to change your practice going forward than to issue any fine straightaway. It is a decision for employers to take.

**The template document has been prepared to help you comply with the new data protection regulations in place from 25<sup>th</sup> May 2018.**

**You must customise the text in the template document to ensure that all the information matches what actually happens in your own organisation – any audit you have carried out in order to prepare for GDPR will help you do that.**

Detailed information is available on the ICO website ([www.ico.org.uk](http://www.ico.org.uk)).