INTERNATIONAL
ASSURANCE

DATA PROTECTION & PRIVACY POLICY

Suite C 208, La Croisette, Grand Baie, Mauritius | Office: +230 269 4400
Fax: +230 269 6400 | info@ialpcc.com | www.international-assurance.com

DATA PROTECTION AND PRIVACY INFORMATION

In its capacity as Data Controller, International Assurance Limited PCC ("IAL") is entitled to process the personal data of its stakeholders (customers, employees, shareholders, suppliers, trustees, internet users, etc.) in the ordinary management of existing relations and to acquire consent if necessary. Data processing for commercial purposes is not carried out.

Only personal data that are strictly necessary are processed both on paper and with the help of electronic instruments; some data may be essential and their lack may prevent the management of existing relations. Such data are processed by our employees in their capacity as Data Processors or Persons in charge of the processing; for some kinds of services we also avail ourselves of outsourcers which carry out technical, organisational and operational tasks on our behalf. Personal data are not subject to dissemination unless specifically provided for by the law.

All Data Subjects can exercise their rights of access and know what personal data are held by us, their origins and how they are used. They shall also be entitled to call for the data to be updated, rectified, supplemented or deleted, ask for them to be blocked or object to their processing, and require further information on the processing of personal data by contacting the Data Processor via customer.services@ialpcc.com.

Further information on the purposes, origin and type of processed data, scope of communication and their dissemination is provided in the following items, divided by purpose and category of Data Subjects.

CUSTOMERS AND POTENTIAL CUSTOMERS

Data processing purposes:

1. Marketing by the means of communication requested by customers and service quality surveys to improve the services provided and advertise the new services provided by the Company.

2. Analysis of the products and services requested by customers, even by electronic means, to identify IAL's customers real needs/preferences and improve our offer.

Data origin: personal data may be provided directly by Data Subjects and databases available to the public.

Processed data types: common personal data (contains; Verification of Identity, verification of address, tax information and source of funds/wealth and other data).

Scope of communication: personal data can be disclosed to entities that shall process customer data for the above purposes or other related purposes, such as agents, appointed financial advisors, outsourcers carrying out IT, computerised, administrative, tax authorities, regulators, governmental institutions and auditing services.

Scope of dissemination: The Company does not disseminate any personal data on its customers unless required by law.

Data Subjects are free to authorise the Company to process personal data for advertising purposes related to the Company, as well as to indicate the means of distance communication by which they prefer to be contacted (see point 1).

In addition, Data Subjects may authorise the Company to carry out the analysis of the products and services required, even by electronic means, to identify their real needs/preferences and improve the Company's offer (see point 2).

POLICYHOLDERS / INSURED PARTIES / BENEFICIARIES / FINANCIAL ADVISORS

Data processing purposes: to ensure the management of Life and Non-life insurance services, with particular reference to the establishment and drawing up of insurance and pension contracts, premium income, claim settlement or payment of insurance benefits, reinsurance, prevention and detection of insurance frauds and relevant legal proceedings, establishment exercise and protection of insurer's rights, fulfilment of specific legal and contractual obligations, internal audit and management, statistical activities.

Data origin: personal data may be provided directly by Data Subjects, their appointed financial advisors or other entities (e.g. individual or collective policyholders providing insured parties' and/or beneficiaries' personal data).

Processed data types: common personal (includes corporate) data (contains; Verification of Identity, verification of address, tax information and source of funds/wealth and other data), and sensitive and judicial data only when strictly necessary.

Scope of communication: personal data can be disclosed to entities belonging to the "insurance chain" (such as agents, financial advisors, insurance brokers, trustees, banks, stockbrokers and other channels negotiating insurance contracts; insurers, reinsurers, pension funds,

actuaries, lawyers and medical officers, technical consultants, insurance adjusters, healthcare facilities, claim settlement companies and other service providers, IAL Group Companies and outsourcers providing contract management services and IT, computerised, financial, administrative, archiving, mail management and auditing services, as well as companies specialised in market research and services quality surveys; entities related to the insurance sector (policyholders, insured parties, members, people who have their interest noted), insurers, reinsurers, trade associations and association bodies for which data communication is functional to provide the above services and to protect the rights of the insurance industry, institutional and public bodies to which data must be disclosed by law (available on request from IAL).

Scope of dissemination: the Company does not disseminate any personal data unless required by law.

DIRECTORS AND INTERNAL AUDITORS

Data processing purposes: to ensure the administrative and accounting management of existing relations and to fulfil any other obligations under contractual, regulatory and legislative, or provided by data protection and control Bodies and/or Authorities.

Data origin: common personal data (contains; Verification of Identity, verification of address and tax information and other data).

Processed data types: Verification of Identity, verification of address and tax information.

Scope of communication: personal data can be communicated to IAL Group companies and to other outsourcers carrying out IT, computerised, financial, Anti Money Laundering, administrative, archiving, mail printing, incoming and outgoing mail sorting and auditing services on the Company's behalf. It is also mandatory to communicate data to other public entities such as the Mauritius Revenue Authority, the Mauritius Data Protection Office, the US Internal Revenue Service's Foreign Account Tax Compliance Act (FATCA) and the Mauritius Financial Services Commission.

Scope of dissemination: personal data may be disseminated in fulfilment of obligations under regulations and legislation, or upon request of data protection and control Bodies and/or Authorities.

SHAREHOLDERS

Data processing purposes: to manage - also from an administrative viewpoint - the relation resulting from the purchase and/or subscription of the Company's shares and to fulfil any other obligations under regulations and legislation, or provided by data protection and control Bodies and/or Authorities.

Data origin: personal data may be provided directly by Data Subjects or other entities (e.g. custodian banks).

Processed data types: common personal data (contains; Verification of Identity, verification of address and tax information and other data).

Scope of communication: personal data can be communicated to the IAL Group companies and to other outsourcers carrying out IT, computerised, financial, Anti Money Laundering, administrative, archiving, mail printing, incoming and outgoing mail sorting, auditing and meeting management services on the Company's behalf. Data communication is also mandatory to public entities such as data protection and control Bodies and/or Authorities, Financial Administration and Judicial Authority.

Scope of dissemination: personal data may be disseminated in fulfilment of an obligation under regulations and legislation, or upon request of data protection and control Bodies and/or Authorities.

INTERNET USERS AND COOKIES

Data processing purposes: ensure the proper functioning of the website, improve customers and potential customers' browsing experience and provide customers with a service in line with their preferences. IAL does not use cookies for commercial profiling.

Data origin: passive collection of the internet Users' information (cookies) stored in their browsers.

Processed data types: common personal data (cookies belonging to the websites' Data Controller or third party).

Scope of communication: cookies stored in users' terminal are used directly by the Data Controller of the website and by Data Controllers of third party's websites that have installed them for the same purposes listed above or other related purposes.

Scope of dissemination: the Company does not disseminate any personal data.

SUPPLIERS AND PROFESSIONALS

Data processing purposes: to ensure the administrative and accounting management of existing relations and to fulfil any obligations under regulations and legislation, or provided by data protection and control Bodies and/or Authorities.

Data origin: personal data may be provided directly by Data Subjects or other entities (e.g. sector databases, Internet, relevant professional bodies etc.).

Processed data types: common personal (includes corporate) data.

Scope of communication: personal data can be communicated to IAL Group companies and to other outsourcers carrying out administrative, IT, computerised, financial, archiving, mail printing, incoming and outgoing mail sorting and auditing services on our behalf. It is also mandatory to communicate data to other public entities such the Mauritius Revenue Authority, the Mauritius Data Protection Office, the US Internal Revenue Service's Foreign Account Tax Compliance Act (FATCA) and the Mauritius Financial Services Commission.

Scope of dissemination: the Company does not disseminate any personal data unless required by law.

COUNTERPARTIES AND LAWYERS

Data processing purposes: to allow for the management of insurance contracts (with specific reference to claim settlement, prevention and identification of frauds and relevant legal proceedings), and to fulfil administrative/accounting obligations within the relation as a collaborator between policyholders and lives assured.

Data origin: personal data may be provided directly by Data Subjects or other entities (e.g. life assured if different to the policyholder).

Processed data types: common personal (includes corporate) data.

Scope of communication: personal data can be communicated to IAL Group companies and to other outsourcers carrying out administrative, IT, computerised, financial, archiving, mail printing, incoming and outgoing mail sorting and auditing services on the Company's behalf.

Data may also be communicated to IAL Group companies for the prevention and identification of insurance frauds; by law or regulation some data may be communicated to the Mauritius Revenue Authority, the Mauritius Data Protection Office, the US Internal Revenue Service's Foreign Account Tax Compliance Act (FATCA) and the Mauritius Financial Services Commission.

Scope of dissemination: the Company does not disseminate any personal data unless required by law.

PROFESSIONAL – INSURANCE ADJUSTERS AND TRUSTEES

Data processing purposes: to ensure the management of existing relationships with our Company as collaborators also from an administrative and accounting point of view, and to fulfil any obligations under regulations and legislation, or provided by data protection and control Bodies and/or Authorities.

Data origin: personal data may be provided directly by Data Subjects or other entities (e.g. sector databases, Internet, relevant professional bodies etc.).

Processed data types: common personal (includes corporate) data (contains; Corporate, Trust and Statutory documents, Verification of Identity, verification of address and tax information and other data).

Scope of communication: personal data can be communicated to entities included in the so-called "insurance chain": agents, financial advisors, insurance brokers; insurers, reinsurers; lawyers, insurance adjusters and health facilities. Such data can also be communicated to IAL Group companies and to other outsourcers carrying out claim management, claim settlement, administrative, IT, computerised, financial, archiving, mail printing, incoming and outgoing mail sorting and auditing services on the Company's behalf. It is also mandatory to communicate data to other public entities such as the Mauritius Revenue Authority, the Mauritius Data Protection Office, the US Internal Revenue Service's Foreign Account Tax Compliance Act (FATCA) and the Mauritius Financial Services Commission.

Scope of dissemination: the Company does not disseminate any personal data unless required by law.

WITNESSES

Data processing purposes: to ensure claims management (with particular reference to claims settlement, prevention and identification of insurance frauds and related legal actions) and to fulfil any other obligations under Mauritius rules and regulations or provided by data protection and control Bodies and/or Authorities.

Data origin: personal data may be provided directly by Data Subjects or other entities (e.g. life assured)

Processed data types: common personal and judicial data if necessary.

Scope of communication: personal data can be communicated to subjects belonging to the so-called "insurance chain": policy holders, agents, financial advisors, insurance brokers, insurers and reinsurers; legal and medical advisers, technical advisers, insurance adjusters.

Such data can be also communicated to IAL Group Companies and other outsourced service companies carrying out claims settlement and management, IT, computerised, financial, archiving, mail printing, incoming and outgoing mail sorting and auditing services on our behalf. Data may also be communicated to IAL Group companies for the prevention and identification of insurance frauds.

Some data may be communicated to institutional bodies such as the Judicial Authority, police forces by law or regulatory bodies.

Scope of dissemination: the Company does not disseminate any personal data.

EMPLOYEES

Please refer to the section called "Privacy" published on the corporate Intranet.

POLICIES AND SECURITY

IAL, acting as Data Controller, attaches utmost importance to confidentiality, protection and safety of information, particularly personal data concerning the Company's customers, potential customers and other people who get in contact with the Company.

This section outlines the methods used to administer the Company's website with regard to the processing of users' personal data. This information is also provided to subjects interacting with the services provided over the Internet by IAL (the Data Controller).

For this reason, internet surfers are invited to preliminarily visit the Company's Data Protection and Privacy Policy, which give an overview of the Company's guidelines on protection of personal data.

Information is provided for and applies to IAL websites only. It is not applicable to any other website linked to the IAL site.

Surfers are required to provide personal data only if they want to get in contact with or contract with IAL. In such cases - totally voluntary - surfers are required to read the Information as established by the Law and to provide only data strictly necessary to handle their requests.

In compliance with the existing data protection legislation, IAL have adopted a specific policy, as described in the IAL data protection and privacy policy information section above.

Surfers browsing IAL's website are not required to provide any personal data. However, as the technology used by the Company stores data concerning tools employed by users, which help track the latter.

On request IAL will provide useful information on the methods of active and passive collection of information concerning subjects/means interacting with its website, as well as on the security measures taken by the Company.

While surfing a website, it is technically possible to collect data even without a user's explicit registration to the service or without the user's active role. This type of collection is called "passive data collection".
The use of IP addresses, cookies and other session identifiers, internet tags, and surfing data, including the possibility to exclude them and their implications, are shown below.

RECRUITMENT AND HIRING

The Company's primary goal when recruiting new employees is to fill vacancies with persons who have the best available skills, abilities, or experience needed to perform the work. Decisions regarding the recruitment, selection, and placement of employees are made on the basis of job-related criteria.

When positions become available, qualified current employees are encouraged and are welcome to apply for the position. As openings occur, notices relating general information about the position are posted. The manager of the department with the opening will arrange interviews with employees who apply.

We encourage current employees to recruit new talent for our Company.

As regards the passive data collection:

- the Company's website does not use IP address (Internet Protocol Addresses) to collect information. However, IP addresses are stored as surfing data;
- the Company's website uses surfing data as aggregate data for statistical purposes only;
- the Company's website uses its own and third parties' cookies and other session identifiers (technical and profiling). Technical cookies are used in order to make surfing possible or provide a service requested by the user. For these purposes consent is not required. Third parties' profiling cookies are not used for statistical purposes - in anonymous form or not - in order to provide users a service in line with their preferences. The cookies for commercial profiling are not used. It is possible to disable the use of cookies depending on the browser, even though in this case surfing may not be equally easy;
- the Company's website does not use Internet tags.

As regards the active data collection - if previewed - it is worth the following policy:

- E-Mail: Data received by e-mails sent via the Company's website is used to reply to requests only. This data is stored for statistical purposes only and to check whether there are any precedents.
- Names may be included in specific Mailing Lists only if expressly requested by Surfers wishing to receive certain documents (product literature, newsletters, etc.) on a periodical basis.
- Registration: To access a number of services, Surfers are required to fill in a specific form. This information is used to reply to the sender's request and to provide requested services only.

IAL process personal data concerning third parties - insured people, real and potential customers, collaborators, etc. IAL have always taken all necessary steps to guarantee data confidentiality and security, in line with new technological developments, particularly in the field of computer technology.

Pursuant to the existing personal data protection legislation, IAL have adopted their own data protection and privacy policy which is based on the following points:

- The Data Controller is the Company, which has appointed a person in charge of the implementation of the data protection legislation at corporate level;
- Compliance Department has been appointed "the department responsible for replying to Data Subjects in the event they exercise their rights under the Data Protection Act 2017". Data Subjects may apply to the Compliance Department to exercise their rights of access and obtain any further information on data protection and privacy;
- Data Processors have been appointed to guarantee compliance with legislation;
- Those who process personal data are referred to as "Persons in charge of the processing". They have been provided with specific instructions, processes and benefit from an ongoing training programme;
- Due to specific technical and organisational requirements, the Company avails itself of third parties who are responsible for parts of the process. They may act in their capacity as "Persons in charge of the processing", or "Data Processors" of the Company, or operate autonomously as "Data Controllers" of subsequent processing having the same purposes as the Company.

The Company can only access personal information as is strictly necessary to perform specific services or for the purposes for which such information has been collected by providing the specific Information (i.e.: on contracts for Life and for Non-life business). Particular importance is attached to sensitive data, which is processed only after having ascertained that processing of such data in anonymous form (on a case by case basis) is not possible.

The Company shall process all personal information by taking all necessary physical and IT security measures, in accordance with the arrangements laid down in the Data Protection Act 2017 and any regulations thereto attached.

At the end of the processing, the Company shall store processed data and, if such obligation does not exist or if such term has elapsed, shall erase or anonymise the data.

Data Subjects may apply to the Company and its Compliance Department for any information on personal data, namely:

- to obtain confirmation as to whether or not personal data concerning him/her exists and communication of such data in intelligible form;
- to be informed of the source of the personal data, of the purposes and methods of the processing and of the logic applied to the processing if the latter is carried out thanks to electronic means;
- to obtain a list of the entities or categories of entity to whom or which the personal data may be communicated and who may get to know said data in their capacity as data processor(s) or person(s) in charge of the processing;
- to require the updating or rectification of the processed data, and erasure, anonymisation or blocking of data that has been processed unlawfully;
- to object, in whole or in part, to the processing of personal data concerning him/her on legitimate grounds or for commercial purposes.

Data Subjects request for information on his/her personal data will be logged in the Company's register per Schedule 1 of this policy.

Should the Data Subject no be fully satisfied, the Data Subject has the right to complain via our website. A complaints policy is also on the Website to guide Data Subjects. All complaints will be registered in the Company's register per Schedule 3.

GLOSSARY

'**Processing'** shall mean any operation, or set of operations, carried out with or without the help of electronic or automated means, concerning the collection, recording, organisation, keeping, interrogation, elaboration, modification, selection, retrieval, comparison, utilization, interconnection, blocking, communication, dissemination, erasure and destruction of data, whether the latter are contained or not in a database.

'Personal data' shall mean any information relating to natural persons that are or can be identified, even indirectly, by reference to any other information including a natural person's name (as well as any former names, any other names used and other aliases), their current residential address, date and place of birth, nationality and any occupation, public position held and where appropriate the name of the employer. Personal data shall also include documentation obtained and retained to verify the information provided by natural persons.

'**Corporate data'** shall mean any information relating to legal persons (bodies corporate, partnerships, associations or any other body of persons other than legal arrangements) that are or can be identified, even indirectly, by reference to any other information including a legal person's name, incorporation number, date and country of incorporation or registration, registered office address and principal place of business, the legal status of the legal person. Corporate data shall also include documentation obtained and retained to verify the information provided by legal persons.

'Sensitive data' shall mean personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade-unionist character, as well as personal data disclosing health and sex life.

'**Judicial data'** shall mean personal data disclosing the criminal records, administrative sanctions and the relevant current charges, or the status of being either defendant or the subject of criminal investigations.

'Data controller' shall mean any natural or legal person, public administration, body, association or other entity that is competent, also jointly with another data controller, to determine purposes and methods of the processing of personal data and the relevant means, including security matters.

'Data processor' shall mean any natural or legal person, public administration, body, association or other agency that processes personal data on the controller's behalf.

'Persons in charge of the processing" shall mean the natural persons that have been authorised by the data controller or processor to carry out processing operations.

'Information to Data Subjects' The Data Subject as well as any entity from whom or which personal data are collected shall be preliminarily informed, either orally or in writing, as to:

a. the purposes and modalities of the processing for which the data are intended;
b. the obligatory or voluntary nature of providing the requested data;
c. the consequences if (s)he fails to reply;
d. the entities or categories of entity to whom or which the data may be communicated, or who/which may get to know the data in their capacity as data processors or persons in charge of the processing, and the scope of dissemination of said data;
e. the rights of Data Subjects as per the Data Protection Act 2017;
f. the identification data concerning the data controller and, where designated, the data controller's representative. If several data processors have been designated by the data controller, at least one among them shall be referred to and the mechanisms for easily accessing the updated list of data processors shall be specified.

'Data Subject' shall mean any natural person that is the subject of the personal data.

"Right to Access Personal Data and other Rights"

A Data Subject shall have the right to obtain confirmation as to whether or not personal data concerning him exist, regardless of their being already recorded, and communication of such data in intelligible form.

a. A Data Subject shall have the right to be informed:
b. of the source of the personal data;
    a. of the purposes and methods of the processing;
    b. of the logic applied to the processing, if the latter is carried out with the help of electronic means;
    c. of the identification data concerning data controllers, data processors and the representative designated;
    d. of the entities or categories of entity to whom or which the personal data may be communicated and who or which may get to know said data in their capacity as designated representative(s) in the State's territory, data processor(s) or person(s) in charge of the processing.

c. A Data Subject shall have the right to obtain:
d. updating, rectification or, where interested therein, integration of the data;
e. erasure, anonymisation or blocking of data that have been processed unlawfully, including data whose retention is unnecessary for the purposes for which they have been collected or subsequently processed;
f. certification to the effect that the operations as per letters a) and b) have been notified, as also related to their contents, to the entities to whom or which the data were communicated or disseminated, unless this requirement proves impossible or involves a manifestly disproportionate effort compared with the right that is to be protected.

g. A Data Subject shall have the right to object, in whole or in part:
h. on legitimate grounds, to the processing of personal data concerning him/her, even though they are relevant to the purpose of the collection;
i. to the processing of personal data concerning him/her, where it is carried out for the purpose of sending advertising materials or direct selling or else for the performance of market or commercial communication surveys.

"Consent" Processing of personal data by private entities shall only be allowed if the Data Subject gives his/her express consent. The Data Subject's consent may refer either to the processing as a whole or to one or more of the operations thereof. The Data Subject's consent shall only be deemed to be effective if it is given freely and specifically with regard to a clearly identified processing operation, if it is documented in writing, and if the Data Subject has been provided with the necessary information. Consent shall be given in writing if the processing concerns sensitive data.

'Communication' shall mean disclosing personal data to one or more identified entities other than the Data Subject, the data controller's representative in the State's territory, the data processor and persons in charge of the processing in any form whatsoever, including by making available or interrogating such data.

'Dissemination' shall mean disclosing personal data to unidentified entities, in any form whatsoever, including by making available or interrogating such data.

'Outsourcer' shall mean any external supplier entrusted with the Company's activities and processes.

DATA BREACH

IAL while having procedures in place to ensure that Data is secured for each Data Subject, acknowledges that personal data breaches may occur.

a. In the case of a personal data breach, the Data Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the data breach to the Commissioner.

b. The notification referred to above shall –

- describe the nature of the personal data breach, including where possible, the categories and approximate number of Data Subjects and the categories and approximate number of data records concerned;
- communicate the name and contact details of any appropriate Data Protection Officer or other contact point where more information may be obtained; and
- recommend measures to address the data breach, including, where appropriate, measures to mitigate the possible adverse effects of the breach.

c. The Data Controller shall specify the facts relating to the data breach, its effects and the remedial action taken so as to enable the Commissioner to verify compliance with the Data Protection Act 2017.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of a Data Subject, the Data Controller shall, after the notification referred to above, communicate the data breach to the Data Subject without undue delay.

The communication to the Data Subject shall describe in clear language the nature of the data breach and set out the information and the recommendations provided above.

The communication of a personal data breach to the Data Subject shall not be required where –

a. the Data Controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the data affected by the breach, in particular, those that render the data unintelligible to any person who is not authorised to access it, such as encryption;
b. the Data Controller has taken subsequent measures to ensure that the high risk to the rights and freedoms of the Data Subject referred to above is no longer likely to materialise; or
c. it would involve disproportionate effort and the Data Controller has made a public communication or similar measure whereby the Data Subject is informed in an equally effective manner.

Where the Data Controller has not already communicated the personal data breach to the Data Subject, the Commissioner may, after having considered the likelihood of the data breach resulting in a high risk, require it to do so.

Records of any breach will be kept in IAL's Register of Breaches per Schedule 2 of this policy.

DUTY TO DESTROY DATA

Pursuant to the Financial Service Act 2007, IAL has an obligation keep data for a period of at least 7 years after the completion of the transaction to which it relates.

Where the purpose for keeping personal (including corporate) data has lapsed, IAL shall –

a. destroy the data as soon as is reasonably practicable; and
b. notify any processor holding the data.

Any processor who receives notification under Rights to Access Personal Data above shall, as soon as is reasonably practicable, destroy the data specified by the Data Controller.

SCHEDULE 1: REGISTER OF DATA REQUEST

INTERNATIONAL ASSURANCE LIMITED PCC									
Register of Data Requests									
Date of Initial Request	Team Member Assigned	Name of Client and IW Number	Details of request	Date of Acknoledgement	Details of Response to Data Subject	Date of Response	Data request Resolved	Data Officer Sign Off	Comments

SCHEDULE 2: REGISTER OF BREACH TO DATA SUBJECT

INTERNATIONAL ASSURANCE LIMITED PCC								
Register of Breach to Data Subject								
Date of Initial Breach	Details of the Breach	Name of Client and IW Number	Date of Disclosure of Breach to Data Subject	Date of Disclosure of Breach to Commissioner	Details of Response from Data Subject	Data Breach Resolved	Data Officer Sign Off	Comments

SCHEDULE 3: COMPLAINTS LOG

INTERNATIONAL ASSURANCE LIMITED PCC										
Complaints Log										
Date of Initial Complaint	Date Complaint Received	Team Member Assigned	Name of Client and IW Number	Details of Complaint	Date of Acknowledgement	Details of Response to Client	Date of Response	Complaint Resolved	Complaints Officer Sign Off	Comments