SIMPLIFY

Employee Privacy Notice

THE PURPOSE OF THIS DOCUMENT
This notice applies to current and former employees, workers, and contractors (hereafter “employees”). It describes how we will collect and use personal data during the employment relationship and thereafter. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

WHO WE ARE
Simplify (hereafter the “Simplify”) was formed in 2019 when My Home Move and The Simplify Group came together.

Simplify is made up of several individual companies. Whenever dealing with one of our companies (hereafter the “Company”), the “controller” of your personal data will be the Company that decides why and how your personal data is processed. This is the Company with whom your contract of employment is with.

Where this document refers to “we,” “our” or “us”, unless mentioned otherwise, this refers to the particular Company that is the controller of your personal data.

THE KIND OF INFORMATION WE HOLD ABOUT YOU
We will collect, store, and use the following categories of personal information about you:

- Personal details such as name, title, addresses, telephone numbers, personal email addresses, date of birth, gender, details of dependants, next of kin and emergency contact information.
- National Insurance number, bank account details, payroll records and tax status information.
- Salary, annual leave, pension, and benefits information.
- Copies of identification documents for example driving licence, passport, marriage certificate
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Professional qualification and status information.
- Employment records (including job titles, work history, working hours, training records, compensation history, performance information, details regarding disciplinary and grievance issues and professional memberships).
- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about your use of our information and communications systems.
- Photographs and videos.
- Inferred data generated by our models (e.g. risk scores).

We may also collect, store, and use the following "special categories" of more sensitive personal information, namely information relating to:

- Your race or ethnicity, religious beliefs, sexual orientation, and political opinions.
- Trade union membership.
- Your health, including any medical condition, and sickness records.
- Criminal convictions and offences.

HOW IS YOUR PERSONAL INFORMATION COLLECTED?
We collect personal information about employees, workers and contactors through the application and recruitment process, and thereafter, during job-related activities throughout the period of you working for us.

HOW WE WILL USE INFORMATION ABOUT YOU

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered with you.
2. Where we need to comply with a legal obligation.
3. 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.

4. Where it is necessary for our recognised legitimate interests which allows security related activities to be considered a legitimate interest by default, such as fraud prevention, public safety, and national security.

The situations in which we will process your personal information are listed below:

- Making decisions about your recruitment, appointment, your continued employment, promotions, remuneration changes and terms of employment.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.
- Benefits administration
- Conducting performance reviews, managing performance, and determining performance requirements.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Education, training, and development requirements.
- Dealing with employee relations and/or legal disputes involving you, or other employees, workers, and contractors, including accidents at work.
- Ascertaining your fitness to work and/or managing sickness absence.
- For the prevention and detection of fraud, crime and/or for health & safety purposes – we may use CCTV to monitor our premises in this regard.
- Carrying out criminal record or credit checks as required by law and/or to meet our lender panel membership obligations.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies and maintain ensure network and information security. We also monitor and record telephone calls to ensure that our clients/customers receive quality advice and care.
- To use artificial intelligence, machine learning and trained reviewers to process information to improve our services to you, to troubleshoot and train our staff. These tools are used on data collected directly and indirectly over electronic communication, call recording and post.
- To develop and operate AI systems to improve communication speed and consistency; and support fraud prevention and quality-assurance objectives.
- Equal opportunities monitoring.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

<u>If you fail to provide personal information</u>
If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations or exercise rights in connection with employment.
3. Where it is needed in the public interest, such as for equal opportunities monitoring, or in relation to our occupational pension scheme.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

<u>Our obligations as an employer</u>
We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
- We will use information about your race or national or ethnic origin, religious, philosophical, or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

Do we need your consent?
We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations, or exercise specific rights in the field of employment law.

INFORMATION ABOUT CRIMINAL CONVICTIONS, CREDIT AND FRAUD CHECKS
We will only collect (and retain) information about criminal convictions if it is appropriate, given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process, or we may be notified of such information directly by you in the course of you working for us.

For certain roles within Simplify, the personal information we have collected from you will be shared with Cifas who will use it to prevent fraud, other unlawful or dishonest conduct, Confidential malpractice, and other seriously improper conduct. If any of these are detected, you could be refused certain services or employment. Your personal information will also be used to verify your identity. Further details of how your information will be used by us and Cifas, and your data protection rights, can be found by contacting the HR Department or our Data Protection Officer.

Please note that lender panels may conduct credit checks on all qualified individuals and/or any employee who signs certificates of titles on behalf of one of Simplify's law firms. We must pass on your personal details to comply with our obligations to them.

AUTOMATED DECISION-MAKING
You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making unless we have a lawful basis for doing so and we have notified you. Where an automated decision has a significant or legal impact on you, we will have sufficient safeguards in place, such as ensuing the decision is subject to meaningful human oversight.

DATA SHARING
We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. "Third parties" includes third-party service providers (including contractors and designated agents) and other companies within Simplify. We only permit third parties to process your personal data for specified purposes and in accordance with our instructions, e.g., for regular reporting activities or in the context of a business reorganisation.

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your personal information with a regulator or to otherwise comply with the law. We may also share your personal information with Cyber and Data Security service providers.

HOW WE USE AI AND AUTOMATION
We employ machine-learning and other artificial-intelligence techniques hosted securely within our cloud infrastructure (primarily Microsoft Azure) to:

- Classify and route customer communications.
- Predict case timelines and outcomes.
- Automate certain internal business processes.
- Generate decision support for our staff.

These activities are carried out either with a qualified specialist reviewing the output ("human in the loop") or, where fully automated, under rigorous testing and ongoing monitoring to ensure accuracy, fairness, and non-discrimination.

If you require further information as to how we use AI, please contact our Data Protection Officer by emailing

DataProtection1@simplify.co.uk.

INTERNATIONAL TRANSFER

Your personal data may be transferred outside of the UK. These countries may not necessarily have data protection laws as comprehensive or protective as countries within the UK however, our collection, storage and use of your personal data will at all times continue to be governed by this Privacy Policy. One of our providers, Team Lease, is situated in India.

Some AI services are provided from approved locations within the EU/UK or, where applicable, the United States under the UK-US Data Bridge adequacy regulations. Certified US providers must adhere to the Data Privacy Framework Principles before we transfer data.

Simplify is comfortable that the data processors that process your data and transfer of data outside of the UK (including Team Lease) are subject to appropriate and adequate safeguards, to ensure compliance with current Data Protection Legislation. Your rights and the legal remedies available to you are enforceable against Simplify and our data processors. Further details can be obtained by emailing DataProtection1@simplify.co.uk.

DATA SECURITY AND RETENTION

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used, or accessed in an unauthorised way, altered, or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

Once you are no longer an employee, worker, or contractor of the company we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

We implement a range of technical and organisational measures to protect personal data from unauthorised access, loss, or misuse. These include access controls, encryption, monitoring systems and data loss prevention (DLP) tools designed to detect and prevent unauthorised access or transmission of data.

DATA RETENTION FOR AI

Personal data used to train or operate AI systems is retained only for as long as needed to achieve the purpose for which it was collected, after which it is securely deleted, aggregated, or anonymised. Model-generated artefacts that can no longer be linked to you may be kept for longer to improve system performance.

KEEPING AI FAIR AND SECURE

We apply proportionate testing for bias, accuracy and security throughout the AI lifecycle and maintain audit logs of model behaviour. Our governance framework assigns clear accountability for AI oversight and regular review.

RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

<u>Your duty to inform us of changes.</u>

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

<u>Your rights in connection with personal information</u>

If you want to review, verify, correct, or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the People Services in writing.

<u>No fee usually required.</u>

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

<u>What we may need from you</u>

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

RIGHT TO WITHDRAW CONSENT
In limited circumstances, you may be able to withdraw your consent to us retaining and processing your data. Please contact People Services or our Data Protection Officer for further information. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

RIGHT TO COMPLAIN
If you believe we have mishandled your personal data, failed to uphold your data protection rights, or not responded appropriately to a data protection request, you may submit a complaint using one of the following methods:

Email: DataProtection1@Simplify.co.uk
Post: Simplify Data Protection Team, 1 Frances Way, Grove Park, Leicester, LE19 1SH

If you remain dissatisfied with our handling of your complaint, you may directly contact the Information Commissioner's Officer (ICO) to ask them to consider the complaint further. Their details are:

Tel: 0303 123 1113
Website: https://ico.org.uk

You can make a complaint through their website. The ICO will expect that you have allowed us to consider and respond to your complaint in the first instance.

CHANGES TO THIS PRIVACY NOTICE
We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact the People Team or the Data Protection Team on DataProtection1@simplify.co.uk.

Last updated July 2025
Date of Next Review: July 2026