

## 1. Introduction

- 1.1. As part of any recruitment process, Lindum Group Ltd (the Company) collects and processes personal data relating to job applicants. The Company is committed to being transparent about how it collects and uses that data while meeting its data protection obligations.

## 2. What information does Lindum collect?

- 2.1. The Company collects a range of information about candidates applying for positions within the Company whether advertised or speculatively. This could include;
- name, address and contact details, including email address and telephone numbers
  - details of qualifications, skills, experience and employment history
  - driving qualification and status
  - information about current level of remuneration, including benefit entitlements
  - disability information which the Company needs to make reasonable adjustments during the recruitment process
  - information about nationality and entitlement to work in the UK
  - equal opportunities monitoring information, including information about ethnic origin, sexual orientation, health, and religion or belief
- 2.2. The Company collects this information in a variety of ways. For example, data might be contained in application forms, CVs or resumes, obtained directly from passport or other identity documents, collected through interviews or other forms of assessment.
- 2.3. The Company may also collect personal data from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks. The Company will seek this information from third parties only when considering making a firm job offer.

## 3. Where does the Company store personal data?

- 3.1. Lindum Group uses an applicant tracking system 'Zoho Recruit'. Candidates applying online will usually be directed to the portal to submit their application or applications received from other sources will be uploaded on to the platform. Data will also be stored in a range of different places, including individual's application record, in the HR management systems and on other IT systems (including email). The Company will not transfer your data outside the European Economic Area. Zoho Recruit is a cloud-based platform and data for EU-based users is held at data centres within the EU.

## 4. How does Lindum protect data?

- 4.1. The Company takes the security of personal data seriously. It has internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and not accessed except by our employees in the proper performance of their duties. Zoho Recruit's accreditations, policies and procedures have been checked and approved by our cyber security team.

## 5. Who has access to data?

- 5.1. The Company will not share applicant's data with any other third parties, unless the application for employment is successful and it becomes necessary to confirm an offer of employment. The Company may then share your data with former employers to obtain references, employment background check providers to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal records checks.
- 5.2. Applicant's information will be shared internally for the purposes of the recruitment exercise. This includes members of the HR team, interviewers and admin staff 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.

## 6. Why does the Company process personal data?

- 6.1. The Company needs to process data to take the necessary steps initiate and carry out the recruitment selection process. It also needs to process the data to enter into a formal contract of employment with successful candidates.
- 6.2. In some cases, the Company 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.

- 6.3. The Company 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 Company to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. The Company may also need to process data from job applicants to respond to and defend against legal claims.
- 6.4. The Company 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.
- 6.5. The Company only processes other special categories of data, such as information about ethnic origin, sexual orientation, health or religion or belief, for equal opportunities monitoring purposes.
- 6.6. For some roles, the Company is obliged to seek information about criminal convictions and offences. Where the Company 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.

## **7. For how long does the Company keep data?**

- 7.1. All unsuccessful applicants' information is retained on file by the Company for a period of 6 months in case there are future employment opportunities for which they may be suited unless candidates specifically withdraw consent to do so.
- 7.2. After 6 months unsuccessful candidate's submitted information is destroyed. A secure log of all applications to join the Company is retained recording name, contact detail, ethnic origin, gender and position applied for equal opportunities monitoring purposes and future employment opportunities. This data is anonymised after 2 years.
- 7.3. Successful applicants will have the personal data gathered during the recruitment process transferred to their personnel file and retained during your employment in accordance with the Company Privacy Policy for personnel records.

## **8. Applicant's rights**

- 8.1. As a data subject, the Company accepts applicants have a number of rights. They can;
  - access and obtain a copy of their data on request in accordance with the Company's Subject Data Access Request Procedure PR/03/01
  - require the Company to change incorrect or incomplete data
  - require the Company to delete or stop processing their data, for example where the data is no longer necessary for the purposes of processing
  - object to the processing of their data where the Company is relying on its legitimate interests as the legal ground for processing
  - request the Company to stop processing data for a period if data is inaccurate or there is a dispute about whether or not their interests override the Company's legitimate grounds for processing data
- 8.2. Any applicant wishing to make a Subject Data Access Request should contact a member of the Lindum HR Team to request a Subject Data Access Request Procedure Form FO/01/21 to complete and submit.
- 8.3. Applicants who believe that the Company has not complied with their data protection rights, can complain to the Information Commissioner.

## **9. What if applicants do not provide personal data?**

- 9.1. Applicants are under no statutory or contractual obligation to provide data to the Company during the recruitment process. However, if they do not provide the information they may place themselves at a disadvantage as the Company may not be able to process their application properly or at all.
- 9.2. Applicants 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.

## **10. Automated decision-making**

- 10.1. Lindum recruitment processes are not based solely on automated decision-making.

### **Related Documents:**

Subject Data Access Request Form FO/01/21  
Lindum Privacy Notice PO/05/04  
Subject Data Access Request Procedure PR/03/01