IMPORTANT NOTICE: CHANGES TO YOUR POLICY DUE TO BREXIT

As a result of the likely departure of the United Kingdom from the European Union (Brexit), **we** have had to make some changes to how **our** policies are underwritten from 1st January 2019.

Please note that the changes referred to in this notice do not affect the cover provided under the policy.

Previously **our** policies were underwritten by Hiscox Underwriting Ltd (HUL) as an intermediary on behalf of the insurers shown in the schedule. Most sections of the policies were insured by Hiscox Insurance Company Limited (HIC), although some sections were insured by other insurers, as detailed on the schedule.

As a result of Brexit, sections of **our** policies that were previously insured by HIC are now insured by Hiscox SA (HSA) directly. HUL will no longer act as intermediary. HSA is an insurance company in the Hiscox group, domiciled and regulated in Luxembourg.

As a result of the change of insurer from HIC to HSA, **we** have had to make a number of changes to the way in which **our** policies are administered, including how complaints are dealt with.

In order to reflect these changes, the following amendments are made to **your policy**, including the schedule:

	Amended to read:
References to Hiscox Insurance Company Limited:	Hiscox SA
Address:	Hiscox SA registered head office: Avenue John F. Kennedy 35F 1855 Luxembourg LUXEMBOURG Local branch office: Hiscox SA (Irish branch) The Observatory 7-11 Sir John Rogerson's Quay Dublin 2 D02 VC42 REPUBLIC OF IRELAND Website: https:\\Hiscox.ie
Company number:	Hiscox SA: Registered in Luxembourg with Trade and Company Register Luxembourg (RCS Luxembourg): registration number B217018 Hiscox SA (Irish branch): Registered in Republic of Ireland with Companies Registration Office: company number 908764
Regulator:	Hiscox SA is subject to the supervision of the Commissariat aux Assurances Local branch regulator: Central Bank of Ireland
Signatory:	Richard O'Dwyer Managing Director, Hiscox SA (Irish branch)
Contact number and email address for Customer Relations	Customer relations: customerrelations.ireland@hiscox.com +353 1 238 1810
Contact numbers and email addresses for Claims	Liability claims: liabilityclaims.ireland@hiscox.com +353 1 238 1811 Commercial property claims: commercialpropertyclaims.ireland@hiscox.com +353 1 238 1812

Complaints:	Customer Relations Hiscox SA (Irish branch) The Observatory 7-11 Sir John Rogerson's Quay Dublin 2 D02 VC42 REPUBLIC OF IRELAND or by telephone on +353 1 238 1810 or +353 1800 901 903 (free toll number), or by email at customerrelations.ireland@hiscox.com.
Complaints (regulator):	If you remain dissatisfied after the internal dispute resolution process, you may have the right to refer your complaint to the Financial Services and Pensions Ombudsman. The Financial Services and Pensions Ombudsman (FSPO) is an independent, impartial, fair and free service that helps resolves complaints with pensions providers and regulated financial services providers. Contact details: Financial Services and Pensions Ombudsman Lincoln House Lincoln Place Dublin DO2 VH29 Phone: +353 1 567 7000 Email: info@fspo.ie Web: www.fspo.ie If you have purchased your policy online you can also make a complaint via the EU's online dispute resolution (ODR) platform. The website for the ODR platform is: http://ec.europa.eu/odr. Alternatively, you can also contact: Commissariat aux Assurances 7, boulevard Joseph II L-1840 Luxembourg LUXEMBOURG e-mail: caa@caa.lu Insurance Ombudsman ACA, 12, rue Erasme, L - 1468 Luxembourg LUXEMBOURG Phone: +352 44 21 44 1 Fax: +352 44-02-89 e-mail: mediateur@aca.lu
In addition, any references to Hiscox Underwriting Ltd in **your policy** are removed.	

Cyber and data
Proposal form

1. Your business

Business name

Main address

Postcode

Year business established:

Website:

1.1 Your employees

Your total number of employees (including subsidiaries)

1.2 Subsidiary or associated companies

Do you require cover for any subsidiary or associated companies? Yes ☐ No ☐

If **yes**, you must ensure that all other information you give in this proposal form incorporates that for the subsidiary or associated companies, including income and claims information.

You must also provide a separate list of subsidiary and associated companies.

1.3 Accredited information security standards

Has your organisation been accredited with any information security standards? Yes ☐ No ☐

If **yes**, please provide details:

1.4 Business activities

Please describe the nature of your business activities and include those of any subsidiaries that you want to be covered:

1.5 Your financial details

Please provide your turnover including fee income:

	Past year ending / /	Current year	Estimate for coming year
Total income	£	£	£
Generated in the USA	£	£	£
Web sales	£	£	£

HISCOX

Cyber and data
Proposal form

1.6 Types, volumes and encryption of personal data

Please provide details of personal information (in both electronic and non-electronic form) you process or store using the following table. N.B. this should include information relating to employees (past, present and prospective), as well as third-parties.

	Type of sensitive information transmitted, processed or stored:					
	Names, addresses and email addresses	Individual taxpayer ID/ NI numbers	Driver's license, passport or other ID numbers	Financial account records	Payment card data	Other: Please specify
Number of records transmitted or processed per year						
Maximum number of records stored on your network at any one time						
Always encrypted while at-rest on the network?	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐
Always encrypted while in-transit within and out of the network?*	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐
Always encrypted on mobile computing devices?**	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐
Always encrypted on portable data storage media?***	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐	Yes ☐ No ☐

*including on wireless networks, in file transfers and in email.
**including laptops, tablets, mobile telephones, PDAs.
*** including USB sticks, flash drives, magnetic tapes.

1.7 Cover required

Please indicate cover required: £

Excess requested: £

1.8 Payment card information

a. Are you compliant with the most recent applicable Payment Card Industry Data Security Standards (PCI DSS)? If Yes: Yes ☐ No ☐ N/A ☐

to what certification level? Level 1 ☐ Level 2 ☐ Level 3 ☐ Level 4 ☐

when was your last assessment?

b. Do you accept credit card payments in your facilities or via the web? If **yes**, please answer the following questions: Yes ☐ No ☐

i. Do you outsource all of your payment processing? Yes ☐ No ☐

ii. Do you ever store or transmit credit card details on your network, even momentarily? Yes ☐ No ☐

HISCOX

Cyber and data
Proposal form

1.9 Security controls

a. Do you have regular (at least every 90 days) mandatory password updates for all systems providing access to personal/confidential information? Yes ☐ No ☐

b. Do you have a defined process implemented to regularly patch your systems and applications? Yes ☐ No ☐

c. Do you use anti-virus software and regularly apply updates/patches? Yes ☐ No ☐

d. Have you installed and do you maintain a firewall configuration to protect data? Yes ☐ No ☐

e. Do you regularly scan your network for weaknesses, including for SQL injection vulnerabilities? Yes ☐ No ☐

f. If you maintain your own backup tapes/cassettes/disks, etc., are these encrypted and stored in a physically secured location? Yes ☐ No ☐

g. Have you installed physical controls to protect sensitive systems and sensitive physical information under your care, custody or control? Yes ☐ No ☐

h. Have you had an external party undertake a penetration test of your network? Yes ☐ No ☐

If **yes**, when was the last test?

i. Have you updated all network passwords (including firewall and telephony) from the defaults? Yes ☐ No ☐

If you have answered **no** to any of the above, please provide additional information.

1.10 Access control

a. Do you track and monitor all access to sensitive information on your network? Yes ☐ No ☐

b. Do you restrict access to all sensitive information stored by you on a business need-to-know basis? Yes ☐ No ☐

c. Do you have procedures in place to restrict or remove login credentials of employees immediately following an employee's departure from your organisation? Yes ☐ No ☐

d. Do you have formalised data destruction procedures in place for data and documents no longer needed by your organisation? Yes ☐ No ☐

e. What is your sensitive data retention policy? How long do you retain personally identifiable information?

Hours: ☐ Days: ☐ Weeks: ☐

Months: ☐ Years: ☐ Indefinitely: ☐

If you have answered **no** to any of the above, please provide additional information.

HISCOX

Cyber and data standalone
Proposal form

1.11 Privacy details

a. Have you conducted a review to determine what personal data you handle and where it is stored? Yes ☐ No ☐

b. Do you have a written privacy policy? If **yes**: Yes ☐ No ☐

i. has the privacy policy been reviewed by a suitably qualified lawyer? Yes ☐ No ☐

ii. does the privacy policy clearly state how someone with a privacy query or complaint can contact you? Yes ☐ No ☐

iii. does the privacy policy clearly disclose who you share personal data with? Yes ☐ No ☐

iv. is it published on your website? Yes ☐ No ☐

c. Has a third-party audited your privacy practices and/or network security in the last two years? Yes ☐ No ☐

If **yes**, have you complied with all of the recommendations provided? Yes ☐ No ☐

d. Do you obtain explicit consent from customers when collecting personal data? Yes ☐ No ☐

e. Is there an individual in your organisation specifically assigned responsibility for information security such as a CISO? Yes ☐ No ☐

f. Do you maintain a written policy that addresses information security which is communicated to all employees? Yes ☐ No ☐

If you have answered **no** to any of the above, please provide additional information.

1.12 Redundancy

a. Do you maintain redundant backups of sensitive and critical system information? Yes ☐ No ☐ N/A ☐

b. Do you have backups stored off-site? Yes ☐ No ☐ N/A ☐

c. Are restore procedures documented and tested? Yes ☐ No ☐ N/A ☐

d. Do you have scheduled backup procedures in place? Yes ☐ No ☐ N/A ☐

e. How often is sensitive information backed-up? Daily ☐ Weekly ☐ Monthly ☐ Annually ☐

f. Do system backups reside with third-parties? Yes ☐ No ☐ N/A ☐

g. How quickly can you obtain backups stored by third-parties?
24-hours ☐ One week ☐ One month ☐ Unknown ☐

h. Do you have a disaster recovery plan and/or incident response plan that takes account of loss of functionality/data as a result of a hack, including provision to notify those affected if their personal data is compromised? DRP ☐ IRP ☐ Neither ☐

If **yes**, when was the last time it was tested?

If you have answered **no** to any of the above, please provide additional information.

HISCOX

Cyber and data standalone
Proposal form

1.13 Cyber crime and telephone hacking

a. Do you use online banking? Yes ☐ No ☐

If **yes**, is two factor authentication required to log in? Yes ☐ No ☐

b. Are telephone calls to premium rate and/or international numbers barred or restricted? Yes ☐ No ☐

c. Is your telephone system switched off, or outgoing calls blocked, out of office hours? Yes ☐ No ☐

d. Are there procedures in place for notifications in the event of your telephone bill hitting certain financial caps? Yes ☐ No ☐

e. Are surplus phone numbers and mailboxes locked and deactivated? Yes ☐ No ☐

If you have answered **no** to any of the above, please provide additional information.

1.14 Sub-contractors

a. What percentage of your turnover is paid to subcontractors including freelancers or other non-employees? ____ %

b. Do you provide your client's personal data or confidential information to your sub-contractors in order for them to fulfil their role? Yes ☐ No ☐

c. Do you always obtain a hold harmless or indemnity from sub-contractors for claims that may arise from a breach of the data provided to them? Yes ☐ No ☐

2. Claims and incidents

a. Have you suffered any loss or has any claim whether successful or not ever been made against you? Yes ☐ No ☐

If **yes**, please specify details (attach additional information if required):

b. Are you aware of any matter which is likely to lead to you suffering a loss or a claim being made against you? Yes ☐ No ☐

If y**es**, please specify details (attach additional information if required):

c. Have you ever been investigated in respect of personally identifiable information, including but not limited to payment card information, or your privacy practices? Yes ☐ No ☐

d. Have you been asked to supply any regulator or similar body with information relating to personally identifiable information or your privacy practices? Yes ☐ No ☐

e. Have you ever been asked to sign a consent order or equivalent in respect of personally identifiable information or your privacy practices? Yes ☐ No ☐

f. Have you ever received a complaint relating to the handling of someone's personally identifiable information? Yes ☐ No ☐

Cyber and data standalone
Proposal form

3. Declaration

Please read the declaration carefully and sign at the bottom.

3.1 Material information

In deciding whether to accept the insurance and in setting the terms and premium, we have relied on the information you have given us.

You must:

- give a fair presentation of the risk to be insured by clearly disclosing all material facts and circumstances (whether or not subject to a specific question) which you, your senior management and those responsible for arranging this insurance ,know or ought to know following a reasonable search;
- take care by ensuring that all information provided is correct, accurate and complete.

3.2 Your information

Hiscox is a trading name of a number of Hiscox companies. The specific company acting as a data controller of your personal information will be listed in the documentation we provide to you. If you are unsure you can also contact us at any time by telephoning 01904 681198 or by emailing us at dataprotectionofficer@hiscox.com.

We collect and process information about you in order to provide insurance policies and to process claims. Your information is also used for business purposes such as fraud prevention and detection and financial management. This may involve sharing your information with, and obtaining information about you from, our group companies and third parties such as brokers, loss adjusters, credit reference agencies, service providers, professional advisors, our regulators or fraud prevention agencies.

We may record telephone calls to help us monitor and improve the service we provide.

For further information on how your information is used and your rights in relation to your information please see our privacy policy at www.hiscox.co.uk/cookies-privacy.

3.3 Declaration

I /we confirm that the information given in this proposal form is correct, accurate and complete and I have made a fair presentation of the risk.

Name of director/officer/board member/senior manager

	/ /
Signature of director/officer/board member/senior manager	Date

A copy of this proposal should be retained for your records.

3.4 Complaints

Hiscox aims to ensure that all aspects of your insurance are dealt with promptly, efficiently and fairly. At all times Hiscox are committed to providing you with the highest standard of service. If you have any concerns about your policy or you are dissatisfied about the handling of a claim and wish to complain you should, in the first instance, contact Hiscox Customer Relations in writing at:

Hiscox Customer Relations
The Hiscox Building
Peasholme Green
York YO1 7PR

or by telephone on 0800 116 4627/01904 681 198
or by email at customer.relations@hiscox.com.

Where you are not satisfied with the final response from Hiscox, you also have the right to refer your complaint to the Financial Ombudsman Service. For more information regarding the scope of the Financial Ombudsman Service, please refer to www.financial-ombudsman.org.uk.