Data Protection Policy

International General Insurance Group (IGI)

September 2019

Authors		
Author	Department	Role
Reem Naouri	Compliance	Senior Compliance Officer
Raid Halaseh	Consulting	Consultant
Ownership		
Document Name	Department Owner	Email
Data Protection Policy	Data Compliance Officer (DCO)	Michael.Farah@iginsure.com

Contributors		
Contributors	Department	Role
Reem Naouri	Compliance Department	Senior Compliance Officer
Raid Halaseh	Consulting	Senior Consultant

Reviewers		
Reviewers	Department	Role
Michael Farah	Consulting Department	Senior Vice President
Rawan Alsulaiman	Legal Department	Chief Legal Officer - Company Secretary

Sign-off Authorities		
Sign-off Authorities	Date or reference of the meeting	Role
Board of Directors	6th March 2019	Board members
Group Audit Committee	12th March 2020	Board members

Classification		
Internal ☐	Public ☒	Confidential ☐

Version Tracking			
Version	Date	By whom?	Amendments
Version 1	24th May 2018	Reem Naouri	First issue at authorisation
Version 2	24th October 2018	Raid Halaseh	Annual review and cosmetic changes
Version 3	16th September 2020	Raid Halaseh	Addition of DIFC Data Protection Law

Distribution List			
Version	Date	To whom?	Other (Name & Company)
Version 1	24th May 2018	Public on IGI website	N/A
Version 2	13th March 2019	Public on IGI website	N/A
Version 2	7th February 2021	Public on IGI website	N/A

Change Mechanism

- Any requirement for change must be addressed to the authors.
- For documents with draft status, the authors may make changes at will.
- For documents with controlled status, changes must be approved by the Head of Department Owner.
- Any question, remarks or suggestions related to the present document should be addressed to Group Compliance at the following email address: data.privacy@iginsure.com

Table of Contents

1. Introduction and background

The purpose of this Policy is to outline how IGI has established measures to maintain compliance with the EU General Data Protection Regulation (hereinafter referred to as the "GDPR"), UK Data Protection Act. and the DIFC Data Protection Law. This policy is specific to IGI employees who are based in the UK, EU or UAE, goods or services offered to EU or UAE data subjects, and the processing and holding of personal data of data subjects residing in the EU or UAE.

The Policy contains two components:

- **Section 2.0:** measures to re-enforce accountability and governance; and
- **Section 3.0:** measures to demonstrate the protection of information rights of the data subject.

1.1. Policy principles

1.1.1. This policy requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR and DIFC Data Protection Law in order to safeguard the rights and freedoms of individuals; and

1.1.2. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. "The controller shall be responsible for, and be able to demonstrate, compliance with the principles".

2. Accountability and governance

This Policy outlines comprehensive but proportionate governance measures designed to achieve and maintain compliance with data protection laws. These measures have been designed to minimise the risk of breaches and uphold the protection of personal data.

This section on accountability and governance considers:

- **Roles and responsibilities:** the responsibilities of the Board, Data Compliance Officers (DCO), information owners and general employees;
- **Documentation:** IGI's requirements in respect of documenting processing;
- **Data protection by design and default:** IGI's requirements for Data Protection Impact Assessments (DPIA);

- **Lawful basis for processing:** IGI's Policy on determining the basis for processing;
- **Security:** "IT Security Policy" and "Information Security Policy" measures designed to protect information confidentiality, integrity and availability;
- **Contracts:** the measures that should be in place to ensure contractual relationships maintaining data protection compliance;
- **International transfer:** Oversight measures for international transfer of data; and
- **Data breaches:** Principles for detecting and responding to data breaches.
- **Compliance and report:** Ensure compliance and reporting with all data protection regulations IGI is implementing
- **Training and awareness:** IGI's plan for employee data protection training and awareness during a financial year
- **Consent withdrawal:** Procedures for data subjects to request consent withdrawals as required.
- **Validity of consents:** Appropriate and proportionate measures to assess the ongoing validity of the consent.

2.1. Roles and responsibilities

Background

2.1.1. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance. IGI has comprehensive but proportionate governance measures.

Policy requirements

2.1.2. IGI has defined Michael Farah as the Data Compliance Officer ("DCO"),.

2.1.3. The DCO's responsibilities include, but are not limited to:

- Informing and advising IGI and its employees about their obligations to comply with the GDPR, DIFC Data Protection Law and other data protection laws;
- Monitoring compliance with the data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits; and
- Acting as the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

2.1.4. The DCO reports to the Group and IGIUK Boards of Directors of the relevant entity on a quarterly basis.

2.1.5. The Board is to provide ongoing Governance framework for GDPR and DIFC Data Protection Law compliance. Reporting lines are put in place to ensure that summarised data protection compliance information is reported to the Executive and that the Board's ongoing support is demonstrable.

2.1.6. Any Data breach that happens within IGI is immediately escalated according to Appendix IV.

2.1.7. Employees are obligated to report any breach to the DCO of the Company or their line Manager as soon as they are aware of it.

2.2. Documentation

Background

2.2.1. The GDPR and DIFC Data Protection Law contains explicit provisions about documenting IGI's processing activities. IGI maintains records on processing purposes, data sharing and retention.

Policy requirement

2.2.2. Where IGI is a controller for personal data, IGI maintains documentation in a manner consistent with Article 30(1) of the GDPR and Article 15(1) of the DIFC Data Protection Law.

2.2.3. Where IGI is processor for personal data, IGI maintains documentation in a manner consistent with Article 30(2) of the GDPR and Article 15(2) of the DIFC Data Protection Law.

2.2.4. If IGI processes special category or criminal conviction and offence data, IGI documents:

- The condition for processing under the Data Protection Act;
- The lawful basis for processing; and
- Whether the personal data is erased and retained in accordance with IGI Data Retention Policy.

2.2.5. IGI conducts regular reviews of the personal data processed and updates documentation accordingly.

2.3. Data protection by design and default

Background

2.3.1. Under the GDPR and DIFC Data Protection Law , IGI has a general obligation to implement technical and organisational measures to show that IGI has considered and integrated data protection into processing activities.

Policy requirements

2.3.2. IGI carries out a DPIA found in Appendix III, when:

- Using new technologies; and
- The processing is likely to result in a high risk to the rights and freedoms of individuals.

2.3.3. Processing that is likely to result in a high risk includes (but is not limited to):

- Systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals; and
- Large scale processing of special categories of data or personal data relation to criminal convictions or offences. This includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms e.g. based on the sensitivity of the processing activity.

2.3.4. The decision of whether to conduct a DPIA is supported by a documented risk assessment and is endorsed by the DCO.

2.3.5. IGI shall consult the DIFC Commissioner where a data protection impact assessment under Article 20 indicates that, despite taking the measures referred to in Article 20(6)(e), the risks to the rights of Data Subjects remain particularly high and the Controller has already carried out or wishes to commence or continue carrying out a Processing activity.

2.4. Lawful basis for processing

Background

2.4.1. Under the GDPR and DIFC Data Protection Law, there are six available lawful bases for processing. IGI has documented the relevant lawful basis for processing and the purpose of that processing in its "Data Audit" that can be found in Appendix I.

2.4.2. The lawful bases for processing are set out in Article 6 of the GDPR and Article 10(1) and DIFC Data Protection Law. At least one of these must apply whenever IGI processes personal data:

- **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose;
- **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract;
- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations);
- **Vital interests:** the processing is necessary to protect someone's life;
- **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law; and
- **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Policy requirements

2.4.3. The lawful basis for processing must be considered and documented in line with the 'Data Audit' as detailed in Appendix I of this Policy.

2.4.4. With new systems or processes, IGI must determine the lawful basis and purpose of processing before beginning processing (usually as a part of the DPIA).

2.4.5. The IGI public privacy notice includes the lawful basis for processing as well as the purposes of the processing.

2.4.6. If IGI is processing special category or criminal offence data, both a lawful basis for processing and a special category condition for processing must be documented in the Data Audit document and DPIA. IGI should document both the lawful basis for processing and the special category condition to demonstrate compliance and accountability.

2.4.7. IGI obtains the consent of possible candidate to process the employment application through the website.

2.5. Security

Background

2.5.1. The data protection laws requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

Policy requirements

2.5.2. IGI has defined and implemented an "IT Security Policy" and "Information Security Policy" and supporting management system to maintain effective and proportionate security.

2.6. Contacts

Background

2.6.1. The data protection laws diligence and clarity in entering into third party relationships. Whether IGI is a processor or controller, there are mandatory requirements relating to the contracts that are in place

Policy requirements

2.6.2. Whenever IGI acts as a controller a written contract must be in place with the processors. Standards to be applied to the contracts as defined by the related regulators..

2.6.3. Whenever IGI acts as a processor, IGI must only act on the documented instructions of a controller (as specified in a valid written contract). Standards to be applied to the contracts as defined by the related regulators.

2.6.4. On an annual basis, the DCO will review third party relationships to determine the risk posed by processing. This will be documented in the "Third Party Processor List" maintained by Group Compliance.

2.6.5. Based on the review, the DCO will determine the most appropriate means to validate that contractual obligations in relation to data processing are being adhered to.

2.6.6. The DCO will present this revision, and the results of compliance visits, to the Board at least annually.

2.6.7. Banks provide financial services, therefore, the bank stands as data controller in relation to its personal customers and corporate clients /.

2.7. International transfers

Background

2.7.1. The GDPR and DIFC Data Protection Law imposes restrictions on the transfer of personal data outside the European Union and DIFC, to third countries or international organisations. These restrictions are in place to ensure that the level of protection is not undermined.

2.7.2. IGI may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. Adequate safeguards may be provided by:

- A legally binding agreement between public authorities or bodies;
- Standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- Standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
- Compliance with an approved code of conduct approved by a supervisory authority;
- Certification under an approved certification mechanism as provided for in the GDPR and DIFC Data Protection Law ;
- Contractual clauses agreed authorised by the competent supervisory authority; or
- Provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

2.7.3. When as asked by an Authority to provide data, exercise reasonable caution, and assess the impact the proposed transfer. Also try to get appropriate written and binding assurance from the requesting authority that it will respect the right of data subject

Policy requirements

2.7.4. Ad-hoc requests for international transfer of data must be submitted to the DCO once for each function, and type of document

2.7.5. Regular international data transfers are covered through internal Servicer Level Agreement that include contractual clauses safeguarding the transfer.

2.7.6. The DCO must record requests for international transfer received.

2.7.7. The DCO will consider the DPIA in relation to this transfer and the appropriate means of adopting safeguards.

2.8. Data breaches

Background

2.8.1. A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

2.8.2. Organisations will introduce a duty on all third parties to report certain types of data breach to the relevant supervisory authority. In some cases, organisations will also have to report certain types of data breach to the individuals affected.

Policy requirements

2.8.3. The DCO must be notified of all breaches to this Policy as soon as possible.

2.8.4. The DCO must record breaches and work with the information owner to consider the likely impact of the breach.

2.8.5. Where a breach is considered notifiable to the ICO and DFIC Commissioner, the DCO must immediately inform the Board.

2.8.6. A notifiable breach has to be reported by the DCO to the relevant supervisory authority within 72 hours of IGI becoming aware of it. The notification must contain:

- The nature of the personal data breach including, where possible;
- The categories and approximate number of individuals concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of the data protection or other contact point for more information;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

2.8.7. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, IGI will notify those concerned directly.

2.8.8. Group Compliance presents an analysis of breaches and near misses to the Board on a quarterly basis.

2.8.9. All employees must be trained to recognise, and escalate breaches.

2.8.10. A detailed Data Breach Procedure is found in Appendix IV.

2.9. Compliance and reporting

Background

2.9.1. Monitoring compliance with the Data Protection Policy is a key role of the DCO'. The DCO must also report compliance to the Board.

Policy requirements

2.9.2. The DCO is responsible for developing a compliance monitoring plan for this Policy.

2.9.3. The compliance monitoring plan should be submitted to the Board for approval at least annually.

2.9.4. Progress to deliver the plan, exceptions noted, breaches and near misses and updates on progress to address material deviations from compliance with the Policy must be reported by the DCO to the Board at least quarterly.

2.10. Training and awareness

Background

2.10.1. Employee awareness on data protection matters, and their role to protect the privacy of data subjects, is core to IGI's compliance programme.

Policy requirement

2.10.2. Employees must be trained on the requirements of this Policy at least annually through the annual Compliance Training and the induction training for new joiners.

2.11. Consent withdrawal

Background

2.11.1. As a data controller, IGI is responsible under the GDPR for administering withdrawal of consent from the data subject under advisement from the DCO

Policy requirement

2.11.2. Withdrawal of consent by the data subject means an indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies withdrawal of consent to the processing of personal data relating to him/her

2.11.3. IGI processes a data subjects consent withdrawal to the processing of his or her personal data once the Data Subject Consent Withdrawal Form is completed and can be found in Appendix VI. The completed form should be sent to data.privacy@iginsure.com.

2.11.4. The DCO will inform the relevant process owner of this change so that processing can be stopped.

2.11.5. The data subjects' rights to be erased also automatically applied when the data subject has withdrawn consent and no other conditions for processing apply

2.12. Validity of consents

Background

2.12.1. As per data protection laws, IGI implements appropriate and proportionate measures to assess the ongoing validity of the consent.

Policy requirement

2.12.2. Review consents to check that the relationship, the processing and the purposes have not changed.

3. Individual rights

The data protection laws provides the following rights for individuals:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erase;
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- Rights in relation to automated decision making and profiling.
- Non-discrimination

3.1. Right to be informed

Background

3.1.1. The right to be informed encompasses IGI's obligation to provide 'fair processing information', typically through a Privacy Notice.

Policy requirements

3.1.2. IGI maintains a Privacy Notice and publishes this publicly (Appendix II).

3.2. Right of access

Background

3.2.1. Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

3.2.2. Under the GDPR, individuals will have the right to obtain:

- Confirmation that their data is being processed;
- Access to their personal data; and
- Other supplementary information – this largely corresponds to the information that should be provided in a Privacy Notice.

Policy requirements

3.2.3. All requests from subjects for access to their data should be submitted to the DCO using the form under Appendix V. The DCO must log the request and will:

- Consider whether the request is manifestly unfounded or excessive;
- Request copies of information held from information owners within IGI;

- Review the information to ensure it does not impair the privacy of another data subject;
- Consider whether the request warrants a fee (if it requires a significant amount of data) and
- Respond to the original request.

3.2.4. A response to the request must be provided without delay and at the latest within one month of receipt. In the event the request is particularly complex or numerous, the period of compliance can be extended by a further two months. If this is the case, the DCO must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

3.2.5. Performance against the response target of one month must be reported to the Board by the DCO at least annually.

3.3. Right to rectification

Background

3.3.1. IGI gives individuals the right to have personal data rectified if it is inaccurate or incomplete.

Policy requirements

3.3.2. Requests for rectification must be treated in the same way as requests for access. The following, additional, measures will apply:

- If IGI has disclosed the personal data in question to third parties, the DCO must inform them of the rectification where possible;
- The DCO must also inform the individuals about the third parties to whom the data has been disclosed where appropriate;
- The information owner will be responsible for ensuring the request for rectification are actioned on the information they are responsible for; and
- The DCO will be responsible for validating whether requests for rectification have been properly addressed.

3.4. Right to be erased

Background

3.4.1. The right to erasure is also known as ‘the right to be forgotten’. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

3.4.2. The right to erasure does not provide an absolute ‘right to be forgotten’. Individuals have a right to have personal data erased and to prevent processing in specific circumstances. These include:

- 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 (i.e. otherwise in breach of the GDPR);
- The personal data must be erased in order to comply with a legal obligation; and
- The personal data is processed in relation to the offer of information society services to a child.

Policy requirements

3.4.3. IGI can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority;
- For public health purposes in the public interest;
- Archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- The exercise or defence of legal claims.

3.4.4. Requests for erasure of data should be submitted to the DCO and will follow the same principles as for right to access and right to rectification.

3.4.5. If IGI has disclosed the personal data in question to third parties, the DCO must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

3.5. Right to restrict processing

Background

3.5.1. Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, IGI is permitted to store the personal data, but not further process it.

3.5.2. IGI is required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, IGI should restrict the processing until IGI has verified the accuracy of the personal data;
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and IGI considers whether its legitimate grounds override those of the individual;
- When processing is unlawful, and the individual opposes erasure and requests restriction instead; or
- If IGI no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

Policy requirements

3.5.3. Requests to restrict processing will be submitted to the DCO and will follow the same principles as for right to access and right to rectification, with the following additional requirements:

- The DCO must inform individuals when IGI decides to lift a restriction on processing.

3.6. Right to data portability

Background

3.6.1. The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

3.6.2. The right to data portability applies:

- To personal data an individual has provided to a controller;
- Where the processing is based on the individual's consent or for the performance of a contract; and
- When processing is carried out by automated means.

Policy requirements

3.6.3. Requests for data under the right to data portability must be submitted to the DCO.

3.6.4. The DCO is responsible for recording these and requesting the information from the information owner(s).

3.6.5. The DCO will also review the data to ensure the privacy of other data subjects is not adversely impacted.

3.6.6. The DCO will provide the personal data in a structured, commonly used and machine readable form, submitted using a secure transfer mechanism.

3.6.7. The information will be provided within one month of the original request.

3.6.8. Performance against this timescale must be reported by the DCO to the Board at least annually.

3.7. Right to object

Background

3.7.1. Individuals have the right to object to:

- Processing for purposes of scientific/historical research and statistics.

Policy requirements

3.7.2. Requests that object to processing must be submitted to the DCO.

3.7.3. The DCO is responsible for recording and assessing these.

3.7.4. Where instructed by the DCO, IGI must immediately stop processing the personal data unless:

- There are demonstrable and compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defence of legal claims.

3.7.5. IGI must inform individuals of their right to object "at the point of first communication" and in its Privacy Notice (Appendix II).

3.8. Automated individual decision-making, including Profiling

Background

3.8.1. A Data Subject shall have the right to object to any decision based solely on automated Processing, including Profiling, which produces legal consequences concerning him or other seriously impactful consequences and to require such decision to be reviewed manual

Policy requirements

3.8.2. IGI does not conduct any automated processing including Profiling, which produces legal consequences concerning him or other seriously impactful consequence

3.9. Non-discrimination

Background

3.9.1. Under the DIFC Employment Law, unlawful discrimination against an employee is divided into three separate categories:

3.9.2. direct discrimination: less favourable treatment on one of the protected classes.

3.9.3. indirect discrimination: the application of neutral provisions, criteria or practices ("PCP") which put employees of a particular protected class at a disadvantage not faced by others who do not share that particular class. For example, a requirement for all staff to be on-site on a Friday lunchtime would disproportionately affect Muslims as Friday prayers take place at that time (salat al-jumu'ah).

3.9.4. harassment: unwanted treatment or conduct which has the purpose or effect of creating an intimidating, hostile, degrading, humiliating or offensive workplace.

Policy requirements

3.9.5. IGI does not tolerate discrimination of employees in any form

3.9.6. As part of the group HR manual, IGI has a grievance policy in place that aims to ensure that employees are treated justly and fairly

3.9.7. The group HR manual provides a detailed straightforward process for dealing with complaints of discrimination, sexual harassment, and vilification

3.9.8. Whistleblowing in place for any discrimination act reporting

Appendix I – Data Audit

Department	What personal data is being processed? (for each reason please fill all columns)			Why is personal data being processed?	Whose personal data is being processed?	When is this personal data being processed?			Where is the data kept?	
	Type	Source	Legal Basis			Originally when was it obtained	updated	Disclosure	Location	Country
Compliance	KYC Documents (KYC questionnaire that includes BOD info, company info, and shareholders info, address, phone number, contact email and name) financial Statements, registration certificates, licenses, organizational chart.	Broker (third party) /internet	legal obligation	legal obligations (due diligence) AML requirements)	Clients	Pre-binding the business, during the process.	Depending on the risk: high- every year medium - every 2 years Low - every 3 years.	NA	Company Servers	Jordan
	Personal information	Legal department/ individuals	legal obligation	legal obligation	Board of Directors	as needed	as required	NA	Company Servers	Jordan
	Employee CVs, Criminal records, passport copies, employment history	HR department / Employee	legal obligation - submission of information to the PRA	legal obligation - submission of information to the PRA	Employees	as needed	as required	PRA	Company Servers and physical files	Jordan
	Employee screening results (due diligence)	third party (Vero screening)	legal obligation - submission of information to the PRA	legal obligation - submission of information to the PRA	Employees	as needed	as required	PRA	Company Servers and physical files	Jordan

Department	What personal data is being processed? (for each reason please fill all columns)			Why is personal data being processed?	Whose personal data is being processed?	When is this personal data being processed?			Where is the data kept?	
	Type	Source	Legal Basis			Originally when was it obtained	updated	Disclosure	Location	Country
Underwriting	Part of our process is saving all emails in the shared folder which might include CVs for pilots, doctors and Engineers containing education and employment record and other personal info like address....etc. Teams are CC'd on KYC emails, content and feedback of how sensitive this is should be confirmed by compliance dept. Details of law case, claims record for doctors.	3rd party being assureds, brokers, insurers and reinsurers. Internet.	legitimate interest	Part of our process is saving all emails in the shared folder which might include such data, and for future reference. Provision of services	Clients being assureds, brokers, insurers and reinsurers.	Originally when slips are reviewed, and at request if reinsurance is required	As required	IGI staff, reinsurers. **In case of FAC, it could be shared with other brokers. If slip leader information could be sent to third parties as lawyers, loss adjusters, engineer**	Electronic records/ Emails and shared folders. IGI offices and info-fort (3rd party storage locations)	IGI offices in Amman, Dubai, Bermuda, London, Casablanca, Malaysia. Info-fort in Amman (we are not aware of such 3rd party facility if the same applies to IGI London)
HR IGI UK	Personal data, passport copies, CV's - education and employment records, references from former employers, pay data	Employee Files	Contractual	Legal obligations and duty of care	Employees	pre and post appointment	yes	Employees allowed access to own files upon request	Hard copy employee files in secure cabinets	UK
	Employee personal data - name, address, date of birth and pay information	Payroll supplier - MoorePay; Childcare Voucher Scheme, Benefits Broker - SecondSight - passed on to BUPA, UNUM and Aviva for employee insurances and pension purposes	Pay & Benefits - consensual	To enable employee benefits to be processed	Employees	pre and post appointment	yes as necessary		Third party systems	UK
	Employee personal data - no pay data	Vero Screening - pre employment checks, third party	Legal requirement (to check right to work) and best practice	For pre-employment checks and FCA checks where required	Employees pre joining	pre-appointment	no required		Third party systems	UK

Department	What personal data is being processed? (for each reason please fill all columns)			Why is personal data being processed?	Whose personal data is being processed?	When is this personal data being processed?			Where is the data kept?	
	Type	Source	Legal Basis			Originally when was it obtained	updated	Disclosure	Location	Country
HR IGI Group	Personal details name, address, email, telephone, date of birth, emergency contacts, CV's etc.	Employees	Legal obligation	Staff Administration	Current Staff	pre appointment	Regularly, when changes occurs	Dept. heads third parties	in-house systems, third party, electronic records, hardcopies	head offices and branches
	Financial details	company & employee	Legal obligation	Legal obligation / staff admin	Current Staff	pre-appointment	when changes occurs	Legal entities, banks Finance Dept. Insurance provider (third parties)	in-house systems, third party, electronic records, hardcopies	head offices and branches
	Medical and Life insurance information	Employees	Legal obligation / staff admin	Staff Administration	Current Staff	appointment	as required	medical and life insurance provider	in-house systems, third party, electronic records, hardcopies	head offices and branches
	Employee Photos	Employee	staff admin	Staff Administration	Current Staff	pre appointment	no update	medical and life insurance provider and IT Dept.	in-house systems, third party, electronic records, hardcopies	head offices and branches
	Employee Passports	Employees	Legal obligation / staff admin	Legal obligation / staff admin	Current Staff	pre appointment	When expired	residency or work permits, visa applications	in-house systems, third party, electronic records, hardcopies	head offices and branches
	National identifications	Employees	Legal obligation / staff admin	Legal obligation / staff admin	Current Staff	pre appointment	When expired	insurance provider Social Security dept. and third parties	in-house systems, third party, electronic records, hardcopies	head offices and branches
	Education and training info	Employees	staff admin	staff admin	Current Staff	pre appointment	as required	third party - ministry of labor	in-house systems, third party, electronic records, hardcopies	head offices and branches

Department	What personal data is being processed? (for each reason please fill all columns)			Why is personal data being processed?	Whose personal data is being processed?	When is this personal data being processed?			Where is the data kept?	
	Type	Source	Legal Basis			Originally when was it obtained	updated	Disclosure	Location	Country
	Social security number	Third parties or employee	Legal obligation	Legal obligation	Current Staff	pre appointment	no update	third parties	in-house systems, third party, electronic records, hardcopies	head offices and branches
	Employment details	Employees	Legal obligation / staff admin	legal obligation	Current Staff	pre appointment	as required	third party - ministry of labor	in-house systems, third party, electronic records, hardcopies	head offices and branches
	Work permits and residency cards	third party	Legal obligation / staff admin	Legal obligation / staff admin	Current Staff	Upon appointment	annual renewal	third party - ministry of labor	in-house systems, third party, electronic records, hardcopies	head offices and branches
Admin	Passport	individual employee	legitimate interest	Staff administration	employees	at request	as required	hotels & travel agent	electronic records	Jordan and London
Legal	Passports	individual	legitimate interest	legal obligations	Directors/ staff	pre appointment	as required	banks at request, internal use	electronic records	Jordan and London
	Personal Data	individual	legitimate interest	legal obligations	Shareholders/ Directors	pre appointment and at request	as required	internal use	electronic records	Jordan and London
	Financial Details	individual	legitimate interest	administration	Shareholders/ Directors	At request	as required	internal use	electronic records	Jordan and London
Claims	Personal Data of clients and experts i.e. qualifications/education/phone numbers/emails/addresses	Third party company's	legitimate interest	provisions of goods and services	third party experts for business contract/suppliers	at request	no	no	in house systems/electronic	Amman/London
	Personal information of medical history	clients/suppliers/third party experts	legitimate interest	Due diligence/provision of goods	Clients/business contacts	at request	no	no	in house systems/electronic	Amman/London

Appendix II – Privacy Notice

INTERNATIONAL GENERAL INSURANCE HOLDINGS LIMITED'S PRIVACY NOTICE

Introduction and background

The purpose of this Notice is to outline how IGI has established measures to protect your privacy and information rights. Please click on, Data Protection Policy, to view the full detailed Policy.

Your rights

We recognize that you have rights as a 'data subject', and that we have an obligation to uphold these.

This Privacy Notice aims to outline how we maintain these rights. In particular, it outlines:

- How we collect and process your information
- Why we do this
- How you can exercise your rights;
- Who to contact in the event you're unhappy with our performance.

Your information rights

Right	Explanation
Right to be informed	This encompasses the obligation for us to be transparent in how we collect and use your personal data.
Right of access	You have the right to access your personal data and supplementary information.
Right to rectification	If the information we hold on you is inaccurate or incomplete, you can request us to correct it.
Right to erasure	You can request we delete or remove personal data where there is no compelling reason for us to continue processing.
Right to restrict processing	You have the right to request we cease processing your data, if: • You consider it inaccurate or incomplete; • Where you object to processing and we are considering whether we still have a legitimate interest to process it; and • Where we don't need the data for the original reason we collected it, but may need it to support a legal claim.
Right to data portability	Where you have consented to the processing of your data, or where the processing is necessary for us to deliver a contract, you can request a copy of that data to be provided to a third party in electronic form.
Right to object	You have the right to object to our processing under certain circumstances.

This Privacy Notice should outline how we are transparent in our processing. Please get in touch with us through the 'contact details' section to find out more or to exercise your information rights.

Information we collect

Please find in the following link Data Protection Policy under Appendix 1.

Transfer of data

We may pass your personal data on to third-party service providers contracted with IGI in the course of dealing with you. Any third parties that we may share your data with are obliged to keep your details securely, and to use them only for the legitimate reasons they were obtained for originally. When they no longer need your data, they will dispose of IGI's procedures as set out in the contracts signed with them. If we wish to pass your sensitive personal data onto a third party we will only do so once we have obtained your consent, unless we are legally required to do otherwise.

Data transfers out of the EEA: The data we receive may be sent to countries outside the European Economic Area (EEA). When they do, there will be a contract in place to make sure the recipient protects the data to the same standard as the EEA. This may include following international frameworks for making data sharing secure.

Retention of data

IGI retains information in accordance with our data retention requirements. We may keep such information for as long as it is required in accordance with regulatory requirements. If you object to this retention, please contact us details provided in the 'Contact' section.

Securing your information

International General Insurance Group places great importance on the security of all personally identifiable information associated with our customers. We have security measures in place to attempt to protect against the loss, misuse and alteration of customer data under our control. While we cannot ensure or guarantee that loss, misuse or alteration of data will not occur, we use our best efforts to prevent this through implementing the following:

- IGI has achieved the Cyber Essentials accreditation;
- IT Security Policy and Procedures;
- IT Risk and Control Register;
- User login and accounts control, password complexity/history controls, patching, regular security updates for servers, network appliances and user machines;
- Physical protection of IGI Data Center and workplace, in addition to environmental monitoring and notification system;
- Latest generations of network firewalls with secure connection between IGI offices, network segmentations and DMZ network for internet facing services;
- Antivirus and E-mail protection system;
- Data classification and labeling;
- Removable storage blocking for user PCs;
- Hardware and software Vendor SLAs, signed NDA when required;
- Security Penetration testing and venerability assessment by a third party; and
- Backup data encryption.

Non-personal information

We may collect non-personal information about you such as the type of internet browsers you use or the Website from which you linked to our Website. You cannot be identified from this information and it is only used to assist us in providing an effective service on this Website. We may disclose aggregate statistics about our Website users to prospective partners, advertisers and other reputable third parties, but these statistics will include no personally identifying information.

Use of Cookies

Cookies are pieces of information that a Website transfers to your internet browsing device to store and sometimes track information about you. Most web browsers automatically accept cookies, but if you prefer, you can change your browser to prevent that. However, you may not be able to take full advantage of a website if you do so. Cookies are specific to the server that created them and cannot legally be accessed by other servers, which means they cannot be used to track your movements around the web. We use cookies to estimate our audience size and patterns; track preferences and improve and update our Website. Please see our cookies section on the cookies we use and how we use cookies.

Below is a full list of the cookies used by IGI along with a description of what they are used for. Where a cookie is a third party cookie, visit the providers' website for more information.

Cookie Name	Cookie Description
_ga / _gid / _gat	Google Analytics - Uses cookies to: • Determine which domain to measure; • Distinguish unique users; • Remember the number and time of previous visits; • Remember traffic source information; • Determine the start and end of a session; and • Remember the value of visitor-level custom variables.
__atuvc	This cookie is associated with the AddThis social sharing widget which is commonly embedded in websites to enable visitors to share content with a range of networking and sharing platforms. It stores an updated page share count.
__RequestVerificationToken	Used as an antiforgery token to protect form data.

Personal Data Breach

With regard to Personal Data Breach caused by IGI, IGI shall:

- In accordance with GDPR Article 33 and 34, (i) notify you without undue delay in the event of any Personal Data Breach involving Personal Data and (ii) provide reasonable assistance to you when you are required to communicate a Personal Data Breach to a Data Subject.
- Use reasonable efforts to identify the cause of such Personal Data Breach and take those steps as IGI deems reasonably practicable in order to remediate the cause of such Personal Data Breach.
- Provide reasonable assistance and cooperation as requested in the furtherance of any correction or remediation of any Personal Data Breach.

Complaints

In the event that you wish to make a complaint about how your personal data is being processed by IGI (or third parties as described in our Data Protection Policy), or how your complaint has been handled, you have the right to lodge a complaint directly with the supervisory authority and IGI's Data Compliance Officer (DCO) at data.privacy@iginsure.com.

Contact details

We recognize that you may have questions on how we process and/or store your data, or may want to change either the data we hold on you or how we communicate with you in the future.

If you have given consent for processing, you are free to withdraw that consent. To do so, please contact the DCO at data.privacy@iginsure.com.

If you have any questions in respect of this Notice, or would like to exercise your rights as a data subject (for example, to correct data or to exercise your right to access) please contact the DCO at data.privacy@iginsure.com.

If you are unhappy that we have responded to your query adequately, or if you have a further complaint, The Information Commissioner's Office can be contacted on 0303 123 1113 (local rate – calls to this number cost the same as calls to 01 or 02 numbers). If you're calling from outside the UK, you may not be able to use the 03 number, so please call +44 1625 545 700.

Other Websites

This Website contains links to other Websites and you may have linked to this Website from another Website. We are not responsible for the Privacy Notice or the content of such Websites. Other associated Websites to International General Insurance Holdings Ltd may contain a Privacy Notice that is different from this Privacy Notice. This Privacy Notice relates to this Website only. When visiting other associated Websites please make sure that you read their Privacy Notices so that you can understand what personal information will be collected through or in relation to that Website and for what purposes.

Appendix III – Data Protection Impact Assessment

1. Identify the need for a DPIA.

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
[text]

2. Describe the processing

2.1. Describe the nature of the processing

How will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?.
[text]

2.2. Describe the scope of the processing

What is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
[text]

2.3. Describe the context of the processing

What is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
[text]

2.4. Describe the purposes of the processing

What do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
[text]

3. Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
[text]

4. Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
[text]

5. Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

6. Identify Measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated reduced accepted	Low medium high	Yes/no

7. Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Appendix IV – Data Breach Procedure

Data breach response procedure

Purpose

This procedure applies to employees, temporary staff and contractors across IGI Group. This procedure applies to all types of personal data held in hard copy, electronic files, and IT systems.

Background

A data breach means:

- The loss of personal information (i.e. leaving documents containing personal information on a train);
- Access to personal information by an unauthorised individual; and
- Unauthorised disclosure of, personal information.

The GDPR, introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority (ICO) within 72 hours of becoming aware of the breach.

Failure to comply could result in IGI Group incurring significant financial penalties.

Procedure

Immediately after you discover a data breach, please follow these steps:

1. Notify your line manager;
2. Notify the Data Compliance Officer, Michael Farah, via insert email address at data.privacy@iginsure.com, or insert extension 270; and
3. Complete the Data Breach Form overleaf, as fully as possible and email to the DCO via the details above.

The DCO will make an assessment on the severity of the data breach, based on the information provided.

If the DCO deems that there has been significant risk to the data rights of individuals, DCO will;

1. Notify the relevant supervisory authority (ICO) – and outline next steps to remedy the breach and mitigate the risk of the breach reoccurring.
2. Notify the data subjects – and outline next steps to remedy the breach and mitigate the risk of the breach reoccurring.
3. Log the data breach on the IGI Group Data Breach Log.

This will ensure all the relevant details of the incident are recorded consistently and communicated on a need-to-know basis to relevant staff so that prompt and appropriate action can be taken to resolve the incident.

Data breach report form

Summary	
Description of the breach:	
Date:	
Your name:	

Detail	
Question	**Response**
How many data subjects (individuals) are impacted by the breach?	
What is the approximate number of personal data records concerned?	
Has 'special category' data been breached? ***(i.e. race, ethnic origin, religion, trade union membership, health, sexual orientation)***	
Has personal data been compromised?	
Have other policies been breached? ***(if relevant)***	
What is the impact and consequence of the personal data breach? ***(Is the breach likely to cause detriment to the data subject?)***	
What measures have been taken, or proposed to be taken, to deal with the personal data breach	

Outcome – To be completed by the DCO	
Based on the assessment of the responses to questions outlined above, there is a significant risk to the information rights of individuals.	Yes/No
DCO Signature:	
Date:	

Appendix V- Subject access request form

Data subject details

Title	Mr ☐	Mrs ☐	Miss ☐	Ms ☐	Other: ☐
Surname					
First name(s)					
Current address					
Telephone number:					
Home					
Work					
Mobile					
Email address					
Date of birth					
Details of identification provided to confirm name of data subject:					
Details of data requested:					

Details of person requesting the information (if not the data subject):

Are you acting on behalf of the data subject with their [written] or other legal authority?	Yes ☐ No ☐
If 'Yes' please state your relationship with the data subject (e.g. parent, legal guardian or solicitor)	
Please enclose proof that you are legally authorised to obtain this information.	

Title	Mr ☐	Mrs ☐	Miss ☐	Ms ☐	Other: ☐
Surname					
First name(s)					
Current address					
Telephone number:					
Home					
Work					
Mobile					
Email address					

Appendix VI – Consent withdrawal procedure

I, ……., withdraw my consent to process my personal data from International General Insurance. International General Insurance no longer has my consent to process my personal data for the purposes stated in my consent, which was previously granted.

Signed by data subject:

Date:

Request actioned by:

Date:

Signature”

This work instruction was approved by the DCO on …… and is stored on IGI GDPR folder maintained on its local servers.

Signature: Date:

Declaration

I, ……, the undersigned and the person identified in (1) above, hereby request that IGI provide me with the data about me identified above.

Signature: Date:

SAR form completed by (employee name):

I, ……, the undersigned and the person identified in (2) above, hereby request that IGI provide me with the data about the data subject identified in (1) above.

Signature: Date:

SAR form completed by (employee name):

This form must immediately be forwarded to IGI's Data Protection Officer / GDPR Owner.