**Company or Trading Name:**

Address:

Post Code:

Telephone:

E-mail:

Website:

Date Business Established       Number of Employees

Do you have a Chief Privacy Officer (or Chief Information Officer)
who is assigned responsibility for your global obligations under
Data Protection and Privacy legislation? Yes [ ]  No [ ]

Desired Coverages

Covers Required Tick

Network Security and Privacy Liability [ ]

Multimedia Liability [ ]

Privacy Regulatory Defence and Penalties [ ]

Business Interruption and Additional Costs of working [ ]

Crisis Management [ ]

Cyber Extortion [ ]

Financial Information

Gross Annual Revenue: Last Year         Current Year         Next Year (est)

% of gross annual revenue account for by sales or operations through your website       %

% of annual transactions paid by debit/credit card       %

Average Transaction value

Percentage of last year’s gross annual revenue generated from:

US/Canadian clients subject to US/Canadian law       %

UK clients subject to UK law       %

RoW client       %

2017 IT system budget

Network and Data Security

Do you store, process and or transmit any Sensitive Data on Your Computer System

 Tick all that apply below

Credit card information [ ]

Customer Information [ ]

Healthcare information [ ]

Money/Securities information [ ]

Trade Secrets [ ]

Intellectual Property Assets [ ]

Do you process payments on behalf of others, including eCommerce transactions? Yes [ ]  No [ ]

Do you outsource any part of Your network, computer system or information security functions?

 Tick all Vendor name
 that apply providing services

Data center hosting [ ]

Managed Security [ ]

Data Processing [ ]

Application service Provider [ ]

Alert log monitoring [ ]

Offsite backup and storage [ ]

Do you require all vendors to whom You outsource data processing or
hosting functions (e.g. data backup, application service providers etc)
to demonstrate adequacy of their IT systems? Yes [ ]  No [ ]

If “yes”, please indicate method of verification:

………………………………………………………………………………………………………

Do you have strict user revocation procedures on user accounts and
inventoried recovery of all information assets following employee termination? Yes [ ]  No [ ]

Do you have anti-virus software on all computer devices, servers and networks
that are updated in accordance with the software providers’ recommendations? Yes [ ]  No [ ]

Do you have firewalls and intrusion monitoring detection in force to prevent
and monitor unauthorised access? Yes [ ]  No [ ]

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 [ ]

Is your network configured to ensure that access to sensitive data is limited
to properly authorised requests? Yes [ ]  No [ ]

Is all sensitive and confidential information stored on your databases,
servers and data files encrypted? Yes [ ]  No [ ]

Do you have a document retention and destruction policy within your organisation? Yes [ ]  No [ ]

Do you provide awareness training for employees in data privacy and security,
including legal liability issues, social engineering issues (e.g. phishing etc)? Yes [ ]  No [ ]

If “Yes” please describe the medium and frequency of such training.

………………………………………………………………………………………………………

Incident response / Crisis Containment

Do you have a security incident response plan in case of a security breach? Yes [ ]  No [ ]

Does your security incident response plan include alternative options to account
for incapacitated third party outsourcing providers who you depend on? Yes [ ]  No [ ]

Have you identified all regulatory and industry compliance frameworks Yes [ ]  No [ ]

Please provide details on the following compliance frameworks:

|  |  |  |
| --- | --- | --- |
| Compliant |  | Date of latest audit |
| Gramm-Leach Bliley Act 1999 | Yes [ ]  No [ ]  |       |
| Health Insurance Portability and Accountability Act of 1996 | Yes [ ]  No [ ]  |       |
| Payment Card Industry (PCI) Data Security StandardIf “Yes”, what level requirement | Yes [ ]  No [ ] 1 [ ]  2 [ ]  3 [ ]  4 [ ]  |       |

Do “You” have a Business Continuity Plan (BCP) and Disaster Recovery (DR) Plan? Yes [ ]  No [ ]

How long does it take to restore your operation after
a computer attack or other loss/corruption of data? 12h or less [ ]  13-24h [ ]  More than 24h [ ]

Indicate time after which the inability of staff
to access your internal computer network
and systems would have a significant
impact on your business Immediately [ ]  After 6h [ ]  After 12h [ ]  After 24h [ ]  After 48h [ ]

Is the operation and connectivity of your computer
network business critical? Yes [ ]  No [ ]

Indicate time after which the inability for customers
to access your website would have a significant
impact on your business? Immediately [ ]  After 6h [ ]  After 12h [ ]  After 24h [ ]  After 48h [ ]

Briefly describe your recovery/contingency plans to avoid business interruption due to IT system failure, and/or alternative working procedures (interdependency, outsourcing etc)

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

Historical Information

Has any insurer ever cancelled or non-renewed a policy that provided the
same or similar coverage as the insurance sought? Yes [ ]  No [ ]

Are You aware of any actual or alleged fact, circumstance, situation,
error or omission, or issue which might give rise to a Claim against
You under the insurance sought? Yes [ ]  No [ ]

If “Yes,” please explain:

Are you aware of any circumstances or incidents that have resulted in any claim
against you and/or a claim against any insurance policy that provides the type of
coverage being requested in this application? Yes [ ]  No [ ]

Have you or any past or present principal, partner, director or employee been
subject to any disciplinary action or governmental action or investigation as a
result of professional activities? Yes [ ]  No [ ]

During the past three years, have You experienced an interruption or suspension
of Your computer system for any reason (not including downtime for planned
maintenance), which exceeded 4 hourss? Yes [ ]  No [ ]

Have you ever suffered an intentional breach of IT security, network damage,
system corruption, or loss of data? Yes [ ]  No [ ]

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 [ ]

During the last three years has any customer or other person or entity alleged
that their personal data has been compromised? Yes [ ]  No [ ]

During the last three years have you notified customers that their information
was or may have been compromised? Yes [ ]  No [ ]

Have You reported any occurrences, claims or losses to any Insurer in the past
5 years that provided the same or similar insurance to the Insurance Sought? Yes [ ]  No [ ]

## Declaration

It is declared that to the best of the knowledge and belief of the insured the statements and replies set out herein are true and that no material facts have been misstated or suppressed after enquiry. The insured undertake to inform insurers of alterations to any facts which are or thereby become material before inception of the contract of insurance.

A material fact is one which would influence the acceptance or assessment of the risk.

 Signed

 Title
 (authorised signatory of the insured)

 Company

 Date

**AIG Europe Limited**

The AIG Building

58 Fenchurch Street

London EC3M 4AB

This insurance is underwritten by AIG Europe Limited which is authorised and regulated by the Financial Services Authority (FSA number 202628). AIG Europe Limited is a member of the Association of British Insurer’s. Registered in England: company number 1486260. Registered address: The AIG Building, 58 Fenchurch Street, London, EC3M 4AB.