



## Aveni Recruitment Privacy Notice

**Effective Date: 10 01 2023**

**Version: 1.0**

### Introduction

Aveni (“we” “our” “us”) is a data controller and responsible for deciding how we collect, store and process personal data on individuals we interact with. This also includes any candidates who apply to any of our job vacancies.

This recruitment privacy notice is designed to ensure any job applicants are aware of how and why personal data will be used for recruitment purposes, for how long it will be retained for and where any recruitment data may be shared to name as a few examples.

We have designed this recruitment privacy notice in accordance with requirements under the UK GDPR. This notice will be reviewed and updated where changes in legislation may occur.

You contact our head office using the following details:

Post:

25 South Lauder Road  
Edinburgh  
EH9 2NB  
Scotland

Email: [info@aveni.ai](mailto:info@aveni.ai)

Phone: +44 (0)3330 165 242

We have also appointed an external data protection officer (DPO) and their details are as follows:

Evalian Limited  
West Lodge  
Leylands Business Park  
Colden Common  
Hampshire  
SO21 1TH  
United Kingdom

Email: [dpo@aveni.ai](mailto:dpo@aveni.ai)

Phone: +44 (0)333 050 0111

Website: [www.evalian.com](http://www.evalian.com)

## **Lawful Basis**

The lawful basis for our recruitment process is contractual obligation, to help us enter into or take the necessary steps required to enter into employment contracts.

## **Personal Data Collected**

Our job vacancies are advertised through several means. We advertise for roles on our website via the careers section and through other websites such as Indeed and LinkedIn. We may also post job roles on multiple other third-party websites and all data received through these websites will be received directly into Aveni. We do not share recruitment data with third party recruitment agencies.

Our website careers section is powered through an online recruitment CRM solution [Zoho Recruit](#).

Our job vacancies on our website require the following personal data:

- Name
- Email
- Phone number
- Address
- Current job details
- Education level
- Past and present work experience
- Social network (optional to include your LinkedIn profile as an example)
- Photos
- CVs

Applications can also be made by applying with your Indeed account which will connect to your profile and other relevant information and documentation (e.g. CV and cover letters).

Applications on LinkedIn will require:

- Contact information
- CV
- Answers to any applicable questions

We may need to process special category personal data (e.g. disability information) as part of the recruitment process which we have detailed below.

## **How We Obtain Personal Data**

During our recruitment process we may obtain personal data about candidates through various means, which include (but is not limited to):

- Directly from the candidate
- DBS check providers

- Credit reference agency
- Specified referees
- Data sharing amongst staff and head office (e.g. recommendations)

### **How Is Personal Data Used?**

Personal data processed as part of the recruitment process can include the following activities:

- To assess your skills, qualifications, and suitability for the role
- Carry out background and reference checks, where applicable
- Communicate with you about the recruitment process
- Keep records related to our hiring processes
- Comply with legal or regulatory requirements
- If successful offer suitable candidates contracts of employment

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history) we will not be able to process your application successfully.

### **Special Category Personal Data**

As mentioned above we may need to process special category personal data to ensure a fair recruitment process. If a candidate informs us that any adjustments are needed (e.g. wheelchair user or visually impaired) we will be sure to document this and keep it safe and secure, and made available to those who need access to this data. This data will also be held for as long as necessary as part of our data retention guidelines.

### **Criminal Conviction and Offences Data**

As mentioned on our privacy notice on our website, our roles require background checks on vacancies applied for. We carry out basic criminal background checks as part of our contractual arrangements with our clients. We will only request checks when a job offer has been made and we use a third party called [CV Insights](#) to help carry out these activity. CV Insights will be in contact with candidates to carry out the checks and will share relevant information to us when a check has been completed.

Where we do process any criminal conviction and offence data we will ensure the safety and security of this data so it is not compromised in any way.

### **Data Sharing**

As mentioned above personal data of job applicants can be shared amongst staff and our head office. We do this to ensure the recruitment process has been carried out in accordance with our recruitment policies and the appropriate files can be created and maintained. We do not share recruitment data with any third parties.

### **International Data Transfers**

We do not transfer any recruitment data outside the UK to other companies or individuals based in the EEA (European Economic Area) or globally.

### **Automated Decision-Making and Profiling**

We do not conduct any automated decision making and profiling as part of our recruitment process.

### **Data Security**

We have certifications with security frameworks such as ISO 27001, and copies of these certificates are available upon request. We also review our certifications annually.

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. If we become aware of any loss, misuse, alteration of personal data we will work closely with our IT team, DPO and other parties as necessary to investigate the incident at hand. We have put into place the relevant procedure and policies in place to investigate, mitigate and report (when needed to relevant parties) such instances.

### **Data Retention**

We retain recruitment data for as long as needed as part of our recruitment process. If you have not been successful we will typically retain this data for a period of 6 months so we can show and evidence a fair recruitment process and there is no discrimination on any protected characteristics/grounds. After this period has ended all relevant data will be securely destroyed.

Successful candidates will have their recruitment data added to their HR file which is maintained and held by our head office.

### **Data Protection Rights**

If you are based in the UK you have several Rights to how an organisation processes your personal data. The Rights are as follows:

- Right to be informed
- Right to access data
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to objection
- Right to portability
- Right not to subject to automated decision making and profiling

If you would like to exercise any of the above Rights you can do so by sending us a written request to our email address mentioned above.

## **Concerns and Complaints**

We understand you may have concerns and complaints to this notice and any aspects to how we process personal data. If you would like to contact us directly to talk to us about a concern or to raise a complaint, you can do so by using our contact details above.

You can also submit a complaint directly to the Information Commissioners Office (the ICO), the UK supervisory authority for data protection in the UK, via this link <https://ico.org.uk/make-a-complaint/>.

## **Review and Updates**

We will review this notice and make changes to it from time to time. We recommend that you check this notice to see where changes have been made and to ensure you are able to review updated information at all times.