Employee Privacy Notice

Contents

[1. Introduction 3](#_Toc155703939)

[2. Definitions 3](#_Toc155703940)

[3. Who this Policy applies to 4](#_Toc155703942)

[4. How we get your Personal Information 4](#_Toc155703943)

[5. The type of Personal Data we collect and why 4](#_Toc155703954)

[6. Lawful Basis for processing your Personal Data 7](#_Toc155703962)

[7. Disclosure to and by Third Parties 8](#_Toc155703967)

[8. How we protect Personal Data 9](#_Toc155703968)

[9. How long we keep Personal Data 9](#_Toc155703969)

[10. Your Responsibilities 10](#_Toc155703970)

[11. Your Rights 10](#_Toc155703971)

[12. Lodging a Complaint 11](#_Toc155703978)

[13. Notice Review 11](#_Toc155703979)

# Introduction

Information about, and which relates to you (“Personal Data”), is protected by law. Your right to privacy and the protection of your personal data is controlled by “Data Protection Laws”. Data Protection Laws will be different depending on the country of your employer. In Europe and the UK, the General Data Protection Regulation (“GDPR”) and associated Domestic Law will protect your data rights. Data Protection Laws regulate the way your personal data is used.

(Insert Company Name) (the “Company”) (“We, “Us”, “Our”) is a "data controller", which means we are responsible for deciding how we hold and use personal information about you. We are required under Data Protection Laws to notify you of the information contained in this privacy notice. This notice should be read in conjunction with our Data Protection Policy.

As an employer, [Insert Company name] must meet its contractual, statutory and administrative obligations. We are committed to ensuring that the personal data of our employees is handled in accordance with the principles set out in Data Protection Laws. This privacy notice tells you what to expect when [Insert Company name] collects personal data about you.

# Definitions

# In this policy, the following definitions will be used for the below terms:

|  |  |
| --- | --- |
| **“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.   1. Regulation (EU) 2016/679 (“**GDPR**”) 2. 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**”). 3. any legislation enacted in the country of establishment[[1]](#footnote-2) 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”** | 1. 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 2. any relevant case law, court order, judgment or decree under applicable law and regulatory requirements. |
| **“Domestic Law”** | 1. means the laws of the country of establishment of the data controller. |

# Who this Policy applies to

This policy applies to all employees, ex-employees, consultants, contractors, directors, secondees, casual workers, agency workers, volunteers and individuals on work experience (“Staff”).

This policy provides you with information regarding the types of personal data that the Company may hold and process about you and why, including with regards to the collection, use, processing, handling, storage and disposal of personal data.

# How we get your Personal Information

# We get information about you from the following sources:

# Directly from you

# Employment agencies

# Your employer if you are a secondee

# Referees, either external or internal

# Background screening checks\*

# Occupational health and other healthcare providers\*

# Pension administrators and other government departments\*

# Providers of staff benefits

# Images from CCTV systems

# The type of Personal Data we collect and why

We may process the following categories of personal data:

## 

## Information related to your Employment

We may use the following information to carry out the contract we have with you, provide you access to business services required for your role and manage our human resources processes.

* Personal contact details such as your name, address, contact telephone numbers and personal email address
* Country and date of birth and gender
* Government ID/NI number/tax number, insurance details\*
* Your photograph
* Passport number, Visa or similar photographic identification and/or proof of address documents
* Marital status
* Employment and education history including your qualifications, job application, employment references and right to work information
* Location of employment
* Details of any secondary employment, political declarations, conflict of interest declarations or gift declarations
* Background screening checks
* Internal identification number and system usernames
* Any criminal convictions that you declare to us
* Responses to staff surveys if this data is not anonymised
* Correspondence with us and other information provided to us by you

## Information related to your Salary, Pension and Loans

We process this information for the payment of your salary, pension and other employment related benefits. We also process it for the administration of statutory and contractual leave entitlements such as holiday or maternity leave.

* Information about your job role and your employment contract, including duties, start and leave dates, salary, changes to your employment contract and working pattern.
* Details of your time spent working and any overtime, expenses or other payments claimed.
* Details of any leave including sick leave, holidays, special leave etc.
* Pension details including membership of both state and occupational pension schemes (current and previous).
* Your bank account details, payroll records and tax status information.
* Details relating to maternity, paternity, shared parental and adoption leave and pay.

## Information relating to your Performance and Training

We use this information to assess your performance, to conduct pay and grading reviews and to deal with any employer/employee related disputes. We also use it to meet the training and development needs required for your role.

* Information relating to your performance at work.
* Grievance and dignity at work matters and investigations to which you may be a party or witness.
* Disciplinary records and documentation related to any investigations, hearings and warnings/penalties issued.
* Information related to your training history and development needs.

## Information relating to Monitoring

We use this information to assess your compliance with corporate policies and procedures and to ensure the security of our premises, IT systems and employees, and to prevent crime and fraud.

* Information about your access to data
* Information derived from monitoring IT acceptable use standards.
* Information obtained through electronic means such as a key fob
* CCTV footage

## 

## Information relating to your Health and Wellbeing

We may collect the following data to ensure the health, safety and wellbeing of our employees:

* Health and wellbeing information either declared by you or obtained from health checks, eye examinations, occupational health referrals and reports, sick leave forms, health management questionnaires, fit notes or drug and alcohol testing.
* Accident records if an accident occurs at work
* Next of kin, emergency contacts and their contact information
* Details of any access needs or reasonable adjustments to working conditions e.g., accessibility (where applicable).

## Special Category and Criminal Offence Data

We may also collect “sensitive personal data” about you. This is a special category of data which requires a higher level of protection under Data Protection Laws. The following information about you may be collected to comply with our legal obligations, for equal opportunities monitoring and other contractual obligations:

* Racial or ethnic origin and religious beliefs\*.
* Biometric data obtained for identification purposes (used only for access control)
* Gender identification.
* Disability information
* Medical and health records (for example, in relation to administering your pension and any insurance benefits)
* Absence records including reasons for absence and self-certification forms
* Criminal record data and driving offences\*
* Data relating to money owed to a creditor\*

Where special category data is collected, a Data Protection Impact Assessment shall be completed.

## Images and Recordings Data

* We may also collect photographs which may be used on the company’s website or other marketing material or internal communications or systems (formal consent will be obtained)
* Any content featuring you produced for use on our website, intranet or social media such as videos, authored articles, blog posts and speech transcripts.

# Lawful Basis for processing your Personal Data

Depending on the processing activity, we may process your personal data for one of the following reasons:

## Comply with Legal Obligations

This is processing which is necessary in order for us to comply with various employment law and other legal and compliance requirements. Data we process on these grounds includes:

* national insurance data, social code or tax information
* data regarding eligibility to work in the relevant country
* criminal records data and checks
* driving license checks to validate licences and check for driving offences
* equal opportunities and disability monitoring data
* medical and health details
* CCTV Images

## Contractual Necessity

This is processing which is necessary in order for us to enter into and perform our contract of employment with you. Data we process on these grounds includes:

* contact details
* salary and payroll details (including bank details and NI number)
* details to administer the contract we have entered into with you, your pension and any benefits we offer to you
* medical and health details

## Legitimate Interest

This is processing where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. Data we process on these grounds includes:

* details provided in your job application to determine suitability for the role applied for and to verify details provided.
* performance related information to assess your career development, conduct appraisals and to provide you with training.
* performance and disciplinary records to identify areas in which we may need to help you improve and/or to investigate if the circumstances warrant this and to take appropriate action.
* your information in management reports processed for statistical and audit purposes.
* monitoring you and your working area for health, safety and environmental matters to assess where we may need to make improvements or changes to our relevant policies and procedures and to ensure that you are complying with our health, safety and environmental policies and procedures.
* compliance with Company policies and procedures to ensure that these are properly observed and to identify where we may need to make improvements or changes to those policies and procedures.
* information available on internal systems to facilitate communication within the Company\*.

## Consent

This is processing where consent has been given for:

* Any content featuring you produced for use on our website, intranet or social media such as videos, authored articles, blog posts and speech transcripts, or any other marketing material or internal communications.
* Your professional experience to be provided to our clients in the context of any tender exercise\*
* Photographs or images of you to be used on our website, IT systems, marketing literature, newsletters and press articles.\*

# Disclosure to and by Third Parties

We may share personal data we hold with any company within the Reconomy Group, including our subsidiaries, our ultimate holding company, and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006. The sharing of personal data within the Reconomy Group of companies is subject to an Intra-Group Data Sharing Agreement.

We may share employee personal data with other parties, such as legal and regulatory authorities, professional bodies, external professional advisors (such as lawyers, accountants etc.), service providers (such as providers of payroll, pension scheme, insurance, medical benefits, human resources services, IT systems and support), and other third parties engaged to assist the Company in carrying out business activities located wherever they operate.

Sharing personal data with external third parties is subject to a Data Processing Agreement where appropriate. Personal data is restricted to authorised people and protected with technical security measures.

Where personal data is transferred to parties outside the EEA/UK, data sharing agreements will be in place and any other additional safeguards, such as International Transfer Agreements, as required by Data Protection Laws.

Access to, use of and other processing of employee personal data will be limited to individuals who need to know the information for the purposes described in Section 6, which may include personnel in HR, IT, Risk, Legal and Finance.

We may also disclose employee personal data to third parties for the following purposes:

* to our customers or prospective customers, for legitimate business purposes (including proposals and customer onboarding)
* if we are required to do so by law, regulation or legal process (such as a court order or subpoena), and in the establishment, exercise or defence of legal claims.
* in response to requests by government agencies;
* when we believe disclosure is necessary or appropriate to prevent physical harm or financial loss or in connection with an investigation of suspected or actual illegal activity.
* in the event of any potential sale of the company or any change of control or any potential transfer of your employment. Disclosure may include change of control or transfer, disclosure to the potential purchaser or investor and their advisors
* in the event of any reorganisation or restructuring of our group of companies
* in order to enforce or apply any contract with the data subject or other agreements
* to protect our rights, property, or the safety of our employees or others

We may also disclose your personal data if we are under a duty to do so in order to comply with any legal or regulatory obligation or request.

# How we protect Personal Data

Your personal data contained within the Group HR system (My Journey) is securely stored electronically on our servers which are located within the UK. (Insert any other Local HR System that you are currently using and the location of the servers).

We have implemented appropriate physical, technical, and organisational security measures designed to secure your personal data against accidental loss and unauthorised access, use, alteration or disclosure. In addition, we limit access to personal data to those employees, agents, contractors and other third parties that have a legitimate business need for such access.

Your personal data may also be stored in hard copy form and will be kept securely.

If at any time we transfer your personal data to, or store it in, countries located outside of the UK or EEA (for example, if our hosting services provider changes), we will ensure that appropriate safeguards, such as International Transfer Agreements are in place for that transfer and storage as required by Data Protection Laws.

# How long we keep Personal Data

Retention periods are set by regulation, or where none exists, is based on business practice. As legislation is regularly updated, the time that information is kept may change.

Personal data gathered during the recruitment process will be transferred to your employee file. We will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment depends on the type of data and the purpose for which it is processed.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

After the retention period, your data will either be deleted completely or anonymised.

# Your Responsibilities

We encourage you to ensure that the information that we hold about you is accurate and up to date by keeping us informed of any changes to your personal data. Please inform your local HR representative of any changes.

As an employee of the Company, you also have obligations under Data Protection Laws and must comply with the Data Protection Policy. Failure by you to follow these rules and procedures may result in disciplinary action being taken against you which could result in your dismissal.

# Your Rights

Under Data Protection Laws, you have certain rights as a “data subject”.

You may make a formal request for access to personal data that [Insert Company] holds about you at any time. This is known as a Subject Access Request (“SAR”). A SAR must be made in writing and must be responded to within one month.

You also have other rights under Data Protection Laws:

Right of access

You have the right to ask us for copies of your personal information.

Right to rectification

You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

Right to erasure

You have the right to ask us to erase your personal information.

Right to restriction of processing

You have the right to ask us to restrict the processing of your personal information.

Right to object to processing

You have the the right to object to the processing of your personal information.

**Your right to data portability:** You have the right to ask that we transfer the personal information you gave us to another organisation, or to you.

You can exercise your rights at any time by emailing [gdpr@reconomy.com](mailto:gdpr@reconomy.com), however there are certain circumstances when a request may be refused, for example when it is manifestly unfounded or excessive, for example when:

* the individual clearly has no intention to exercise their right of access.
* the request is malicious in intent and is being used to harass an organisation with no real purpose other than to cause disruption.
* the request is clearly or obviously unreasonable.; the request should be proportionate when balanced with the burden or costs involved in dealing with the request.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

# Lodging a Complaint

If you would like to make a complaint to the Reconomy Group, email [gdpr@reconomy.com](mailto:gdpr@reconomy.com).

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**.](https://edpb.europa.eu/about-edpb/about-edpb/members_en)

The ICO’s address: [replace with alternative supervisory authority if different)

Information Commissioner’s Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Helpline number: 0303 123 1113

ICO website: [https://www.ico.org.uk](https://www.ico.org.uk/)

# Notice Review

This Notice will be reviewed annually. If there are amendments, you will be notified of the changes.

If you have any questions about any matter relating to data protection or the personal data that we process about you, please contact your local Data Protection Champion.

\*This data type shall not be processed in certain jurisdictions, including Germany.

1. See recital 22 of GDPR. An establishment ‘*implies the effective and real exercise of activities through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.* [↑](#footnote-ref-2)