Data Retention Policy

1. **Introduction**

1.1. This policy sets the required retention periods for specified categories of personal data and sets out the minimum standards to be applied when destroying certain information within INA Prime Solutions.

1.2. This policy applies to all business units, processes, and systems in all countries in which INA conducts business and has dealings or other business relationships with third parties.

1.3. This policy applies to all INA employees, agents, affiliates, contractors, consultants, advisors or service providers that may collect, process, or have access to data (including personal data and/or sensitive personal data). It is the responsibility of all of the above to familiarize themselves with this policy and ensure adequate compliance with it.

1.4. This policy applies to all information used at INA. Examples of documents include:

- Emails
- Hard copy documents
- Soft copy documents
- Video and audio
- Data generated by physical access control systems

2. **Retention General Principle**

2.1. In the event, for any category of documents not specifically defined elsewhere in this policy (and in particular within the Data Retention Schedule) and unless otherwise mandated differently by applicable law, the required retention period for such a document will be deemed to be 3 years from the date of creation of the document.

3. **Retention General Schedule**

3.1. The Chief Financial Officer defines the time period for which the documents and electronic records should be retained through the Data Retention Schedule.

3.2. As an exemption, retention periods within the Data Retention Schedule can be prolonged in cases such as:

- If there is a chance records of personal data are needed by INA to prove compliance with any legal requirements; or
- When exercising legal rights in cases of lawsuits or similar court proceedings recognized under local law.

4. **Safeguarding of Data during Retention Period**

4.1. The possibility that data media used for archiving will wear out shall be considered. If electronic storage media are chosen, any procedures and systems ensuring that the information can be accessed during the retention period (both with respect to the information carrier and the readability of formats) shall also be stored in order to safeguard the information against loss as a result of future technological changes. The responsibility for the storage falls to the Vice President - IT & Operations.

5. **Destruction of Data**

5.1. INA Prime Solutions and its employees should, on a regular basis, review all data, whether held electronically on their device or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant. See Appendix for the retention schedule. Overall responsibility for the destruction of data falls to the Chief Financial Officer.

5.2. Once the decision is made to dispose according to the Retention Schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality. The method of disposal varies and is dependent upon the nature of the document. For example, any documents that contain sensitive or confidential information (and particularly sensitive personal data) must be disposed of as confidential waste and be subject to secure electronic deletion; some expired or superseded contracts may only warrant in-house shredding. The Document Disposal Schedule section below defines the mode of disposal.

5.3. In this context, the employee shall perform the tasks and assume the responsibilities relevant for the information destruction in an appropriate way. The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the Chief Financial Officer subcontracts for this purpose. Any applicable general provisions under relevant data protection laws and INA's Personal Data Protection Policy shall be complied with.

5.4. Appropriate controls shall be in place that prevent the permanent loss of essential information of the company as a result of malicious or unintentional destruction of information – these controls are described in the company's IT Security Policy.

5.5. The Chief Financial Officer shall fully document and approve the destruction process. The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed.

6. **Breach, Enforcement and Compliance**

6.1. The person appointed with responsibility for Data Protection, the Chief Financial Officer, has the responsibility to ensure that each of INA's offices complies with this policy. It is also the responsibility of the Chief Financial Officer to assist any local office with enquiries from any local data protection or governmental authority.

6.2. Any suspicion of a breach of this policy must be reported immediately to the Chief Financial Officer. All instances of suspected breaches of the policy shall be investigated and action taken as appropriate.

6.3. Failure to comply with this policy may result in adverse consequences, including, but not limited to, loss of customer confidence, litigation and loss of competitive advantage, financial loss and damage to INA's reputation, personal injury, harm or loss. Non-compliance with this policy by permanent, temporary or contract employees, or any third parties, who have been granted access to INA's premises or information, may therefore result in disciplinary proceedings or termination of their employment or contract. Such non-compliance may also lead to legal action against the parties involved in such activities.

7. **Routine Disposal Schedule**

7.1. Records which may be routinely destroyed unless subject to an on-going legal or regulatory inquiry are as follows:

- Announcements and notices of day-to-day meetings and other events including acceptances and apologies;
- Requests for ordinary information such as travel directions;
- Reservations for internal meetings without charges / external costs;
- Transmission documents such as letters, fax cover sheets, e-mail messages and similar items that accompany documents but do not add any value;
- Superseded address list, distribution lists etc.;
- Duplicate documents such as CC and FYI copies, unaltered drafts, snapshot printouts or extracts from databases and day files;
- Stock in-house publications which are obsolete or superseded; and
- Trade magazines, vendor catalogs, flyers and newsletters from vendors or other external organizations.

7.2. In all cases, disposal is subject to any disclosure requirements which may exist in the context of litigation.

8. **Destruction Method**

8.1. Level I documents are those that contain information that is of the highest security and confidentiality and those that include any personal data. These documents shall be disposed of as confidential waste (cross-cut shredded and incinerated) and shall be subject to secure electronic deletion. Disposal of the documents should include proof of destruction.

8.2. Level II documents are proprietary documents that contain confidential information such as parties' names, signatures and addresses, or which could be used by third parties to commit fraud, but which do not contain any personal data. The documents should be cross-cut shredded and then placed into locked rubbish bins for collection by an approved disposal firm, and electronic documents will be subject to secure electronic deletion.

8.3. Level III documents are those that do not contain any confidential information or personal data and are published INA documents. These should be strip-shredded or disposed of through a recycling company and include, among other things, advertisements, catalogs, flyers, and newsletters. These may be disposed of without an audit trail.

9. **Data Retention Schedule**

9.1. Financial Records

Personal data record category	**Mandated retention period**	**Record owner**
Payroll records	Seven years after audit	Finance
Supplier contracts	Seven years after contract is terminated	Finance
Chart of Accounts	Permanent	Finance
Fiscal Policies and Procedures	Permanent	Finance
Permanent Audits	Permanent	Finance
Financial statements	Permanent	Finance
General Ledger	Permanent	Finance
Investment records (deposits, earnings, withdrawals)	7 years	Finance
Invoices	7 years	Finance
Cancelled checks	7 years	Finance
Bank deposit slips	7 years	Finance
Business expenses documents	7 years	Finance
Check registers/books	7 years	Finance
Property/asset inventories	7 years	Finance
Credit card receipts	3 years	Finance
Petty cash receipts/documents	3 years	Finance

9.2. **Business Records**

Personal data record category	**Mandated retention period**	**Record owner**
Article of Incorporation to apply for corporate status	Permanent	Finance

Board policies	Permanent	Finance
Board meeting minutes	Permanent	Finance
Tax or employee identification number designation	Permanent	Finance
Office and team meeting minutes	Permanent	Finance
Annual corporate filings	Permanent	Finance

9.3. **HR Employee Records**

Personal data record category	**Mandated retention period**	**Record owner**
Disciplinary, grievance proceedings records, oral/verbal, written, final warnings, appeals oral/verbal, written, final warnings, appeals	As per legal requirement	HR
Bank details – current	Duration of employment	HR
Payrolls/wages	Duration of employment	HR
Employee address details	Duration of employment	HR
Applications for jobs, interview notes – Recruitment/promotion panel Internal - Where the candidate is unsuccessful - Where the candidate is successful	Delete immediately Duration of employment	HR
Job history including staff personal records: contract(s), Ts & Cs; previous service dates; pay and pension history, pension estimates, resignation/termination letters	As per legal requirement	HR
Payroll input forms, wages/salary records, overtime/bonus payments Payroll sheets, copies	7 Years	HR
Expense claims	As per legal requirement	HR
Annual leave records	Duration of employment	HR
Accident books	As per legal requirement	HR
Accident reports and correspondence	As per legal requirement	HR
Certificates and self-certificates unrelated to workplace injury; statutory sick pay forms	As per legal requirement	HR
Pregnancy/childbirth certification	As per legal requirement	HR

Parental leave	Duration of employment	HR
Maternity pay records and calculations	As per legal requirement	HR
Redundancy details, payment calculations, refunds, notifications	As per legal requirement	HR
Training and development records	Duration of employment	HR

9.4. **Contracts**

Personal data record category	**Mandated retention period**	**Record owner**
Signed	Permanent	Finance
Contract amendments	Permanent	Finance
Successful tender documents	Permanent	Finance
Unsuccessful tenders' documents	Permanent	Finance
Tender – user requirements, specification, evaluation criteria, invitation	Permanent	Finance
Contractors' reports	Permanent	Finance
Operation and monitoring, eg complaints	Permanent	Finance

9.5. **Customer Data**

Personal data record category	**Mandated retention period**	**Record owner**
Platform data – inclusive of Video data, comments, attachments, profile picture, email address, first and second name	Retained whilst a client remains a customer or deleted by user. Once an client requests all records to be deleted, data will be removed from the back-ups within 9 months	Customer
CRM data – inclusive of Name, Email address, mobile number, address, emails and phone call summaries	Retained whilst a client remains a customer or deleted by user. Once an client requests all records to be deleted, data will be removed from the back-ups within 2 months	Support

Live chat history	Records deleted after 1 year unless it pertains to a booking	Support
Screen recordings from support session	Automatically deleted after 90 days	Support
Metrics data	Retained whilst clients remain a customer or deleted by user. Once a client requests all records to be deleted, data will be anonymised	Development Team

9.6. **Non - Customer Data**

Personal data record category	**Mandated retention period**	**Record owner**
Name, email address	Kept until person unsubscribes / requests to be removed from system	Marketing & Sales
Call recordings	Deleted 12 months after completion of trip	Sales

9.7. **IT**

Personal data record category	**Mandated retention period**	**Record owner**
Recycle Bins	Cleared monthly	Individual employee
Downloads	Cleared monthly	Individual employee
Inbox	All emails containing PII attachments deleted after 3 years.	Individual employee
Deleted Emails	Cleared monthly	Individual employee
Personal Network Drive	Reviewed quarterly, any documents containing PII deleted after 3 years	Individual employee
Local Drives & files	Moved to network drive monthly, then deleted from local drive	Individual employee
Google Drives, drop box	Reviewed quarterly, any documents containing PII deleted after 3 years	Individual employee

Review and update of this document will take place when changes require revising the **Data Retention Policy**. Such modifications may relate to changes in roles and responsibilities, release of new legislation or the identification of a new policy area, in consultation with appropriate members and their approval on all revisions to this Data Retention Policy. When approved a new version of the policy will be issued and all affected departments will be informed of the changes.