Recruitment Privacy Policy

Introduction
This Recruitment Privacy Policy explains how Proeon Systems Limited collects, uses, and protects personal data relating to job applicants and candidates who apply for roles with us. We are committed to protecting personal data and handling it responsibly in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This policy applies to all individuals who apply for employment, whether directly or via recruitment agencies or other recruitment channels.

Data Controller

The data controller is:
Proeon Systems Limited
Registered address:
Email: DataSecurity@proeon.co.uk

Data Protection Officer (DPO):
Sharon Ware
Email: Sharonw@proeon.co.uk

Personal Data We Collect

We may collect and process the following categories of personal data during the recruitment process:

a) Identification and contact details
- Name
- Email address
- Telephone number
- Postal address

b) Recruitment and application data
- CVs and cover letters
- Education, qualifications, and employment history
- Professional certifications
- Skills and experience

c) Assessment and interview data
- Interview notes and feedback
- Technical test or assessment results

d) Online and publicly available data
- LinkedIn profiles or other professional online information where relevant and voluntarily provided

e) Administrative data

- Correspondence with us or group company
- Availability
- Salary expectations

f) Right to work information

- Information required to verify eligibility to work in the UK

g) Special category data

We do not intentionally collect special category personal data unless:

- it is required to comply with employment or equality law (e.g. disability information to make reasonable adjustments), or
- it is voluntarily disclosed by the candidate.

Any special category data is processed with enhanced safeguards.

How We Collect Personal Data

We collect personal data through:

- Applications submitted via our careers website
- Applications via our group company
- Email or direct submissions
- Recruitment agencies
- Professional networking platforms
- Employee referrals
- Interviews, assessments, and recruitment communications

Purposes and Lawful Bases for Processing

We process personal data for the following purposes and under the following lawful bases:

Purpose	Lawful Basis (UK GDPR)
Managing and accessing job applications	Legitimate interests or steps prior to entering into a contract
Communicating with candidates	Legitimate interests
Conducting interviews and assessments	Legitimate interests
Verifying qualifications, experience, and right to work	Legal obligation
Making hiring decisions	Legitimate interests
Maintaining recruitment records	Legitimate interests
Keeping a talent pool (where applicable)	Legitimate interests or consent
Defending or pursuing legal claims	Legitimate interests

Where consent is used as a lawful basis, it may be withdrawn at any time without affecting the lawfulness of processing carried out before withdrawal.

Automated Decision-Making

We do not use automated decision-making or profiling that produces legal or similarly significant effects on candidates.

Data Sharing and Recipients

We may share personal data with:

- Employees involved in recruitment and hiring
- Recruitment agencies acting on our behalf
- Recruitment & HR department of our group company
- IT service providers and recruitment systems (e.g. applicant tracking systems)
- Professional advisers (legal, audit)
- Regulatory or public authorities where required by law

All third parties are required to process personal data securely and in accordance with our instructions.

International Transfers

If personal data is transferred outside the UK, we ensure appropriate safeguards are in place, such as:

- UK adequacy regulations
- International Data Transfer Agreements (IDTAs)

Data Retention

We retain recruitment personal data only for as long as necessary for the purposes for which it was collected:

- Unsuccessful candidates: typically retained for 6 months after the recruitment process concludes
- Successful candidates: relevant data becomes part of the employee personnel file
- Talent pool candidates: retained for as long as appropriate or until an objection is raised

Retention periods may be extended where required to comply with legal obligations or to establish, exercise, or defend legal claims.

Data Security

We have implemented appropriate technical and organisational measures to protect personal data, including:

- Access controls and role-based permissions
- Secure IT systems and networks
- Confidentiality obligations for staff
- Data minimisation and secure storage practices

Your Data Protection Rights

Under UK data protection law, candidates have the right to:

- Access their personal data
- Request rectification of inaccurate or incomplete data
- Request erasure of personal data
- Restrict processing
- Object to processing based on legitimate interests
- Request data portability
- Withdraw consent (where applicable)

Requests can be made by contacting: DataSecurity@proeon.co.uk

Complaints

If you have concerns about how your personal data is handled, you have the right to lodge a complaint with the Information Commissioner's Office (ICO).

Changes to This Policy

We may update this Recruitment Privacy Policy from time to time. The most recent version will always be published on our website.

Richard Miller

Managing Director – Proeon Systems Limited