

BEAZLEY BREACH RESPONSE – IRISH EDITION

INFORMATION SECURITY & PRIVACY INSURANCE WITH BREACH RESPONSE SERVICES

NOTICE: INSURING AGREEMENTS I.A., I.C., I.D. AND I.F. OF THIS POLICY PROVIDE COVERAGE ON A CLAIMS MADE AND REPORTED BASIS AND APPLY ONLY TO CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR THE OPTIONAL EXTENSION PERIOD (IF APPLICABLE) AND REPORTED TO THE UNDERWRITERS DURING THE POLICY PERIOD OR AS OTHERWISE PROVIDED IN CLAUSE X. OF THIS POLICY. AMOUNTS INCURRED AS CLAIMS EXPENSES UNDER THIS POLICY SHALL REDUCE AND MAY EXHAUST THE LIMIT OF LIABILITY AND ARE SUBJECT TO RETENTIONS.

INSURING AGREEMENT I.B. OF THIS POLICY PROVIDES FIRST PARTY COVERAGE ON AN INCIDENT DISCOVERED AND REPORTED BASIS AND APPLIES ONLY TO INCIDENTS FIRST DISCOVERED BY THE INSURED AND REPORTED TO THE UNDERWRITERS DURING THE POLICY PERIOD.

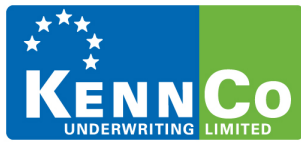
PLEASE READ THIS POLICY CAREFULLY.

Please fully answer all questions and submit all requested information.

Full Name:			
Mailing Address:		Country of Incorporation:	
No. of Employees:		Date Established:	
Website URL's:			
Authorised Officer 1:		Telephone:	
		E-mail:	
Breach Response Contact 2:		Telephone:	
		E-mail:	
Applicant Business Activities:			
1. Business Description:			
2. Does the Applicant provide data processing, data storage, or data hosting services to third parties?			<input type="checkbox"/> Yes <input type="checkbox"/> No
3. Does the Applicant distribute any products on a wholesale basis?			<input type="checkbox"/> Yes <input type="checkbox"/> No
4. If yes , please confirm the percentage of revenue generated by wholesale distribution:			%
Revenue Information:			
*Please provide Gross Revenue information			
	Most Recent Twelve (12) months: (ending: __/__/__)	Previous Year	Next Year (estimate)
Total Revenue:	€	€	€
US/Canada Revenue:	€	€	€
EU Revenue:	€	€	€
Please attach a copy of your most recently audited annual financial statement.			
Are significant changes in the nature or size of the Applicant's business anticipated over the next twelve (12) months? Or have there been any such changes within the past twelve (12) months?			<input type="checkbox"/> Yes <input type="checkbox"/> No
If yes , please explain:			

¹ The officer of the Applicant that is designated to receive any and all notices from the Insurer or its authorised representative(s) concerning this insurance.

² The employee of the Applicant that is designated to manage a response, including consumer notification, in response to a data breach event.



Has the Applicant within the past twelve (12) months completed or agreed to, or does it contemplate entering into within the next twelve (12) months, a merger, acquisition, consolidation, whether or not such transactions were or will be completed? Yes No

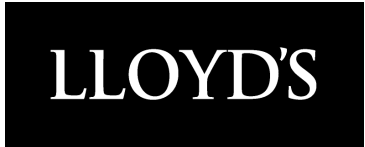
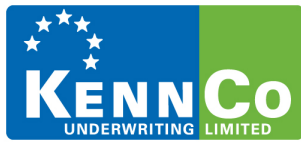
If **yes**, please explain:

I. MANAGEMENT OF PRIVACY EXPOSURES

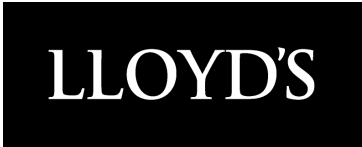
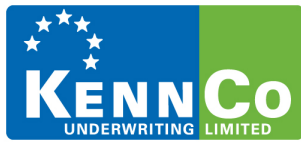
1. Has the Applicant designated a Chief Privacy Officer? Yes No
If **no**, please indicate what position (if any) is responsible for privacy issues:
2. Does the Applicant have a written corporate-wide privacy policy? Yes No
If **yes**, please attach a copy of the privacy policy to this application.
3. Is the Applicant in compliance with its privacy policy? Yes No
If **no**, please provide details regarding such non-compliance:
4. Does the Applicant accept credit cards for goods sold or services rendered? Yes No
If yes:
 - A. Please state the Applicant's approximate percentage of revenues from credit card transactions in the most recent twelve (12) months: _____ %
 - B. Is the Applicant compliant with applicable data security standards issued by financial institutions with which the Applicant transacts business (e.g. PCI standards)? Yes No
If the Applicant is not compliant with applicable data security standards, please describe the current status of any compliance work and the estimated date of completion:
5. Does the Applicant restrict employee access to personally identifiable on a business-need to know basis? Yes No
6. Does the Applicant require third parties with which it shares personally identifiable information or confidential information to indemnify the Applicant for legal liability arising out of the release of such information due to the fault or negligence of the third party? Yes No
7. Has the Applicant implemented an identity theft prevention program? Yes No
8. If the Applicant is in the healthcare industry, does the Applicant host, operate, or manage a Healthcare Information Exchange on which other organisations may store personal health information? Yes No

II. COMPUTER SYSTEMS CONTROLS

1. Has the Applicant designated a Chief Security Officer as respects computer systems? Yes No
If **no**, please indicate what position is responsible for computer security:
2. Does the Applicant publish and distribute written computer and information systems policies and procedures to its employees? Yes No
3. Does the Applicant conduct training for every employee user of the information systems in security issues and procedures for its computer systems? Yes No
4. Does the Applicant have :
 - A. a disaster recovery plan? Yes No
 - B. a business continuity plan? Yes No
 - C. an incident response plan for network intrusions and virus incidents? Yes No
 How often are such plans tested?
5. Does the Applicant have a program in place to test or audit security controls on an annual or more frequent basis? Yes No
If **yes**, please summarise the scope of such audits and/or tests:



6. Does the Applicant terminate all associated computer access and user accounts as part of the regular exit process when an employee leaves the company?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
7. Is all valuable/sensitive data backed up by the Applicant on a daily basis? If no , please describe exceptions:	<input type="checkbox"/> Yes	<input type="checkbox"/> No
8. Is at least one complete back-up file generation stored and secured off-site separate from the Applicant's main operations in a restricted area? If no, describe the procedure used by the Applicant, if any, to store or secure copies of valuable/sensitive data off-site?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
9. Does the Applicant have and enforce policies concerning when internal and external communication should be encrypted?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
A. Are users able to store data to the hard drive of portable computers or portable media devices such as USB drives?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
B. Does the Applicant encrypt data stored on laptop computers and portable media?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
C. Please describe any additional controls the Applicant has implemented to protect data stored on portable devices:	<input type="checkbox"/> Yes	<input type="checkbox"/> No
10. What format does the Applicant utilise for backing up and storage of computer system data? <input type="checkbox"/> Tape or other media <input type="checkbox"/> Online backup service <input type="checkbox"/> Other:		
A. Are tapes or other portable media containing backup materials encrypted?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
B. Are tapes or other portable media stored offsite using secured transportation and secured storage facilities?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
1) If stored offsite, are transportation logs maintained?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If stored onsite, please describe physical security controls:		
11. Does the Applicant enforce a software update process including installation of software "patches"? If Yes , are critical patches installed within thirty (30) days of release?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
12. Please describe your network infrastructure:		
<div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> Primary vendor: Other significant vendor: </div> <div style="width: 40%; text-align: center;"> Anti-virus Firewall ISP Intrusion Detection </div> </div>		
13. How often are virus signatures updated? <input type="checkbox"/> Automatic Updates <input type="checkbox"/> Weekly <input type="checkbox"/> Monthly <input type="checkbox"/> Other		
14. Does the Applicant require computer service providers who may have access to confidential information or personally identifiable information to demonstrate adequate security policies and procedures?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
A. Are computer service providers required by contract to indemnify the Applicant for harm arising from a breach of the provider's security?	<input type="checkbox"/> Yes	<input type="checkbox"/> No



III. WEBSITE CONTENT CONTROLS

1. Please check all descriptions of website content posted by the Applicant:

No Website
 Information created by the Applicant
 Content under licence from a third party
 Streaming video or music content
 Unlicensed third party content (e.g. – Blog/Message Boards/Customer Reviews)

2. Does the Applicant have a procedure for responding to allegations that content created, displayed or published by the Applicant is libelous, infringing, or in violation of a third party's privacy rights? Yes No

3. Does the Applicant have a process to review all content prior to posting on the Insured's Internet Site? Yes No
 If yes: is the review performed by qualified legal counsel? Yes No
 Does the review include screening the content for the following:

A. disparagement issues? Yes No
B. copywriting infringement? Yes No
C. trademark infringement? Yes No
D. invasion of privacy? Yes No

If the Applicant does not have a process to review all content prior to posting, please describe procedures to avoid the posting of improper or infringing content:

4. Has the Applicant screened all trademarks used by the Applicant for infringement with existing trademarks prior to first use? Yes No

A. Has the Applicant acquired any trademarks from others in the past three (3) years? Yes No
 If **Yes**, were acquired trademarks screened for infringement? Yes No

IV. PRIOR INSURANCE

1. Does the Applicant currently have insurance in place covering media, privacy or network security exposures? Yes No
 If **yes**, please provide the following:

Insurer	Limits	Deductible	Policy Period	Premium	Retroactive Date

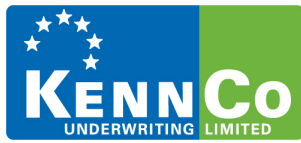
2. Has any professional liability, privacy, network security or media insurance ever been declined or canceled? Yes No
 If **yes**, please provide details:

V. PRIOR CLAIMS AND CIRCUMSTANCES

1. Does the Applicant or other proposed insured, or any director, officer or employee of the Applicant or other proposed insured have knowledge of or information regarding any fact, circumstance, situation, event or transaction which may give rise to a claim or loss or obligation to provide breach notification under the proposed insurance? Yes No
 If **yes**, please provide details:

2. During the past **5 years** has the Applicant:

A. received any claims or complaints with respect to privacy, breach of information or network security, unauthorised disclosure of information, or defamation or content infringement? Yes No
B. been subject to any government action, investigation or subpoena regarding any alleged violation of a privacy law or regulation? Yes No



C. notified consumers or any other third party of a data breach incident involving the Applicant? Yes No

D. Experienced an actual or attempted extortion demand with respect to its computer systems? Yes No

If **yes**, please provide details of any such action, notification, investigation or subpoena:

IMPORTANT NOTICE:

- It is your duty to disclose all material facts to Underwriters. A material fact is one which may influence an Underwriter's judgement in the consideration of your proposal. If your proposal is a renewal, it is likely that any change in facts previously advised to Underwriters will be material and such changes should be highlighted. If you are in any doubt as to whether a fact is material you should consult your broker or disclose it.
- Failure to so inform us may invalidate this insurance or any claim made under it.
- The particulars provided by, and statements made by, or on behalf of the Applicant(s) contained in this application form and any other information submitted or made available by, or on behalf of the Applicant(s) are the basis for the proposed policy and will be considered as being incorporated into and constituting a part of the proposed policy.
-

DATA PROTECTION NOTICE:

Beazley Furlonge Limited will collect certain information about individuals within or connected to your company and any subsidiaries ("data subjects") in the course of considering your application and, if we issue a policy, in conducting our relationship with you. This information will be processed for the purpose of underwriting your insurance coverage, managing any policy issued, providing risk management advice and administering claims. We may pass the information to our reinsurers, legal advisers, loss adjusters, group companies or agents for these and other purposes. This may involve its transfer to countries which do not have data protection laws.

Some of the information we collect may be classified as 'sensitive' - that is, information about disciplinary proceedings, convictions, sentences or alleged criminal activities. Data protection laws impose specific conditions in relation to sensitive information including, in some circumstances, the need to obtain the explicit consent of data subjects before we process the information.

Data subjects have a right of access to, and correction of, information that we hold about them. If they would like to exercise either of these rights, they should contact our Data Protection Compliance Officer at Beazley Furlonge – Sian Coope, Plantation Place South, 60 Great Tower Street, London EC3R 5AD, England.

By signing this proposal form you confirm the consent of the data subjects to the processing and transfer of information (including sensitive information) described in this notice, and that you have taken all steps necessary to inform them of our processing and your disclosure of information to us for the purposes described above. Without this consent and your confirmation of these matters, we would not be able to consider your application.

