Data Protection Policy

1. **Introduction**

1.1. The protection of individuals via the lawful, legitimate and responsible processing and use of their personal data is a fundamental human right. Individuals may have a varying degree of understanding or concern for the protection of their personal data, but INA Prime Solutions must respect their right to have control over their personal data and ensure it acts in full compliance with legislative and regulatory requirements at all times. If clients (and staff) feel that they can trust INA as a custodian of their personal data, this will also help INA fulfill its wider objectives.

2. **Purpose of this Policy**

2.1. This Policy sets out how INA Prime Solutions will process the personal data of its staff and clients.

2.2. This Policy applies to all personal data that INA processes regardless of the format or media on which the data are stored or who it relates to.

2.3. A glossary of the terms used throughout the Policy can be found in Schedule 1.

3. **Scope of this Policy**

3.1. This Policy applies to all members of staff employed by INA Prime Solutions, (full time and part time) who are carrying out work on behalf of INA involving the handling of personal data.

3.2. Compliance with this Policy and the related policies and procedures is mandatory. Any breach of this Policy and any related policies and procedures may result in disciplinary action.

3.3. All staff of INA must read, understand and comply with this Policy when processing personal data in the course of performing their tasks and must observe and comply with all controls, practices, protocols and training to ensure such compliance.

3.4. INA's CFO, VP of Technology & Operations and the HR General Manager are responsible for overseeing the implementation and review of this Policy (and the related policies and procedures).

3.5. If staff do not feel confident in their knowledge or understanding of this Policy, or they have concerns regarding the implementation of this Policy, it is important that they raise this issue with their manager as soon as possible or use the contact details above to seek advice.

4. Further advice regarding this Policy

4.1. INA Prime Solutions' CFO, VP of Technology & Operations and the HR General Manager can be contacted for general advice and if the staff:

- wish to process personal data for any purpose and they are unsure whether INA has a lawful basis for doing so
- need to rely on consent and/or require explicit consent
- are unsure whether to delete, destroy or keep any personal data
- are unsure about what security or other measures they need to take to protect personal data
- know or suspect that there has been a personal data breach
- if they need assistance in dealing with the exercise of any rights by data subjects
- if they plan to use personal data for any purposes other than those they were originally collected for
- if they are considering the processing of personal data in a new or different way
- if they are unsure of the legal requirements relating to any direct marketing activities
- if they need help with contracts or any other areas in relation to sharing personal data with a third party

5. **Data Protection Principles**

5.1. INA Prime Solutions must observe and comply with core principles at all times - from the moment when personal data is collected until the moment the personal data is archived, deleted or destroyed. INA must ensure that all personal data are:

- Processed lawfully, fairly and in a transparent manner
- Collected only for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed
- Accurate and where necessary kept up to date
- Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed

- Processed in a manner that ensures its security using appropriate technical and organizational measures to protect against unauthorized or unlawful processing and against accidental loss, destruction or damage

5.2. Additionally, INA must ensure that:

- INA allows data subjects to exercise their rights in relation to their personal data

5.3. INA is responsible for, and must be able to demonstrate compliance with, all of the above principles.

6. **Lawfulness, fairness and transparency**

6.1. **Lawfulness and fairness**

6.1.1. In order to collect and process personal data for any specific purpose, INA Prime Solutions must always have a lawful basis for doing so. Without a lawful basis for processing, such processing will be unlawful and unfair and may also have an adverse impact on the affected data subjects. No data subject should be surprised to learn that their personal data has been collected, consulted, used or otherwise processed by INA.

6.1.2. Processing personal data will only be lawful where at least one of the following lawful bases applies:

- The data subject has given their consent for one or more specific purposes
- The processing is necessary for the performance of a contract to which the data subject is a party (for instance a contract of employment or registration with INA)
- To comply with INA's legal obligations
- To protect the vital interests of the data subject or another person (this will equate to a situation where the processing is necessary to protect the individual's life)
- To pursue INA's legitimate interests where those interests are not outweighed by the interests and rights of data subjects (only available to INA in some circumstances)

6.1.3. INA must identify and document the lawful basis relied upon by it in relation to the processing of personal data for each specific purpose or group of related purposes.

6.2. **Consent as a lawful basis for processing**

6.2.1. There is no hierarchy between the lawful bases for processing above, of which a data subject's consent is only one. Consent may not be the most appropriate lawful basis depending on the circumstances.

6.2.2. In order for a data subject's consent to be valid and provide a lawful basis for processing, it must be:

- specific (not given in respect of multiple unrelated purposes)
- informed (explained in plain and accessible language)
- unambiguous and given by a clear affirmative action (meaning opt-in: silence, inactivity or pre-ticked boxes will not be sufficient)
- separate and unbundled from any other terms and conditions provided to the data subject
- freely and genuinely given (there must not be any imbalance in the relationship between INA and the data subject and consent must not be a condition for the provision of any product or service)

6.2.3. A data subject must be able to withdraw their consent as easily as they gave it. Once consent has been given, it will need to be updated where INA wishes to process the personal data for a new purpose that is not compatible with the original purpose for which they were collected.

6.2.4. Unless INA is able to rely on another lawful basis for processing, a higher standard of explicit consent (where there can be no doubt that consent has been obtained, for example a signed document or a Yes/No option accompanied by clear consent wording) will usually be required to process special categories of personal data, for automated decision-making and for transferring personal data outside of the EEA (only applies to INA's European clients)

.

6.2.5. Where INA needs to process special categories of personal data, it will generally rely on another lawful basis that does not require explicit consent; however, INA must provide the data subject with a fair processing notice explaining such processing.

6.2.6. If INA is unable to demonstrate that it has obtained consent in accordance with the above requirements, it will not be able to rely upon such consent.

6.3. **Transparency**

6.3.1. The concept of transparency requires INA Prime Solutions to ensure that any information provided by INA to data subjects about how their personal data will be processed is concise, easily accessible, easy to understand and written in plain language. Where INA has not been transparent about how it processes personal data, this will call the lawfulness and fairness of the processing into question.

6.3.2. INA Prime Solutions can demonstrate transparency through providing data subjects with appropriate privacy notices or fair processing notices before it collects and processes their personal data and at appropriate times throughout the processing of their personal data.

6.3.3. A list of information must be contained in all privacy notices and fair processing notices, including the types of personal data collected; the purposes for which they will be processed; the lawful basis relied upon for such processing (in the case of legitimate interests, INA must explain what those interests are); the period for which they will be retained; who INA may share the personal data with; and, if INA intends to transfer personal data outside of the EEA (for INA's EEA clients).

6.2.4. Where INA obtains any personal data about a data subject from a third party (for example, resumes from recruitment agents for potential employees) it must check that it was collected on a lawful basis by the third party and where the sharing of the personal data with INA was clearly explained to the data subject.

7. **Purpose limitation**

7.1. INA Prime Solutions must only collect and process personal data for specified, explicit and legitimate purposes that have been communicated to data subjects before the personal data have been collected.

7.2. INA Prime Solutions must ensure that it does not process any personal data obtained for one or more specific purposes for a new purpose that is not compatible with the original purpose. Where INA intends to do so, it must inform the data subjects before using their personal data for the new purpose and, where the lawful basis relied upon for the original purpose was consent, obtain such consent again.

8. **Data minimization**

8.1. The personal data that INA Prime Solutions collects and processes must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed.

8.2. Staff must only process personal data when necessary for the performance of their duties and tasks and not for any other purposes. Accessing personal data that the staff are not authorized to access, or that they have no reason to access, may result in disciplinary action and in certain circumstances, may constitute a criminal offense.

8.3. Staff may only collect personal data as required for the performance of their duties and tasks and should not ask a data subject to provide more personal data than is strictly necessary for the intended purposes.

8.4. Staff must ensure that when personal data are no longer needed for the specific purposes for which they were collected, that such personal data are deleted, destroyed or anonymized.

8.5. Staff must observe and comply with INA 's Data Retention Policy.

9. **Accuracy**

9.1. The personal data that INA Prime Solutions collects and processes must be accurate and, where necessary, kept up-to-date and must be corrected or deleted without delay when INA discovers, or is notified, that the data are inaccurate.

9.2. Staff must ensure that they update all relevant records if they become aware that any personal data is inaccurate. Where appropriate, any inaccurate or out-of-date records should be deleted or destroyed.

10. **Storage limitation**

10.1. The personal data that INA Prime Solutions collects and processes must not be kept in a form that identifies a data subject for longer than is necessary in relation to the purposes for which it was collected (except in order to comply with any legal, accounting or reporting requirements).

10.2. Storing personal data for longer than necessary may increase the severity of a data breach and may also lead to increased costs associated with such storage.

10.3. INA will maintain policies and procedures to ensure that personal data are deleted, destroyed or anonymized after a reasonable period of time following expiry of the purposes for which they were collected.

10.4. Staff must regularly review any personal data processed by them in the performance of their duties and tasks to assess whether the purposes for which the data were collected have

expired. Where appropriate, staff must take all reasonable steps to delete or destroy any personal data that INA.

10.5. All privacy notices and fair processing notices must inform data subjects of the period for which their personal data will be stored or how such period will be determined.

10.6. Staff must observe and comply with INA 's Data Retention Policy.

11. Security, integrity and confidentiality

11.1. Security of personal data

11.1.1. The personal data that INA Prime Solutions collects and processes must be secured by appropriate technical and organizational measures against accidental loss, destruction or damage, and against unauthorized or unlawful processing.

11.1.2. INA will develop, implement and maintain appropriate technical and organizational measures for the processing of personal data taking into account the:

- nature, scope, context and purposes for such processing
- volume of personal data processed
- likelihood and severity of the risks of such processing for the rights of data subjects

11.1.3. INA will regularly evaluate and test the effectiveness of such measures to ensure that they are adequate and effective.

11.1.4. Staff are responsible for ensuring the security of the personal data processed by them in the performance of their duties and tasks. Staff must ensure that they follow all procedures that INA has put in place to maintain the security of personal data from collection to destruction.

11.1.5. Staff must ensure that the confidentiality, integrity and availability of personal data are maintained at all times:

- **Confidentiality:** means that only people who need to know and are authorized to process any personal data can access it
- **Integrity:** means that personal data must be accurate and suitable for the intended purposes
- **Availability:** means that those who need to access the personal data for authorized purposes are able to do so

11.1.6. Staff must ensure that they observe and comply with INA's "*Information security Policy*".

11.1.7. Staff must not attempt to circumvent any administrative, physical or technical measures INA has implemented as doing so may result in disciplinary action and in certain circumstances, may constitute a criminal offense.

11.2. **Reporting personal data breaches**

11.2.1. INA Prime Solutions has put in place appropriate procedures to deal with any personal data breach and will notify the data subjects where INA is legally required to do so.

11.2.2. If staff know or suspect that a personal data breach has occurred, they must contact the IT Department immediately to report it and obtain advice, and take all appropriate steps to preserve evidence relating to the breach.

12. **Sharing personal data**

12.1. Staff are not permitted to share personal data with third parties unless INA Prime Solutions has agreed to this in advance, and this has been communicated to the data subject in a privacy notice or fair processing notice beforehand. Where such a third party is processing the personal data on our behalf, INA has undertaken appropriate due diligence of such processor and entered into an agreement with the processor that complies with the necessary requirements for such agreements.

12.2. The transfer of any personal data to an unauthorized third party would constitute a breach of the lawfulness, fairness and transparency principle and, where caused by a security breach, would constitute a personal data breach. Staff must not share any personal data with third parties, including the use of freely available online and cloud services for work-related purposes, unless they are certain that the conditions outlined above apply. Staff need to seek advice from the IT Department or their direct manager, if they are unsure.

13. **Transfers outside of the European Economic Area (EEA) (for INA Prime Solutions' UK and European Clients)**

13.1. The GDPR (General Data Protection Regulation) prohibits the transfer of personal data outside of the EEA in most circumstances in order to ensure that personal data is not transferred to a country that does not provide the same level of protection for the rights of data subjects. In

this context, a “transfer” of personal data includes transmitting, sending, viewing or accessing personal data in or to a different country.

13.2. INA Prime Solutions may only transfer personal data outside of the EEA if one of the following conditions applies:

- the European Commission has issued an “adequacy decision” confirming that the country to which we propose transferring the personal data ensures an adequate level of protection for the rights and freedoms of data subjects (this applies to only a small number of countries)
- appropriate safeguards are in place, such as binding corporate rules, standard contractual clauses that have been approved by the European Commission
- the data subject has given their explicit consent to the proposed transfer, having been fully informed of any potential risks
- the transfer is necessary in order to perform a contract between INA and a data subject, for reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject in circumstances where the data subject is incapable of giving consent
- the transfer is necessary, in limited circumstances, for INA’s legitimate interests

13.3. Staff must ensure that they do not transfer any personal data outside of the EEA except in the circumstances set out above and provided that INA has agreed to this in advance.

14. **Data subject rights and requests**

14.1. Data subjects have a number of rights in relation to their personal data. These include:

- **Right to withdraw consent:** where the lawful basis relied upon by INA is the data subject’s consent, the right to withdraw such consent at any time without having to explain why
- **Right to be informed:** the right to be provided with certain information about how INA collects and processes the data subject’s personal data
- **Right of subject access:** the right to receive a copy of the personal data that INA holds, including certain information about how INA has processed the data subject’s personal data
- **Right to rectification:** the right to have inaccurate personal data corrected or incomplete dated completed
- **Right to erasure (right to be forgotten):** the right to ask INA to delete or destroy the data subject’s personal data if: the personal data are no longer necessary in relation to the purposes for which they were collected; the data subject has withdrawn their consent (where relevant); the data subject has objected to the processing; the

processing was unlawful; the personal data have to be deleted to comply with a legal obligation; the personal data were collected from a data subject under the age of 13, and they have reached the age of 13

- **Right to restrict processing:** the right to ask INA to restrict processing if: the data subject believes the personal data are inaccurate; the processing was unlawful and the data subject prefers restriction of processing over erasure; the personal data are no longer necessary in relation to the purposes for which they were collected but they are required to establish, exercise or defend a legal claim; the data subject has objected to the processing pending confirmation of whether INA's legitimate interests grounds for processing override those of the data subject
- **Right to data portability:** in limited circumstances, the right to receive or ask INA to transfer to a third party, a copy of the data subject's personal data in a structured, commonly-used machine-readable format
- **Right to object:** the right to object to processing where the lawful basis for processing communicated to the data subject was INA's legitimate interests and the data subject contests those interests
- **Right to object to direct marketing:** the right to request that we do not process the data subject's personal data for direct marketing purposes
- **Right to object to decisions based solely on automated processing (including profiling):** the right to object to decisions creating legal effects or significantly affecting the data subject which were made solely by automated means, including profiling, and the right to request human intervention
- **Right to be notified of a personal data breach:** the right to be notified of a personal data breach which is likely to result in a high risk to the data subject's rights or freedoms
- **Right to complain:** the right to make a complaint to an appropriate supervisory authority

14.2. Staff must be able to identify when a request has been made and must verify the identity of the individual making a request before complying with it. Staff should be wary of third parties deceiving them into providing personal data relating to a data subject without their authorisation.

14.3. Staff must immediately forward any request made by a data subject (even if they are uncertain whether it represents a request as set out above) to their manager. INA PRIME Solutions will only have 30 days to respond in most circumstances.

15. **Accountability and record-keeping**

15.1. INA Prime Solutions is responsible for and must be able to demonstrate compliance with the data protection principles and other obligations in order to protect the rights of data subjects.

15.2. INA Prime Solutions must ensure that it has adequate resources, systems and processes in place to demonstrate compliance with INA's obligations including:

- ensuring that at the time of deciding how INA will process personal data, and throughout its processing, implementing appropriate technical and organizational measures that are designed to ensure compliance with the data protection principles (known as 'Data Protection by Design')
- ensuring that, by default, only personal data that are necessary for each specific purpose are processed both in relation to the nature, extent and volume of such personal data, the period of storage and the accessibility of the personal data (known as 'Data Protection by Default')
- ensuring that where any intended processing presents a high risk to the rights and freedoms of data subjects, INA has carried out an assessment of those risks and is taking steps to mitigate those risks
- integrating data protection into INA's internal documents, privacy policies and fair processing notices
- regularly training INA staff on this policy and INA's related policies and procedures
- regularly testing the measures implemented by INA and conducting periodic reviews to assess the adequacy and effectiveness of this policy, and INA's related policies and procedures

15.3. Staff must ensure that they have undertaken the necessary training provided by INA and, where they are responsible for other members of staff, that they have done so.

15.4. Staff must further review all the systems and processes under their control to ensure that they are adequate and effective for the purposes of facilitating compliance with INA's obligations under this policy.

15.5. Staff must ensure that they observe and comply with all policies and guidance which form INA's Information Governance Framework.

16. **Direct marketing**

16.1. INA Prime Solutions is also subject to more specific rules in relation to direct marketing by email, fax, SMS or telephone.

16.2. INA Prime Solutions must ensure that it has appropriate consent from individuals to send them direct marketing communications, and that when a data subject exercises their right to object to direct marketing it has honored such requests promptly.

17. **Changes to this policy**

17.1. When amendments are made to this policy it is important that staff are notified and instructed to view the latest version.

18. **Policy Compliance**

18.1. INA Prime Solutions expects that all users will achieve compliance to the directives presented within this policy.

19. **Penalties**

19.1. Non-compliance is defined as any one or more of the following:

- Any breach of policy statements or controls listed in this policy
- Unauthorized changes to information
- Any person who knows of or suspects a breach of this policy must report the facts immediately to the IT Department or senior management.
- Any violation or non-compliance with this policy may be treated as serious misconduct.
- Penalties may include termination of employment or contractual arrangements, civil or criminal prosecution.

Schedule 1 – Glossary

consent	any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data about them

controller	the person or organization that determines the purposes and means of processing personal data
criminal convictions and offences	personal data relating to criminal convictions, the commission or alleged commission of an offence, proceedings for the commission or alleged commission of an offence and sentencing
data subject	an individual to whom personal data relates and who can be identified or is identifiable from personal data
Data Protection Officer (DPO)	a person required to be appointed in specific circumstances and who must have expert knowledge of data protection law and practice
explicit consent	a higher standard of consent that requires a very clear and specific statement rather than an action which is suggestive of consent
fair processing notices	a notice setting out information that must be provided to data subjects before collecting personal data from them, including notices aimed at a specific group of individuals or notices that are presented to a data subject on a 'just- in-time' basis (also known as 'privacy notice' or 'data protection notice')
personal data	any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes criminal convictions and offences data, special categories of personal data and pseudonymized personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour
personal data breach	a breach of security lead to the accidental or unlawful destruction, loss,

	alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed and which compromises the confidentiality, integrity, availability and/or security of the personal data
privacy notices	see fair processing notices above
process, processes, processing	any activity or set of activities which involves personal data including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or making available, alignment or combination, restriction, erasure or destruction
pseudonymized, pseudonymization	replacing information that directly or indirectly identifies an individual with one or more artificial identifiers (for example, a numerical identifier or other code) or pseudonyms so that the data subject cannot be identified without combining the identifier or pseudonym with other information which has been kept separately and securely. Personal data that have been pseudonymized is still treated as personal data (unlike personal data which has been anonymized)
staff	INA's agents, consultants, contractors, employees, and other representatives, including hourly paid staff holding a position of employment

Schedule 2 – Related Policies & Procedures

This Policy forms part of a broader Information Governance Framework with other policies, guidance and procedures listed here. Compliance with these is mandatory. Any breach of the requirements contained in these documents may result in disciplinary action.

Access Control Policy

Data Classification Policy

Data Retention Policy

Review and update of this document will take place when changes require revising the **Data Protection 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 Protection Policy. When approved a new version of the policy will be issued and all affected departments will be informed of the changes.