



Privacy Questionnaire

You can complete this form on-screen and e-mail it to your insurance broker or adviser. Simply click the cursor to the right of 'Company name' below then use the 'tab' key to move through the form. Alternatively, print out the form, complete it manually and post or fax it to your insurance broker or adviser.

TO E-MAIL THE FORM, SAVE WHEN COMPLETED AND SEND AS AN ATTACHMENT

Company or trading name

1 Transaction information

- a Percentage of gross annual revenue accounted for by sales or operations through your website %
- b Percentage of annual transactions paid for by debit/credit card %
- c Average transaction value

2 Business continuity

- a Briefly describe your recovery/contingency plans to avoid business interruption due to IT system failure, and/or alternative working procedures (interdependency, outsourcing, alteration of process, additional employment, redundant servers etc). Use a separate sheet if necessary.

- b Is this plan regularly tested and updated? Yes No
- c Have you recently carried out an IT security audit? Yes No

If 'Yes', who did it and when was it performed?

Audited by	DD	MM	YY
------------	----	----	----

- d When was your last external penetration test carried out? DD MM YY
- e Was any serious concern raised with any aspect of the network where immediate correction was advised? Yes No
- If 'Yes' to (e) above, were the recommendations carried out? Yes No

3 Network security

- a Do you employ a Chief Privacy Officer, or Chief Information Officer, who has responsibility for meeting your worldwide obligation under privacy and data protection laws? Yes No
- b Does your security and privacy policy include mandatory training for all employees? Yes No
- c Are all employment positions analysed and employees assigned specified rights, privileges and unique user ID and passwords, which are changed periodically? Yes No
- d Do you have strict user revocation procedures on user accounts and inventoried recovery of all information assets following employment termination? Yes No
- e Do you conduct regular reviews of your third party service providers and partners to ensure that they meet your requirements for protecting sensitive information in their care? Yes No

Section 3 continued

- f Do you enforce provisions for non compliance by employees, contractors and others? Yes No
- g Do you have antivirus software on all computer devices, servers and networks which are updated in accordance with the software providers' recommendations? Yes No
- h Do you have firewalls and intrusion monitoring detection in force to prevent and monitor unauthorised access? Yes No
- i Do you have access control procedures and hard drive encryption to prevent unauthorised exposure of data on all laptops, PDAs, smartphones (e.g. BlackBerry), and home-based PCs? Yes No
- j Have you configured your network to ensure that access to sensitive data is limited to properly authorised requests? Yes No
- k Do you ensure that all wireless networks have protected access? Yes No
- l Do you encrypt all sensitive information that is physically removed from the premises by tape, disk hard drive or other means? Yes No
- m Is all sensitive and confidential information that is transmitted within and from your organisation encrypted using industry grade mechanisms? Yes No
- n Is all sensitive and confidential information stored on your databases, servers and data files encrypted? Yes No

4 Information and data management

- a Does your information asset programme include a data classification standard (e.g. public, internal use only, confidential)? Yes No
- b Do you post a privacy policy on your website which has been reviewed by a qualified lawyer? Yes No
- c Do you have an information asset inventory that lists the owners and sources of all data? Yes No
- d Do you have procedures in force for honouring the specific marketing 'opt-out' requests of your customers that are consistent with the terms of your published privacy policy? Yes No
- e Do you have procedures in force to monitor the period for which customer data is held, and have processes for deleting this information at the end of that period? Yes No
- f Do you have procedures in force for deleting all sensitive data from systems and devices prior to their disposal from the company? Yes No
- g Is all information held in physical form (paper, disks, CDs etc) disposed of or recycled by confidential and secure methods which are recognised throughout the organisation? Yes No
- h Do you keep an incident log of all system security breaches and network failures? Yes No
- i Have you identified all relevant regulatory and industry compliance frameworks Yes No

Please provide details:

Compliant				Date of latest audit
Gramm-Leach Bliley Act of 1999	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>	
Health Insurance Portability & Accountability Act of 1996	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>	
Payment Card Industry (PCI) Data Security Standard	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>	
If 'YES', what level requirement?	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/> 4 <input type="checkbox"/>	
Other				

5 Network incidents (claims and circumstances)

- a Have you ever suffered an intentional breach of IT security, network damage, system corruption or loss of data? Yes No
- b Have you ever sustained a material or significant system intrusion, tampering, virus or malicious code attack, loss of data, hacking incident, data theft or similar incident or situation? Yes No
- c During the last three years has any customer or other person or entity alleged that their personal information was compromised? Yes No
- d During the last three years have you notified customers that their information was or may have been compromised? Yes No

Data Protection

By accepting this insurance you consent to Barbican using the information we may hold about you for the purpose of providing insurance and handling claims, if any, and to process sensitive personal data about you where this is necessary (for example health information or criminal convictions). This may mean we have to give some details to third parties involved in providing insurance cover. These may include insurance carriers, third party claims adjusters, fraud detection and prevention services, reinsurance companies and insurance regulatory authorities.

Where such sensitive personal information relates to anyone other than you, you must obtain the explicit consent of the person to whom the information relates both to the disclosure of such information to us and its use by us as set out above. The information provided will be treated in confidence and in compliance with relevant Data Protection legislation. You have the right to apply for a copy of your information (for which we may charge a small fee) and to have any inaccuracies corrected.

Important Privacy Questionnaire Statement of Fact

By accepting this insurance you confirm that the facts contained in this questionnaire are true. These statements, and all information you or anyone on your behalf provided before we agree to insure you, are incorporated into and form the basis of your policy. If anything in these statements is not correct, we will be entitled to treat this insurance as if it had never existed. You should keep this Statement of Fact, a copy of the completed application form and a copy of this questionnaire for your records.

This questionnaire must be signed by the applicant. Signing this form does not bind the company to complete the insurance.

With reference to risks being applied for in the United States, please note that in certain states, any person who knowingly and with intent to defraud any insurance company or other person submits an application for insurance containing any false information, or conceals the purpose of misleading information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime.

The undersigned is an authorised principal, partner, director, risk manager, or employee of the applicant and certifies that reasonable inquiry has been made to obtain the answers herein which are true, correct and complete to the best of his/her knowledge and belief. Such reasonable inquiry includes all necessary inquiries to my fellow principals, partners, directors, risk managers, or employees to enable me to answer the questions accurately.

Signature

Name

Position

For and on behalf of

Date

DD

MM

YY



Barbican Insurance
33 Gracechurch Street
London EC3V 0BT
+44 (0)20 7082 1955
www.barbicaninsurance.com

Barbican Managing Agency Limited manages Syndicate 1955 at Lloyd's and is authorised and regulated by the Financial Services Authority. It is registered in England and Wales under company number 6948515 with its Registered Office at 33 Gracechurch Street, London EC3V 0BT.