

## Job Applicant Privacy Notice

This privacy notice describes how the US-UK Fulbright Commission (the “Data Controller”) will collect and process personal data relating to job applicants. We are committed to being transparent about how we collect and use that data and to meet our data protection obligations.

### What information do we collect?

We collect and process a range of information about you.

- Your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history; including start and end dates, with previous employers;
- information about your current level of remuneration, including benefit entitlements;
- whether or not you have a disability for which the organisation needs to make reasonable adjustments during the recruitment process; and
- information about your nationality and entitlement to work in the UK;
- information about your criminal record;
- equal opportunities monitoring information including information about your ethnic origin, sexual orientation and religion or belief.

We collect this information in a variety of ways. For example, data is collected through application forms, CVs or resumes; obtained from your passport or other identity documents; or collected through interviews or other forms of assessment.

We may collect personal data about you from third parties, such as references supplied by former employers. We will seek information from third parties only once a job offer to you has been made and will inform you that we are doing so.

Data will be stored in a range of different places, including on your application record and in other IT systems (including our email system).

### What is the legal basis for processing your personal data?

We need to process data to ensure that we are complying with our **legal obligations**. For example, we are required to check a successful applicant's eligibility to work in the UK before employment starts.

In other cases, we have a **legitimate interest** in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows us to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. We may also need to process data from job applicants to respond to and defend against legal claims.

We may need to process data to enter into an **employment contract** with you if your application is successful.

We process special categories of data, such as information about ethnic origin, sexual orientation or religion or belief, for the purposes of equal opportunities monitoring. Data that we use for these purposes is collected with the **express consent** of the applicant.

Applicants are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

We may also collect information about whether or not applicants are disabled to make reasonable adjustments for candidates who have a disability. We process such information to carry out our obligations and exercise specific rights in relation to employment.

For some roles, the organisation is obliged to seek information about criminal convictions and offences. Where the organisation seeks this information, it does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to employment.

### **Who has access to the data?**

Your information may be shared internally and externally for the purposes of the recruitment exercise. This includes the shortlisting and interview panel involved in the recruitment process including external panel members, the Executive Assistant/HR Manager and the Executive Director.

We will not share your data with third parties such as former employers unless we have your permission and are intending to make you an offer of employment.

The organisation will not transfer your data outside the European Economic Area unless we have your consent.

### **What if you do not provide personal data?**

You are under no statutory or contractual obligation to provide data to the organisation during the recruitment process. However, if you do not provide the information, the organisation may not be able to process your application properly or at all.

### **How do we protect data?**

We take the security of your data seriously. We have internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties.

### **For how long do we keep data?**

If your application for employment is unsuccessful, we will hold your data on file for up to eight months after the end of the recruitment process. At the end of that period, your data is deleted or destroyed.

The special categories of data such as information about ethnic origin, sexual orientation or religion or belief, that we collect for the purposes of equal opportunities monitoring are anonymised eight months after the end of the recruitment process and then retained for statistical purposes.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment. The periods for which your data will be held will be provided to you in a new privacy notice.

### **Your rights**

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require us to change incorrect or incomplete data;

- require us to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where we are relying on our legitimate interests as the legal ground for processing.

If you would like to exercise any of these rights, please contact our Data Protection Co-ordinator, [dpo@fulbright.org.uk](mailto:dpo@fulbright.org.uk)

If you believe that we have not complied with your data protection rights, you can complain to the Information Commissioner's Office (ICO) and they can be contacted on 0303 123 1113.

*Version 2 – 14 November 2018*