Brambles

Global Record Retention Policy

Brambles Limited

Revised: 1 January 2020

Version 2.0

Global Record Retention Policy

1 Policy Statement

The purpose of this Records Retention Policy ("**Policy**") is to specify how business records created and maintained by Brambles are to be retained and destroyed, in compliance with applicable laws and best practices for the retention of records. This Policy applies to all directors, officers, and employees of Brambles and each subsidiary, partnership, and those ventures and business associations effectively controlled by Brambles, either directly or indirectly, including distributors, agents and as well as certain third parties who adopt this Policy by contract or upon the request of Brambles, including contractors, agents, and providers of outsourced services in all jurisdictions in which Brambles operates ("**Covered Person**" or "**Covered Personnel**").

Adherence to this Policy will allow Brambles to comply with applicable legal retention and production requirements (e.g., for litigation, audits and government/regulatory investigations), while ensuring business continuity, reducing legal exposure, and reducing the business costs associated with retaining and producing records (e.g., storing, identifying, retrieving, assembling, formatting and delivering).

In general, Brambles retains records only for the minimum periods set forth in the attached Records Retention Schedule ("**Retention Schedule**", set out in Schedule 1), or for such longer periods as such records are necessary for Brambles' legal or business requirements in accordance with applicable laws. While this Policy describes Brambles' general records retention policies and procedures, it does not address every issue or situation that may arise. Any person with questions regarding this Policy should consult with the Legal and Compliance Team before retaining or destroying a particular record. Nothing in this Policy is intended to alter any contractual or legal requirement that Brambles or its employees may have to retain, return or destroy records provided to Brambles or such employee.

It is the responsibility of each Covered Person to ensure that all records she or he creates or uses in connection with Brambles' business operations are retained in accordance with this Policy and Retention Schedule. The local business units are responsible for ensuring compliance with this Policy and that their Covered Personnel are aware of and trained on the Retention Schedule (to include any applicable Country Exceptions set out in the Retention Schedule). While the Global IT Team may implement general retention settings in line with this Policy, they may not be in line with specific data retention requirements, particularly when Country Exceptions to the global retention rule exist.

All records created or used in connection with Brambles' business operations are the property of Brambles and must be retained and/or destroyed in accordance with the procedures set forth in this Policy. Any deviations from this Policy must be specifically approved by the Legal and Compliance Team.

2 References

This Policy must be read in conjunction with the Global Data Classification and Handling Policy.

3 Scope

This Policy governs the retention and destruction of all records of Brambles, its subsidiaries, and affiliated companies (including those records in the possession of third parties) regardless of format, media, location, workplace venue, computer network systems and communication devices, including, but not limited to, portable or handheld computing devices, wireless technologies, external hard drives/USB drives and removable portable storage media.

In this Policy, the term "**records**" is used in the broadest sense regardless of physical form or media and applies to any and all materials created or received by Brambles in connection with transacting its business, including, but not limited to, printed hard copy documents, handwritten documents, blueprints, photographs, videos, electronic or digital recordings, product designs, advertising media, promotional materials, email messages, instant and text messaging, voicemail, web pages, digital files and images, computer programs and other electronically stored documents and data, agreements, invoices, internal and external correspondence and memoranda, presentations, analyses and reports created by or on behalf of Brambles.

All Covered Personnel are required to familiarize themselves with this Policy, and to take all necessary steps to comply with it.

4 Retention of Records – Retention Schedule

The **Retention Schedule** is attached to this Policy and shows record categories by business function along with record type descriptions and applicable retention periods. The business functions identified in the Retention Schedule refer to functional areas of business operations from a records management perspective, as informed by applicable legal requirements. They are not intended to reflect Brambles' organizational structure. The Retention Schedule groups records according to the following business functions:

1. Accounting, Finance & Tax
2. Corporate Organization, Legal & Compliance
3. Environment, Health & Safety
4. Human Resources
5. Internal Services & Administration
6. Marketing, Sales & Customer Service
7. Risk & Insurance
8. Transportation & Logistics

The Retention Schedule provides Retention Rules for the retention of records. The Retention Rules specified in the Retention Schedule are Brambles' official retention periods for records. Covered Personnel who create and manage records must retain them for the retention periods identified in the Retention Schedule (subject to the exceptions discussed in Section 5 of this Policy) and dispose of them in accordance with Section 16 of this Policy. Unless specified to the contrary in the Retention Schedule, all record retention periods should start on the last day of the calendar year in which the records were completed, finalized or became inactive.

Not every record can be explicitly listed in the Retention Schedule, so Covered Personnel should use common sense, experience, and judgment in identifying the most appropriate record category for the retention of records. Where a record could fall under more than one record category, Covered Personnel should be guided by the relevant business function (or department) and should normally choose the record type with the longest retention period. This retention period will be subject to any local exceptions based upon data privacy considerations which may impose specific maximum (MAX) retention periods. (This reflects the general principle that records containing personal information must not be kept longer than necessary to comply with applicable law or to achieve the business purpose for which the information was collected and retained. See Section 14.)

In the event that compliance with any section of this Policy (including the Retention Schedule) would violate any applicable local legal requirement, Covered Personnel are required to promptly notify the Legal and Compliance Team about the conflict between this Policy (including the Retention Schedule) and the applicable local law, and Covered Personnel are, subject to any written guidance provided by the Legal and Compliance Team, required to comply with the local legal requirement, even where it differs from the requirements set out in this Policy (including the Retention Schedule). The Legal and Compliance Team will verify the legal requirement and, if necessary, update this Policy (including the Retention Schedule) accordingly.

5 Retention of Records – Exceptions

Legal Hold

A legal hold is a mandatory requirement to preserve and retain records in the event of a pending, threatened or reasonably foreseeable legal claim, litigation, regulatory audit, governmental inquiry or investigation, or similar action or proceeding, as determined by the Legal Team.

In the event that certain records are subject to a legal hold, you will be notified by a member of the Legal Team and given specific instructions regarding the preservation of certain records. In such event, no Covered Personnel shall conceal, destroy, or alter any such records (including electronic records). Destruction of such records can only take place with the specific written authorization of the Legal Team or Brambles' outside legal counsel handling the matter.

Business Requirement

When Covered Personnel identifies and reports a bona fide business requirement to retain a record beyond the retention period set out in the Retention Schedule, he or she may submit a request to the Legal and Compliance Team. The record may be retained beyond its required retention period only if the Legal and Compliance Team grants approval. Records retained for such purposes will be reviewed annually to determine if there remains a continuing need for retention.

Contractual Obligation

If Brambles has entered into an agreement to extend the statute of limitations or the retention period for certain records, then the periods set forth in the Retention Schedule must be extended for the same amount of time as the extension. Any extension of a retention period must be approved by the Legal and Compliance Team. When a contract specifies the manner and time within which to collect, maintain and/or destroy certain records, consult the Legal and Compliance Team to determine whether this Policy or the contract applies.

Company Acquisition

Where Brambles acquires another company, the acquired company's records are subject to this Policy, unless terms of the acquisition dictate otherwise. Unless otherwise notified, any pre-acquisition legal holds or contractual obligations, as well as all Brambles legal holds and contractual obligations, apply. If in doubt, consult the Legal and Compliance Team.

6 Media / Format of Records

To preserve record integrity, records should be retained in a format that fulfills Brambles' processes and complies with applicable laws or regulations. Covered Personnel should contact the Legal and Compliance Team to obtain further information.

7 Scanning and Preservation of Original Physical Records

Records can be scanned and stored in an electronic system. The scanned image must be clear, legible, and complete. The record owner must be able to demonstrate the integrity of the record (e.g., all the content of the document is retained) and the scanned record must be easily accessible for subsequent reference.

In general, once a record had been scanned the original physical record may be destroyed. However, the following types of documents **must not be destroyed** even if they have been scanned:

- Original company books and documents, including:
    - articles of organization, certificates of registration of business name and other constitutional documents;
    - member agreements;
    - annual statements and other official business reports;
    - minute books, including minutes of meetings of members, directors, debenture holders, auditors or corporate committees;
    - reports, consents and powers of auditors, managers, board committees, board observers, and any other person who has control or supervision of the company;
    - registers/registries of membership interests, managers; and
    - any other document that relates to corporate decisions and powers;
- Real property agreements, deeds, judgments, assignments, mortgages, or legal charges relating to land;
- Official documents issued by a court or arbitration panel;
- Agreements or contracts that contain original signatures unless (i) they are of minimal importance, or (ii) written approval from the Legal and Compliance Team has been obtained;
- Records of licenses, permits , or certifications;
- Wills, trusts, public deeds, powers of attorney, documents required to be stamped, documents that have been notarized, government conditions of grant, and government leases;
- Oaths and affidavits, statutory declarations, judgments. and court warrants;
- Securities and negotiable instruments;
- Affidavits or other sworn declarations; and

- Any document that may be required for existing or anticipated legal proceedings.

8 Storage and Security of Records

Covered Personnel must comply with applicable security policies and take all reasonable measures to ensure the integrity, confidentiality, and availability of the records they create and retain. Records must be stored in a manner that permits access only to those individuals who are properly authorized to do so and ensures a level of security that is commensurate with the degree of sensitivity of those records. Storage of electronic records in electronic form should be on a medium that has been approved by the Global IT Team. Covered Personnel should contact the Global IT Team to obtain further information.

All paper records required to be retained in their original physical form must be stored in the jurisdiction in which they were issued or received. Original company books and documents must be kept at the registered address of the company.

9 Back-Up Records

Brambles retains back-up records for disaster recovery purposes only. Back-up records must **not** be relied upon by Covered Personnel as a tool or method for archiving records that are required to be maintained under this Policy. In some of our businesses, back-up records are maintained and stored at an off-site facility managed by third party vendor(s) specializing in back-up records storage and protection. Covered Personnel must ensure that records sent to any off-site facility are classified, packed, and labeled in a way that will facilitate their identification, retrieval, and eventual destruction.

10 Drafts and Copies

If copies of a record exist, Brambles may designate one copy as the official record for purposes of complying with the retention requirements set forth in the Retention Schedule. All other copies of the official record may be destroyed. A copy is an exact replica of the original record. Prior drafts, revisions, or original documents that have additional handwritten notes or other material notations are not considered copies of the original record. In no instance shall a copy of a record be kept longer than the official record.

Prior to disposing of a copy, the person who wishes to dispose of the copy must confirm with the person who is routinely charged with the maintenance of the record (e.g., the relevant financial officer in the case of financial records, or an attorney in the case of corporate transactional records) that the copy is an exact replica of the original record and the original record is being maintained in accordance with the provisions of this Policy.

Drafts of agreements or documents (in electronic or physical form) must be destroyed after finalization of such agreements or documents, or the consummation or abandonment of the transaction contemplated by the documents. However, legal counsel involved in the transaction may retain drafts beyond such time if necessary for Brambles' business requirements and if approved by the Legal and Compliance Team in accordance with Section 5 of this Policy.

Persons who receive a copy of a paper or electronic record (such as a "cc" or "bcc") are under no obligation to retain correspondence under this Policy if the author(s) or primary recipient(s) is subject to this Policy. In this case, such persons can assume that the author(s) or primary recipient(s) will retain the record in accordance with this Policy. If neither the author(s) nor primary recipient(s) is subject to this

Policy, then copies of the record shall be retained in accordance with the specified retention periods in the Retention Schedule.

11 E-Mail and Other Electronic Records

Email[1] and other electronic records including, but not limited to, voice mail, faxes, instant messages, and text messages, are considered record formats rather than record types. The substance or content of the email or other electronic record will determine the record type and applicable retention period.

Email and similar electronic communications present a unique records retention issue because such communications may contain attachments. In considering the content or substance of email for retention purposes, the email should be considered as a whole, including any attachments. If one retention period applies to an email and a different retention period applies to the email attachment(s), the email and its attachment(s) should be retained for the longer of the two retention periods.

Copies retained in electronic form need not be retained if the physical copy is properly stored so as to protect its integrity and authenticity.

12 Transitory Records

Transitory records are short-term records that are not covered by any record category in the Retention Schedule. Examples may include reference materials and notes, out-of-office replies, routine system messages and log files, correspondence, emails, and voicemails with no ongoing business value (when not otherwise covered by the Retention Schedule). These records should be retained only as long as they are needed for immediate operational purposes or are necessary to serve the business need. When no longer needed, these records should be destroyed. Transitory records are not to be considered records within the scope of this Policy, unless a legal hold is placed on such records in accordance with Section 5 of this Policy.

13 Records of Departing Employees

All records covered by this Policy are the property of Brambles and remain confidential business documents and information. Brambles reserves the right to examine all records that any employee leaving the employment of Brambles requests to retain, copy, download or export in order to determine ownership and to approve the release, removal, copying, downloading or exporting of those records. All requests must be made in writing to the departing employee's manager or director and include a detailed description of the records in question. Any questions regarding this section should be directed to an attorney in the Legal and Compliance Team.

Each departing employee's manager shall be responsible for: (a) retaining and destroying the records of employees who leave the department in accordance with the provisions of this Policy and the Retention Schedule, and (b) ensuring that the Global IT Team preserves the electronic records of departing employees in accordance with the provisions of this Policy.

---

[1] For avoidance of doubt, email stored in a Brambles employee's inbox are currently retained for a period of 10 years (2 years in the active directory and 8 years in an archive). Any employee needing to retain an email to comply with this Policy beyond 10 years should either create a physical or hard copy or follow the procedures set out in Schedule 2 to properly retain an electronic record.

14 Records Containing Personal Information

Personal information is information that directly identifies an individual or that can lead to the identification of an individual (e.g., name, email address, date of birth, personal financial information, health information, photos of individuals). Personal information should not be collected or retained unless required by law or reasonably necessary to conduct business-related tasks. Where records include personal information, the records should be deleted or destroyed, or the personal information should be redacted, when it no longer serves a reasonably necessary purpose and it is not needed to comply with a legal obligation. Any questions regarding the appropriateness of collecting or retaining personal information should be directed to the Legal and Compliance Team.

15 Transfer of Records

Covered Personnel must not transfer records outside of the jurisdiction in which they were created, unless an applicable Intracompany Transfer Agreement is in place or the written approval of the Legal and Compliance Team is obtained. All records leaving Brambles must be recorded, tracked and, where applicable, signed for upon receipt. Transfer arrangements must be documented and agreed with the recipient in advance of the records leaving Brambles.

16 Destruction of Records

Records that are appropriate for disposal shall be destroyed as follows and consistent with the Global Data Classification and Handling Policy:

1. Public paper records may be recycled, shredded or otherwise destroyed;
2. General, Confidential, and Highly Confidential paper records (records that contain personal, proprietary, confidential, trade secret, or financial information) must be: (a) shredded with a cross-cut shredder before disposal, (b) placed in a shredding bin so that an authorized third party can securely dispose of the records, or (c) otherwise rendered unreadable.; and
3. General, Confidential, and Highly Confidential electronically stored records may be erased or destroyed using a method that is approved by the IT Department, as determined by their data classification and the Global Data Classification and Handling Policy.

Please contact the Legal and Compliance Team for information regarding the destruction of records that are not suitable for destruction using the above methods.

17 Violations

It is a violation of the law and this Policy to make a false statement or to conceal information called for in a government report, investigation, application or filing. It is against the law to knowingly alter, destroy, mutilate, conceal, cover-up, or falsify any record with the intent to impede, obstruct, or influence a governmental investigation or administrative action.

Any questions regarding the destruction of records, including whether specific records are or may be relevant to a particular litigation, audit, or government/regulatory investigation, should be directed to the Legal and Compliance Team prior to any action being taken.

18 Contact / Questions

This Policy is administered by the Legal and Compliance Team. If you have any questions regarding this Policy, you may direct those questions to the Legal and Compliance Team.

19 Policy Review

This Policy supersedes any and all prior Brambles records management policies. Brambles reserves the right to amend, modify or discontinue this Policy at any time, for any reason.