DATA PRIVACY PROTECTION POLICY

GDPR, Irish Data Protection and FIDI FAIM aligned

Protecting the confidentiality, integrity and availability of personal information entrusted to AMC Removals & Storage.

Document Control

Document title	Data Privacy Protection Policy	**Version**	4.0
Document owner	Director of Operations / Data Protection Lead	**Approved by**	Managing Director
Effective date	01.08.2026	**Review frequency**	Annually
Applies to	All AMC personnel, contractors and relevant service providers	**Classification**	Internal / Controlled
Reference framework	EU GDPR; Data Protection Act 2018; FIDI FAIM Quality Standard	**Related records**	Retention schedule; breach register; processing records

1. Purpose

AMC Removals & Storage is committed to protecting the privacy, confidentiality and security of personal information entrusted to us. This policy defines how personal data is collected, used, shared, retained, transferred and securely disposed of in connection with our moving, packing, storage, commercial relocation and related services.

The policy is designed to support compliance with the EU General Data Protection Regulation (GDPR), the Irish Data Protection Act 2018 and the data-protection and risk-management expectations of the FIDI FAIM Quality Standard.

2. Scope

This policy applies to personal data relating to customers, prospective customers, transferees, employees, job applicants, suppliers, contractors, overseas agents, business partners, visitors and other individuals whose information AMC processes.

It applies to all directors, employees, temporary staff, casual staff, contractors and any third party acting on AMC's behalf, and to information held electronically, on paper, in photographs, audio recordings, video recordings or any other structured format.

3. Policy Principles

- Lawfulness, fairness and transparency - personal data will be processed fairly, openly and on a valid legal basis.
- Purpose limitation - information will be collected for specified, explicit and legitimate purposes and will not be used incompatibly with those purposes.
- Data minimisation - AMC will collect only the information reasonably required to provide services, meet legal obligations and operate the business.
- Accuracy - reasonable steps will be taken to keep personal data accurate and up to date.

- Storage limitation - personal data will not be kept longer than required by the applicable retention schedule or legal obligations.
- Integrity and confidentiality - appropriate technical and organisational safeguards will protect personal data against unauthorised or unlawful processing, accidental loss, destruction or damage.
- Accountability - AMC will maintain records and evidence demonstrating how data-protection responsibilities are managed.

4. Governance and Responsibilities

4.1 Management

Senior management is responsible for ensuring that appropriate resources, controls and oversight are in place. A nominated Data Protection Lead oversees implementation of this policy, coordinates privacy enquiries, supports breach assessment and maintains relevant compliance records.

4.2 Employees and Contractors

All personnel must protect personal information, follow approved procedures, access data only where necessary for their role, and report any suspected loss, disclosure, misuse or security incident immediately. Confidentiality obligations continue after employment or engagement ends.

4.3 Managers

Managers must ensure staff receive appropriate induction and refresher training, that access rights remain suitable, and that corrective action is taken where procedures are not followed.

5. Information AMC May Process

Depending on the service provided, AMC may process the following categories of personal data:

- Identity and contact details, including names, addresses, telephone numbers and email addresses.
- Move and service information, including collection and delivery addresses, inventories, access details, survey notes, photographs and special handling requirements.
- International move and customs information, including passport or identification details, visa or residency documents, customs declarations and shipment documentation where required.
- Financial and transaction information, including invoices, payment status and limited payment information required to process a transaction.
- Communications, customer feedback, complaints, claims and service records.
- Employee and applicant information, including employment, payroll, attendance, training, licence, safety and performance records.
- Supplier, contractor and partner contact, contractual and compliance information.
- CCTV, access-control and visitor information where used for security and operational purposes.

6. Lawful Bases and Consent

AMC will identify an appropriate lawful basis before processing personal data. Depending on the activity, this may include:

- Performance of a contract or steps requested before entering into a contract, such as preparing a quotation or carrying out a move.
- Compliance with a legal obligation, including tax, employment, customs, safety, insurance and record-keeping requirements.
- Legitimate interests, where processing is necessary for proportionate business, security, quality, claims-management or customer-service purposes and does not override individual rights.
- Consent, where consent is the appropriate basis, including certain optional communications or uses of information.
- Vital interests or public-interest grounds in exceptional circumstances permitted by law.

Consent will not be treated as the default basis for all processing. Where AMC relies on consent, it must be freely given, specific, informed and unambiguous, and individuals may withdraw it without affecting processing already lawfully carried out.

7. Privacy Information and Transparency

AMC will provide clear and accessible privacy information explaining what information is collected, why it is needed, the lawful basis, intended recipients, relevant international transfers, retention arrangements, individual rights and how to contact AMC. Privacy information may be provided through quotations, terms and conditions, forms, the website, employee documentation or other suitable notices.

8. Collection and Use

Personal data must be collected by fair and lawful means and used only for defined business or legal purposes. Staff must not collect information merely because it may be useful in future. Material changes in use must be assessed and, where required, communicated to the individual before the new processing begins.

9. Sharing and Third-Party Service Providers

AMC may share the minimum necessary personal data with trusted third parties where required to provide services, administer the business or comply with law. Recipients may include:

- FIDI affiliates, overseas destination or origin agents, removal partners and approved subcontractors.
- Shipping lines, airlines, freight forwarders, port or terminal operators, customs brokers and customs or border authorities.
- Insurers, claims handlers, professional advisers and legal representatives.
- IT, software, communications, payment, payroll, document-storage and secure-destruction providers.
- Revenue Commissioners, regulatory authorities, law-enforcement bodies or courts where disclosure is legally required.

Third parties receiving personal data on AMC's behalf must be subject to appropriate contractual, confidentiality, security and data-protection obligations. AMC will review relevant providers based on the nature and risk of the service.

10. International Data Transfers

International relocations may require customer information to be transferred outside the European Economic Area to overseas agents, transport providers, customs authorities or other parties involved in the move. AMC will limit such transfers to information necessary to complete the service and will use an appropriate transfer mechanism or lawful derogation where required by GDPR.

Where relevant, safeguards may include an adequacy decision, approved contractual clauses, binding rules or a transfer that is necessary to perform the customer's contract. The chosen mechanism and any material transfer risk should be documented.

11. Retention and Secure Disposal

Personal data will be retained only for as long as required for the purpose collected, to meet contractual, tax, employment, customs, insurance, claims or other legal obligations, or to establish and defend legal rights. Retention periods must be set out in AMC's Data Retention Schedule and reviewed periodically.

- Paper records must be securely shredded or destroyed through an approved confidential-waste provider.
- Electronic records must be securely deleted, anonymised or rendered inaccessible when no longer required.
- Payment card details must not be copied or retained unnecessarily and must be securely destroyed once processing is complete, subject to the approved payment process.
- Legal holds, complaints, claims, audits or investigations may require relevant records to be preserved beyond the normal retention period.

12. Information Security

AMC will apply proportionate technical and organisational measures based on the sensitivity and risk of the information. Measures may include:

- Role-based access, strong passwords and multi-factor authentication where available.
- Up-to-date endpoint protection, patching, backups, firewalls and secure configuration.
- Encryption or other secure transfer methods where appropriate to the risk.
- Locked offices, cabinets and controlled warehouse or records access.
- Clear-desk and clear-screen practices and secure printing or disposal.
- Verification of recipients before sending personal or confidential information.
- Prompt removal or adjustment of access when roles change or employment ends.
- Staff awareness training covering phishing, social engineering, device security and incident reporting.

Confidential information must not be provided to a subcontractor, supplier or agent beyond what is reasonably required to carry out the agreed service.

13. Individual Rights

Subject to applicable conditions and exemptions, individuals may have the right to:

- Be informed about processing of their personal data.
- Request access to their personal data and related processing information.
- Request correction of inaccurate or incomplete information.
- Request erasure where the legal conditions are met.
- Request restriction of processing in certain circumstances.
- Receive data in a portable format where the right applies.
- Object to processing based on legitimate interests and object at any time to direct marketing.
- Withdraw consent where processing relies on consent.
- Request human review of certain solely automated decisions, where applicable.
- Lodge a complaint with the Irish Data Protection Commission.

Requests must be forwarded immediately to the Data Protection Lead. Identity may be verified before information is released. AMC will respond within the statutory timeframe and will document any lawful extension, refusal or restriction.

14. Data Protection by Design and Risk Assessment

Privacy and security must be considered when introducing new systems, services, forms, suppliers or processing activities. Where processing is likely to create a high risk to individuals, AMC will assess whether a Data Protection Impact Assessment is required and implement appropriate risk controls before proceeding.

15. Personal Data Breach Management

A personal data breach includes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Examples include sending information to the wrong person, lost paperwork or devices, compromised email accounts, unauthorised system access, malware, insecure disposal or inappropriate verbal disclosure.

15.1 Immediate Reporting

Any actual or suspected breach must be reported immediately to the Director of Operations / Data Protection Lead by the fastest available method. Staff must not delay reporting while attempting to investigate or resolve the matter themselves.

15.2 Response Procedure

1. Contain the incident and protect affected systems, records and individuals.
2. Preserve relevant evidence and establish what happened, when, and which information and individuals may be affected.
3. Record the incident in the breach register, including decisions and risk assessment.
4. Assess the likelihood and severity of risk to the rights and freedoms of individuals.
5. Notify the Data Protection Commission without undue delay and, where feasible, within 72 hours of awareness where the breach is likely to result in a risk.
6. Inform affected individuals without undue delay where the breach is likely to result in a high risk, unless a lawful exception applies.
7. Implement corrective and preventive action and review whether procedures, training, supplier controls or security measures require improvement.

All breaches must be recorded, including incidents that are assessed as not requiring notification. The reasons for notification or non-notification must be documented.

16. Day-to-Day Data Protection Procedure

- Only access or share personal data where required for an authorised business purpose.
- Check email addresses, attachments and recipients before sending information.
- Use approved email, secure portals, tracked courier or other authorised channels appropriate to the sensitivity of the information.
- Keep hard-copy customer and employee records in secure cabinets or controlled office areas when not in use.
- Do not leave files, inventories, customs documents or contact details unattended in vehicles or public areas.
- Do not use personal email, unapproved cloud storage or messaging applications for company records unless expressly authorised.
- Destroy temporary notes and duplicate copies securely once no longer required.
- Report lost documents, misdirected emails, suspicious messages, compromised accounts or unauthorised access immediately.

17. Data Processing Overview

Source	Typical information	Main purpose	Typical recipients
Customers / transferees	Contact details, inventory, addresses, move and customs records, communications	Quotation, contract, move delivery, claims and customer service	Agents, transport and customs providers, insurers, authorities
Employees / applicants	Personnel, payroll, attendance, licence, training and safety records	Employment administration, payroll, legal and safety obligations	Revenue, payroll providers, advisers and authorities
Agents / contractors	Contact, booking, shipment, compliance and service information	Service coordination, supplier management and payment	Customers where necessary, finance, professional advisers
Website / enquiries	Contact details, enquiry content and technical records	Responding to enquiries, website operation and security	Approved website, IT and communications providers

18. Staff Training and Awareness

Data-protection responsibilities will be communicated through induction, the employee handbook, relevant policies, workplace notices, manager briefings and refresher training. Training will be proportionate to role and risk, and completion records will be retained.

Staff handling customer move files, customs documentation, payroll, recruitment, claims, IT administration or overseas-agent communications may receive additional role-specific guidance.

19. Monitoring, Audit and Enforcement

AMC will monitor implementation of this policy through management review, internal checks, incident and complaint analysis, access reviews, supplier review, training records and internal or external audits. Non-compliance may result in corrective action, retraining, restriction of access, disciplinary action or termination of a contract, as appropriate.

Corrective and preventive actions will be recorded and followed through to completion in line with AMC's quality management arrangements.

20. Review of Third Parties

Before appointing a service provider that will process personal data, AMC will consider the nature of the information, the service provider's security and privacy arrangements, location of processing, subcontracting, breach-reporting arrangements, deletion or return of information, and contractual protections. Reviews will be proportionate to risk and repeated when services materially change.

21. Policy Review

This policy will be reviewed at least annually and sooner where necessary following:

- Changes to data-protection law, regulatory guidance or FIDI FAIM requirements.
- A material personal data breach, complaint, audit finding or identified control weakness.
- Introduction of a significant new system, supplier, service or international data flow.
- Changes to AMC's organisational structure, responsibilities or business operations.

Approved changes will be communicated to relevant personnel and supported by updated training or procedures where required.

22. Contact and Complaints

Questions, rights requests, privacy concerns or suspected breaches should be directed to AMC's Director of Operations / Data Protection Lead using the company's published contact details. Individuals also have the right to raise a concern with the Irish Data Protection Commission.

Policy Approval

Approved by	Aubrey McCarthy	**Role**	Managing Director
Signature		**Date**	01.08.2026
Next review	31.07.2027	**Version**	4.0

Reference Note

This policy is an operational management document and should be used with AMC's privacy notice, records of processing, retention schedule, information-security procedures, supplier agreements and breach-response records. It is designed to support, but does not replace, specialist legal advice where required.