HUGHES PLANE
INSURANCE BROKERS

Data Protection Policy

1. Introduction

This Policy sets out the Firm's obligations regarding data protection and the rights of the Firm's clients and business contacts in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines personal data as any information relating to an identified or identifiable natural person (a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy also sets the Firm's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Firm, its employees, agents, contractors, or other parties working on behalf of the Firm.

The Firm is committed to the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data, including the Firm, must comply. All personal data must be:

2.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2.2 Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

2.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

2.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

2.6 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.

3. The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects:

3.1 The right to be informed (Section 12).

3.2 The right of access (Section 13);

3.3 The right to rectification (Section 14);

3.4 The right to erasure (also known as the 'right to be forgotten') (Section 15);

3.5 The right to restrict processing (Section 16);

3.6 The right to data portability (Section 17);

3.7 The right to object to processing (Section 18); and

3.8 Rights with respect to automated decision-making (section 19) and profiling (Section 20).

4. **Lawful, Fair, and Transparent Data Processing**

4.1 The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR further states that processing of personal data shall be lawful if at least one of the following applies:

4.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes;

4.1.2 The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;

4.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject;

4.1.4 The processing is necessary to protect the vital interests of the data subject or of another natural person;

4.1.5 The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

4.1.6 The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data.

4.2 If the personal data in question is “special category data” (also referred to as sensitive personal data), for example health and criminal conviction data, at least one of the following conditions must be met:

4.2.1 The data subject has given their explicit consent to the processing of such data for one or more specified purposes;

4.2.2 The processing is necessary for substantial public interest reasons, which includes the processing of data for arranging insurance protection and the efficient administration and payment of insurance claims;

4.2.3 The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; or

4.2.4 The processing relates to personal data which is clearly made public by the data subject.

5. **Specified, Explicit, and Legitimate Purposes**

5.1 The Firm collects and processes the personal data collected directly from data subjects and obtained from third parties.

5.2 Data subjects are kept informed at all times of the purpose or purposes for which the Firm uses their personal data.

6. **Adequate, Relevant, and Limited Data Processing**

The Firm shall only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Section 5.

7. **Accuracy of Data and Keeping Data Up-to-Date**

7.1 The Firm shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Section 14, below.

7.2 The accuracy of personal data shall be checked by the Firm's staff when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. **Data Retention**

8.1 The Firm shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

8.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise securely dispose of it without delay.

8.3 For details of the Firm's approach to data retention, including retention periods for specific personal data types held by the Firm, reference should be made to the Firm's Data Retention Policy.

9. **Secure Processing**

The Firm shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Sections 21 and 22 of this Policy.

10. **Accountability and Record-Keeping**

10.1 The Firm's Data Protection Officer is Iain Jamieson.

10.2 The holder of the role specified in 10.1 shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy and all applicable data protection legislation.

10.3 The Firm shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

10.3.1 The name and details of the Firm and any applicable third-party data processors;

10.3.2 The purposes for which the Firm collects, holds, and processes personal data;

10.3.3 Details of the categories of personal data collected, held, and processed by the Firm, and the categories of data subject to which that personal data relates;

10.3.4 Details of any third-party data processors;

10.3.5 Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

10.3.6 Details of how long personal data will be retained by the Firm (reference should be made to the Firm's Data Retention Policy); and

10.3.7 Detailed descriptions of all technical and organisational measures taken by the Firm to ensure the security of personal data.

11. **Data Protection Impact Assessments**

11.1 The Firm shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.

11.2 Data Protection Impact Assessments shall be overseen by the holder of the role specified in 10.1 and shall address the following:

11.2.1 The type(s) of personal data that will be collected, held, and processed;

11.2.2 The purpose(s) for which personal data is to be used;

11.2.3 The Firm's objectives;

11.2.4 How personal data is to be used;

11.2.5 The parties (internal and/or external) who are to be consulted;

11.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

11.2.7 Risks posed to data subjects;

11.2.8 Risks posed both within and to the Firm; and

11.2.9 Proposed measures to minimise and handle identified risks.

12. **Keeping Data Subjects Informed**

12.1 The Firm shall provide the information set out in Section 12.2 to every data subject:

12.1.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

12.1.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

a) if the personal data is used to communicate with the data subject, when the first communication is made; or

b) if the personal data is to be transferred to another party, before that transfer is made; or

c) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

12.2 The following information shall be provided:

12.2.1 Details of the Firm including the Data Protection Officer;

12.2.2 The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;

12.2.3 Where applicable, the legitimate interests upon which the Firm is justifying its collection and processing of the personal data;

12.2.4 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

12.2.5 Where the personal data is to be transferred to one or more third parties, details of those parties;

12.2.6 Where the personal data is to be transferred to a third party that is located outside the EEA, details of that transfer, including but not limited to the safeguards in place (see Section 23 of this Policy for further details);

12.2.7 Details of data retention;

12.2.8 Details of the data subject's rights under the GDPR;

12.2.9 Details of the data subject's right to withdraw their consent to the Firm's processing of their personal data at any time;

12.2.10 Details of the data subject's right to complain to the Information Commissioner's Office;

12.2.11 Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

12.2.12 Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13. **Data Subject Access**

13.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Firm holds about them, what it is doing with that personal data, and why.

13.2 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

13.3 The handling of all SARs shall be overseen by the person specified in 10.1.

13.4 The Firm does not charge a fee for the handling of normal SARs. The Firm reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests which are reasonably considered to be unfounded or excessive, particularly where such requests are repetitive.

14. **Rectification of Personal Data**

14.1 Data subjects have the right to require the Firm to rectify any of their personal data that is inaccurate or incomplete.

14.2 The Firm shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Firm of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

14.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15. **Erasure of Personal Data**

15.1 Data subjects have the right to request that the Firm erases the personal data it holds about them in the following circumstances:

15.1.1 It is no longer necessary for the Firm to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

15.1.2 The data subject wishes to withdraw their consent to the Firm holding and processing their personal data;

15.1.3 The data subject objects to the Firm holding and processing their personal data and there is no overriding legitimate interest to allow the Firm to continue doing so (reference should be made to Section 18 of this Policy for further details concerning the right to object);

15.1.4 The personal data has been processed unlawfully;

15.1.5 The personal data needs to be erased in order for the Firm to comply with a particular legal obligation.

15.2 Unless the Firm has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

15.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. **Restriction of Personal Data Processing**

16.1 Data subjects may request that the Firm ceases processing the personal data it holds

about them. If a data subject makes such a request, the Firm shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

16.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it, unless it is impossible or would require disproportionate effort to do so.

17. **Data Portability**

17.1 The Firm processes certain personal data using automated means where this is required for the performance of a contract between the Firm and the data subject.

17.2 Data subjects have the right to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

17.3 To facilitate the right of data portability, the Firm shall make available all applicable personal data to data subjects in a generally recognised electronic format.

17.4 Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

17.5 All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

18. **Objections to Personal Data Processing**

18.1 Data subjects have the right to object to the Firm processing their personal data based on legitimate interests and for direct marketing (including profiling).

18.2 Where a data subject objects to the Firm processing their personal data based on its legitimate interests, the Firm shall cease such processing immediately, unless it can be demonstrated that the Firm's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

18.3 Where a data subject objects to the Firm processing their personal data for direct marketing purposes, the Firm shall cease such processing immediately.

19. **Automated Decision-Making**

19.1 The Firm may from time to time use personal data in automated decision-making processes.

19.2 Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge to such decisions under the GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Firm.

19.3 The right described in Section 19.2 does not apply in the following circumstances:

19.3.1 The decision is necessary for the entry into, or performance of, a contract between the Firm and the data subject;

19.3.2 The decision is authorised by law; or

19.3.3 The data subject has given their explicit consent.

20. **Profiling**

20.1 The Firm may from time to time use personal data for profiling purposes.

20.2 When personal data is used for profiling purposes, the Firm shall ensure the following:

20.2.1 Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;

20.2.2 Appropriate mathematical or statistical procedures shall be used;

20.2.3 Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and

20.2.4 All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling.

21. **Data Security - Transferring Personal Data and Communications**

The Firm shall ensure that the following security measures are taken with respect to all communications and other transfers involving personal data:

21.1 Upon request emails containing personal data can be sent to recipients outside the Firm's email system using password protection. Instructions are available from Gareth Hughes or Stuart Plane.

21.2 Notwithstanding Section 21.1, in certain exceptional situations, permission may be granted by Gareth Hughes or Stuart Plane to email personal data without protection. Such situations might be where: the data is already in the public domain; there is considered to be an insufficient risk of 'damage or distress' to the individual; there is considered to be an insufficient risk of interception or mis-addressing.

21.3 Personal data must be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

21.4 Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

21.5 Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

21.6 Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using Royal Mail;

21.7 No personal data may be shared informally and if an employee, agent, contractor or other party working on behalf of the Company requires access to any personal data to which they do not already have legitimate access, such access should be formally requested from Gareth Hughes or Stuart Plane;

21.8 All hard copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;

21.9 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Firm or not, without the authorisation of Gareth Hughes and Stuart Plane;

21.10 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, contractors or other parties at any time;

21.11 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

21.12 Any unwanted copies of personal data (i.e. print-outs or electronic duplicates) that are no longer needed should be disposed of securely. Hard copies should be shredded and electronic copies should be deleted securely using Acturis;

21.13 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Firm or otherwise without the formal written approval of Gareth Hughes or Stuart Plane and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;

21.14 No personal data should be transferred to any device personally belonging to an

employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Firm where the party in question has agreed to comply fully with the letter and spirit of this Policy and GDPR (which may include demonstrating to the Firm that all suitable technical and organisational measures have been taken);

21.15 All personal data stored electronically should be backed up with backups stored off site. All backups should be encrypted using Acturis;

21.16 All passwords used to protect personal data must comply with the Firm's Data Security Policy. All software used by the Firm is designed to require such passwords;

21.17 All personal data held by the Firm shall be regularly reviewed for accuracy and completeness. Where the Firm has regular contact with data subjects, any personal data held about those data subjects should be confirmed at least annually. If any personal data is found to be out of date or otherwise inaccurate, it should be updated and/or corrected immediately where possible. If any personal data is no longer required by the Firm, it should be securely deleted and disposed of using Acturis;

21.18 Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of Gareth Hughes or Stuart Plane to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service. Such details should be checked at least annually; and

21.19 When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, reference should be made to the Firm's Data Retention Policy.

22. **Organisational Measures**

The Firm shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

22.1 All employees, agents, contractors, or other parties working on behalf of the Firm shall be made fully aware of both their individual responsibilities and the Firm's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;

22.2 Only employees, agents, contractors, or other parties working on behalf of the Firm that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Firm;

22.3 All employees, agents, contractors, or other parties working on behalf of the Firm handling personal data will be appropriately trained to do so;

22.4 All employees, agents, contractors, or other parties working on behalf of the Firm handling personal data will be appropriately supervised;

22.5 All employees, agents, contractors, or other parties working on behalf of the Firm handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

22.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

22.7 All personal data held by the Firm shall be reviewed periodically, as set out in the Firm's Data Retention Policy;

22.8 The performance of those employees, agents, contractors, or other parties working on behalf of the Firm handling personal data shall be regularly evaluated and reviewed;

22.9 All employees, agents, contractors, or other parties working on behalf of the Firm handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;

22.10 All agents, contractors, or other parties working on behalf of the Firm handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Firm arising out of this Policy and the GDPR; and

22.11 Where any agent, contractor or other party working on behalf of the Firm handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Firm against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

23. Transferring Personal Data to a Country Outside the EEA

23.1 The Firm may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

23.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

23.2.1 The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

23.2.2 The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

23.2.3 The transfer is made with the informed consent of the relevant data subject(s);

23.2.4 The transfer is necessary for the performance of a contract between the data subject and the Firm (or for pre-contractual steps taken at the request of the data subject);

23.2.5 The transfer is necessary for important public interest reasons;

23.2.6 The transfer is necessary for the conduct of legal claims;

23.2.7 The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

23.2.8 The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

24. Data Breach Notification

24.1 All personal data breaches must be reported immediately to the person specified in 10.1.

24.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the person specified in 10.1 must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

24.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Section 24.2) to the rights and freedoms of data subjects, the person specified in 10.1 must ensure that all affected data subjects are informed of the breach directly and without undue delay.

24.4 Data breach notifications shall include the following information:

24.4.1 The categories and approximate number of data subjects concerned;

24.4.2 The categories and approximate number of personal data records concerned;

24.4.3 The contact point within the Firm where more information can be obtained;

24.4.4 The likely consequences of the breach;

24.4.5 Details of the measures taken, or proposed to be taken, by the Firm to address the breach including, where appropriate, measures to mitigate its possible adverse effects.