Arranged by

Insured by

APPENDIX D: First Party Computer Security Coverage Endorsement

This endorsement modifies the Beazley Breach Response Cover and shall be read as if incorporated within it:

It is understood and agreed that, for the purposes of this endorsement only:

1. Section B.1.2. **Extensions** is amended with the addition of the following extensions:

a. Cyber Extortion

We will indemnify **You** for **Cyber Extortion Loss** incurred by **Your Organisation** as a direct result of an **Extortion Threat** first made against **Your Organisation** during the **Policy Period** by a person, other than **Your Management, Your Organisation**'s **Employees**, contractors, outsourcers, or any person in collusion with any of the foregoing. Coverage under this extension is subject to the applicable conditions and reporting requirements, including those stated in Clause C below, Obligations In The Event of an Extortion Threat.

The maximum amount payable for the **Policy Period** in respect of this extension a) (Cyber Extortion) shall not exceed EUR100,000 in the aggregate.

Excess will be EUR500 each **Extortion Threat.**

b. First Party Data Protection

We will indemnify **You** for **Data Protection Loss** incurred by **Your Organisation** as a direct result of:

1. alteration, corruption, destruction, deletion or damage to a **Data Asset**, or
2. inability to access a **Data Asset**,

that first takes place during the **Policy Period** and is directly caused by a failure of **Computer Security** to prevent a **Security Breach**; provided that such **Security Breach** must take place on or after the **Retroactive Date** and before the end of the **Policy Period**.

Excess will be EUR500 each **Security Breach**

c. First Party Network Business Interruption

We will indemnify **You** for **Business Interruption Loss** incurred by **Your Organisation** during the **Period of Restoration** or the **Extended Interruption Period** (if applicable) as a direct result of the actual and necessary interruption or suspension of **Computer Systems** that first takes place during the **Policy Period** and is directly caused by a failure of **Computer Security** to prevent a **Security Breach**; provided that such

Security Breach must first take place on or after the **Retroactive Date** and before the end of the **Policy Period**.

Excess for each **Security Breach** under this extension will be:

i. Income Loss: EUR500
ii. Extra Expense: EUR500
iii. **Waiting Period:** 12h

The maximum amount payable for the **Policy Period** in respect of both extensions b. (First Party Data Protection) and c. (First Party Network Business Interruption) of this endorsement shall not exceed EUR100,000 in the aggregate.

In relation to extension c. (First Party Network Business Interruption) of this endorsement, the following sublimits of liability apply:

i. **Hourly sublimit:** EUR10,000
ii. **Dependent Business Interruption sublimit:** not given
iii. **Forensic Expense sublimit:** Same amount as the amount stated in the Schedule for Legal and Forensic Services covered under B.2.a. This sublimit is part of and not in addition to this Legal and Forensic Services sublimit covered under B.2.a.

2. Exclusions applicable to coverage given under the extensions of this endorsement.

We will not make any payment for or in respect of any **Loss** covered under extensions a, b and c above, for, arising out of, or resulting from:

a. any criminal, dishonest, fraudulent, or malicious act, error or omission, any **Security Breach**, **Extortion Threat**, or intentional or knowing violation of the law, if committed by any member of **Your Management** or any person in participation or collusion with any member of **Your Management**;

b. in relation to extensions b. (First Party Data Protection) and c. (First Party Network Business Interruption) of this endorsement:

i. any failure or malfunction of electrical or telecommunications infrastructure or services, provided that this exclusion shall not apply to any otherwise covered **Claim** or **Loss** arising out of failure of **Computer Security** to prevent a **Security Breach** that was solely caused by a failure or malfunction of telecommunications infrastructure or services under **Your Organisation**'s direct operational control;
ii. fire, flood, earthquake, volcanic eruption, explosion, lighting, wind, hail, tidal wave, landslide, act of God or other physical event; or
iii. any satellite failures;

c. in relation to extensions a. (Cyber Extortion) of this endorsement:

i. any threat to physically harm or kidnap any person; or

ii. any threat to harm, take, or transfer property other than any **Data Asset**, even if such threat is made in conjunction with a threat to a **Data Asset** or by carrying out such threat to, harm, theft, or transfer, a **Data Asset** may be damaged, corrupted, altered, taken, disseminated or transferred;

d. any seizure, nationalisation, confiscation, or destruction of **Computer Systems** or **Data Assets** by order of any governmental or public authority.

3. Definitions applicable to coverage given under this endorsement

a. **Business Interruption Loss** means the total of:

i. **Income Loss** and **Extra Expense** during the **Period of Restoration**; and

ii. **Extended Income Loss** if the **Income Loss** during the **Period of Restoration** is in excess of the applicable excess.

Provided that **Business Interruption Loss** shall not mean any of the following: loss arising out of any liability to any third party for whatever reason; legal costs or legal expenses of any type; loss incurred as a result of unfavorable business conditions, loss of market or any other consequential loss; or costs or expenses **Your Organisation** incurs to identify and remove software program errors or vulnerabilities.

All **Business Interruption Loss** resulting from multiple covered interruptions or suspensions of **Computer Systems** that that arise out of the same or a continuing **Security Breach**, from related or repeated **Security Breaches**, or from multiple **Security Breaches** resulting from a failure of **Computer Security** shall be deemed to be a single **Business Interruption Loss**; provided, however, that a separate **Waiting Period** shall apply to each **Period of Restoration**.

b. **Cyber Extortion Loss** means:

i. any **Extortion Payment** that has been made under duress by or on behalf of **Your Organisation** with **Our** prior written consent, but solely to prevent or terminate an **Extortion Threat** and in an amount that does not exceed the covered **Damages** and **Claims Expenses** that would have been incurred had the **Extortion Payment** not been paid;

ii. an otherwise covered **Extortion Payment** that is lost in transit by actual destruction, disappearance or wrongful abstraction while being conveyed by any person authorised by or on behalf of **Your Organisation** to make such conveyance; and

iii. fees and expenses paid by or on behalf of **Your Organisation** for security consultants retained with Underwriter's prior written approval, but solely to prevent or terminate an **Extortion Threat**.

c. **Computer Security** for the purpose of coverage given under this endorsement, also means **Your Organisation**'s written information security policies and procedures, the function or purpose of which is to prevent **Unauthorised Access or Use**, a denial of service attack against **Computer Systems**, infection of **Computer Systems** by malicious code or transmission of malicious code from **Computer Systems**.

d. **Computer Systems** for the purpose of coverage given under extension c.(First Party Network Business Interruption) of this endorsement also means computers and associated input and output devices, data storage devices, networking equipment and back up facilities operated by a third party service provider and used for the purpose of providing hosted computer application services to **Your Organisation** or for processing, maintaining, hosting or storing **Your Organisation's** electronic data, pursuant to written contract with **Your Organisation** for such services, provided such coverage is subject to the sublimit of liability stated above in respect of both extensions b. (First Party Data Protection) and c. (First Party Network Business Interruption) of this endorsement.

e. **Data Asset** means any software or electronic data that exists in **Computer Systems** and that it is subject to regular back-up procedures.

f. **Data Protection Loss** means:

i. with respect to any **Data Asset** that is altered, corrupted, destroyed, deleted or damaged the actual, reasonable and necessary costs and expenses incurred by **Your Organisation** to restore a **Data Asset** from back-ups or from originals or to gather, assemble and recollect such **Data Asset** from other sources to the level or condition in which it existed immediately prior to its alteration, corruption, destruction, deletion or damage; or

ii. with respect to any **Data Asset** that **Your Organisation** is unable to access, the lesser of the actual, reasonable and necessary costs and expenses incurred by **Your Organisation** to:

(a) regain access to such **Data Asset**; or

(b) restore such **Data Asset** from back-ups or originals or gather, assemble and recollect such **Data Asset** from other sources, to the level or condition in which it existed immediately prior to **Your Organisation's** inability to access it;

Provided that if such **Data Asset** cannot reasonably be accessed, restored, gathered, assembled or recollected, then **Data Protection Loss** means the actual, reasonable and necessary costs and expenses incurred by **Your Organisation** to reach this determination.

Provided further that **Data Protection Loss** shall not exceed, and shall not mean, any amount in excess of the amount by which the net profit before income taxes of **Your Organisation** would have decreased had **Your Organisation** failed to restore, gather, assemble or recollect as set forth in sub-paragraphs f.i and f.ii above.

A **Data Protection Loss** will be deemed to occur at the time such alteration, corruption, destruction, deletion or damage to or inability to access a **Data Asset** is first discovered by **You**. All **Data Protection Loss** that arises out of the same or a continuing **Security Breach**, from related or repeated **Security Breaches**, or from multiple **Security Breaches** resulting from a failure of **Computer Security** shall be deemed to be a single **Data Protection Loss**.

Data Protection Loss shall not mean:

1. costs or expenses incurred by **Your Organisation** to identify or remediate software program errors or vulnerabilities or update, replace, restore, gather, assemble, reproduce, recollect or enhance a **Data Asset** or **Computer Systems** to a level beyond that which existed prior to the alteration, corruption, destruction, deletion or damage of such **Data Asset**;

2. costs or expenses to research or develop any **Data Asset**, including but not limited to trade secrets or other proprietary information;

3. the monetary value of profits, royalties, or lost market share related to a **Data Asset**, including but not limited to trade secrets or other proprietary information or any other amount pertaining to the value of the **Data Asset**;

4. loss arising out of any liability to any third party for whatever reason; or

5. legal costs or legal expenses of any type.

g. **Dependent Business** means any third party service provider that provides hosted computer application services to **Your Organisation** or processes, maintains, hosts or stores **Your Organisation's** electronic data, pursuant to written contract with **Your Organisation** for such services.

h. **Extended Income Loss** means the Income Loss during the **Extended Interruption Period**.

i. **Extended Interruption Period** means the period of time that:

1. begins on the date and time that the **Period of Restoration** ends; and

2. terminates on the date and time **You** restore, or would have restored if **You** had exercised due diligence and dispatch, the net profit before income taxes that would have been earned by **You** directly through its business operations had the actual and necessary interruption or suspension of **Computer Systems** not occurred; provided that in no event shall the **Extended Interruption Period** mean more than or exceed thirty (30) days.

j. **Extortion Payment** means cash, marketable goods or services demanded to prevent or terminate an **Extortion Threat**.

k. **Extortion Threat** means a threat to breach **Computer Security** in order to:

1. alter, destroy, damage, delete or corrupt any **Data Asset**;

2. prevent access to **Computer Systems** or a **Data Asset**, including a denial of service attack or encrypting a **Data Asset** and withholding the decryption key for such **Data Asset**;

3. perpetrate a theft or misuse of a **Data Asset** on **Computer Systems** through external access;

4. introduce malicious code into **Computer Systems** or to third party computers and systems from **Computer Systems**; or

5. interrupt or suspend **Computer Systems**;
unless an **Extortion Payment** is received from or on behalf of **Your Organisation**.

Multiple related or continuing **Extortion Threats** shall be considered a single **Extortion Threat f**or purposes of this Policy and shall be deemed to have occurred at the time of the first such **Extortion Threat**.

l. **Extra Expense** means:

1. reasonable and necessary expenses that are incurred by **Your Organisation** during the **Period of Restoration** to minimize, reduce or avoid an **Income Loss**, provided:

   (a) that such expenses are over and above those **Your Organisation** would have incurred had no interruption or suspension of the **Computer Systems** occurred; and

   (b) do not exceed the amount by which the **Income Loss** in excess of the excess and covered under this Policy is thereby reduced; and

2. **Forensic Expenses**;
provided that **Extra Expense** shall not mean expenses incurred **You** to update, upgrade, enhance or replace **Computer Systems** to a level beyond that which existed prior to the actual and necessary interruption or suspension of **Computer Systems**; or the costs and expenses incurred by **Your Organisation** to restore, reproduce, or regain access to any **Data Asset** that was altered, corrupted, destroyed, deleted, damaged or rendered inaccessible as a result of the failure of **Computer Security** to prevent a **Security Breach**.

m. **Forensic Expenses** means reasonable and necessary expenses incurred by **Your Organisation** to investigate the source or cause of the failure of **Computer Security** to prevent a **Security Breach**.

n. **Income Loss** means:

1. the net profit before income taxes that **Your Organisation** is prevented from earning through its business operations or the net loss before income taxes that **Your Organisation** is unable to avoid through its business operations as a direct result of the actual and necessary interruption or suspension of **Computer Systems**; and

2. fixed operating expenses incurred by **Your Organisation** (including payroll), but only to the extent that a. such operating expenses must necessarily continue during the **Period**

of Restoration (or **Extended Interruption Period**, if applicable); and b. such expenses would have been incurred by **Your Organisation** had such interruption or suspension not occurred.

Income Loss shall be reduced to the extent **You** or **Dependent Business** (if applicable) is able, with reasonable dispatch and due diligence, to reduce or limit such interruption or suspension of **Computer Systems** or conduct its business operations by other means.

In determining **Income Loss**, due consideration shall be given to the prior experience of **Your Organisation's** business operations before the beginning of the **Period of Restoration** and to the probable business operations **Your Organisation** could have performed had no actual and necessary interruption or suspension occurred as result of a failure of **Computer Security** to prevent a **Security Breach**.

Income Loss will be calculated on an hourly basis based on **Your Organisation's** net profit (or loss) and fixed operating expenses as set forth above.

o. **Loss** for the purposes of coverage given under this endorsement also means **Cyber Extortion Loss**, **Business Interruption Loss** and **Data Protection Loss**.

p. **Period of Restoration** means the time period that:

1. begins on the specific date and time that the actual and necessary interruption or suspension of **Computer Systems** first occurred; and

2. ends on the specific date and time that the actual and necessary interruption or suspension of **Computer Systems** ends, or would have ended had **You** or **Dependent Business** (if applicable) acted with due diligence and dispatch;
provided that in no event shall the **Period of Restoration** mean more than or exceed thirty (30) days; and provided further that restoration of **Computer Systems** will not end the **Period of Restoration** if such systems are actually and necessarily interrupted or suspended again within one hour of such restoration due to the same cause as the original interruption or suspension.

q. **Waiting Period** means the period of time beginning when the **Period of Restoration** begins and expiring after the elapse of the number of hours stated above. A **Waiting Period** shall apply to each **Period of Restoration**.

4. Section E.1 **What You and Your management must do** is amended with the addition of the following in relation to coverage provided under this endorsement:

f. With respect to extension a of this endorsement (Cyber Extortion) in the event of an **Extortion Threat** to which this Policy applies, **Your Management** shall notify **Us** immediately upon receipt of any **Extortion Threat**, and shall thereafter also provide written notice by telecopy, email or express mail within five (5) days following the **Extortion Threat**.

g. With respect to extension b of this endorsement (First Party Data Protection) **Your Management** must forward to **Us** written notice by express mail, email or telecopy immediately upon discovery of alteration, corruption, destruction, deletion or damage to or inability to access a **Data Asset** to which this Insurance

applies; provided that all covered **Data Protection Loss** must be discovered and reported (in accordance with Clause A below., Proof of Loss and Appraisal) to **Us** no later than six (6) months after the end of the **Policy Period**.

h. With respect to extendion c of this endorsement (First Party Network Business Interruption) **Your Management** shall forward immediately to **Us** written notice of the interruption or suspension of **Computer Systems** to which this Insurance applies in the form of a telecopy, email or express mail. Such notice must be provided during the **Policy Period**, or no later than ten (10) days after the end of the **Policy Period** for interruptions or suspensions occurring within ten (10) days of the end of the **Policy Period**; provided, all covered **Business Interruption Loss** must be reported to **Us** (in accordance with Clause A below., Proof of Loss and Appraisal) no later than six (6) months after the end of the **Policy Period**.

5. Specific clauses applicable to extensions under this endorsement.

A. **Proof and Appraisal of Loss**

1. **Proof of Loss**. With respect to both extensions b. (First Party Data Protection) and c. (First Party Network Business Interruption) of this endorsement, before coverage will apply, **You** must:

a. prepare and submit to **Us** a written and detailed proof of loss sworn by one of **Your** officer within ninety (90) days after **You** discover a **Data Protection Loss** or **Your Organisation** sustains a **Business Interruption Loss** (as applicable), but in no event later than six (6) months following the end of the **Policy Period** (unless such period has been extended by **Our** written consent). Such proof of loss shall include a narrative with full particulars of such **Data Protection Loss** or **Business Interruption Loss**, including, the time, place and cause of the **Data Protection Loss** or **Business Interruption Loss,** a detailed calculation of any **Data Protection Loss** or **Business Interruption Loss**, **Your Organisation's** interest and the interest of all others in the property, the sound value thereof and the amount of **Data Protection Loss** or **Business Interruption Loss** or damage thereto and all other insurance thereon; and

b. upon **Our** request, submit to an examination under oath and provide copies of the underlying documents, data and materials that reasonably relate to or are part of the basis of the claim for such **Data Protection Loss** or **Business Interruption Loss**.

The costs and expenses of preparing and submitting a proof of loss, and establishing or proving **Data Protection Loss, Business Interruption Loss** or any other **Loss** under this Policy shall be **Your** obligation, and are not covered under this Policy.

2. **Appraisal of Loss**. If **You** and **Us** do not agree on the amount of a **Loss**, each party shall select and pay an appraiser or other qualified expert (the "Appraiser") to state the amount of the loss or reasonable expenses, and the Appraisers shall choose an umpire. If the Appraisers cannot agree on an umpire, **You** or **Us** may request a judge of a court having jurisdiction to make the selection. Each Appraiser shall submit the amount of the **Loss** or reasonable expenses to the umpire, and agreement by the umpire and at least one of the Appraisers as to the amount of a **Loss** shall be binding on all **Insureds** and **Us**. **You** and **Us** will equally share the costs of the umpire and any other costs other than the cost of the Appraisers. This provision shall govern only the appraisal of the amount of a **Loss**, and shall not

control the determination of whether such **Loss** is otherwise covered by the Policy. **We** will still retain and do not waive their rights to deny coverage or enforce any obligation under this Policy.

B. **Recovered Property**

If **You** or **Us** recover any property, money or **Data Assets** after a loss payment is made, the party making the recovery must give prompt notice of the recovery to the other party. If the recovered property is money or other funds, the recovery shall be applied first to any costs incurred by **Us** in recovering the property, second to loss payments made by **Us**, and third to any excess payment made by **You**. If property other than money or funds is recovered, then **You** may keep the recovered property and return the loss payment, plus the any costs of recovery incurred by **Us**, or keep the loss payment less the costs of recovery incurred by **Us** and transfer all rights in the property to **Us**.

C. **Obligations In The Event Of An Extortion Threat**

1. **Your Duty of Confidentiality**

You must use its best efforts at all times to ensure that knowledge regarding the existence of this insurance for **Cyber Extortion Loss** afforded by this Policy is kept confidential. **We** may terminate the insurance provided by this policy for **Cyber Extortion Loss** upon ten (10) days written notice to **You** if the existence of insurance for **Cyber Extortion Loss** provided by this Policy becomes public knowledge or is revealed to a person making an **Extortion Threat** through no fault of **Us**.

2. **Your Organisation's Obligation to Investigate Extortion Threat and Avoid or Limit Extortion Payment**

Prior to the payment of any **Extortion Payment**, **Your Organisation** shall make every reasonable effort to determine that the **Extortion Threat** is not a hoax, or otherwise not credible. **Your Organisation** shall take all steps reasonable and practical to avoid or limit the payment of an **Extortion Payment**.

3. **IMPORTANT CONDITION**

The following are **IMPORTANT CONDITIONS** under this Policy. Coverage under this Policy will not be available unless **You** comply with these important conditions:

a. **Your Obligation to Demonstrate Duress**

Your Organisation must be able to demonstrate that the **Extortion Payment** was surrendered under duress.

b. **Notification of Police**

Your Organisation shall allow **Us** or our representative to notify the police or other responsible law enforcement authorities of any **Extortion Threat**.

All other terms and conditions of this Policy remain unchanged.