

1. POLICY STATEMENT

[Company Name] (“we” or “us” or “our” or “the Company”) respects the privacy of our users. This Data Retention Policy (“Policy”) sets out the principles for the effective maintenance, retention and destruction of personal data records, information, and data.

The Company only retains personal data for legitimate or legal business reasons and always complies fully with the applicable data protection laws, guidance, and best practice.

2. PURPOSE

This Policy sets out the type(s) of personal data held by the Company, the period(s) for which that personal data will be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with the local privacy compliance law [(GDPR, CCPA, LGPD, PDPA, PDPB)], please refer to the Company’s Data Privacy Policy.

3. OBJECTIVES

The privacy compliances impose obligations on the Company, as a Data Controller, to process personal data in a fair and secure manner which notifies the data subjects of the purposes of data processing and to the retention period of the data for no longer a period than is necessary to achieve the purposes abovementioned.

The Company’s objectives and principles in relation to Data Retention are to:

- mitigate against risks or breaches in relation to confidential information;
- ensure the integrity, security, and availability of data;
- comply with applicable laws and regulations that prescribe minimum and maximum time periods for the retention of data including personal data;
- preserve, review, and retain data that is necessary for the protection; and [periodically delete any unnecessary data];
- [anonymise the data so that it cannot be identified to a specific data subject];
- support the safe and efficient retrieval, transfer and storage of data; and
- provide for the safe and secure disposal and destruction of data that is no longer required.

4. SCOPE

This Policy applies to all persons within the Company (meaning permanent, fixed term, temporary staff and sub-contractors engaged with the Company). Adherence to this Policy is mandatory and non-compliance could lead to disciplinary or legal action as per the terms of employment/contract.

5. RESPONSIBILITIES

Heads of departments and information asset owners have overall responsibility for the management of records and data generated by their departments' activities, namely to ensure that the records created, received, and controlled within the purview of their department, and the systems (electronic, physical or otherwise) and procedures they adopt, are managed in a way which meets the aim of this Policy.

Where a DPO has been designated, he/she must be involved in any data retention processes and record maintenance or all archiving, and destructions must be retained. Individual employees must ensure that the record for which they are responsible are complete and accurate records of their activities, and that they are maintained and disposed of in accordance with the Company's protocols.

6. PRIVACY COMPLIANCE

The Company needs to collect personal information about job applicants, the people we employ, work with, or have a business relationship with, to effectively and compliantly carry out our everyday business functions and activities, and to provide the services defined by our business type. This information can include but is not limited to, name, address, email address, date of birth, identification number, private and confidential information, sensitive information, and bank details.

In addition, we may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however, we are committed to collecting, processing, storing, and destroying all information in accordance with the applicable data protection law and any other associated legal or regulatory body rules or codes of conduct that apply to our business and/or the information we process and store.

7. GUIDELINES & PROCEDURES

The Company retains data records efficiently and systematically, in a manner consistent with the local privacy compliance law and regulatory codes of practice on records management. This Policy is widely disseminated to ensure a standardised approach to data retention and records management.

Records will be retained to provide information about, and evidence of the Company's transactions, customers, employment, and activities. Retention schedules will govern the period that records will be retained and can be found in the Record Retention Periods document.

7.1. Retention Period Protocols

All Company and employee information is retained and stored for a period of [insert number] years and is thereafter [anonymised or] destroyed in line with legislative and regulatory guidelines. However, data retention period would be prolonged for such period as may be applicable in case of

ongoing investigations with Government authorities or when exercising any legal rights in court proceedings, as described in Paragraph 7.2.

For all data and records obtained, used, and stored within the Company, we:

Establish and carry out periodical reviews of the data retained, checking purpose, continued validity, accuracy, and requirement to retain:

- Establish and verify retention periods for the data, with special consideration given in the below areas:
 1. the requirements of the Company;
 2. the type of personal data;
 3. the purpose of processing;
 4. lawful basis for processing;
 5. the categories of data subjects
- Where it is not possible to define a statutory or legal retention period, as per the GDPR requirement, the Company will identify the criteria by which the period can be determined and provide this to the data subject on request and as part of our standard information disclosures and privacy notices.
- Have processes in place to ensure that records pending audit, litigation or investigation are processed and retained as per applicable law.

7.2. Suspension of Record Disposal for Litigation or Claims

If the Company is served with any legal request for records or information, any employee becomes the subject of an audit or investigation or we are notified of the commencement of any litigation against our Company, we will suspend the disposal of such records that are required for the legal process.

7.3. Storage & Access of Records and Data

Documents are always retained in a secure location, with authorised personnel being the only ones to have [password only] secure access. The documents are also stored in such manner in order to safeguard the information against loss as a result of any technological changes. Once the retention period has elapsed, the documents are reviewed, archived, [anonymised] or confidentially destroyed/deleted depending on their purpose for which those documents were created is no longer relevant.

7.4. Expiration of Retention Period

Once a record or data has reached its designated retention period date, the asset owner should refer to the retention register for the action to be taken.

7.5. Destruction and Disposal of Records & Data

All information of a confidential or sensitive nature on paper or electronic media must be securely destroyed when it is no longer required. The method of disposal adopted by the Company varies

depending on the nature of confidentiality of the document. This ensures compliance with the data protection laws and the duty of confidentiality we owe to our employees, clients, and customers.

The Company is committed to the secure and safe disposal of any confidential waste and information assets in accordance with our contractual and legal obligations and that we do so in an ethical and compliant manner. We confirm that our approach and procedures comply with the laws and provisions made in the applicable local privacy compliance laws and that the Company's staff is trained and assumes the responsibility in accordance with the procedures and controls put in place. by the Company.

7.5.1. Paper Records

Due to the nature of our business, the Company retains paper based personal information and as such, has a duty to ensure that it is disposed of in a secure, confidential, and compliant manner. The Company utilises a Professional Shredding Service Provider to dispose of all paper materials. Employee shredding machines and confidential waste disposal units are made available throughout the building and where we use service provider disposals, regular collections take place to ensure that confidential data is disposed of appropriately.

7.5.2. Electronic & IT Records and Systems

The Company uses numerous systems, computers, and technology equipment in the running of our business. From time to time, such assets must be disposed of and due to the information held on these whilst they are active, this disposal is handled in an ethical and secure manner. The deletion of electronic records must be organised in conjunction with the IT Department who ensures that the removal of all data from the medium so that it cannot be reconstructed.

8. ERASURE

In specific circumstances, data subjects' have the right to request that their personal data is erased, however the Company recognises that this is not an absolute 'right to be forgotten' and is subject to the limitations as prescribed under law. Data subjects only have a right to have personal data erased and to prevent processing if one of the below conditions applies:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- When the individual withdraws consent;
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
- The personal data was unlawfully processed;
- The personal data must be erased in order to comply with a legal obligation.

For further information on other aspects of data erasure process and compliance, please refer to the Company's Procedure for Handling of Individual Rights.

9. COMPLIANCE AND MONITORING

The Company is committed to ensuring the continued compliance with this Policy and any associated legislation and undertakes regular audits and monitoring of its records, its management, archiving and retention. Asset owners are tasked with ensuring the continued compliance and review of records and data within their remit.

10. RETENTION PERIODS

Please refer to data retention schedule for further reference.

