

Data Protection Policy
UAV Talent (Nicoll Global Holdings Ltd)
Effective Date: 23/06/2024

1. Introduction

UAV Talent (“we,” “our,” or “us”) is committed to protecting and respecting the privacy and security of personal data. This policy outlines how we comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, ensuring the confidentiality, integrity, and lawful processing of all personal data we handle.

2. Scope

This policy applies to all employees, contractors, consultants, and any other individuals or organizations working on behalf of UAV Talent. It covers all personal data we process in relation to our operations, including data concerning employees, job applicants, contractors, and third parties.

3. Data Protection Principles

We adhere to the following principles under the UK GDPR:

1. **Lawfulness, Fairness, and Transparency:** Personal data shall be processed lawfully, fairly, and transparently.
 2. **Purpose Limitation:** Data shall be collected for specified, explicit, and legitimate purposes and not further processed in an incompatible manner.
 3. **Data Minimization:** Data collected shall be adequate, relevant, and limited to what is necessary.
 4. **Accuracy:** Personal data shall be accurate and kept up to date.
 5. **Storage Limitation:** Data shall be retained only for as long as necessary for its intended purposes.
 6. **Integrity and Confidentiality:** Data shall be processed securely to prevent unauthorized access, loss, destruction, or damage.
 7. **Accountability:** We shall be responsible for and able to demonstrate compliance with these principles.
-

4. Types of Data We Collect

We may collect and process the following types of personal data:

- **Contact Information:** Names, email addresses, phone numbers.
 - **Employment Information:** CVs, employment history, references.
 - **Financial Information:** Bank details for payment processing.
 - **Technical Information:** IP addresses, cookies, and activity logs when using our online services.
-

5. Lawful Bases for Processing

We process personal data under one or more of the following lawful bases:

- **Consent:** The individual has given clear consent for the processing of their data.
- **Contract:** Processing is necessary for a contract with the individual or to take steps at their request before entering into a contract.
- **Legal Obligation:** Processing is necessary for compliance with a legal obligation.

- **Legitimate Interests:** Processing is necessary for our legitimate interests or those of a third party, provided these are not overridden by the individual's rights.
-

6. Data Subject Rights

Under the UK GDPR, individuals have the following rights:

1. **The right to be informed:** About how and why we process their data.
 2. **The right of access:** To their personal data and supplementary information.
 3. **The right to rectification:** To correct inaccurate or incomplete data.
 4. **The right to erasure:** To have their data erased under certain conditions.
 5. **The right to restrict processing:** To limit the way their data is used.
 6. **The right to data portability:** To obtain and reuse their data across services.
 7. **The right to object:** To certain types of processing, such as direct marketing.
 8. **Rights related to automated decision-making and profiling:** To not be subject to decisions made solely by automated processes.
-

7. Data Retention and Storage

Personal data will be retained only as long as necessary to fulfil its purposes or as required by law. We implement secure storage solutions to protect data and ensure secure deletion or anonymization when no longer needed.

8. Data Security

We implement appropriate technical and organizational measures to safeguard personal data, including:

- Encryption and pseudonymization of data where appropriate.
 - Regular security assessments and training for staff.
 - Access controls to limit data access on a need-to-know basis.
-

9. Data Sharing

We will not share personal data with third parties unless:

- It is necessary for fulfilling a contract or legal obligation.
 - We have obtained explicit consent from the individual.
 - It is required for legitimate business interests, and appropriate safeguards are in place.
-

10. Data Breaches

In the event of a data breach, we will:

1. Assess the breach's scope and impact.
 2. Notify the Information Commissioner's Office (ICO) within 72 hours, if required.
 3. Inform affected individuals where there is a high risk to their rights and freedoms.
 4. Document the breach and implement measures to prevent recurrence.
-

11. Data Protection Officer (DPO)

Tom Graham-Nicoll

Email: hello@uavtalent.com

Phone: +44 330 133 8371

The DPO is responsible for overseeing this policy's implementation and ensuring compliance with data protection laws.

12. Complaints and Queries

For any questions, concerns, or complaints regarding this policy or data processing, please contact:

Email: hello@uavtalent.com

Address: 167-169 Great Portland Street, London, England, W1W 5PF

Individuals also have the right to lodge a complaint with the ICO at www.ico.org.uk.

13. Policy Review

This policy will be reviewed annually or as necessary to reflect changes in legislation, regulatory requirements, or our operations.
