	**Data Privacy and Protection Policy**
Owned by: Director of Compliance	Approved by: Executive Management
Effective Date: August 2, 2021	Revision Date: April 15, 2024

I. Purpose:

Americold's (or, "**the Company**") Data Privacy and Protection Policy outlines our commitment to treat the Personal Information of associates, customers, vendors, stakeholders, and other interested Data Subjects (collectively, "**Data Subjects**") with the utmost care and confidentiality.

For the purposes of this policy, "**Personal Information**" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal Information includes information referred to as "personal data", "personal information", "personally identifiable information" and such similar references as codified in applicable data protection laws.

II. Scope:

All Americold associates, including the associates of Americold's subsidiaries, must follow this policy.

III. Policy and Principles:

As part of our regular operations, Americold obtains and processes Personal Information of various Data Subjects including associates, vendors and customers, advisors and others.

The Company collects, uses, retains and discloses this Personal Information in accordance with the following principles:

Americold will have processes in place that are designed to ensure that Personal Information is:

- Processed lawfully, fairly and in a transparent manner. Where there is likely to be a high risk to Data Subjects' rights and freedoms due to a processing activity, the Company will first undertake a Data Protection Impact Assessment prior to processing;
- Accurate and kept up-to-date;
- Protected against unauthorized or illegal access, use or disclosure by internal and

external Data Subjects and and against accidental loss, destruction or damage;

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The purpose for which Personal Information is processed shall be recorded by the Company.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, and;
- Kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Information are processed.
- Only transferred to organizations, states or countries that have adequate data protection controls in place;
- Only disclosed to third Data Subjects: (i) who are Americold's service providers, or; (ii) with a Party's written consent (exempting legitimate requests from law enforcement authorities); and
- Subject to data protection practices (i.e., secure destruction, secure storage, regular backups, and access control.)

Refer to Appendix A for the procedures and controls in place for processing HR related data in Europe.

IV. Rights of Data Subjects

Data Subjects are granted various rights under data protection laws enacted around the world. While all data protection laws are not identical, the rights afforded to Data Subjects tend to be similar. Americold complies with data protection laws and recognizes Data Subject rights, as applicable. Those rights may include:

- The right to be informed in clear and transparent language about how Americold uses Personal Information;
- The right to have access to the Personal Information Americold holds about them;
- The right to receive and transfer the Personal Information in a common and machine-readable electronic format;
- The right to have one's Personal Information erased;
- The right to have one's Personal Information corrected when it is inaccurate or incomplete;
- The right to object to the processing of one's Personal Information;
- The right to limit the extent of the processing of one's Personal Information; and
- The right not to be subject to decisions made without human involvement.

V. Exceptions

Requests for exceptions to these Policy commitments must be submitted in writing to the Director of Compliance or Chief Legal Officer for review and approval.

VI. Compliance and Enforcement

This policy and the Company's associated processes will be reviewed on at least an annual

basis by the Director of Compliance, and updated as appropriate. The Director of Compliance is responsible for overseeing implementation and compliance with the policy.

All associates who will be handling Personal Information on behalf of the Company will be appropriately trained, supervised where necessary and bound by obligations of confidentiality. Non-compliance with this policy is cause for disciplinary actions up to and including termination for cause to the extent permissible under local law. Americold will take appropriate steps to ensure consultants, business partners, vendors, or other parties who will be handling Personal Information on behalf of the Company provide required assurances regarding the proper handling of Personal Information, including training and supervision.

VII. Contact Details

The Compliance Department at corporate.compliance@americold.com or privacy@americold.com

VIII. Supplemental Materials

Americold's *Associate Data Protection Notice*

Americold's *Code of Business Conduct and Ethics*

Americold's *Encryption Policy*

Americold's *Information Security Policy*

Americold's *Records Management Policy*

Document Control: Use the following table to enter the revision history including a brief summary of any changes to the policy.

Revision History			
Revision No.	**Revision Date**	**Summary of Changes**	**Author**
1	1/26/2023	Added Appendix A covering HR related data	Jeff Hecker

APPENDIX A

PROCCESSES AND PROCEDURES FOR EUROPEAN HR RELATED DATA

EUROPE HR DATA POLICY
(including IT and Accounting department)

1. INTRODUCTION

1.1 This Policy sets out the Data Protection Principles which Americold must comply with when processing personal data, including its collection, use, disclosure and deletion.

1.2 This Policy contains further information on how to ensure compliance with our *Data Privacy and Protection Policy*, *Associate Data Privacy Notice*, and *Global Records Management Policy* when processing Personal Data by or on behalf of Americold in the context of **employment and Talent Acquisition** ("**HR data**"). This includes the personal data of Americold associates as well as our external workforce (e.g. consultants, contractors, temporary agency workers, students, etc.) and beneficiaries / dependents of current and former associates.

1.3 This Policy provides examples and guidance for common data protection issues when handling HR data. It is divided into the following sections:

- Processing HR Data for Talent Acquisition
- Processing HR Data within Americold
- Sharing HR Data outside Americold

1.4 This Policy applies to all associates who process HR Data.

2. TALENT ACQUISITION

2.1 ADVERTISING VACANCIES

All job vacancies, wherever possible, should be advertised via approved job sites or the "Careers" section of Americold's website.

However, there may be occasions when a vacancy is advertised via other methods, e.g. via third party recruitment websites or hard copy application forms. In these circumstances, you should make sure that the job advertisement identifies the Americold entity which will be the employer. If for a particular reason the relevant Americold entity will not be identified in the advertisement, applicants must be notified of the identity of the employer within a reasonable time of receipt of their application.

2.2 APPLICATION FORMS

2.2.1. Giving Notice

When collecting HR Data, applicants should be properly **informed** about how their personal data will be used (for example, this may be provided via the iCIMS online applicant tracking system). If for some reason the notice cannot be provided at the outset, it must be provided to the applicant as soon as possible thereafter.

2.2.2 Applications received via a third party

Where the HR Data is obtained from a third party (e.g. a recruitment agency), Americold should provide the applicant with the information how their personal data shall be used within a reasonable period of time after receiving the personal data, and at least: (a) at the time of Americold's first direct contact with the applicant; or (b) within one month after receiving the HR Data, whichever is earlier.

2.3 DECIDING WHAT HR DATA TO COLLECT

2.3.1 Americold should only collect personal data for Talent Acquisition purposes which are adequate, relevant and not excessive. These same principles apply if you collect HR Data via any other means. This means you should only collect information which is **necessary to assess** the individual for the role they are applying for. Individuals may **voluntarily** provide information which is not necessary, but wherever possible you should limit this (for example, by providing a list of options instead of free text fields).

2.3.2 Information about criminal convictions (spent and unspent) and sensitive personal data must not be collected from the individual unless Company is legally permitted to do so. Contact Americold's Legal or Compliance Departments if you are unsure.

2.3.3 You should only collect sensitive personal data where it is absolutely necessary to do so, and only at the latest possible stage in the Talent Acquisition process.

3. SELECTING AND SHORTLISTING CANDIDATES

3.1 BACKGROUND CHECKING

3.1.1 "Background Checking" is the process whereby Americold verifies HR Data provided during the Talent Acquisition process, for example by checking academic qualifications and/or by collecting information from external sources such as former employers. Data Subjects (Individuals) must be informed by Americold that they will be subject to Background Checking. In some cases, it will also be necessary to obtain the individual's consent before contacting the party who will be verifying the information.

3.1.2 If Background Checking is to be carried out, the following steps must be followed:

- Provide notice to individuals in advance that Background Checking will take place.

- Information about criminal convictions (if collected) must only be collected through authorized sources and where legally permitted (contact Americold's Legal or Compliance Departments if you are unsure), including where the applicant has given their explicit, informed consent and the information can be justified for the specific role offered.

- Only contact third-party sources where the individual has first given their consent if consent is required by the third-party source.

- Applicants should be informed if Background Checking reveals any discrepancies which may have a negative impact on their application. Applicants should be given an opportunity to explain these discrepancies.

Any Background Checking should also:

- Be carried out ***only*** where it is genuinely necessary. It may not be proportionate or necessary to carry out Background Checking where an individual is applying for an administrative role with no access to sensitive or confidential information, whereas such Background Checking may be appropriate for roles with access to financial and business sensitive information; and

- be targeted at the collection of specific and not general information.

3.2 INTERVIEWING CANDIDATES

During the interview process only collect information that is relevant for the job that the candidate is applying for. Remember that the individual is entitled to request a copy of their personal data which may be contained within any notes of the interview, including handwritten notes.

3.3 ACCESS TO HR DATA OBTAINED DURING THE TALENT ACQUISITION PROCESS

Access to documents obtained during the Talent Acquisition Process, such as CVs, Covering Letters and the results of any assessments or tests should be limited to a 'need-to-know' basis within Americold. Who has a 'need-to-know' will be determined depending on the role the Individual is applying for and who within the HR team is managing the application process. In most cases, it should be limited to Americold associates involved in the interviewing and assessment process and those Americold associates who need access in order to administer the Individual's application. If the Individual in question is subsequently hired then the information obtained during the

Talent Acquisition process may be placed on their Employees File, in which case those with a 'need-to-know' may become broader and extend to the Individual's manager(s). For more guidance on who will have a 'need-to-know' see further guidance in the box below.

Such documents shall be stored securely with access controls (for example, a username and password authentication) and/or kept in a locked filing cabinet.) The access controls and security measures referred to above should be applied whether the candidate is internal or external.

Which Americold associates will have a 'Need-to-Know'?

The concept of 'Need-to-Know' is used to determine which Americold associates need to have access to which categories of HR Data. It is a concept used to decide the access controls and security which should be in place. This is important because data protection legislation requires there to be appropriate security applied to personal data. In an HR context this is particularly important as much of the data will be sensitive personal data.

It is difficult to be prescriptive. Those with a 'need-to-know' should be assessed depending on the category of HR Data in question. Generally, it will be Americold associates who need to access the information in order to achieve a business need which has been identified and in order to administer the employee relationship.

When deciding who within Company has a 'need-to-know' consider the following in relation to the relevant category of HR Data:

- **Identify Management and Responsibility** – Americold associates with management roles or responsibility are more likely to have a 'need-to-know' for HR Data relating to associates they have management or responsibility for.
- **Identify the Business Need or Purpose for the HR Data** – Consider what the purpose of collecting the HR Data is and who needs to have access in order to ensure that purpose or business need is fulfilled. For example, where an Individual applies for a job then those with a 'need-to-know' would be the members of the Talent Acquisition Team who are handling the application. For example, the members of the HR team who are doing a first-round review of the applications or collating applications to be reviewed. The Americold associates involved in the recruitment process will also have a 'need-to-know' as they will not be able to assess the candidates without having certain information about the Individual. Another example, would be in the context of payroll. The payroll department will have a 'need-to-know' for certain categories of HR Data, for example, salary and personal bank account details so that they can ensure Americold Associates receive their salary into the right account. The IT department will need to receive at least some Personal data to create e-mail accounts, user login data to the PC.

4. RETAINING TALENT ACQUISITION DOCUMENT

Talent Acquisition documents (e.g., written applications, CVs, interview notes) must be handled in accordance with Americold's ***Global Records Management Policy*** and all applicable data privacy laws, specifically the General Data Protection Regulation (GDPR). The ***Global Records Management Policy*** includes a specific section on HR data and explain the different retention periods for which the information should be retained. This Policy will also explain how the retention periods may vary depending on the type of HR Data in question, for example, where the information constitutes Sensitive Personal Data**.**

The period of time for which Talent Acquisition documents can be retained will depend on whether the individual is successful or unsuccessful in their job application.

- If an individual is **successful** in their job application and accepts the position, HR Data collected during the Talent Acquisition process should be stored on the individual's Associate file. The retention period for this file will generally be the individual's term of employment plus 2 years.
- If an individual is **unsuccessful** in their job application (or rejects the position), the majority of their HR Data should be destroyed within one year of its collection.

Therefore, an unsuccessful applicant's full application may be held for up to 1 year if:

  - there is a real possibility they may be suitable for alternative roles in the future, and retaining their application would be useful for such future hire (e.g. to contact them); and

  - the applicant has either given his/her consent to their personal data being retained for this purpose or been specifically informed that his/her personal data will be retained for this purpose and given the opportunity to object.

5. PROCESSING PERSONAL DATA WITHIN AMERICOLD

This includes activities relating to the employment relationship, such as:

- assessment and training;
- payment of salaries and administration of benefits; (done by Accounting department)
- administration of pension ;
- management and development of careers (including talent management);
- employment analysis (for example, comparing the success of various Talent Acquisition programs);
- handling grievance or disciplinary procedures;

- promotion and career planning; and

- any other identified and necessary for HR purposes which shall be clearly communicated to Data Subjects.

5.1 COLLECTING HR DATA IN THE COURSE OF THE EMPLOYMENT RELATIONSHIP

5.1.1 Giving Notice

Whenever HR Data is collected, directly or indirectly, associates must be properly **informed** about how their personal data will be used. Generally, this requirement should be met by providing this information to every new associate in a suitable via the Associate Data Privacy Notice, which can be found at https://americold.sharepoint.com/sites/BusinessEthicsAndCompliance/SitePages/Data-Privacy-%F0%9F%94%8F.aspx

5.2 FOR WHAT PURPOSES CAN HR DATA BE COLLECTED?

5.2.1 HR Data should only be collected for activities relating to the employee relationship (an illustrative list of what constitutes such activities is provided at the start of this section 5). Only collect HR Data that is needed for specific purposes. For example, do not collect HR Data simply because it may be useful later, for an as yet, unspecified purpose.

5.2.2 If you intend to use HR Data in a way that is significantly different to the purpose(s) communicated to the individual when it was collected, you will need to provide the individual with a further notice explaining the proposed change(s), the reasons for doing so and any likely consequences of this for the individual. Depending on the nature of the new use, it may be necessary to obtain the individual's consent before implementing the proposed change.

5.2.3 If the new purpose is likely to result in a high risk to associates, Americold will need to complete a Privacy Impact Assessment.

5.3 ABSENCE AND SICKNESS RECORDS

Information relating to absence and sickness records must be handled with particular reference to the following:

5.3.1 Access must be strictly limited to associates who have a legal or legitimate business 'need-to-know' (including where such records are managed by an external provider), for example,

where a senior manager needs to access the record of an individual they are responsible for in order to investigate repeated or long-term absence.

5.3.2 The minimum amount of information necessary should be recorded. In many circumstances it should not be necessary to record details of the individual's particular illness, merely a record of their absence (for example, holiday, paternity leave, sickness etc.).

5.3.3 Absence and sickness records should only be disclosed outside Americold where:

- there is a legal obligation to do so;
- it is necessary for legal proceedings;
- the individual has given explicit consent to the disclosure. This means the individual must have been given a genuine choice as to whether the records can be shared with a specified third-party, for a particular purpose; or
- otherwise with the approval of Americold's Legal or Compliance Departments.

5.4 MONITORING OF ASSOCIATES

5.4.1 Associates must be informed where they will be subject to monitoring. Examples of monitoring include, email and internet monitoring and use of CCTV. The information provided to individuals must be sufficiently detailed to ensure that Associates have an understanding of the following:

- when information about them may be obtained, for example:
  - email usage, including (where permitted by applicable law) email content;
  - internet and web browsing activity;
  - use of other Americold equipment (e.g. mobile phones); and/or
  - their movements within Americold premises.
- why the monitoring is being conducted;
- how this information may be used; and
- to whom it may be disclosed.

Americold's ***Acceptable Use Policy*** covers email and internet monitoring.

5.5 KEEPING HR DATA ACCURATE AND SECURE

5.5.1 **Accuracy** - Associates shall inform the HR department to amend and correct their HR Data if there are any changes.

5.5.2 **Security** - There must be appropriate physical (e.g. secure cabinets), technical (e.g. passwords, encryption) and organisational (e.g. access controls, audit trails) security

measures in place to limit the risk of unauthorised access to, accidental loss of, destruction of, or damage to HR Data. What will be appropriate will depend on the nature and the sensitivity of the HR Data in question.

For further information on IT Security, please refer to Americold's global IT policies.

5.5.3 Access controls - Access to HR Data contained in our HR systems (e.g. PeopleSoft) is granted only to relevant individuals on a business 'need-to-know' basis.

6. PERFORMANCE IMPROVEMENT PLANS, DISCIPLINE, GRIEVANCE AND DISMISSAL

6.1 Information relating to performance improvement plans, grievances and dismissal should be accurate and objective and at all times visible to the Associate in question.

6.2 Records relating to disciplinary and grievance matters must be accurate, held securely and only made available to associates on a legitimate 'need-to-know' basis.

6.3 You should ensure all records used in the course of disciplinary and grievance proceedings are accurate and sufficiently detailed to support any conclusion drawn about the individual from them. When employment is terminated the reason for this must be accurately recorded and the record must accurately reflect what the individual has been told about the termination and their responses. Where required by applicable law, such records must be kept securely and only made available to those staff whose duties require they should have access to them.

6.4 Do not access or use HR Data in connection with a disciplinary or grievance investigation if it is incompatible with the purposes for which it was obtained, or it would be disproportionate to the matter under investigation.

7. REQUESTS FROM INDIVIDUALS IN RELATION TO THEIR HR DATA

Please see Americold's ***Associate Data Privacy Notice*** for information on how to handle an individual rights request from an applicant, Americold Associates or former associates.

7.1 SHARING HR DATA WITHIN AMERICOLD

You may share HR Data within the Americold if the following conditions are met:

- the individual has been informed of the sharing (included in the ***Associate Data Privacy Notice***);
- the purpose for the data sharing has been explained to the individual;
- the HR Data to be shared is limited to that which is necessary to fulfil the purpose; and

- the recipient has a business 'need-to-know' in respect of the HR Data.

When deciding whether you may share HR Data within Americold, you should be sure to understand why this information is needed. You should only share HR Data if this purpose is compatible with the purpose for which HR Data was initially collected. If you are unsure whether the sharing satisfies the above conditions, please contact the Legal or Compliance Departments.

8. SHARING HR DATA OUTSIDE THE GROUP

8.1 GENERAL PRINCIPLE

HR Data should generally not be shared outside Americold. However, HR Data can be shared outside Americold under the following circumstances:

- the individual has provided their freely given and informed consent (for example, where they request a reference to be provided to their new employer);
- to engage a third-party supplier:
- to protect an individual's vital interests (i.e. where it is a matter of life or death);
- when required by law, regulation or court order to do so;
- in connection with a legitimate request for assistance by the police or other law enforcement agency;
- to seek legal advice from Company' external lawyers;
- with respect to a legal dispute or administrative claim between Americold and a third party (e.g. to that third party and lawyers representing them);
- to engage professional advisers (e.g. lawyers, accountants, external auditors) and liaise with potential customers, vendors and suppliers in connection with the disposal or acquisition by Americold of a company or a company's assets;
- to administer Americold's contractual relationship with organizations who provide "external workforce" by disclosing relevant information about the individuals provided (e.g. number of days worked);
- to provide a third-party (such as a potential customer or supplier) with a means of contacting Company in the course of its normal business, for example, by providing an associate's business contact details, such as those found on a business card; or
- to engage external auditors to validate Company' financial accounts.

In all cases, the sharing must satisfy the following conditions:

- where the third party is outside the European Economic Area, there must be a data transfer solution in place which satisfies the requirements of applicable law; and

- you must only share the minimum amount of HR Data necessary to fulfill the purpose for which it is being shared.

If the data sharing is likely to result in a high risk to the Employees, Americold will need to conduct a Privacy Impact Assessment. If you think any sharing has the potential to be high risk, you should consult the Legal or Compliance Departments.

The remainder of this Policy provides more detail on the necessary steps to take if Americold will be sharing HR Data outside of the company in the circumstances set out above.

8.2 PROVIDING REFERENCES FOR COMPANY ASSOCIATES

8.2.1 In the event that an Individual who is (or has previously been) employed by Americold decides to pursue alternative employment or an opportunity with another organization, Americold may receive a request to provide a reference for that Individual. It may be that the request comes from the Individual themselves or from the organization which the Individual seeks to work for or join. The reference sought may be a 'Company Reference' which is likely to involve details such as the Individual's job title, start and end date and years of service. Alternatively, it may be a 'Personal Reference' which will be provided by a particular, named Americold associates and will provide detail on the Individual's character and capabilities.

8.2.2 Providing a reference as outlined above will involve sharing Personal Data outside Americold and there are certain factors which should be taken into consideration when providing a reference.

8.2.3 You should observe the following steps when providing a reference for an Individual:

- Only provide a reference with the consent of the Individual to whom the reference relates. If you receive a request for a reference from anyone other than the Individual (for example, from the organization they are joining) you must obtain the consent of the Individual before sharing the information.

- Only provide as much information as is necessary for the purpose it is required. For example, if you have been asked to provide a 'Company Reference' with specific, limited information then you should not provide additional information about the Individual's capabilities or character unless this has been specifically requested by the Individual and approved by Legal or Compliance Departments.

8.3 REQUESTS FROM LAW ENFORCEMENT OR OTHER REGULATORY AUTHORITIES

8.3.1 It will sometimes be necessary for Americold to provide passport and nationality information to immigration and customs authorities in order to facilitate the entry of associates into the relevant country, when they are travelling for work purposes. In other circumstances, you should always consult Americold's Legal or Compliance Departments before responding to a request from law enforcement or another regulatory authority for access to HR Data.

8.3.2 If Americold's Legal or Compliance Departments authorizes the disclosure of HR Data, the disclosure should be limited to that which is necessary to achieve the requestor's specified purpose. Ensure, that as part of this process, a record is maintained of the information disclosed, discussions with Americold's Europe Legal function, and the steps taken.

8.4 PENSION, INSURANCE SCHEMES AND OTHER BENEFITS

8.4.1 When an individual joins, insurance or other benefits scheme, ensure that is it clear to the individual what, if any, HR Data is passed between the benefits scheme provider and Americold, and how it will be used.

8.4.2 The HR Data required by the third party to administer a scheme or benefit must not be accessed or used for general employment purposes. For instance, an individual's medical report needed for the pension scheme may not be used in connection with decisions about the individual's eligibility for sick pay. As a result, use confidential ways to prevent HR Data to leak from a scheme (e.g. a sealed envelope).

8.4.3 Limit your exchange of HR Data with a benefits provider to that necessary for the operation of the scheme.