



Effective date: 1 January 2021

GUIDELINES FOR INSURANCE COMPANIES AND TAKAFUL OPERATORS
NOTICE NO. TIU/G-1/2020/11

GUIDELINES ON ONLINE DISTRIBUTION



1. INTRODUCTION

- 1.1. These Guidelines are issued pursuant to Section 88 of the Insurance Order, 2006 and section 90 of the Takaful Order, 2008 [“the Orders”] to provide guidance on the Notice No. TIU/N-1/2019/11 “Notice on Application for approval of Outsourcing arrangement for Insurance Companies and Takaful operators”, and to set standards for sound practices on risk management of material outsourcing arrangements. The extent and degree to which an insurer implements the Guidelines should be commensurate with the nature of risks in, and materiality of, the outsourcing arrangement.
- 1.2. These Guidelines shall be read in conjunction with the following:
 - 1.2.1. Insurance Order, 2006;
 - 1.2.2. Takaful Order, 2008;
 - 1.2.3. Notice on Corporate Governance for Insurance Companies and Takaful Operators [Notice No. TIU/N-3/2017/7];
 - 1.2.4. Notice on Early Detection of Cyber Intrusion and Incident Reporting [Notice No. FTU/N-1/2017/1];
 - 1.2.5. Notice for the Establishment of a Complaints Handling Function within Financial Institutions [Notice No. FCIU/N1/2017/1];
 - 1.2.6. Guidelines on Product Transparency and Disclosure [Guidelines No. FCI/G4/2019/1 and FCI/G5/2019/1];
 - 1.2.7. Guidelines on Outsourcing Arrangement for Insurance Companies and Takaful Operators [Guidelines No. TIU/G-1/2019/10];
 - 1.2.8. Guidelines on Risk Management and Internal Controls for Insurance Companies and Takaful Operators [Guidelines No. TIU/G-3/2018/8]; and
 - 1.2.9. Any other notices, directives or guidelines, which the Authority may issue from time to time.
- 1.3. These Guidelines do not apply to the following:
 - 1.3.1. Use of e-mail via an internet provider between the insurer and its customer on an ad-hoc basis for general enquiries only, for example, inquiry on status of policy and clarification on terms and conditions of the policy; and
 - 1.3.2. Use of e-mail via an internet provider within the company, for example between the insurer and its head office and branches, as well as between the insurer and its related parties, such as reinsurers, brokers and agents, which does not involve transmission of



files containing customers' information.

1.4. These Guidelines take effect on 1 January 2021.

2. DEFINITIONS

2.1 For the purpose of these Guidelines:

- 2.1.1. "Complaints handling function" have the same meaning with Notice No. FCIU/N1/2017/1;
- 2.1.2. "Insurance" includes takaful;
- 2.1.3. "Insurer" means a registered insurance company under Insurance Order, 2006 and a registered takaful operator under Takaful Order, 2008, unless it is otherwise specified;
- 2.1.4. "Intermediary" refers to insurance agents and brokers registered under Insurance Order, 2006 or Takaful Order, 2008, unless otherwise specified;
- 2.1.5. "Online direct channel" refers to any web portal or application on the internet created, developed and maintained or operated by any insurer or intermediary on which a client may purchase an insurance policy;
- 2.1.6. "Online insurance services" refers to the use of the internet as a channel to conduct insurance business transactions with customers and/or a platform for transmission of customers' information. Such services include, but is not limited to, the following:
 - a) Displaying information about the insurers, intermediaries and their insurance products or services;
 - b) Advising existing or potential policyholders on the terms of their insurance policies, their insurance needs, etc.;
 - c) Quoting and comparing insurance premiums and terms for a particular type of insurance product offered by one or more insurers;
 - d) Obtaining clients' personal information with an aim to providing insurance services to them;
 - e) Collecting insurance premiums;
 - f) Issuing or renewing insurance policies;
 - g) Providing a channel for policyholders to make enquiries, update personal information or report claims;



- h) Handling complaints or insurance matters; and
- i) Making refunds, reimbursements or claims payments to policyholders;

2.1.7 “Service provider” has the meaning ascribed to it in the Notice on Application for Approval of Outsourcing Arrangement for Insurance Companies and Takaful Operators (Notice No. TIU/N-1/2019/11); and

2.1.8. “Third party website” refers to any person that provides services on behalf of the insurer to conduct online insurance services on its website.

3. ONLINE INFORMATION

3.1 An insurer or intermediary should explicitly provide information about itself on its own online direct channel, or, if applicable, on the third party’s website(s) through which it provides online insurance services.

3.2 An insurer or intermediary should provide contact information including its full name, office address, e-mail address, and telephone number on its online direct channel.

4. TYPES OF ONLINE DIRECT CHANNEL

4.1 Online direct channels that fall under these Guidelines may be categorised into three [3] types:

4.1.1. Information-based website, which provides predefined publicly available marketing information about the insurer, such as products and services offered:

- a) Policyholders may be able to make monologue e-mail contact with the insurer;
- b) Products offered on information-based websites should not include commissions to agents, bancassurance/bancatakaful or financial advisers in the pricing of any product;

4.1.2. Interactive-based website, which should permit transactions to be carried out that may or may not involve online payments, such as soliciting insurance proposals, purchasing and renewing policies, etc.; and

4.1.3. Mobile applications, which should be able to perform the same functions stated in paragraphs 4.1.1 and 4.1.2.

5. THIRD PARTY WEBSITES

5.1 If an insurer or intermediary conducts online insurance services through third party websites, it should ensure that:

5.1.1. Its registration or approval status in Brunei is clearly stated on the third party website;



- 5.1.2. Its insurance products are clearly identifiable from other insurers' on the third party website;
 - 5.1.3. The information about its insurance products displayed on the third party website are authorised by it and are accurate and up-to-date;
 - 5.1.4. There are adequate security measures in place to protect their interests and their clients' interests; and
 - 5.1.5. The role of the third party is clearly identified and be properly appointed or authorised.
- 5.2 Enquiries or advisory services related to the insurer's products and services should be directed at and handled by the insurer.

6. PRODUCTS AND SERVICES OFFERED

- 6.1. An insurer should carefully select what products and services it wishes to offer/serve on its online direct channel. It should first assess whether the product or service is suitable for distribution online.
- 6.2. The insurer should consider the non-advisory nature of carrying out its business on an online direct channel and carefully evaluate the following:
 - 6.2.1 Whether the product or service's features can be easily understood by customers without live, face-to-face advice;
 - 6.2.2 Whether there is an adequate disclaimer as to the risk of buying certain products or services online;
 - 6.2.3 Whether the product or service's exclusions, terms and conditions are concise, unambiguous and clearly explained; and
 - 6.2.4 Whether the risks of mispurchase by customers are limited.

7. REGISTRATION AND IDENTIFICATION PROCESS

- 7.1. An insurer or intermediary should not allow a customer to purchase insurance policies online or receive online insurance services until the customer has completed the registration and identity verification process of the insurer or intermediary. The registration and identity verification process should, among other things, require basic information that the customer must fill out to verify their identity.
- 7.2. The insurer or intermediary should specify on its online direct channel:
 - 7.2.1. Any information which is legally required;



- 7.2.2. A declaration of consent to purchasing insurance policies online or receiving online insurance services; and
- 7.2.3. The customer's disclosure obligations and should assure its customers that their personal information will not be shared without their permission.
- 7.3 In addition to paragraph 7.2, an insurer or intermediary should ensure that its registration and identity verification process will not commence on its online direct channel until its customer has indicated that they have read any applicable disclosure clauses and consented to purchasing insurance policies online and/or receiving online insurance services.
- 7.4 After a successful registration and identity verification, the online direct channel should provide the customer with an account number, a one-time password (OTP) or verification link and prompt the customer to enter the OTP for completion of identity confirmation.

8. HANDLING OF QUERIES, COMPLAINTS AND CLAIMS

- 8.1. An insurer should set up appropriate avenues to address general queries from the public relating to the insurance policies offered on its online direct channel, including but not limited to, telephone or email helplines in accordance with the requirements in Notice No. FCIU/N-1/2017/1.
- 8.2. An insurer should also provide information, such as contact details, information on the claims process and the process for filing complaints, on its online direct channel.
- 8.3. Every insurer offering products and services online should provide a client charter which should state, at a minimum, the insurer's commitment to:
 - 8.3.1. Providing safe and secure operations;
 - 8.3.2. Maintaining customer privacy;
 - 8.3.3. Providing reliable and quality services;
 - 8.3.4. Providing comprehensive and transparent product information and services; and
 - 8.3.5. Providing prompt response to enquiries and complaints.
- 8.4. A client charter may be made public on the insurer's online direct channel. The client charter should provide for the turnaround time for responses to enquiries and complaints. There should also be adequate monitoring mechanisms to ensure that the insurer adheres to the client charter.
- 8.5. An insurer should ensure that the clients have agreed with any applicable terms and conditions before agreeing to any transactions.



9. PROCEDURE FOR PURCHASING INSURANCE POLICIES ONLINE OR RECEIVING ONLINE INSURANCE SERVICES

- 9.1. The insurer should provide on its online direct channel a description of all the products and services that may be purchased online, as well as the terms and conditions of its insurance policies for customers to browse through any time.
- 9.2. The full text of an insurance policy and any other important content of the insurance product should be provided once the customer enters the necessary application data and selects the insurance product to be purchased.

10. RISK MANAGEMENT AND INTERNAL CONTROLS

- 10.1. An insurer should have adequate policies, procedures and controls to mitigate money laundering risks, terrorism financing risks, and any other specific risks associated with non-face-to-face contact business relations with a client.
- 10.2. Internal policies and processes should be implemented to address technological risks. An insurer should:
 - 10.2.1. Establish a sound and robust technology risk management framework;
 - 10.2.2. Strengthen system security, reliability, resiliency and recoverability; and
 - 10.2.3. Deploy strong authentication to protect customer data, transactions and systems.
- 10.3. An insurer should also put in place an appropriate business continuity plan approved by its board of directors to minimise system downtime or component failures to the online direct channel, and to ensure the functionality and continued operation of the online direct channel. The plan should include data recovery, alternate data processing capabilities, order priority for resumption of business applications and processes, emergency staffing, public relations and outreach strategy to respond promptly to customer and media reaction to system failure or unauthorised intrusions.

11. SECURITY ARRANGEMENTS

- 11.1. An insurer should take all practicable steps to ensure that:
 - 11.1.1. A comprehensive set of security policies and measures are in place and keep it up to date with the advancement of internet security technologies;
 - 11.1.2. Mechanisms are in place to maintain the confidentiality, integrity and availability of data stored in the insurer's system hardware, whilst in transit and as displayed on its online direct channel;



- 11.1.3. Appropriate backup procedures for the database and application software are implemented;
 - 11.1.4. A client's personal information [including password, if any] is protected at all time against loss, unauthorised access, use, modification, disclosure, etc.;
 - 11.1.5. The electronic payment system [e.g. credit card payment system] is secure by way of encryption or any other method;
 - 11.1.6. A valid insurance contract is not cancelled accidentally, maliciously or as a consequence of careless computer handling; and
 - 11.1.7. It has in place a combination of critical technologies and comprehensive security procedures, in accordance with its risk exposures and needs, which may include firewalls, anti-virus or virus protection, virtual private networks, time stamping and audit trails.
- 11.2. Insurers should display on their online direct channel a security statement expressing that adequate security measures are in place to instill customer confidence. This statement should be clear and easily understood.

12. SECURITY BREACHES, SYSTEM DOWNTIME AND DEGRADATION IN SYSTEM PERFORMANCE

- 12.1. An insurer or intermediary is required to report successful cyber intrusions or major IT incidents promptly to BDCB in accordance with the requirements in Notice No. FTU/N-1/2017/1. In addition to this, insurers, intermediaries or service providers should also report material security breaches, system downtime and degradation in system performance to its management and BDCB.
- 12.2. Insurers should state the requirements and standards in paragraph 12.1 in their security policies.
- 12.3. The insurer should have an incident response team or preparedness plan to provide a platform from which an insurer can respond quickly to a problem situation subject to the level and complexity of the online insurance services.

**MANAGING DIRECTOR
BRUNEI DARUSSALAM CENTRAL BANK**

Issue Date: 13 Jamadilakhir 1441H / 7 February 2020M