CNA HARDY SUPPLIER CODE (Processor Version)

Duly signed as valid and binding contract by an authorised representative of:

"**Supplier**": _____

Signed: _____

Name _____

Date: _____

CNA Services (UK) Limited ☐

or

CNA Insurance Company (Europe) S.A. ☐

in either case, for itself and for and on behalf of its Affiliates (which include the operating entities referred to in Attachment 3) (each referred to as "**Company**" as the context requires)

Date: _____

ARTICLE 1: DATA PRIVACY AND PROTECTION LAWS

The Company and the Supplier acknowledge that:

(a) The Agreement in place between Company and Supplier may require the processing of personal data by the Supplier on behalf of Company; and

(b) the Company shall determine the purposes for which and the manner in which personal data will be processed by the Supplier on behalf of the Company under the Agreement.

.

Where, in connection with the provision of any service or the Agreement, the Supplier process personal data on behalf of the Company, the Supplier shall comply with the requirements of Schedule 1 at all times.

ARTICLE 2: COUNTERPARTS AND ELECTRONIC SIGNATURES

This Code may be executed in one or more counterparts, each of which will be deemed to be an original copy of this Code and all of which, when taken together, will be deemed to constitute one and the same agreement. The facsimile, email or other electronically delivered signatures of the parties shall be deemed to constitute original signatures, and facsimile or electronic copies hereof shall be deemed to constitute duplicate originals.

ARTICLE 3: VARIATION

No variation of this Code shall be effective unless it is in writing and signed by the parties (or their authorised representatives), any variation to this Code purported to be made pursuant to any original Agreement shall only be effective where referencing this Code and the amendments to this Code being proposed to be made and made in writing and signed by the parties.

ARTICLE 4: PRIMACY AND EFFECT

Notwithstanding anything to the contrary in any Agreement, course of dealing or undertaking made by the Supplier or the Company, it is agreed by the Supplier and the Company that this Code shall take precedence over and have primacy to, any existing agreement, contractual terms or course of dealings, irrespective of any statement contained in such to the contrary. It is agreed by the Supplier and the Company, that this Code constitutes a valid amendment and variation to any existing Agreement, notwithstanding any formalities stated in such Agreement to effect such.

It is agreed by the Supplier and the Company, that in the situation that the Supplier has not acknowledged and signed this Code electronically or in wet copy or raised any proposed issue in agreeing to such, the continued dealings or course of business conduct between the Supplier and the Company shall be taken as evidence and agreement by the Supplier to its agreement to the Code and that the Code shall have the effect set out above in this article.

ARTICLE 5: LAW AND JURISDICTION

The construction, validity and performance of this Agreement shall be governed exclusively by the laws of England and Wales and the parties hereby submit irrevocably to the exclusive jurisdiction of the English courts to resolve any dispute between them.

DATA PROTECTION REQUIREMENTS
(including EU Standard Contractual Clauses)

This Data Processing Addendum (**DPA**) forms part of this Agreement between Supplier and Company. Capitalised terms used but not defined herein shall have the meaning set out in this Agreement. This DPA consists of (a) the main body of the DPA; (b) the Data Processing Details Attachment 1; (c) the Security Terms at Attachment 2; and (d) the Standard Contractual Clauses incorporated by reference.

1 Definitions

The following terms have the following meanings when used in this DPA:

Affiliate means with respect to a party, an entity that (directly or indirectly) controls, is controlled by or is under common control with, such party, where control refers to the power to direct or cause the direction of the management policies of another entity, whether through ownership of voting securities, by contract or otherwise.

Agreement means the agreement between the Company and the Supplier to which this DPA is attached.

Controller means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

Data Protection Laws means all laws and regulations applicable to the Processing of Personal Data under the Agreement including the laws and regulations of the applicable Extended EEA Country that relate to the Processing of Personal Data, including the UK GDPR, the UK Data Protection Act 2018 (**DPA 2018**) and GDPR (as applicable).

Data Subject means the individual to whom Personal Data relates.

Data Subject Request means a Data Subject's request to exercise that person's rights under Data Protection Laws in respect of that person's Personal Data, including, without limitation, the right to access, correct, amend, transfer, obtain a copy of, object to the Processing of, block or delete such Personal Data.

EEA means the European Economic Area.

Extended EEA Country means a country within the European Economic Area (including EU member states), Switzerland or UK.

GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).

Losses means all losses, liabilities, damages, costs, charges, and expenses (including reasonable legal fees on a solicitor and own client basis, other reasonable professional advisers' fees, and costs and disbursements of investigation, litigation, settlement, judgment, interest, fines, penalties and remedial actions) and **Loss** shall be construed accordingly.

Personal Data means any personal data (as defined in the GDPR), which is Processed by the Supplier on behalf of the Company pursuant to this Agreement.

Personal Data Breach means a breach of security that has resulted in, or is reasonably likely to result in, the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, access to or encryption of Personal Data transmitted, stored or otherwise Processed.

Processing or **Process** means any operation or set of operations which is performed by or on behalf of the Supplier upon Personal Data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Processor means the entity which Processes Personal Data on behalf of the Controller. **Regulator** means the data protection authority or other regulatory, governmental or supervisory authority which is responsible for regulating over all or any part of (a) the provision or receipt of the Services; (b) the Processing of Personal Data in connection with the Services; or (c) Supplier's business or personnel relating to the Services.

Services means the services to be provided by the Supplier to the Company and its Affiliates under this Agreement.

Standard Contractual Clauses means the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission decision of 4 June 2021 and published under document number C(2021) 3972 currently available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=en&uri=CELEX:32021D0914 which are hereby incorporated by reference.

Sub-processor means a Processor that Processes Personal Data on behalf of another Processor.

Third Country means a country not deemed adequate to receive Personal Data under the Data Protection Laws of the applicable Extended EEA Country.

UK Addendum means the International Data Transfer Addendum to the Standard Contractual Clauses issued by the Information Commissioner's Office (version B1.0, in force 21 March 2022), as amended from time to time and hereby incorporated by reference.

UK GDPR means GDPR as amended and transposed into the laws of the United Kingdom pursuant to the European Union (Withdrawal) Act 2018 and the European Union (Withdrawal Agreement) Act 2020.

1 Relationship with this Agreement

1.1 This DPA sets out the mandatory provisions that are required to be put in place between Controllers or Processors and Processors or Sub-processors under the Data Protection Laws. In the event of a conflict between this DPA and the Agreement that pertain to the Processing of Personal Data, the terms of this DPA shall prevail.

1.2 In the event of a conflict between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

2 Processing of Personal Data

2.1 Roles of the Parties

(a) The Company is a Controller or Processor (as applicable) and the Supplier is a Processor or Sub-processor (as applicable) acting on the Company's behalf.

(b) The Supplier shall also provide the Services to, and Process Personal Data provided by or on behalf of Affiliates of the Company and each Affiliate has the same rights that the Company has under this DPA. Reference to the "Company" in this DPA shall be construed as reference to the applicable Company Affiliate

2.2 Purpose; categories of Personal Data and Data Subjects

The purpose of the Processing of Personal Data by the Supplier is to support the supply of the Services pursuant to this Agreement. The types of Personal Data Processed under this DPA and categories of Data Subjects are further specified in Attachment 1 (*Data Processing Detail*).

3 Data Processor obligations

Compliance with Company instructions

3.1 The Supplier shall in respect of all Personal Data:

(a) only Process Personal Data on the Company's behalf in compliance with Data Protection Laws, and in accordance with the Company's instructions unless required to do so by UK, Union or Member State law (as applicable) to which the Supplier is subject. In such a case, the Supplier shall inform the Company of that legal requirement before Processing unless that law prohibits such information on important grounds of public interest. The Company instructs the Supplier to Process the Personal Data to the extent and in such manner as is necessary for the supply of the Services;

(b) notify the Company immediately if, in its opinion, an instruction it receives from the Company infringes Data Protection Laws;

(c) not disclose Personal Data to any third parties without the consent of Company other than to the extent required by a court of law or as expressly permitted in the Agreement; and

(d) treat the Personal Data as confidential information subject to the confidentiality provisions of the Agreement.

Security

3.2 The Supplier shall:

(a) implement and maintain appropriate technical and organisational security measures to adequately protect Personal Data against the risks inherent in the Processing of Personal Data for the purposes identified in the Agreement (as applicable) and the locations in which it is Processed and against the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data in accordance with Data Protection Laws. Without limiting the generality of the foregoing, the Supplier shall comply with the requirements set out in Attachment 2 (*Security Terms*);

(b) if required by the Company, promptly provide a written description of the technical and organisational security measures employed for Processing Personal Data and notify the Company of any material changes to such security measures from time to time;

(c) take reasonable steps to ensure the reliability of the Supplier's Personnel required to access Personal Data and ensure that such Personnel are regularly trained in respect of data security and data protection and are subject to enforceable duties of confidence in respect of the Personal Data; and

(d) maintain, and provide to the Company upon request, proper records of all Processing of Personal Data (including an up-to-date log of which Supplier Personnel have or have had access to Personal Data at any time during the Term of this Agreement, what Processing has been undertaken, which Sub-processors have been involved and the geographic location of all of the Processing).

Personal Data Breach management

3.3 The Supplier shall immediately notify the Company upon becoming aware of the occurrence of a Personal Data Breach and provide the Company with the following information without undue delay and in any event within 48 hours:

(a) full details of the Personal Data Breach, including, details of the likely consequences of the Personal Data Breach, a description of the nature of the Personal Data Breach, data records concerned and the categories and approximate number of Data Subjects concerned;

(b) the name and contact details of the Supplier contact, from whom more information can be obtained;

(c) a description of the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects; and

(a) whether any regulatory authority, the Data Subjects themselves and / or the media have been informed or are otherwise already aware of the Personal Data Breach and their response.

3.4 The Supplier shall provide such cooperation as is required by the Company in order to mitigate the effect of the relevant Personal Data Breach and to develop the content of any notification to the affected Data Subjects and/or the relevant Regulators that are required in connection with the Personal Data Breach.

Sub-processors

3.5 The Supplier may engage third-party Sub-processors in connection with the provision of the Services, subject to paragraphs 3.6 to 3.9 and the other provisions of this Agreement.

3.6 The Supplier shall ensure that the subcontract entered into with any Sub-processor imposes on the Sub-processor substantially the same obligations as those to which the Supplier is subject under this DPA.

3.7 Upon request, the Supplier shall provide the Company with a current list of the names, jurisdiction in which they Process Personal Data, and contact information of any Sub-processors (the "**Sub-processor List**"). The Supplier shall provide 60 days' prior notice by email at Legal.int@cnahardy.com to the Company of any addition, of a new Sub-processor to the Sub-processor List or replacement thereby giving Company the opportunity to object to such changes prior to the engagement of the Sub-processor(s).

3.8 If the Company objects in writing to the Supplier's proposed use of a new Sub-processor, the Supplier will use reasonable efforts to stop such proposed Sub-processor from Processing Personal Data without adverse impact on the Services. If the Supplier determines that it cannot stop the Processing with adverse impact, it shall notify the Company of such determination. Upon receipt of such notice, the Company may terminate this Agreement without penalty or liability whatsoever, other than for charges due and owing to the Supplier under the Agreement for Services supplied prior to such termination, such termination effective immediately upon giving notice of such termination to the Supplier. The Supplier shall promptly refund the Company any pre-paid charges for the period following the effective date of termination.

3.9 The Supplier shall:

(a) procure that its Sub-processors comply with the Supplier's obligations under this DPA as if they were the Supplier; and

(b) be responsible and liable for the acts, omissions or defaults of its Sub-processors in the performance of the Sub-processor's obligations under relevant Agreement as if they were the Supplier's own acts, omissions or defaults.

Return and deletion of Personal Data

3.10 On termination of this Agreement for any reason, or upon written request from the Company at any time, the Supplier shall:

(a) cease to Process any Personal Data; and

(b) at the Company's direction, return to Company (or, at its direction, delete) any Personal Data in the Supplier's or its Personnel's or Sub-Processor(s)' possession or control, except as required by law.

Data Subject Requests

3.11 The Supplier shall, to the extent permitted by law, notify the Company promptly and, in any event, not later than 3 days following receipt of a Data Subject Request. The Supplier shall not respond to any such Data Subject Request without the Company's prior written instructions.

3.12 The Supplier shall provide such assistance and take such action as the Company may reasonably request (including assistance by appropriate technical and organisational measures) to allow the Company to fulfil obligations to clients and to Data Subjects under Data Protection Laws.

Other complaints and requests

3.13 The Supplier shall, to the extent permitted by law, notify the Company promptly and, in any event, not later than 3 days following receipt of any complaint or request (other than Data Subject Requests or enquiries of Regulators described in paragraph 5.1) relating to the Personal Data and / or the Company's obligations under Data Protection Laws.

3.14 The Supplier shall promptly provide such co-operation and assistance as the Company and/or the Company's Controller(s) may reasonably request in relation to such complaint or request and in relation to:

(a) the obligation to notify a Regulator and / or Data Subject of a Personal Data Breach; and

(b) the obligation to carry out a data protection impact assessment, including consulting with the data protection authority.

Documentation and compliance

3.15 Subject to reasonable and appropriate confidentiality undertakings, the Supplier shall provide to the Company all necessary information to demonstrate the Supplier's compliance with the obligations in this DPA and, at the Company's request permit the Company (or its authorised representative) to inspect and audit the Supplier's data Processing activities (and/or those of its Personnel which Process Personal Data on the Supplier's behalf) and comply with all reasonable requests or directions by the Company to enable it to verify that the Supplier, its Personnel are in full compliance with data protection obligations under this Agreement and take such remedial actions as are reasonably required by the Company following such audit.

4 Data transfers

Controls on transfers from an Extended EEA Country

4.1 The Supplier shall not permit Personal Data originating from a an Extended EEA Country to be Processed in a Third Country without the Company's prior written consent. If the Company provides this consent, the Supplier shall ensure that any Processing of Personal Data in a Third Country is carried out in accordance with Data Protection Laws and the remainder of this paragraph 4.

4.2 Prior to consenting to the transfer of Personal Data under paragraph 4.1 above and in respect of any countries to which the Company has given its consent under the terms of this Agreement, the Company may request that the Supplier provides to Company the information set out in paragraph 4.14 and Supplier shall provide such information promptly (and in any event within 14 days) of receipt of such a request.

4.3 The Standard Contractual Clauses shall apply between the Company (as data exporter) and the Supplier (as data importer) where:

(a) the Company is:

(i) located in an Extended EEA Country; or

(ii) located outside the Extended EEA Countries, but Processes Personal Data directly subject to the Data Protection Laws of an Extended EEA Country; or is contractually obliged to impose safeguards that are equivalent to those safeguards required under the Data Protection Laws of an Extended EEA Country with whom they share the Personal Data; and

(b) the Supplier is established in a Third Country,

unless the Company agrees in writing that an export derogation or alternative export framework recognised by the Data Protection Laws of the applicable Extended EEA Country applies instead of the Standard Contractual Clauses. The Standard Contractual Clauses shall be construed and interpreted in accordance with the remainder of this paragraph 4. The Standard Contractual Clauses shall constitute a separate agreement between the Company acting as a data exporter and the Supplier acting as a data importer.

4.4 Except to the extent that the Standard Contractual Clauses or Data Protection Law of an Extended EEA Country would require otherwise, the parties' respective obligations under the Standard Contractual Clauses shall be governed by the law(s) of, and subject to the jurisdiction of, the courts of, and the supervisory authority shall be the supervisory authority of Luxembourg.

4.5 Where the applicable Extended EEA Country in which the Company is established is not a member state of the EU or the UK or where the Personal Data is subject to the Data Protection Laws of an Extended EEA Country that is not a member of the EU or the UK, references in the Standard Contractual Clauses to:

(a) "European Union" ("EU"), the "EU" a "Member State", an "EU Member State" or "one of the EU Member States" shall refer to the applicable non-EU country;

(b) "Regulation (EU) 2016/679" shall refer to the applicable Data Protection laws of the applicable non-EU country; and

(c) "supervisory authority" shall be construed as per paragraph 4.4 above.

4.6 Where the applicable Extended EEA Country in which Company is established is the UK or where the Personal Data is subject to the UK GDPR, the Standard Contractual Clauses are hereby amended by the UK Addendum in respect of such transfers and Part 1 of the UK Addendum shall be populated as set out below:

(a) Table 1. The "start date" will be the date this DPA enters into force. The "Parties" are the Company (as per the applicable details in Attachment 3) and the Supplier (as set out on the first page of this Code).

(b) Table 2. The "modules of the Standard Contractual Clauses are as per paragraph 4.7 of this DPA.

(c) Table 3. The "Appendix Information" is as per paragraphs 4.8 - 4.12 of this DPA.

(d) Table 4. The exporter may end the UK Approved Addendum in accordance with its Section 19.

Modules and interpretation of the Standard Contractual Clauses

4.7 The Standard Contractual Clauses shall be construed as follows:

(a) where the applicable sections of the Standard Contractual Clauses require the data exporter and the data importer to select a module, the Supplier acknowledges that:

(i) Module Two of the Standard Contractual Clauses (*Transfer controller to processor*) shall apply where the Supplier, as data importer, is acting as the Company's Processor; and

(ii) Module Three of the Standard Contractual Clauses (*Transfer processor to processor*) shall apply where the Supplier, as data importer, is acting as the Company's Sub-processor;

(b) the instructions to the Supplier are as per paragraph 3.1(a) of this DPA, which in the case of Module Three, constitute the instructions of the relevant Controller(s);

(c) the Supplier's storage, erasure and return of Personal Data shall be construed by reference to the provisions regarding deletion and return of Personal Data in paragraph 3.10 of this DPA; and

(d) the Recipient Supplier Entity's ability to engage sub-processors shall be construed by reference to paragraph 3.5 of this DPA.

Completion of Annexes of Standard Contractual Clauses

4.8 Annex I, Part A (*List of parties*) of the Standard Contractual Clauses is hereby deemed to be completed with: (i) the details of the Company (as per the applicable details in Attachment 3),as data exporter and Controller or Processor (as applicable); and (ii) the details of the Supplier (as set out on the first page of this Code), as data importer and, Processor or Sub-processor (as applicable)).

4.9 Annex I, Part B (*Description of the transfer*) of the Standard Contractual Clauses is hereby deemed to be completed with the information set out in Attachment 1 of this DPA..

4.10 Annex II of the Standard Contractual Clauses (*Technical and organisational measures including technical and organisational measures to ensure the security of the data*) is hereby deemed to be completed with the requirements set out in Attachment 2 (*Security Terms*).

4.11 Where applicable, Annex III of the Standard Contractual Clauses (*List of Sub-processors*) is hereby deemed completed by reference to the list of Sub-processors in accordance with paragraph 3.7 of this DPA.

4.12 The Supplier agrees to execute additional documents (including updates to the Annexes of the Standard Contractual Clauses) and apply additional protections, as may be necessary for the transfer and storage of Personal Data transferred pursuant to the Standard Contractual Clauses.

Supplier in an Extended EEA Country

4.13 Subject to paragraph 4.1, where the Supplier is established in an Extended EEA Country or a country considered adequate under the Data Protection Laws of the applicable Extended EEA Country,, the Supplier

shall enter into the appropriate module of the Standard Contractual Clauses, as amended to comply with applicable Data Protection Laws, with any third party located in a Third Country (including any Supplier Affiliate) to whom the Supplier transfers such Personal Data before making such transfer, unless the Company agrees otherwise in writing. The Supplier shall ensure that the Annexes of the Standard Contractual Clauses reflect the information set out at paragraphs 4.9 and 4.10 of this DPA. In all cases the Supplier shall comply with applicable Data Protection Laws in relation to such transfer (including undertaking an appropriate transfer impact assessment in respect thereof).

Provision of information relating to transfer impact assessments

4.14 Upon request, Supplier will provide the following information to the Company in respect of transfers made under this paragraph 4:

(a) the assessment made in relation to the transfers;

(b) a summary of the access laws and practices of the relevant Third Country that were assessed in respect of the transfers;

(c) a summary of the contractual, technical and organizational measures put in place in respect of the transfers; and

(d) to the extent not prohibited by law, details of the number of legally binding requests that the Supplier, importer or any Sub-processor has received from a public authority in the relevant Third Country in each 12 month period over the last 24 months.

Additional country requirements

4.15 If the Supplier at any time Processes Personal Data originating from the Company in any country which restricts the Processing, export, or use of the Personal Data outside that country (including an Extended EEA Country), the Supplier will, on the Company's instructions, take all necessary actions and execute such agreements as may be necessary under applicable data protection law in such country to legitimise any Processing or data transfer of Personal Data to the Supplier and to ensure an adequate level of protection for the relevant Personal Data.

4.16 In the event that any competent judicial or supervisory authority holds that a data transfer mechanism relied on by the Parties (including pursuant to paragraph 4.14 above) is invalid, or any competent judicial or supervisory authority requires transfers of Personal Data made pursuant to such mechanism to be suspended, then the Company may, at its discretion, require the Supplier to cease Processing Personal Data, or co-operate with it to facilitate use of an alternative transfer mechanism and the Supplier shall comply with the Company's instructions.

5 Co-operation with Regulators and conduct of claims

5.1 The Supplier shall promptly notify the Company of all enquiries from a Regulator that the Supplier receives which relate to the Processing of Personal Data, the provision or receipt of the Services or either Party's obligations under this Agreement, unless prohibited from doing so at law or by the Regulator.

5.2 Unless the Company notifies the Supplier that the Supplier will be responsible for handling a particular communication or correspondence with a Regulator or a Regulator requests in writing to engage directly with the Supplier, Company will handle all communications and correspondence relating to Personal Data and the provision or receipt of the Services.

5.3 The Company shall have the right, at its sole discretion, to assume control of the defence and settlement of any third-party claim that relates to the Processing of Personal Data, including claims against the Supplier, its Personnel or Sub-processors, provided that the Company shall not enter into any settlement of such claim or compromise any such claim without the Supplier's prior written consent if such compromise or settlement would assert any liability against the Supplier, increase the liability (including under an indemnity) of the Supplier, or impose any obligations or restrictions on the Supplier, such as imposing an injunction or other equitable relief upon the Supplier. Where required, such consent shall not be unreasonably withheld or delayed. The Company's exercise of such right under this paragraph 5.3 shall:

(a) not be construed to require the Company to bear the costs of such defence and settlement; and

(b) be without prejudice to its contractual, legal, equitable or other rights to seek recovery of such costs.

5.4 Where the Supplier interacts directly with a Regulator in accordance with paragraph 5.2, the Supplier shall do so in an open and co-operative way at its own expense and in consultation with the Company. With respect to such interaction with a Regulator, the Supplier shall (and shall cause its Personnel and Sub-processors to):

(a) make itself readily available for meetings with the Regulator as reasonably requested;

(b) subject to paragraph 5.4(c), answer the Regulator's questions truthfully, fully and promptly; and provide the Regulator with such information and co-operation as the Regulator may require; and

(c) where permitted by law, notify the Company of any Regulator's request for information relating to the Company or the Personal Data and before disclosing such requested information, co-operate with the Company's efforts to prevent the disclosure of, or obtain protective treatment for, such information, and comply with the Company's reasonable instructions regarding the response to such request. Any confidential information disclosed by the Supplier in accordance with this paragraph 5.4 shall be disclosed subject to this Agreement's confidentiality provisions.

5.5 Indemnity

5.6 The Supplier shall, at all times during and after the term of the Agreement, indemnify the Company and its Affiliates and other Service Recipients against all Losses incurred by them arising out of or in connection with:

(a) any breach of the Supplier's obligations under this DPA;

(b) the Supplier's negligence or wilful misconduct under this DPA; or

(c) any Personal Data Breach.

6 General

Liability

6.1 The Parties agree that no limitations or exclusions of liability set out in this Agreement shall apply to any Party's liability to Data Subjects under the third-party beneficiary provisions of the Standard Contractual Clauses to the extent that such limitations or exclusions are prohibited by Data Protection Laws.

Severability

6.2 If any provision or part-provision of this DPA is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this DPA, and if it so deemed deleted, the Parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

Exclusion of third-party rights

6.3 All third-party rights are excluded (except those granted to Company Affiliates under paragraph 2.1(b) and to Data Subjects under the Standard Contractual Clauses).

Governing Law

6.4 To the extent required by applicable Data Protection Laws (e.g. in relation to the governing law of the Standard Contractual Clauses) this DPA shall be governed by the law of the applicable jurisdiction. In all other cases, this DPA shall be governed by the laws of the jurisdiction specified in this Agreement.

ATTACHMENT 1

DESCRIPTION OF PROCESSING OF PERSONAL DATA WHICH MAY (SUBJECT ALWAYS TO THE DATA PROTECTION LEGISLATION AND DEPENDING ON THE NATURE OF THE SERVICES) OCCUR UNDER THIS AGREEMENT

The duration of the processing and frequency of transfer

The personal data processed by the Supplier under this Agreement may only be processed for the term of this Agreement and thereafter it shall be securely deleted and hard copies destroyed or delievered up in accordance with the relevant provisions of this Agreeemnt.

The personal data is regularly accessed by the Supplier on an ongoing basis.

The categories of data subjects

The personal data processed by the Supplier under this Agreement may relate to any or all of the following categories of data subjects:

For **insurance administration purposes**:

- Brokers and employees of broker entities (or brokers if individuals)
- Customers and employees of client companies
- Insureds persons ("insureds") and their employees
- Claimants
- Complainants, correspondents and enquirers
- The subjects of any such complaints, correspondence and enquiries
- Staff including employees, contractors, consultants and volunteers
- Agents, temporary and casual workers
- Relatives, guardians and associates of the complainants or of the subjects of the complaints (if need be and depending on the nature of the policy underwritten by the complainants)
- Any other data subject with whom the data controller does business or has some other contractual, licensing or other legal arrangement and their employees (as applicable).

For **information technology management and database administration purposes**:

- Current or potential customers, insureds, clients and their employees
- Complainants, correspondents and enquirers and their employees
- The subjects of any such complaints, correspondence and enquiries
- Staff including employees, contractors, consultants and volunteers
- Agents, temporary and casual workers
- Relatives, guardians and associates of the data subject including dependents of employees
- Employees of supplier entities and potential supplier entities (or suppliers themselves if individuals)
- Any other data subject in any way using or accessing the information technology infrastructure of the data controller (and/or the data processor as relevant).

For **compliance purposes** and to the extent allowed by applicable laws:

- Staff including employees, officers, directors, contractors, consultants and volunteers
- Agents, temporary and casual workers
- Any other data subject with whom the data controller does business or has some other contractual, licensing or other legal arrangement and their employees (as applicable and lawful)
- Any data subject in any way involved or referred to in a matter relating to compliance purposes, including employees, family members, friends or other acquaintances of any of the data subjects, in accordance with applicable laws.

The subject matter, nature and purposes of the processing

The personal data processed by the Supplier under this Agreement may be for any or all of the following purposes:

- **Insurance administration** including approval and review of the decisions in relations with customers/clients of the data controller, insureds and claimants; and deciding whether to accept any person as a customer/client or, if individual, as a broker, in each case including the administration of life, health, pensions, property, motor and other insurance business of the data controller and any other commercial issue in which the data controller is involved
- **Information technology management and database administration purposes** carried out by the data processor in its data controller capacity
- **Compliance purposes** to ensure compliance of the data controller with applicable legislation, or to respond to authorities' requirements, to the extent permitted by applicable laws

The categories / type of personal data

The personal data processed by the Supplier under this Agreement may relate to any or all of the following categories of data:

For **insurance administration purposes**:

- Personal details
- Contact details
- Education (for some employees within broker companies and in certain cases, for claimants)
- Banking details (for the payment of brokers when individuals, or for the payment of claimants)
- Physical or mental health or condition
- Offences (included alleged offences) (to the extent permitted under applicable law)
- Criminal proceedings, outcomes and sentences (to the extent permitted under applicable law).

For **information technology management and database administration purposes**:

- Name
- Date and place of birth (for employees of the data controller only)
- Country of residence
- Nationality / Visa status / Mobility (for employees of the data controller only)
- Gender
- Marital status
- Address and email address
- Telephone and other contact numbers (business and personal)
- Military status (if applicable)
- Employer
- Employee status
- Employment history (for employees of the data controller only; for example information on hiring, termination, career, perspective career developments, expected retirement date, and termination)
- Job title, position level and job assignments
- Job performance (including comments made by the employee and their manager), project ratings and reviews, employee job objectives for the year (for employees of the data controller only)
- Absence information: start date/end date, absence type (e.g., sickness or parental leave), sickness reasons (only if and to the extent necessary to comply with obligations of the data controller who is employer)
- Emergency contact information and details (for example emergency contact name, phone number, relationship only if relevant and contact details; for the employees of the data controller only. This information is optional and may be entered/updated by the employees of the data controller)
- Parental Leave: employee dependent name/address details, dependent relationship to employee
- Education and training details including employee development plans (for employees of the data controller only)
- Disciplinary notices and information (for employees of the Data controller only)
- Benefit data (for employees of the data controller only)
- Language spoken
- National ID
- Personal national identification (fiscal code)

- Racial, ethnic origin, religious, philosophical or other beliefs, political opinions
- Comprehensive background investigations (for claimants) to the extent permitted by applicable laws (i.e., Sensitive Data)
- Banking details (for the payment of brokers when individuals, for the payment of claimant, or for the purposes of the payment of the salaries of employees of the data controller
- Information on company's property assigned to personnel (for the employees of the data controller only; for example business credit cards and other benefits)
- Comprehensive background investigations in accordance with applicable law (for employees of the data controller only and, in certain cases, for claimants)
- Financial and payroll data (for employees of the data controller only and, in certain cases, for claimants; for example pay grade, compensation and annual compensation, salary plan, information on participation to and management on benefit programs of the data controller).

For **compliance purposes**:

- any information necessary to comply with applicable by law or authorities' requests, to the extent allowed by applicable laws; this includes but is not limited to all of the data categories listed above and below in the “categories of data” section of this Part 1 of Annex B.

Recipients

Subject always to the provisions in this Agreement which govern the onward dislcosure of personal data by the Supplier to third parties, the personal data processed by Supplier under this Agreement may be disclosed to any or all of the following categories of recipients:

For **insurance administration**:

- Managers within the data controller and/or the data processor who are in charge of the approval and review of the decisions made by the data controller regarding underwriting and claims
- External business consultants and service providers (such as legal, finance and accounting, information technology and human resources advisors and/or similar consultants and advisors) of the data controller and/or the data processor with a need to know for the achievement of the relevant purpose.

For **information technology management and database administration purposes**:

- Designated personnel of IT and HR department of the data controller and/or the data processor with a need to know, such as IT administrators and technical HR support staff
- External business consultants and service providers (such as legal, finance and accounting, information technology and human resources advisors and/or similar consultants and advisors) of the data controller and/or the data processor with a need to know for the achievement of the relevant purpose.

For **compliance purposes**:

- Designated personnel of IT and HR department of the data controller with a need to know, such as IT administrators and technical HR support staff
- Law enforcement authorities, subject to applicable legal requirements
- External business consultants and service providers (such as legal, finance and accounting, information technology and human resources advisors and/or similar consultants and advisors) of the data controller with a need to know for the achievement of the relevant purpose.

Special categories of personal data and criminal convictions and offences personal data

The personal data processed by Supplier under this Agreement may relate to any or all of the following categories of special categories of personal data and/or criminal convictions and offences personal data and it is in respect of the data subjects described above (as relevant):

- commission or alleged commission of any offence
- criminal proceedings
- physical or mental health conditions

- employee absence information: start date/end date, absence type (e.g., sickness or parental leave), sickness reasons (only if and to the extent necessary to comply with obligations of the employer)
- Information on claimants' health for the purposes of the assessment of the damages and the administration of the claim
- Information on applicant's or insured's physical or mental health condition for the purpose of reviewing and approving decisions made by the data controller regarding underwriting and claims
- Claimants' and employees' judicial information, to the extent permitted by applicable law and as far as necessary for the purpose of managing claims and legal proceedings, including the protection of the interests of the claimants and the management of the data controller in litigation
- Non-identifying judicial information about insured and applicants, to the extent permitted by applicable law
- Racial or ethnic origin of the data subjects above identified only when strictly necessary to achieve the purposes of the transfers above specified and in accordance with applicable law
- Religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade-unionist character of the data subjects above identified only when strictly necessary to achieve the purposes of the transfers above specified and in accordance with applicable law
- Personal data disclosing health of the data subjects above identified only when strictly necessary to achieve the purposes of the transfers above specified and in accordance with applicable law.

ATTACHMENT 2

Pursuant to clause (h) the Supplier hereby agrees to meet the following additional specific Security Measures:

Security Program. Supplier shall use all reasonable commercial endeavors to implement and maintain comprehensive information security standards and a written program of such ("**Security Program**") that (i) complies with all applicable laws and regulations, including all Data Protection Legislation and (ii) contains reasonable and appropriate administrative, organisational, and physical safeguards, policies and procedures to preserve and protect the security, integrity, availability and confidentiality of all personal and commercially sensitive data being processed on behalf of CNA Hardy group.

Such safeguards and procedures shall include, at a minimum the use of all reasonable commercial endeavors to observe the following standards:

General Controls

(i) Conduct regular risk assessments, penetration tests, vulnerability scans and disaster recovery exercises.

(ii) All operating systems and applications must be under current support. Operating system and application security patches should be installed on all computing devices and kept up to date (e.g. desktops, laptops, tablets, mobile phones, servers, firewalls, switches).

(iii) Anti-virus/malware software must be installed and enabled to detect malicious programs (e.g. viruses, Trojans).

Network Security

(i) Deploy encryption and network segregation both internally and in relation to connectivity to external entities such as 3rd parties and internet facing to limit the exposure of sensitive information. Monitor network traffic to detect and react to any network intrusions. Utilising firewalls and intrusion detection systems, antivirus and malware detection, whilst ensuring that these are installed and maintained by qualified staff.

(ii) Secure wireless devices to trusted wireless networks, again utilising network segregation and relevant encryption practices.

(iii) Deploy security (and where possible encryption of data flow) in the connectivity to CNA Hardy group (and its group companies and group branch offices) and all third parties who may access Supplier's network;

(iv) Enable secure administration – utilising user access controls along with regular UAR and PUAR reviews.

User Access Controls

(i) All user access, and in particular privileged user access, should be appropriately approved and reviewed regularly

(ii) User Access should be controlled through updated protection programs, including Multi-Factor Authentication and access controls within media, applications, operating systems, and equipment;

(iii) Operating systems or applications having the capability to electronically capture and store user access must be installed and enabled. At a minimum, 14 days of relevant user access information should be maintained.

(iv) User IDs and passwords must be unique to each user and may not be shared.
(v) Strong password requirements must be enabled (e.g. alpha-numeric characters, minimum length, complexity, re-use restrictions).

Personal Data
(i) Personal data should be processed, stored, and transmitted in a secure manner including, without limitation, by means of encryption.
(ii) Personnel with access to personal data should be appropriately trained.
(iii) Internal systems or applications storing personal data should limit rights and privileges to those required in order to fulfill position requirements.

Back Ups
(i) Appropriate data backup and restoration procedures should be conducted at regular intervals for applications and information systems storing personal data.
(ii) Backup media must be secured from unauthorized physical access. If stored offsite, the backup media must be encrypted.

Physical Security
(i) Systems must be physically secured in areas with restricted access;
(ii) Portable computer or storage devices must be physically secured (e.g. cable & lock) if left unattended for extended periods of time.

Network Diagram. Supplier shall at any time upon on request, provide CNA Hardy group with a network diagram that outlines Supplier's information technology network infrastructure and all equipment used in relation to fulfilling its obligations under this Agreement, including, without limitation: (i) connectivity to CNA Hardy group (and its group companies and group branch offices) and all third parties who may access Supplier's network; (ii) all network connections, including remote access services and wireless connectivity; (iii) all access control measures (for example, firewalls, packet filters, intrusion detection and prevention services, and access-list-controlled routers); (iv) all back-up or redundant servers; and (v) permitted access through each network connection. Supplier shall promptly provide CNA Hardy group with an updated network diagram in the event Supplier makes any material changes to its infrastructure and/or equipment.

Right to Audit.
In addition to all audit rights under the main body of this Agreement, Supplier shall provide CNA Hardy group and any of its designated third party auditors with access to, and assistance and information regarding the service locations and the Security Program as necessary to confirm compliance with the terms of this Appendix. During any such audit, Supplier shall provide all assistance reasonably required in order to verify the adequacy and ensure continued maintenance of Supplier's Security Program. Additionally, CNA Hardy group and any of its designated third party auditors may conduct authorized intrusion attacks on the Supplier system; provided, that: (i) Supplier is notified of such attack in advance; and (ii) the parties mutually agree upon the intrusion testing plan. The frequency of any audit under this provision shall be at such intervals as deemed reasonably necessary by CNA Hardy group, in its sole discretion.

"Multi-Factor Authentication" means authentication through verification of at least two of the following types of authentication factors:

Knowledge factors, such as a password; or
Possession factors, such as a token or text message on a mobile phone; or
Inherence factors, such as a biometric characteristic.

ATTACHMENT 3

UK Registered Companies

	Company Name	Company Number	Registered Office
1	Hardy (Underwriting Agencies) Limited	1264271	20 Fenchurch Street, London, EC3M 3BY, United Kingdom
2	Hardy Underwriting Limited	02981735	20 Fenchurch Street, London, EC3M 3BY, United Kingdom
3	CNA Insurance Company Limited	950	20 Fenchurch Street, London, EC3M 3BY, United Kingdom
4	CNA Europe Holdings Limited	3526047	20 Fenchurch Street, London, EC3M 3BY, United Kingdom
5	CNA Services (UK) Limited	8836589	20 Fenchurch Street, London, EC3M 3BY, United Kingdom
6	Maritime Insurance Company Limited	4000324	20 Fenchurch Street, London, EC3M 3BY, United Kingdom
7	CNA Hardy International Services Limited	09849484	20 Fenchurch Street, London, EC3M 3BY, United Kingdom
8	CNA Insurance Company (Europe) S.A.	FC035780	20 Fenchurch Street, London, EC3M 3BY, United Kingdom

European Branches/Company

	Company Name	Company Number	Branch Office
1	CNA Insurance Company (Europe) S.A.	CNA Insurance Company (Europe) S.A., registered with the Luxembourg Trade and Companies Register under number B222697	35F, avenue John F. Kennedy, L-1855 Luxembourg
2	CNA Hardy Belgium Branch	CNA Insurance Company (Europe) S.A., registered with the Luxembourg Trade and Companies Register under number B222697	Succursale Belge, Avenue Charles-Quint 586, 1082 Bruxelles, Belgium
3	CNA Hardy Denmark Branch	CNA Insurance Company (Europe) S.A., registered with the Luxembourg Trade and Companies Register under number B222697	Hammerensgade 6, 1 sal, 1267 København K, Danmark
4	CNA Hardy France Branch	CNA Insurance Company (Europe) S.A., registered with the Luxembourg Trade and Companies Register under number B222697	5th Floor, 52-54 rue de la Victoire, 75009 Paris, France
5	CNA Hardy Germany Branch	CNA Insurance Company (Europe) S.A., registered with the Luxembourg Trade and Companies Register under number B222697	Im Mediapark 8, D-50670 Cologne, Germany, HRB 63197
6	CNA Hardy Italy	CNA Insurance Company (Europe) S.A., registered with the Luxembourg Trade and Companies Register under number B222697	Via Albricci 8, 20122, Milano, Italy
7	CNA Netherlands Branch	CNA Insurance Company (Europe) S.A., registered with the Luxembourg Trade and Companies Register under number B222697	Polarisavenue 140, 2132 JX Hoofddorp, Netherlands

International Registered Companies

	Company Name	Company Number	Registered Office
1	Hardy Underwriting Asia PTE Limited	Reg. No. 201018369K a Lloyd's Asia service company trading on behalf of Hardy Syndicate 382.	138 Market Street, Capita Green, #03-03, Singapore 048946
2	Hardy Bermuda Limited	43005	Crawford House, 50 Cedar Avenue, Hamilton, HM11, Bermuda
3	Hardy Underwriting Bermuda Limited	40834	Crawford House, 50 Cedar Avenue, Hamilton, HM11, Bermuda
4	Hardy Underwriting Labuan Limited	LL14346	Kensington Gardens, No. U1317, Lot 7616, Jalan Jumidar Buyong, 87000 Labuan F.T., Malaysia