

# Job applicant privacy notice (compliant with the GDPR)

**Data controller: Powys County Council**

**Data protection officer: Helen Dolman - County Hall, Llandrindod Wells, LD1 5LG**

As part of any recruitment process, the organisation collects and processes personal data relating to job applicants. The organisation is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

## **What information does the organisation collect?**

The organisation collects a range of information about you. This includes

- your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history;
- 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;
- information about your entitlement to work in the UK; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health, and religion or belief.

The organisation collects this information in a variety of ways. For example, data might be contained in application forms, CVs or resumes, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment, including online tests.

The organisation will also collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks. The organisation will seek information from third parties only once a job offer to you has been made and will inform you that it is doing so.

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

## **Why does the organisation process personal data?**

The organisation needs to process data to take steps at your request prior to entering into a contract with you. It also needs to process your data to enter into a contract with you.

In some cases, the organisation needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check a successful applicant's eligibility to work in the UK before employment starts.

The organisation has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the organisation to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. The organisation may also need to process data from job applicants to respond to and defend against legal claims.

Where the organisation relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

The organisation processes health information if it needs to make reasonable adjustments to the recruitment process for candidates who have a disability. This is to carry out its obligations and exercise specific rights in relation to employment.

Where the organisation processes other special categories of data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is for equal opportunities monitoring purposes.

The organisation will not use your data for any purpose other than the recruitment exercise for which you have applied.

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

Your information will be shared internally for the purposes of the recruitment exercise. This includes [members of the HR and recruitment team, interviewers involved in the recruitment process, managers in the business area with a vacancy and IT staff if access to the data is necessary for the performance of their roles.

The organisation will not share your data with third parties, unless your application for employment is successful and it makes you an offer of employment. The organisation will then share your data with [former employers to obtain references for you, employment background check providers to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal records checks].

The organisation will not transfer your data outside the European Economic Area.

#### **How does the organisation protect data?**

The organisation takes the security of your data seriously. It has 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 does the organisation keep data?**

If your application for employment is unsuccessful, the organisation will hold your data on file for 6 months after the end of the relevant recruitment process. At the end of that period [or once you withdraw your consent], your data is deleted or destroyed.

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 the organisation to change incorrect or incomplete data;
- require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing; and
- ask the organisation to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the organisation's legitimate grounds for processing data.

[If you would like to exercise any of these rights, please contact Helen Dolman – County Hall, Llandrindod Wells, LD1 5LG. You can make a subject access request by completing the organisation's form for making a subject access request.

If you believe that the organisation has not complied with your data protection rights, you can complain to the Information Commissioner.

### **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.

You are under no obligation to provide information for equal opportunities monitoring purposes and there are no consequences for your application if you choose not to provide such information.

### **Automated decision-making**

Recruitment processes are not based solely on automated decision-making.

## **Law relating to this document**

### **Leading statutory authority**

General Data Protection Regulation (2016/679 EU)  
Data Protection Bill

The General Data Protection Regulation (GDPR) requires employers to be transparent about the personal data that they hold and how it is used. The GDPR requires employers to provide the following information to job applicants at the point that data is collected from them:

- the identity and contact details of the organisation;
- the contact details of the data protection officer, if relevant;

- the purposes for which the personal data will be processed, as well as the legal basis for the processing;
- if the employer is relying on its legitimate interests as the lawful condition for processing, what those legitimate interests are;
- the recipients or categories of recipients of the personal data;
- any transfer of the data outside the European Economic Area and the basis for such transfer;
- the period for which data will be stored, or the criteria used to determine how long data will be retained;
- the individual's rights to subject access, rectification or erasure of personal data, and the right to restrict processing or object to processing;
- the right to withdraw consent to processing at any time, if the data controller is relying on consent as a ground for processing;
- the right to lodge a complaint with the Information Commissioner;
- whether or not providing the data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, and whether or not the data subject is obliged to provide the personal data, and the consequences of failing to provide the data;
- the existence of any automated decision-making and meaningful information about the logic involved and the consequences of any such processing for the individual; and
- where data is obtained from a third party, the source of the data, including if it came from publicly accessible sources.

Employers are required to provide the information in a concise, transparent, intelligible and easily accessible form. It must be in writing, and written in clear and plain language.

Where an employer wishes to process existing personal data for a new purpose, it must inform the job applicant of that further processing.

Organisations are required to appoint a data protection officer under the GDPR if they are a public authority, if their core activities include the regular and systemic monitoring of data subjects on a large scale, or if their core activities consist of processing special categories of personal data or data relating to criminal convictions and offences on a large scale.

The GDPR and the Data Protection Bill place restrictions on the processing of special categories of personal data and data on criminal convictions and offences. Under the GDPR, special categories of personal data are defined as information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data. Data on criminal convictions and offences includes information relating to criminal allegations and proceedings. These types of data were previously known as "sensitive personal data" under the Data Protection Act 1998.

In order to process special categories of employment data, such as disability information, or data on criminal convictions and offences of job applicants, employers are likely to rely on the ground that processing is necessary to perform or exercise obligations or rights under employment law.

Where an employer collects applicant data for equal opportunities monitoring purposes, it may rely on a limited exception under the Data Protection Bill for processing data related to racial or ethnic origin, sexual orientation, health and religious or belief only.