

Cyber and Technology Professional Indemnity

PROPOSAL FORM

Contents

Section 1 – General Information

Section 2 – Cover Required and Current Insurance Information

Section 3 – Organisation and Financial Information

Section 4 – Personnel Policies and Procedures and Vendor Management (1st and 3rd Party Cyber)

Section 5 – Computer System and Information Security Programme (1st and 3rd Party Cyber)

Section 6 – Technology Professional Indemnity

Section 7 – Technology Professional Indemnity – Intellectual Property Rights (IPR)

Section 8 – Declaration

Important

Please answer all questions in sections 1, 2, 3, 4 and complete the declaration in Section 8

Only complete sections 5, 6, or 7, where cover is required for those sections.

The word 'you' or 'your' used in this form will refer to all identified entities in addition to the Proposer in Q1

Please complete in BLOCK CAPITALS

Tick the appropriate boxes where necessary and supply any further information requested. If there is insufficient space to complete any answer, please continue at the end of this form or on a separate sheet of paper.

Whilst we ask for your website address this in no way derogates from your duty of utmost good faith in answering this proposal form. Even if some or all of the answers can be given by reference to your website, you should nonetheless set out your full answers here and also provide us with any other material information.

Please take all reasonable care to answer all of the questions honestly and to the best of your knowledge. If you do not answer the questions correctly, your policy may be cancelled and any claim rejected or not fully paid. The completion and signature of this proposal does not bind the proposer or Travelers to complete a contract of insurance. Please refer to the policy wording for details of the cover provided.

SECTION 1 - GENERAL INFORMATION

1. Full name of Proposer including trading names if any (if not a limited company include full names of partners):

Date Established:

2. Correspondence Address

Postcode:

3. Website address(es):

4. Business Description (to appear on the policy):

SECTION 2 – COVER REQUIRED AND CURRENT INSURANCE INFORMATION

5. Please complete those sections for which you are requesting coverage:

Cover title	Cover required Y/N	Retroactive Date required	Limit of Indemnity required	Deductible required
Cyber Business Costs (1st Party Cyber)	Yes No	N/A		
Cyber Business Costs Optional Cover – Social Engineering Fraud	Yes No	N/A		
Technology Professional Indemnity	Yes No			
Intellectual Property Rights	Yes No			
Cyber Liability (3rd Party Cyber)	Yes No			

6. Which of the following Cyber Business Interruption Basis of Settlement(s) do you require if purchasing Cyber Business Costs cover:

Cyber Business Interruption Basis Of Settlement options	Required? Y/N	
Gross Profit Flexible Limit of Loss (incl. ICOW)?	Yes	No
Gross Revenue Flexible Limit of Loss (incl. ICOW)?	Yes	No
Continuing Expenses and Research and Development ICOW?	Yes	No

7. Date cover required from:

8. Do you currently have cover in place for the risks you wish to insure? Yes No

If 'Yes', please give details below:

Cover title	Insurer	Policy number	Retroactive Date	Limit	Expiry Date
Professional Indemnity					
Intellectual Property Rights					
Cyber Liability (3rd Party Cyber)					
Cyber Business Costs (1st Party Cyber)			N/A		

9. For the sections you wish to cover has any insurer ever:

- a) Declined your proposal? Yes No
- b) Declined to pay a claim in full or in part? Yes No
- c) Cancelled or declined to renew your insurance? Yes No
- d) Applied special terms? Yes No

If you have answered 'Yes' to any of the above, please give details:

10. Have you or any partner or director ever been:

- | | | |
|---|-----|----|
| a) Convicted of or charged (but not yet tried) with a criminal offence other than a motoring offence or “spent” conviction as allowed for under the Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016 (Ireland) or the Rehabilitation of Offenders Act 1974 (UK). | Yes | No |
| b) A partner or director of a company which went into liquidation, receivership or administration? | Yes | No |
| c) Declared bankrupt? | Yes | No |
| d) Disqualified from being a director? | Yes | No |

If you have answered ‘Yes’ to any of the above, please give details:

11. Please give details of your claims history for the previous five years. For each claim, provide details of the action you have taken to prevent a reoccurrence (use the Additional Information box at the end of this proposal form):

Cyber (if purchasing 1st or 3rd Party Cyber)		
Year	Claim details	Total Payment
		£
		£
		£
		£

Technology Professional Indemnity / Intellectual Property Rights (if purchasing either cover)		
Year	Claim details	Total Payment
		£
		£
		£
		£
		£

SECTION 3 – ORGANISATION AND FINANCIAL INFORMATION

12. Please provide details of any subsidiaries, partnerships or joint ventures for which cover is required. If there are none, please leave this question blank.

Name	Status (e.g. subsidiary)	Country	Nature of activities	Date established

13. Has the name of the business changed or have any mergers, acquisitions or divestitures taken place during the past five years?

Yes No

If 'Yes',

a) Please give details including the dates of the transaction(s):

b) Did your due diligence process include the following:

- i. Review of prior and pending litigation? Yes No
- ii. Evaluation of all outstanding contracts or service agreements that will be included as part of the transaction? Yes No
- iii. Analysis of intellectual property rights of that entity, including any third party interest in, or liens on those rights? Yes No

14. Please give details of your Turnover:

Source	For the last financial year ending	For the current financial year ending	Estimated for the forthcoming financial year ending
UK	£	£	£
Europe	£	£	£
Rest of the World ex USA/Canada	£	£	£
USA/Canada	£	£	£
Total Turnover	£	£	£

15. Please give the appropriate percentage of Turnover derived from:

Description		Percentage for the current financial year	Percentage for the forthcoming year
Consultancy	Work under clients control	%	%
	General consultancy/advice	%	%
	System or programme design and/or advice	%	%
	Project management	%	%
Software	Distribution of third party software	%	%
	Package software writers	%	%
	Third party software without subrogation	%	%
	Tailoring of software modified for specific client(s)	%	%
	Bespoke software provision	%	%

Description		Percentage for the current financial year	Percentage for the forthcoming year
Internet	Web design, passive	%	%
	Web design, interactive	%	%
	Web design including e-commerce	%	%
	Data facility management & hosting	%	%
Computer Hardware	Distribution of computer hardware and peripherals	%	%
	Manufacture of computer hardware and peripherals	%	%
	Maintenance including software configuration	%	%
Electronic Components	Supply of passive components	%	%
	Supply of active components including lasers	%	%
	Supply of semiconductors	%	%
Electronic Equipment	Supply of telecommunications hardware (not mobiles)	%	%
	Manufacture of robotics, process control equipment or control panels	%	%
	Software for electronic equipment	%	%
Other		%	%

16. Identify the principal markets for your products or services:

Description	Percentage For the Current Financial Year	Percentage For the Forthcoming Year
Government		
Defence		
Financial &/or Trading Systems/Services		
Critical control equipment		
Energy/Utilities/Nuclear/Petrochemical		
Gaming/Gambling		
Healthcare/Medical		
Emergency Services		
Aviation/Aircraft/Aerospace		
Railway		
Automotive		
Other (please give details)		

SECTION 4 – PERSONEL POLICIES AND PROCEDURES AND VENDOR MANAGEMENT

(Only complete this section if you require cover for Cyber Business Costs or Cyber Liability as indicated in Q.5)

17. a) Do you conduct training regarding security issues and procedures for employees that utilise computer systems? Yes No
- b) If yes, are your employees periodically tested? Yes No
18. Do you publish and distribute written computer and information systems policies and procedures to your employees? Yes No
19. Do you terminate all associated computer access and user accounts as part of the regular exit process when an employee leaves the company? Yes No
20. Do you have regular (at least every 90 days) mandatory password updates for all systems providing access to personal and confidential information or other business critical operations? Yes No
21. Do you currently use a Cloud Service Provider in the course of business operations? Yes No

Name of Cloud Provider(s):

SECTION 5 – COMPUTER SYSTEM AND INFORMATION SECURITY PROGRAMME

(Only complete this section if you require cover for Cyber Business Costs or Cyber Liability as indicated in Q.5)

22. Who is responsible for information security within your organisation?

Name and Job Title:

23. Do you have a comprehensive written information security programme, including procedures documenting how any changes are made to the programme? Yes No
24. Do you have a company policy or procedure for secure care, handling and storage of private, sensitive or confidential information on portable communication devices (e.g. laptops, tablets or smartphones)? Yes No
25. Are you compliant with the Payment Card Industry Data Security Standard (PCI-DSS)? Yes No
- If 'Yes',
- a) What is your Merchant Level i.e. 1, 2, 3, or 4?
- b) What is your total number of annual credit card transactions?
- c) Have you successfully completed an annual cycle of compliance for the framework? Yes No
26. Do you currently hold or are you compliant with any of the following:
- a) Cyber Essentials Certificate? Yes No
- b) Cyber Essentials Plus Certificate? Yes No
- c) ISO27001 (Information Security Management System)? Yes No
27. Is remote access for portable communication devices restricted to Virtual Private Networks (VPNs)? Yes No
28. Do you have a written privacy policy? Yes No
- If 'Yes',
- a) Does it specify the specific data you may collect and how you or others may use data? Yes No
- b) Does it identify if you share or sell any user/customer data with other parties? Yes No
- c) Does it specify how your users/customers can opt in or opt out regarding privacy? Yes No
- d) Does it specify how your user/customer information is secured? Yes No
- e) Is it publicly available on your website? Yes No
- f) How often do you review and update your privacy policy? Annually Bi-Annually
- g) How often do you perform audits to ensure compliance? Annually Bi-Annually

29. Is user specific, private, sensitive or confidential information stored on your servers encrypted? Yes No
- If 'Yes',
- a) Is data at rest encrypted? Yes No
- b) Is data in transit encrypted? Yes No
30. a) Do you have multi-factor authentication for all employees when accessing e-mail through a website or cloud based service. Yes No
Email is not web based
- b) Do you have multi-factor authentication for all remote access to the network provided to employees, contractors, or 3rd party service providers. Yes No
- c) In addition to remote access, do you have multi-factor authentication for the following, including where such access is provided to employees, contractors, or 3rd party service providers:
- All internal and remote administrative access to directory services (active directory, LDAP, etc.). Yes No
- All internal and remote administrative access to network backup environments. Yes No
- All internal and remote administrative access to network infrastructure (firewalls, routers, switches, etc.). Yes No
- All internal and remote administrative access to the organization's endpoints/servers. Yes No
- If 'No' to any of the above, explain why you do not have them:
-
-
31. Are all your mobile computing devices (including tablets, mobile phones, laptops and any personal employee devices where these are used to access your network) and portable data storage (including USB sticks, portable hard drives and flash drives) encryption enabled? Yes No
32. Is the responsibility for the secure care, handling and storage of private, sensitive or confidential information of others addressed in your contracts with your customers? Yes No
33. Is the responsibility for the secure care, handling, and storage of private, sensitive or confidential information others addressed in your contracts with your sub-contractors, independent contractors or third-party vendors who may have access to or use of this information? Yes No
- If 'Yes',
- a) Does this include a condition that third party vendors are responsible for end of life-cycle document destruction? Yes No
- b) Does this include third party custodians such as housekeeping or maintenance or others who may regularly have access to your premises? Yes No
34. Do you have a data segmentation programme that separates data by sensitivity levels? Yes No
- If 'Yes' for which of the following do you have varying protections based on the level of sensitivity of data? (select all that apply):
- Access control Data Destruction Encryption Data Handling and Retention Other
35. Do you run anti-virus software across all components of your network? Yes No

36. Do you have in place Endpoint Detection and Response (EDR)? Yes No
- If 'Yes', what specific service is used?
- Bitdefender GravityZone Ultra
 - Blackberry Cylance CylanceOPTICS
 - CrowdStrike Falcon
 - Cybereason Ultimate
 - Elastic Security
 - Kaspersky EDR
 - McAfee MVISION EDR
 - Microsoft Defender Advanced Threat Protection
 - Palo Alto Networks Cortex XDR
 - SentinelOne Complete
 - Symantec (Broadcom) Complete Endpoint Defense
 - Trend Micro Apex One with Endpoint Sensor
 - VMware Carbon Black
 - Other (provide details regarding vendor and the specific product)
37. Do you maintain computer system logs and generate exception reports to monitor:
- a) Unacceptable or restricted transactions? Yes No
 - b) Correcting or reversing entries? Yes No
 - c) Unsuccessful attempts to access restricted information on the site? Yes No
38. Identify who provides or maintains the following safeguards:
- a) Intrusion detection software? You Vendor N/a
 - b) Vulnerability or penetration testing? You Vendor N/a
 - c) Backup and recovery processes? You Vendor N/a
39. a) How often is valuable / sensitive data backed up?
- b) How often do you verify that the back-up was successful?

40. Do you have a process in place to ensure all antivirus protection, software updates/patches and equipment security settings are properly installed in a timely manner? Yes No
41. Do you have regular policies and procedures for identifying computer system vulnerabilities and obtaining remedial software patches? Yes No
42. Do you have a firewall installed and configured (hardened) to protect your computer system? Yes No
43. Do you have an outside party conduct an audit of your internal work or computer systems? Yes No

If 'Yes',

- a) How often is the audit conducted?
- b) What date was the last audit?
- c) Explain any recommendations not yet implemented?

44. Do you have a written policy for document retention along with end of lifecycle destruction that includes paper and electronic records? Yes No
- If 'Yes', do you use a third-party vendor? Yes No

45. With respect to computer systems, do you have? (select all that apply):

Secondary/Back up computer systems	Business Continuity Plan	Disaster Recovery Plan	Incident Response Plan for computer system intrusions and virus incidents
------------------------------------	--------------------------	------------------------	---

If 'Yes' to any of the above,

- a) How often are such plans tested?
- b) If a secondary/back up system is in place, how long before this system becomes operational?
- c) If you have a Business Continuity Plan for your computer systems, does your plan address a disruption to an IT provider * or an Outsource provider**? IT Provider Outsource N/a

* Provides IT services such as web hosting, software, platform and infrastructure services, telecommunications, electronic data or back-up storage services

** Provides any service (except IT) necessary to conduct your business

46. Please indicate which of the following types of data are collected, received, processed, transmitted, or maintained as part of your business activities:

- | | | |
|---|-----|----|
| a) Credit or debit card data | Yes | No |
| b) Bank accounts and records | Yes | No |
| c) National Insurance numbers | Yes | No |
| d) General customer information (e-mails, user ID's, passwords) | Yes | No |
| e) Medical information/health records | Yes | No |
| f) Employee/HR information | Yes | No |
| g) Intellectual property of others | Yes | No |
| h) Children's information | Yes | No |
| i) Other | Yes | No |

If Other, please specify:

47. What is the maximum number of unique individuals for whom you collect, store or process any amount of confidential information (annually)?

- | | | | |
|----------|---------------------|-----------------------|------------|
| <500,000 | 500,001 - 1 million | 1 million - 5 million | >5 million |
|----------|---------------------|-----------------------|------------|

48. Do you outsource any of the following:

- | | | |
|--|-----|----|
| a) Web hosting/Data centre operations? | Yes | No |
| b) Data/Transaction processing? | Yes | No |
| c) Computer system security? | Yes | No |
| d) Customer service? | Yes | No |

List all IT or outsource providers, along with the service they provide for you:

49. Do your contracts with your IT service providers or outsource providers for the above services address the following:

- | | | |
|---|-----|----|
| a) Provide you with indemnification for provider misconduct, errors, omissions and negligence? | Yes | No |
| b) Identify the provider's responsibilities for safeguarding customer and confidential information? | Yes | No |
| c) Identify the security measures that the provider will provide or follow? | Yes | No |

50. Do you have formal procedures for reviewing IT or outsource providers' security practices? Yes No

51. Do you have a written data breach response plan in place? Yes No

If 'Yes': How often is this plan tested?

What was the date of the last test?

Explain any recommendations not yet implemented:

52. Has your company contracted with outside vendors (e.g. forensics, legal services, public relations and prearranged services) to assist in the event that you would need to execute your data breach response plan? Yes No

53. Do you have an alternative means of transacting business in the event of a computer system or website outage? Yes No

54. The following questions (a) – (j) must be answered if you require cover for Social Engineering Fraud as indicated in Q5.

a) Do you make payments to third parties via a wire-transfer system? Yes No

If Yes, how frequently are such payments made:

b) Do you provide anti-fraud training, including social engineering, phishing, masquerading, and other fraud schemes, to all employees responsible for authorising and executing payments or funds transfer requests? Yes No

c) Do payments or funds transfers of a certain amount require dual authorisation? Yes No

d) Do you have procedures in place to verify the receipt of inventory, supplies, goods, or services against an invoice prior to paying a vendor? Yes No

e) Do you confirm all change requests regarding vendor account information (including changes to bank account information, invoice changes, telephone or fax numbers, location, and contract information) by a direct call to the vendor using only the telephone number provided by the vendor before the change request was received? Yes No

f) Do you accept payments or funds transfer instructions from clients relating to a refund or repayment of goods, services, or funds held in your custody? Yes No

If Yes, describe the communication methods by which such instructions are deemed acceptable (e.g. telephone, email, text message, fax, general mail, etc.):

g) Do you confirm all such payments or funds transfer instructions made by clients by a direct call to the client using only the telephone number provided by the client before the payment or funds transfer request was received? Yes No

h) Do you have procedures in place to verify the authenticity of any payment or funds transfer request made by an internal company source (e.g. another employee, subsidiary, location, or department) and which was received by an employee authorised to initiate such payment or transfer request? Yes No

If Yes, describe such procedures:

i) If you answered No to any part of Questions d, e, f, g, or h, provide details here:

j) Have you sustained any Computer or Social Engineering Fraud losses during the past three years? Yes No

If Yes, please include the details in Q11.

55. Have you discovered any telecommunications theft or been contacted by any provider regarding possible abuse of your telecommunication system within the past 5 years? Yes No

56. Does each location or system have the Call Detail Recording feature? Yes No

If 'Yes', how often is this information reviewed?

57. What procedures do you have to risk review your website content and mitigate any issues identified?

58. Do you offer bulletin/chat room or other third party discussion/comment facilities through your website? Yes No

If 'Yes' please provide details of any pre or post publication moderation and your takedown procedure in the event of a complaint regarding third party content being received:

59. a) What percentage of your software updates are sent via e-mail/internet? %

b) What is the approximate number of your updates provided each year?

60. Within the past 5 years, have you:

- | | | |
|--|-----|----|
| a) Sustained any computer system intrusion, virus attack, hacking incident, data theft or similar event? | Yes | No |
| b) Experienced a computer system or website outage as a result of a computer system disruption? | Yes | No |
| c) Ever been the subject of a ransomware attack? | Yes | No |
| d) Ever been the subject of any other type of cyber extortion attack? | Yes | No |
| e) Had to notify customers or employees that their private, sensitive or confidential information may have been compromised? | Yes | No |

If you have answered 'Yes' to any of the above, please advise when and what steps have been taken to minimise recurrence of such an event:

- | | | |
|--|-----|----|
| 61. After enquiry, are you or any of your partners, directors, employees aware of any incident that could reasonably give rise to a claim for the Cyber Business Costs or Cyber Liability covers you are now requesting in Q5? If so, please provide full details. | Yes | No |
|--|-----|----|

SECTION 6 – TECHNOLOGY PROFESSIONAL INDEMNITY
 (Only complete this section if you require cover for Technology Professional Indemnity as indicated in Q.5)

- | | | |
|--|-----------|---------------|
| 62. Please tick the basis of cover required: | Aggregate | Any One Claim |
|--|-----------|---------------|

63. What is the average size of your contracts currently in force?

Length (average number of months)	Average contract value
	£
	£
	£

64. Please give details of the 3 largest contracts currently in force:

Customer (type or name)	Length (average number of months)	Contract value (full contract)	Service provided
		£	
		£	
		£	

65. In the event of the failure of any of your products or services, please estimate the level of financial loss which your clients could sustain:

- | | | |
|--------------------------------------|-----|----|
| Insignificant? | Yes | No |
| Minor affecting one party? | Yes | No |
| Minor affecting multiple parties? | Yes | No |
| Moderate affecting one party? | Yes | No |
| Moderate affecting multiple parties? | Yes | No |
| Severe affecting one party? | Yes | No |
| Severe affecting multiple parties? | Yes | No |

If you have answered 'Yes' to any of the above, please provide details:

66. Are you certified (or accredited), or in the process of becoming certified (or accredited), to a recognised industry standard e.g. ISOEN 9001:2015? Yes No
- If 'No' is anyone responsible for Quality control? Yes No
- If 'Yes' does the person report to senior management? Yes No

If 'Yes' what certifications and accreditations do you hold or are working towards:

67. What do you consider to be the most significant potential risks associated with the activities declared and how have these been minimised?

68. Do you always prepare and agree a written specification of the intended work with your clients (including written confirmation of verbal instructions) before contracts are accepted and are amendments made to the same as appropriate during contract stages?

Yes No

If 'No' please provide details as to why not:

69. Please indicate the percentage of contracts where your standard terms are used:

Please supply a copy.

70. What is the typical liability cap in your contracts?

71. Do you use conditions of contract in every case?

Yes No

If 'No' please provide an explanation.

72. Do your contracts include any Hold Harmless agreements or guarantees?

Yes No

If 'Yes' please give details:

73. Do you negotiate contracts or agreements in which you accept liability for consequential damages? Yes No

If 'Yes' what is the maximum limit of liability:

£

74. Do you intend to undertake or have you ever undertaken any contracts which go beyond the provision of reasonable skill and care? Yes No

If 'Yes' please give details:

75. Does your legal counsel review all contracts and agreements other than standard contracts that you use? Yes No

Why and when would you involve your legal counsel for contracts:

76. Do you carry out an appropriate and effective testing or acceptance process (whether conducted in stages or not) to establish whether products & services function as intended by you and the client? Yes No

If 'No' please give details as to why not

77. a) Do you have a formal procedure for customer complaints? Yes No

b) Are customer complaints reviewed by senior management at regular intervals? Yes No

If 'Yes', how often are they reviewed:

78.

a) Do you engage independent or specialist consultants or sub-contractors? Yes No

If 'Yes' please provide the following details as they apply to the consultants or sub-contractors:

Type of work	Location	Amount paid (annually)	Insurer providing Professional Indemnity Insurance	Limit of indemnity

b) Have they entered into a binding contract with you accepting full responsibility for their own professional neglect, error or omissions? Yes No

c) Please provide details of how you manage the quality and timeliness of consultant and sub-contractor services (for example through the use of an on-site manager/periodic visits etc.): Yes No

d) Within the past 5 years, have you changed any consultant or sub-contractor due to breach of a service agreement or quality of deliverable? Yes No

If 'Yes', please give details:

79. Within the past 5 years, have you sued any customers for non-payment of fees? Yes No

80. After enquiry, are you or any of the partners, directors or employees aware of any pending loss, dispute, fact, circumstance, situation, event or act that could reasonably give rise to a claim? Yes No

If 'Yes', please provide full details:

SECTION 7 – TECHNOLOGY PROFESSIONAL INDEMNITY - INTELLECTUAL PROPERTY RIGHTS (IPR)

(Only complete this section if you require cover for Intellectual Property Rights as indicated in Q.5)

81. What percentage of turnover is derived from:

a) Products (including software) less than 1 year old?

 %

b) Products (including software) over 1 year old?

 %

c) Upgrades for existing Products (including software)?

 %

82. How much original content is created by you?

 %

83. Please advise whether legal counsel are consulted in respect of the following:

- | | | |
|--|-----|----|
| a) Prior to release of new software/products (including review of content, characters and any original game software)? | Yes | No |
| b) Searches for all trademarks, patents and other intellectual property rights | Yes | No |
| c) Use of third party rights through licences and permissions? | Yes | No |

If you answered 'Yes' to any of the above please advise name and address of external legal counsel (or if in-house counsel are used please confirm this):

If you answered 'No' to any of the above please advise what steps are taken to reduce the risk of breaching a third party's IPR:

84. Do your contracts include, specifically in respect of intellectual property rights, subrogation rights against third party suppliers of any products which are found to be in breach? Yes No

85. What measures do you follow to ensure that new employees are aware of and comply with duties of confidentiality in connection with former employers' intellectual property rights and other proprietary information?

86. Within the past five years, have you received any notification that any of your material content, products or services infringe on the intellectual property rights of another party? Yes No

If 'Yes' please give full details:

Additional Information

Please use this space to disclose any further relevant information or if there is insufficient space available to answer any of the questions fully, clearly identifying the question number in each case:

SECTION 8 – DECLARATION

Must be signed by a Partner / Director

I/We declare that to the best of my/our knowledge or belief, the statements and particulars given in this proposal are true and complete and that no material facts that are likely to influence the acceptance and assessment of this proposal have been withheld. (If you are in any doubt as to whether a fact is material, you should disclose it).

I/We agree to inform Travelers of any change to any material fact.

I/We also declare that if any information on this proposal has been written by another person on my/our behalf, that person acted as my/our agent for that purpose.

I/We have read the above and declare that to the best of my/our knowledge and belief the statements are true and complete.

Signature of the Proposer

Print Name and position held:

For and on behalf of *(insert name of company/firm)*

Date:

NO COVER IS IN FORCE UNTIL THIS PROPOSAL HAS BEEN ACCEPTED BY THE COMPANY AND THE PREMIUM PAID, EXCEPT AS PROVIDED BY AN OFFICIAL COVERING NOTE ISSUED BY THE COMPANY.

PLEASE RETAIN A COPY OF THIS COMPLETED PROPOSAL FORM FOR YOUR RECORDS.

USING PERSONAL INFORMATION

How we treat information about you and your rights under data protection legislation.

In order to provide our insurance services, we (Travelers acting as a Data Controller) will collect certain personal information about you. The type of information that we collect will depend on our relationship with you. For example, you may be a Travelers policyholder, prospective policyholder or a third party making a claim under a Travelers insurance policy.

If you provide us with personal information about a third party, you should share this notice with them.

We will also collect different types of information depending upon the kind of insurance cover we are being asked to provide or the kind of claim we are being asked to assess or pay.

Some of the information we collect may be classified as 'special category data', which is data that may contain information about physical or mental health, religious beliefs and criminal and disciplinary offences (including convictions).

Your personal information may be used in a number of ways including:

- considering an application for insurance,
- providing and administering an insurance policy,
- handling claims including claims validation,
- preventing and detecting fraud, including providing information to the relevant authorities.

Where relevant, we will share your information with other companies in the Travelers group, third parties such as claims handlers, loss adjusters, other insurers and reinsurers, fraud prevention agencies, service companies associated with our products, or as required by law (including providing the information to government or regulatory authorities). This may involve the transfer of your information to countries inside and outside the European Economic Area.

We may also use your personal information for marketing purposes, but only in accordance with your marketing preferences.

For more information about how we process your data and the rights you have please click www.travelers.co.uk/privacy-policy



Travelers operates through several underwriting entities through the UK and across Europe.
Please consult your policy documentation or visit the websites below for full information.