Reconomy

# Privacy Policy

## PinPoint-Onboarding

# Contents

# 1. Introduction

This Privacy Policy explains how Reconomy ("we", "us", "our", "company") collects, uses, stores, and shares personal data submitted by job applicants ("you", "your") through our Applicant Tracking System (ATS) named PinPoint.

We are committed to protecting your privacy and complying with the Data Protection Laws.

Reconomy acts as the data controller for the processing of personal data described in this Privacy Policy. Further details regarding the relevant employing entity will be provided during the recruitment or onboarding process.

# 2. Definitions

**"Data Protection Laws"**: Means applicable law and regulatory requirements relating to the processing, privacy and use of personal data and protection of individuals, including, but not limited to:

(i) Regulation (EU) 2016/679 ("GDPR")
(ii) Regulation (EU) 2016/679 ("GDPR") as incorporated into domestic UK law by the European Union (Withdrawal Agreement) Act 2020 and amended by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020 (together the "UK GDPR").
(iii) any legislation enacted in the country of establishment of the data controller in respect of the protection of personal data or any corresponding or equivalent national laws or regulations.
all as amended, updated, or replaced from time to time;

**"Relevant Guidance"**: means

(i)guidance and codes of practice issued from time to time by a data protection regulator and/or the European Data Protection Board (previously known as the Article 29 Working Party); and
(ii)any relevant case law, court order, judgment or decree under applicable law and regulatory requirements.

**"Domestic Law"** Means the laws of the country of establishment of the data controller.

**"Personal Data"** Means any information relating to an identified or identifiable natural person, who can be identified, directly or indirectly, such as a name, identification number, location, online identifier.

# 3. What Personal Data We Collect

We may collect the following categories of personal data for employment and onboarding documentation, which may vary depending on the country of employment and applicable legal requirements, including for the EU and the UK, such as:

- Full name and contact details (email, phone, address);
- Employment details (start date, job title, contract type);
- Proof of identity and right to work (passport, national ID card, residence permit, visa, biometric residence permit);
- Identification and statutory information, such as national identification numbers or ID card details, date of birth, sex, marital status, number of dependents or children (where required for tax or benefits registration) to fulfil legal, payroll, tax, or social security obligations;
- Social security or national insurance information;
- Tax-related forms and declarations (e.g. tax identification numbers, tax residency declarations);
- Employment eligibility and statutory declarations;
- Bank account details for salary payments;
- Signed employment agreements, policies, and acknowledgements;

- Background or reference check documentation, where permitted by law.

In certain jurisdictions, we may also collect and process special category personal data and criminal conviction data where permitted and required by law, for employment and onboarding purposes.

This may include:

- Medical or health-related information, such as fitness-to-work assessments or mandatory occupational health checks;
- Criminal conviction or background check information, where required by law or permitted for the role.

Such data is processed strictly in accordance with applicable Data Protection Laws and only where appropriate legal safeguards are in place.

The specific documents requested depend on local legal, regulatory, and employment requirements applicable in the relevant EU Member State or the United Kingdom.

## 4. Legal Basis for Processing

We process your data under the following lawful bases:

- Compliance with a legal obligation

Certain onboarding data must be processed in order to meet our obligations under employment, tax, social security, health and safety, and identity-verification laws (e.g., social security number, ID documents, statutory declarations, medical examination scheduling when required by law).

Processing of special category data and criminal conviction data is carried out where necessary to comply with employment, health and safety, occupational health, or legal screening obligations, and in accordance with Articles 9(2) and 10 GDPR, as applicable.

- Performance of a contract

We process personal data because it is necessary to take steps prior to entering an employment contract and to perform our contractual obligations once the employment relationship begins (e.g., preparing employment documents, creating user accounts, and granting system access).

- Consent:

For optional data (e.g., equal opportunity monitoring) and marketing communications

## 5. How We Use Your Data

We use your personal data for:

- Organizing pre-employment or onboarding checks, such as your first medical examination or identity verification, where required by law or internal policies;
- Preparing and issuing your employment documents;
- Managing mandatory administrative steps, including creating your employee profile, generating your employee ID, and setting up your access permissions;
- Ensuring legal and HR compliance, such as employment, tax, and social security obligations.
- Verifying your eligibility to work in the relevant jurisdiction and complying with EU and UK employment, immigration, tax, and social security laws.

We do not carry out automated decision-making or profiling within the meaning of Article 22 GDPR that produces legal effects or similarly significant effects on you.

## 6. Data Sharing

We may share your data with:

- Payroll and benefits providers
- Third-party service providers who support payroll processing, tax administration, pension schemes, medical or other insurance, wellbeing platforms or other employment-related benefits. Occupational health, medical service providers and health and safety

Where required for mandatory pre-employment or onboarding medical checks , workplace health and safety assessments, risk evaluations, or statutory compliance.

- IT and system service providers

Vendors who provide tools used for onboarding, identity verification, access management, or internal communication platforms.

- Regulatory and governmental authorities

When required to comply with legal obligations related to employment, tax, social security, immigration, health and safety, or other statutory requirements

- Background screening and verification providers

Third-party providers performing background, reference, or right-to-work checks, where permitted by applicable law.

- Professional advisors

Legal, tax, audit, or HR advisors, where necessary for compliance with legal or regulatory obligations.

- Regulatory and governmental authorities

When required to comply with legal obligations related to employment, tax, social security, immigration, health and safety, or other statutory requirements.

- Other companies within the Reconomy, where necessary for internal HR administration or group-wide compliance purposes.

All third parties are bound by data protection agreements and must comply with Data Protection Laws.

## 7. Data Retention

We retain personal data collected during the onboarding process only for as long as necessary for employment and legal purposes, including:

- During your employment: Onboarding personal data becomes part of your employee file and is kept for the duration of your employment.
- After employment ends: Certain information may be retained for mandatory legal, tax, social security, audit, or employment law retention periods, depending on local regulatory requirements.
- Where no specific legal period applies: Data is retained only for as long as necessary for the purpose for which it was collected, and then securely deleted or anonymised.
- Local regulatory requirements: Retention periods may vary by country, and we apply all applicable local statutory retention

8. Your Rights

## 8. Your rights

Under GDPR, you have the right to:

- Access your data
- Rectify inaccurate data
- Erase your data ("right to be forgotten")
- Restrict or object to processing
- Data portability
- Withdraw consent at any time

To exercise your rights, contact us at gdpr@reconomy.com.

## 9. International Transfers

If your data is transferred outside the UK or EU, we ensure appropriate safeguards are in place, such as Standard Contractual Clauses or adequacy decisions.

Due to the international nature of the Company's operations, personal data may be disclosed to countries outside of the UK and/or the European Economic Area (EEA).

If a Company controller transfers personal data to a third country i.e., outside the European Economic Area for an EU Controller or outside the UK for a UK Controller, the Company will seek to put in place appropriate safeguards to ensure that personal data remains adequately protected.

We will ensure that all legal requirements in respect to international data transfers will be followed.

## 10. Complaints

If you believe your data rights have been violated, you can contact:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113
ICO website: https://www.ico.org.uk

You can also complain to your local Supervisory Authority ("SA") if you are unhappy with how we have used your data. A list of EU SAs is maintained by the European Data Protection Board (EDPB) and can be accessed here.