Customer Onboarding Portal Data Privacy Notice

Introduction

Simplify Moving Limited ("Simplify", "we", "our" and "us") collects, uses and shares information about you so that we can provide you with access to the Customer Onboarding Portal and related services. Simplify Moving Limited is the controller for personal data processed in connection with the Portal, except where another organisation decides why and how it uses personal data for its own purposes.

This Privacy Notice explains how we collect, use and share your information when you use the Customer Onboarding Portal ("the Portal"), including information about the device used to access the Portal, such as your mobile phone or tablet. The Portal is provided by Simplify Moving Limited to support identity verification, proof of funds, source of funds, customer due diligence and transaction information services requested by or relevant to Trusted Third Parties involved in your property transaction.

Where we decide the purpose and means for which personal data supplied through or in connection with the Portal is processed, Simplify Moving Limited is the data controller. Trusted Third Parties, such as estate agents, conveyancers, solicitors, licensed conveyancers, mortgage brokers, lenders or other professional advisers, may also act as independent controllers where they receive and use your personal data for their own legal, regulatory, anti-money laundering, fraud prevention, professional or transaction management purposes. If you have any questions or comments about this Privacy Notice or how we use your personal data, please contact our Data Protection Officer:

The Data Protection Officer

Simplify Moving Limited

1 Frances Way

Grove Park

Enderby

Leicester

LE19 1SH

Email: dataprotection1@simplify.co.uk

The Types of Personal Data We Collect and Use

Customers

Whether or not your transaction proceeds, we may use your personal data for the reasons set out below. We collect most information directly from you through the Portal, but we may also receive information from Trusted Third Parties and others involved in your property transaction. You are responsible for ensuring that any information and documentation you provide through the Portal is accurate, complete, current and not misleading.

- Full name and personal details including contact information (e.g. work and home address, email addresses, telephone numbers (home and work), job title and company details and comments)

- Date of birth (for identity purposes and to ensure you are of an age to purchase a property in the UK).
- Records of the services you have obtained or applied for, how you use them, and the relevant technology used to access or manage them (e.g. mobile phone location data, IP address, MAC address).
- Information from credit reference agencies, electoral roll, court records of debt judgements and bankruptcies and other publicly available sources.
- Family, lifestyle or social circumstances if relevant to the transaction (e.g. number of adult occupiers).
- Personal data about other individuals involved in the transaction. You must have their authority to provide their personal data to us and share this data protection statement with them beforehand.
- Identity verification results, copies of identification documents, proof of funds information, source of funds information, bank account information, financial transaction information, supporting documentation and relevant transaction information.
- Biometric data used for identity verification, such as facial likeness checks or voice recordings where applicable.
- Customer communications (such as emails and web-chat content);
- Case data you or your representatives provide;
- Inferred data generated by our models (e.g. risk scores).

Providing Your Personal Data

We will tell you if providing some personal data is optional, including asking for your consent to process it. In all other cases, you must provide your personal data to enable us to provide services to you.

Monitoring of Communications

Subject to applicable laws, we may monitor and record calls, emails, text messages, social media messages, web-chat messages and other communications relating to your dealings with us and your use of the Portal. We do this to meet legal and regulatory requirements, prevent and detect crime, protect our systems, check for inappropriate content, support quality control, audit, supervision, case escalation, service improvement and staff training. We may also use security technologies, including Data Loss Prevention tools, to help detect unauthorised sharing of personal data, malware, cyber threats, fraud risks and other security risks. These systems may automatically scan emails, attachments and electronic communications where necessary to protect you, us, the Simplify group, Trusted Third Parties, our suppliers, staff and systems. Supervisors, compliance teams, security teams and quality assurance teams may access Portal records, files and communications where necessary for these purposes.

Using Your Personal Data: The Legal Basis and Purposes

We process your personal data for the following reasons:

As necessary to perform our contract with you for the Portal and related services:

a) To take steps at your request prior to entering into the contract.

b) To allow you to decide whether to enter into the contract.

c) To manage and provide access to the Portal and related services, including identity verification, proof of funds, source of funds, customer due diligence, transaction information services, payment processing, administration and support services.

d) To obtain, review, record and share information and supporting documentation relating to your property transaction where this is requested by or relevant to Trusted Third Parties, including third-party lawyers and other professional advisers outside the Simplify group.

e) To update your records.

As necessary for our own legitimate interests or those of other persons and organisations, for example:

a) For good governance, accounting, and managing, and auditing of our business operations.

b) To monitor emails, calls, other communications, and activities on the website.

c) For market research, analysis, and developing statistics.

d) To send you marketing communications.

e) To monitor the progress, operation and use of the Portal and related services.

f) To enable satisfaction surveys to be conducted.

g) 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.

h) To use automated tools, including profiling, to support the services we provide to you. We may generate risk indicators, fraud indicators, service quality indicators or workflow priority scores from information we hold. These are used to support our staff in managing services, preventing fraud, improving service quality and identifying issues requiring review. We do not currently make decisions based solely on automated processing that produce legal or similarly significant effects without human involvement. Where automated tools are used to support decisions, they assist our staff and do not replace human judgement.

i) To develop and operate AI-assisted tools to improve communication speed and consistency, support fraud prevention and support quality assurance.

As necessary for Simplify's recognised legitimate interest, which allows the following security-related activities to be considered a legitimate interest by default:

a) Fraud prevention;
b) Public safety; and
c) National security.

As necessary to comply with a legal obligation, for example:

a) When you exercise your rights under data protection law and make request.
b) For compliance with legal and regulatory requirements and related disclosures.
c) For the establishment and defence of legal claims.

d) For activities in relation to the prevention, detection, and investigation of crime.
e) To monitor emails, calls, other communications, and activities.

Based on your consent, for example:

a) When you request us to disclose your personal data to other people or organisations, such as a company handling a claim on your behalf, or otherwise agree to disclosures.
b) When we process any special categories of personal data about you at your request (e.g., your biometric data, data concerning your health).
c) To send you marketing communications where we have asked for your consent to do so.

Please note that you are free at any time to change your mind and withdraw your consent. The consequence might be that we cannot do certain things for you.

Who we might share your information with

Subject to applicable data protection laws, we may share your data with:

- Our group of companies, including Simplify Moving Limited and its group companies such as My Home Move Ltd, Move with Us Ltd, Premier Property Lawyers Limited, Advantage Property Lawyers, JS Law Limited and Dorling Cottrell Limited, where they help provide, support or administer the Portal and related services, take or process payment, process information, provide transaction support or provide legal or conveyancing services where separately instructed.
- Sub-contractors and other persons who help us provide the Portal, identity verification, proof of funds, source of funds, customer due diligence, transaction information services, payment processing, administration and support services.
- Companies and other persons or agencies providing services to us including but not limited to electronic and facial recognition ID verification and bank/funding validation providers.
- To the introducer, estate agent, relevant conveyancer, solicitor, licensed conveyancer, mortgage broker, lender, third-party lawyer or other professional adviser involved in your property transaction who has asked us to complete or support electronic identity verification, facial recognition identity verification, proof of funds, source of funds, customer due diligence or transaction information services.
- Where a conveyancer, solicitor or licensed conveyancer originally involved in your transaction is unable to act, we may share identity verification, proof of funds, source of funds and other customer due diligence information with a replacement conveyancer, solicitor or licensed conveyancer involved in the same transaction where necessary for legal, regulatory, anti-money laundering, fraud prevention and transaction management purposes.
- Our legal and other professional advisors, including our auditors and insurers.
- Courts, to comply with legal requirements, and for the administration of justice.
- In an emergency or to otherwise protect vital interests.
- To third parties to protect the security or integrity of our business operations.
- To third parties when we restructure or sell our business or its assets or reorganise or merge.
- Market research organisations who help to improve our services.
- Cyber and Data Security service providers.
- Anyone else where we have your consent or as required by law.

- Trusted Third Parties involved in your property transaction may use this information for their own legal, regulatory, anti-money laundering, fraud prevention, professional or transaction management purposes and will normally act as independent controllers of your personal data.
- Where a member of the Simplify group is instructed to provide legal, conveyancing or other professional services in relation to your property transaction, it may act as an independent controller and process personal data in accordance with its own privacy information, regulatory obligations and professional obligations.

How we use AI and automation

We use approved technology, including AI-assisted tools, to help us provide the Portal and related services efficiently, securely and consistently. These tools may help our staff organise and route communications, analyse emails, letters and other communications received from you or third parties, identify the correct record or transaction, classify communications, extract relevant information, summarise information, identify possible issues for review, support fraud prevention and quality assurance, assist with case handling, improve communication speed and consistency, and prepare suggested responses for staff to consider. They may use personal data contained in communications, call recordings, post, Portal records, transaction information and documents where this is necessary for those purposes. These tools support our staff but do not replace human judgement.

We may use AI-assisted tools to help manage telephone enquiries. This may include transcribing calls, recording relevant information and helping answer common questions before transferring you to a member of staff where appropriate. If an AI-assisted system handles an enquiry, you may ask to speak with a member of staff. These tools do not provide legal advice or make legal decisions.

We may generate risk indicators, fraud indicators, service quality indicators or workflow priority scores from information we hold. These indicators help our staff manage services, prevent fraud, improve service quality and identify issues requiring review. They are not used as the sole basis for decisions that have legal or similarly significant effects on you.

We do not currently make decisions based solely on automated processing that produce legal or similarly significant effects without human involvement. Where automated tools are used to support decisions, they assist our staff and do not replace human judgement. If this changes, we will give you meaningful information about how the processing works, why it matters, the likely impact on you and the safeguards available to you, including the right to ask for human intervention, give your point of view and challenge the decision.

We operate governance, testing and oversight processes for AI-assisted tools, including review of accuracy, security, fairness, reliability and compliance requirements before and during deployment.

We may also use personal data, where necessary and proportionate, to test, monitor and improve these tools. This helps us check that they are working accurately, fairly and securely. We use approved systems, restrict access to personal data, monitor performance, apply staff oversight and use anonymised, aggregated or minimised data where appropriate. We do not use your personal data to train public AI models.

International Transfers

Information you provide to us is stored on secure servers in the UK. Some personal data may also be transferred to, or processed in, countries outside the UK. Simplify India and TeamLease may access and process personal data where they provide operational and support services in connection with the Portal. We also use trusted third-party technology providers, including AI, communication, anti-money laundering, identity verification, bank or funding validation, indemnity, security and support providers, that may store or process personal data outside the UK. Examples of countries where personal data may be processed include India, the United States and Canada. Where personal data is transferred outside the UK, we use an appropriate legal safeguard, such as adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to Standard Contractual Clauses or another lawful transfer mechanism. We take appropriate steps to ensure your information is treated securely and in line with this Privacy Notice.

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.

If you require further information about where your personal data is transferred to, including where processing involves international transfers, and the measures we have implemented to safeguard that information, please contact our Data Protection Officer by emailing DataProtection1@simplify.co.uk.

Credit Reference Agencies

In order to provide the Portal and related services, and to support identity verification, proof of funds, source of funds, customer due diligence, fraud prevention and transaction information requirements requested by or relevant to Trusted Third Parties, we may perform identity checks through credit reference agencies. To do this, we will supply your personal data to the credit reference agency, and they will give us information about you. The credit reference agencies may check your details against databases they can access, including public databases, and may use your details in the future to help other companies verify identity. A record of the search will be kept by us, the relevant Trusted Third Party where applicable, and the credit reference agency. This does not affect your credit score, and lenders cannot see it. Further details of how your information will be used by us, and the credit reference agencies can be obtained by emailing Dataprotection1@simplify.co.uk.

Direct Marketing Communications

If you have chosen to opt-in to our direct marketing communications, we will use your information to tell you about products and services available from us which may be of interest to you. We may also use your information to tell you about products and services we can introduce from selected businesses.

You have a right to opt-out of our direct marketing communications at any time. You can opt-out by following the Unsubscribe instructions at the bottom of the communication or by emailing Dataprotection1@simplify.co.uk.

What if I am aged 18 or under?

You must be 18 years or older to use the Portal and related services. Individuals under 18 are unable to purchase a property in the United Kingdom and must not use the Portal or provide personal information through it unless we expressly permit this and appropriate consent or authority is in place.

Data Security

We use technical and organisational measures to protect personal data from unauthorised access, loss or misuse. These include access controls, encryption, monitoring systems, data loss prevention tools, security event monitoring, threat detection, alert review and other controls designed to detect and prevent unauthorised access or transmission of data.

We may review communications, system logs, file access records, user activity information and other relevant information as part of cyber-security monitoring, incident response, fraud investigations, forensic analysis or personal data breach investigations.

We may create secure backup copies of information and restore data where necessary to maintain business continuity, system resilience and disaster recovery capabilities.

Links to Websites of Other Providers/Third Parties

Please note that this data privacy policy only applies to us, and we are not responsible for, and have no control over, information that is submitted to or collected by third parties, such as those where the Portal may provide links and banner advertisements to third-party sites. Since we do not control those websites, you are responsible for reviewing and abiding by the privacy policies of these third-party sites to ensure they comply with the applicable data protection regulations.

Website Analytics and Cookies

You can visit the Portal or our website without giving us personal information directly. We may use essential cookies to operate the Portal or website and analytics cookies, such as Google Analytics where used, to understand how the Portal or website is used, improve user experience and monitor service performance. The information collected is mainly anonymous traffic data, such as browser information, device information, language and approximate location based on IP address. Where required, we will ask for your consent before using non-essential cookies. You can manage or withdraw your cookie consent through the cookie settings available on the Portal or website or through your browser settings. Please refer to our cookie policy for more information about cookies, what they are used for and your rights to object to them.

How long we'll keep your information

Where possible, we will take steps to erase any personal data that is no longer necessary for the purposes for which it is collected or otherwise processed, or if you have withdrawn consent for its processing and retention.

The following criteria are used to determine data retention periods for your personal data:

Retention in accordance with legal, regulatory, audit and business requirements: We will retain your personal data where required for legal, regulatory, audit, fraud prevention, complaint handling, dispute management, security, operational or business administration purposes.

Retention in case of claims: We will retain your personal data for as long as you may bring a legal claim.

Retention in case of queries: We will retain your personal data for as long as we are legally able to do so to enable us to deal with any queries relating to the Portal, the services provided through it, or information shared with relevant Trusted Third Parties.

Data retention for AI

Personal data used to operate, test, monitor or improve AI-assisted tools is kept only for as long as needed for the relevant purpose. AI-generated metadata, inference records, monitoring logs, system records, incident logs and governance records are normally retained for limited periods to support security, audit, quality assurance, compliance monitoring and incident investigation. After that, they are securely deleted, aggregated or anonymised where appropriate. Information that can no longer identify you may be kept for longer to help evidence testing, support audit activity, maintain security and improve system performance. We use anonymised, aggregated or minimised data where appropriate.

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.

Protecting Your Privacy

To protect the personal data collected from you by us against accidental or deliberate manipulation, loss, destruction, or the access of unauthorised persons, technical and organisational security measures are constantly improved as part of our technological development. In addition, our employees, subcontractors, and other support staff are obligated to observe confidentiality and data privacy.

Any access to your data that is stored at our company only takes place through an encrypted connection. Our website, internal systems and external portals are encrypted using an SSL/TLS connection. SSL/TLS is an industry standard and is used by many websites to help protect online transactions and communications.

Wherever possible, we have tried to create a secure and reliable website for our users. However, you recognise that your use of the Internet and our website is entirely at your own risk, and we have no responsibility or liability for the security of personal information transmitted via the Internet. All passwords and usernames allocated to you must be kept secret and must not be disclosed to anyone without our prior written authorisation. You must not use any false identity or email, or other network communications and you must not attempt or participate in the unauthorised entry or viewing of another user's account or into another system.

It is your responsibility to ensure that your computer is virus protected. We accept no responsibility for any loss you may suffer as a result of accessing and downloading information from this portal.

You must not use the services and/or network systems or any part thereof for fraudulent activities, or to breach another organization's security (cross-network hacking). You must not use any computer, computer equipment, network resources, or any services provided by us for any illegal

purpose, or for accessing, receiving, or transmitting any material deemed illegal, indecent, offensive, or otherwise unacceptable under UK Law.

We will monitor network traffic from time to time for the purposes of backup and problem-solving and to ensure that you are not misusing any of the services provided to you.

Your Rights Under Applicable Data Protection Law

- The right to be informed about how we are processing your personal data.
- The right to have your personal data corrected if it is inaccurate and to have incomplete personal data completed.
- The right to object to the processing of your personal data.
- The right to restrict processing of your personal data.
- The right to have your personal data erased.
- The right to request access to your personal data and information about how we process it.
- The right to move, copy, transfer your personal data ("data portability"). Rights in relation to automated decision-making including profiling. Where a decision produces legal or similarly significant effects for you and is based solely on automated processing, you have the right to:

    i. Obtain meaningful information about the logic involved
    ii. Request human intervention and to express your point of view
    iii. Challenge the decision

You may also ask for further information about our use of profiling, AI and automated processing where applicable.

Where we process your personal data based on legitimate interests, including where we receive or exchange information with Trusted Third Parties, you have the right to object at any time. We will consider any objection carefully and stop the processing unless we have compelling legitimate grounds to continue or the processing is needed for legal claims.

If you would like to exercise any of the above rights, please contact our Data Protection Officer in writing:

Data Protection Officer

Simplify Moving Limited

1 Frances Way

Grove Park

Leicester

LE19 1SH

Dataprotection1@simplify.co.uk

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:

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

If you remain dissatisfied with our handling of your complaint, you may contact the Information Commissioner's Office (ICO) directly and 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.

Data Anonymisation and aggregation

Your personal data may be converted into statistical or aggregated data which cannot be used to identify you, then used to produce statistical research and reports. This aggregated data may be shared and used in all the ways described above.

Group Companies

For more information on the Simplify group companies, please contact Dataprotection1@simplify.co.uk.

Changes to the Privacy Policy

This policy will be reviewed and may change from time to time as a result of further development of the portal, changes to legislation, or the implementation of new technologies. We reserve the right to change this data protection information at any time with effect for the future. The revised policy will be posted on this page so that you are always aware of the information we collect, how we use it, and under what circumstances we disclose it. We, therefore, recommend you read the current data protection information again from time to time.

Last updated: July 2026

Date of Next Review: July 2027