



Effective Date: February 13, 2026

Associate Data Privacy Notice

Who We Are and How to Contact Us

Unless a local supplement says otherwise, Americold Logistics LLC and relevant local affiliates (“**Americold**”) determine the means and purposes of processing your personal data.

All questions and concerns relating to this notice should be directed to privacy@americold.com.

You may also contact your local HR team or submit a report via the Americold Ethics Helpline: <http://americoldethicshelpline.com> (online or by phone, with anonymous reporting available).

What This Notice Covers

This Notice explains:

- What personal data we collect about you
- How and why we use it.
- Who we might share it with.
- How long we keep it.
- The rights available to you.

This Notice does not form part of any employment contract and may be updated from time to time. If we make material changes, we will notify you in advance.

What Personal Data We Process

Depending on your role and location, Americold may process the following types of personal data, subject to applicable local law:

- **Identification and contact details** (e.g., name, photograph, employee ID, contact details, national ID number where required)
- **Personal background information** (e.g., date and place of birth, nationality, marital status)
- **Financial and payroll information** (e.g., bank details, tax information, compensation and benefits)
- **Emergency contact details**
- **Employment and education records** (e.g., work history, qualifications, references)
- **Performance and conduct records** (e.g., evaluations, training records, grievances or disciplinary actions)
- **Attendance and leave information** (e.g., working hours, vacation, sickness or other leave)

- **Organizational information** (e.g., job title, department, work location, seniority)
- **IT and systems data** (e.g., user IDs, access rights, usage logs)
- **Recorded communications**, where applicable and lawful (e.g., recorded training sessions or meetings)
- **Information you choose to provide voluntarily.**

Why We Use Your Data and Primary Legal Bases

We use your personal data for the purposes below and rely on one or more legal bases under applicable law.

Purpose	Examples	Primary Legal Bases
<u>Recruitment & Onboarding</u>	Process applications, conduct interviews, offers, pre-employment checks, provisioning accounts	Necessary for the performance of a contract; Legitimate interests
<u>Employment Administration</u>	HR records, organizational charts, scheduling, time & attendance, leave management	Necessary for the performance of a contract; Legal obligation relating to labor or tax law
<u>Payroll & Benefits</u>	Payroll, tax reporting, pensions, insurance, expenses	Necessary for the performance of a contract; Legal obligation relating to labor or tax law
<u>Performance, Development & Talent</u>	Reviews, coaching, promotion/succession, training	Legitimate interests relating to business operations & workforce planning
<u>Health, Safety & Wellbeing</u>	Occupational health, incident management and necessary accommodations	Legal obligation relating to health & safety law; Vital interests of the data subject
<u>IT, Security & Monitoring</u>	Access control, threat detection, fraud/misuse, asset protection	Legitimate interests; Legal obligations relating to information security, labor law and regulatory compliance
<u>Compliance & Investigations</u>	Respond to regulators/courts, internal investigations and whistleblowing	Legal obligations relating to financial crime, whistleblower protection, and regulatory compliance
<u>Communications & Collaboration</u>	Emails, Teams, internal directories and communications	Legitimate interests
<u>Corporate Transactions</u>	M&A, restructuring, outsourcing/insourcing	Legitimate interests

Legitimate Interests: Where we rely on legitimate interests, we assess whether our interests are balanced against your rights and freedoms. You have the right to object to this processing (see **Your Rights** below).

Special Category Data: (e.g., health or biometric data) is processed only where permitted by law and with additional safeguards.

Criminal Convictions or Offences Data: processed only where authorized by law and subject to increased protections.

Who We Share Your Data With

We share personal data on a need-to-know basis for the purposes mentioned above with:

- Other Americold entities for internal business purposes,
- Service providers (e.g., HR systems, payroll, IT and security vendors) acting on our instructions and bound by contractual safeguards,
- Financial, insurance, and pension institutions where needed for benefits administration,
- Professional advisors and auditors,
- Public authorities or courts where legally required,
- Prospective counterparties in corporate transactions, subject to confidentiality.

We do not sell your personal data.

International Data Transfers

Because Americold operates globally, your data may be transferred to countries outside your home country, including the United States. Where required, we use appropriate safeguards, such as:

- Adequacy decisions (where applicable),
- EU/UK Standard Contractual Clauses, and
- Additional technical and organizational measures (e.g., encryption and access controls).

You may request further information about these safeguards by contacting privacy@americold.com.

Use of Artificial Intelligence, Automated Decision Making and Profiling

Americold uses certain AI-assisted tools to support business activities.

What this means for you:

- We do not use fully automated decision making for hiring, termination, or disciplinary decisions.
- We do not make solely automated decisions that produce legal or similarly significant effects without:
 - Notifying you in advance,
 - Explaining the role and logic of the automation, and
 - Providing human review and the opportunity to express your view and contest the outcome.

- We inform associates when AI is meaningfully involved in a process affecting them.
- Only data necessary for the defined purpose is used, and sensitive data is excluded unless legally required.

If you have questions or concerns about AI use, contact privacy@americold.com or your local HR representative.

Workplace Monitoring

Where permitted by law, Americold may conduct proportionate monitoring for specific purposes such as security, regulatory compliance, and incident investigation.

This may include:

- Access badges and physical security systems,
- CCTV in public or secured areas,
- IT and network security logs, and
- Limited review of communications content where necessary and lawful.

We prioritize targeted methods, apply access controls and audit logs, consult worker representatives where required, and provide advance transparency (e.g., policies and signage). Covert monitoring is not carried out except in very limited circumstances where legally permitted.

How Long We Keep Your Data

We retain personal data only for as long as necessary for the purposes described above and to meet legal, tax, or regulatory requirements. Retention periods depend on the type of data and typically extend for the duration of employment and a limited period afterward.

Legal holds may require us to retain data longer until the hold is lifted. Further details are available in the Global Records Management Policy.

Your Rights

Depending on your location, you may have the right to:

- Access your personal data.
- Correct inaccurate or incomplete data.
- Request deletion in certain circumstances.
- Restrict processing in limited cases.
- Receive a copy of certain data in a portable format.
- Object to processing based on legitimate interests or to direct marketing.
- Withdraw consent where processing is based on consent.
- Obtain human review of certain automated decisions.

You can also lodge a complaint with a supervisory authority, such as:

- EU/EEA: Your local authority or the [Autoriteit Persoonsgegevens](#) [our Lead Supervisory Authority]; and
- UK: [Information Commissioner's Office](#) (ICO).

To exercise your rights, contact privacy@americold.com. We may need to verify your identity and will respond within applicable legal timeframes.

Security Measures

We use technical and organizational measures as deemed appropriate to mitigate risk, including access controls, encryption where appropriate, network and physical security, vendor oversight, training, and incident response processes.

Updates and Questions

We may update this Notice from time to time. The most current version is available on the Compliance SharePoint. Material changes will be communicated in advance.

If you have questions about this Notice or how we handle your personal data, contact: privacy@americold.com or use the [Americold Ethics Helpline](#).