LOT J

CYBER RISK POLICY

This policy is agreed between

EUROPEAN UNIVERSITY INSTITUTE
VIA DEI ROCCETTINI, 9
50014 SAN DOMENICO DI FIESOLE (Florence)
Tax ID 80020410488

and

the Insurance Company

……

(Branch)

……

Duration of the contract
From 24.00:00 on: 30/06/2026
To 24.00:00 on:30/06/2030

With periods of insurance
after the first one fixed
At 24.00 of every 30/06

In consideration of the payment of the premium and in accordance with the terms and conditions of this Policy (including the Policy Schedule on the front page), the Policyholder and the Insurer agree as follows:

1. SUBJECT OF INSURANCE: BASIC COVERAGES

Att.ne: The coverages set out in the following article apply only if indicated as such in the Policy Schedule.

Each Cyber Incident, Business Interruption, Cyber Extortion Event and/or Privacy and Network Security Event shall be classified as either a Limited Impact Event or a Widespread Impact Event. Coverage for a Limited Impact Event is provided pursuant to the operative coverages set out in this article and the following article, and to the applicable Sublimits, as reported in Section 3 of the Policy Schedule. Coverage for a Widespread Impact Event is provided pursuant to the operative coverages set out in this article and the following article, and to the operative Sublimits, as well as to the Policy Period Limits, Deductibles and Additional Coinsurance shown in the table "Sublimits – Coverage Extensions for Widespread Impact Events" in Section 3 of the Policy Schedule.

First-Party Damage Coverages:

The Insurer shall pay on behalf of the Insured:

1.1 Incident Response Costs
Incident Response Costs as a consequence of a Cyber Incident or a Business Interruption first discovered by a member of the Control Group during the Policy Period. Such Cyber Incident or Business Interruption must have been reported to the Insurer in accordance with Art. 5.8 "Claims Notification – Insureds' Obligations".

The Insurer shall reimburse the Insured for:

1.2 Business Interruption Losses
Business Interruption Losses and Extra Expenses during the Indemnity Period arising from a Business Interruption that exceeds the Waiting Period and was first discovered by a member of the Control Group during the Policy Period. Such Business Interruption must have been reported to the Insurer in accordance with Art. 5.8 "Claims Notification – Insureds' Obligations".

1.3 Data and Systems Recovery Costs
Data and Systems Recovery Costs during the Indemnity Period arising from a Business Interruption first discovered by a member of the Control Group during the Policy Period. Such Business Interruption must have been reported to the Insurer in accordance with Art. 5.8 "Claims Notification – Insureds' Obligations".Data and Systems Recovery Costs during the Indemnity Period arising from a Business Interruption first discovered by a member of the Control Group during the Policy Period. Such Business Interruption must have been reported to the Insurer in accordance with Art. 5.8 "Claims Notification – Insureds' Obligations".

1.4 Cyber Extorsion
Cyber Extortion Funds and Cyber Extortion Expenses as a consequence of a Cyber Extortion Event first discovered by a member of the Control Group during the Policy Period. Such Cyber Extortion Event must have been reported to the Insurer in accordance with Art. 5.8 "Claims Notification – Insureds' Obligations".

Third-Party Liability Coverages:

The Insurer shall reimburse the Insured for:

1.5 Privacy and Network Security Liability
Damages and Claim Expenses relating to Privacy and Network Security Claims arising from a Privacy and Network Security Claim first made during the Policy Period as a result of a Privacy and Network Security Event occurring after the Retroactive Date and before the expiration of the Policy Period. Such Privacy and Network Security Claim must have been reported to the Insurer in accordance with Art. 5.8 "Claims Notification – Insureds' Obligations".

1.6 Media Liability
Damages and Claim Expenses relating to Media Claims arising from a Media Claim first made during the Policy Period as a result of a Media Wrongful Act occurring after the Retroactive Date and before the expiration of the Policy Period. Such Media Claim must have been reported to the Insurer in accordance with Art. 5.8 "Claims Notification – Insureds' Obligations".

2. SUBJECT OF INSURANCE: COVERAGE EXTENSIONS

Attention: The following coverages apply only if indicated as such in the Policy Schedule.

Each Cyber Incident, Business Interruption, Cyber Extortion Event and/or Privacy and Network Security Event shall be classified as either a Limited Impact Event or a Widespread Impact Event. Coverage for a Limited Impact Event is provided pursuant to the operative coverages set out in this article and the preceding article, and to the applicable Sublimits, as reported in Section 3 of the Policy Schedule. Coverage for a Widespread Impact Event is provided pursuant to the operative coverages set out in this article and the preceding article, and to the operative Sublimits, as well as to the Policy Period Limits, Deductibles and Additional Coinsurance shown in the table "Sublimits – Coverage Extensions for Widespread Impact Events" in Section 3 of the Policy Schedule.

The Insurer shall pay on behalf of the Insured:

2.1 Emergency Incident Response Costs

Emergency Incident Response Costs incurred within the first 48 hours immediately following the first-time discovery during the The Insurer shall reimburse the Insured for:le **Spese di Emergenza di Incident Response** sostenute nelle prime 48 ore immediatamente successive alla scoperta da parte di un membro del **Gruppo di Controllo** per la prima volta durante il **Periodo Assicurativo** di un **Incidente Informatico** o un'**Interruzione dell'Attività Aziendale**, la cui sussistenza sia stata accertata, nel caso in cui tale **Incidente Informatico** o un'**Interruzione dell'Attività Aziendale** richiedano un'attenzione immediata al fine di mitigare il danno, gli effetti e i costi ad essi associati. Tali **Incidente Informatico** o **Interruzione dell'Attività Aziendale** dovranno essere stati denunciati all'**Assicuratore** ai sensi dell'art. 5.8 "Denuncia dei Sinistri – Obblighi degli Assicurati".

The Insurer shall pay on behalf of the Insured:

2.2 Improvement Costs

Improvement Costs arising from a Business Interruption covered pursuant to Art. 1.3 "Subject of Insurance: Basic Coverages". Such Business Interruption must have been reported to the Insurer in accordance with Art. 5.8 "Claims Notification – Insureds' Obligations".

2.3 Cyber Crime

The Direct Financial Loss resulting exclusively from the Theft of Money or Securities of an Insured Company due to the Fraudulent Use of, or Fraudulent Access by, a Third Party to an Insured Computer System or a Shared Computer System, first discovered by a member of the Control Group during the Policy Period. Such Fraudulent Use or Access must have been reported to the Insurer in accordance with Art. 5.8 "Claims Notification – Insureds' Obligations".

2.4 Reward Payment

The Reward Payment, only to the extent that it has been used in direct connection with a Cyber Extortion Event covered pursuant to Art. 1.4 "Subject of Insurance: Basic Coverages". Such Cyber Extortion Event must have been reported to the Insurer in accordance with Art. 5.8 "Claims Notification – Insureds' Obligations".

2.5 Telecommunications Fraud

Telecommunications Expenses caused by a Fraudulent Telecommunications Act or by the Fraudulent Use of, or Fraudulent Access by, a Third Party to an Insured Telecommunications System or a Shared Telecommunications System, first discovered by a member of the Control Group during the Policy Period. Such Fraudulent Act or Fraudulent Use or Access must have been reported to the Insurer in accordance with Art. 5.8 "Claims Notification – Insureds' Obligations".

2.6 Hardware Replacement:

Hardware Replacement Costs arising exclusively and directly from a Network Security failure that results in Hardware being rendered electrically inoperable, reduced in its functionality, or rendered unfit for its intended purpose, provided that such Network Security failure is discovered by a member of the Control Group during the Policy Period and is reported to the Insurer in accordance with Art. 5.8 "Claims Notification – Insureds' Obligations".

2.7 Reputational Damage Loss

The Insurer shall reimburse the Insured for Reputational Damage Loss incurred during the Reduced Activity Period that is the exclusive consequence of a Reputational Event first discovered by a member of the Control Group during the Policy Period and reported to the Insurer in accordance with Art. 5.8 "Claims Notification – Insureds' Obligations".

3. GENERAL POLICY DEFINITIONS

The terms listed below, used in this Policy in **bold**, whether in the singular or plural, shall have the following meaning:

3.1 Insured: the Insured Company and each Insured Person.

3.2 Insurer: the insurance company underwriting the risk.

3.3 Privacy and Network Security Event: any actual or alleged event, even if arising from the Insured's gross negligence, consisting of:
A. failure of Network Security, including any failure to deter, detect, prevent or defend against a Malicious Computer Act or Unauthorized Use or Access, even if resulting in Personal Injury; or
B. error or inability by the Insured or by an external service provider for whom the Insured is legally responsible, to handle, process, store, destroy or otherwise control:
i. Personal Data, even if resulting in Personal Injury; or
ii. private business information of third parties not in the public domain, in any format, provided to the Insured; or
C. unintentional breach of the Insured's privacy policy that causes a violation of a Privacy and Network Security Regulation, including but not limited to:
i. the unlawful and unintentional use or collection of Personal Data by the Insured; and/or
ii. processing, transfer, disclosure, sharing, retention or storage, sale, profiling, acquisition, improper handling, provision or failure to provide access to or correction of Personal Data by the Insured.

3.4 Telecommunications Wrongful Act: any fraudulent act committed against an Insured Telecommunications System or a Shared Telecommunications System, or any fraudulent access to or hacking of an Insured Telecommunications System or a Shared Telecommunications System, for the purpose of creating, deleting, obtaining, collecting, modifying or destroying Telecommunications Data or services. The term Telecommunications Wrongful Act includes "Distributed Denial of Service (DDoS)" attacks, the introduction of malicious code, ransomware, cryptoware, viruses, trojans, worms and logic or time bombs, or any other malware, program, file or harmful instruction that could disrupt, damage, prevent access to, or otherwise corrupt the operations of an Insured Telecommunications System, a Shared Telecommunications System, Telecommunications Data or software therein.

3.5 Media Wrongful Act: any actual or alleged:
A. disparagement or harm to the reputation or good name of a person or organization, libel, slander, product disparagement, false statements relating to the quality of products or services, infliction of emotional distress or mental anguish, or maliciously false statements made with intent to cause economic harm;
B. wiretapping, false imprisonment, malicious prosecution;
C. plagiarism, piracy or misappropriation of ideas in connection with Multimedia Content;
D. infringement of copyright, domain names, trade dress, titles or slogans, or dilution or infringement of trademarks, service marks, service names or trade names, in any case excluding any actual or alleged infringement of any patent or Trade Secret;
E. negligence in connection with the creation or dissemination by the Insured of Multimedia Content;

committed by the Insured, even with gross negligence, exclusively in the course of providing Multimedia Services.
The term Media Wrongful Act does not include any form of discrimination or discriminatory conduct, nor any alleged Media Claim arising from the inability to access, or limitations on access to, the Insured's website and/or Multimedia Content.

3.6 Malicious Computer Act: a fraudulent act committed against an Insured Computer System or a Shared Computer System, or fraudulent access to or hacking of an Insured Computer System or a Shared Computer System, for the purpose of creating, deleting, misappropriating, collecting, altering or destroying Data or services, without causing any physical damage to an Insured Computer System or a Shared Computer System, a device or a telecommunications infrastructure. The term Malicious Computer Act includes a distributed "denial of service" attack or the introduction of malicious code, actual or alleged ransomware, cryptoware, viruses, trojans, worms and logic or time bombs, or any malware, program, file or harmful instruction that may disrupt, damage, prevent access to, or otherwise impair an Insured Computer System or a Shared Computer System, Data or software therein.

3.1 Widespread Cause:
(i) a single act or a series of interrelated acts committed by one person or by a coordinated group of persons who are external to the Insured Company; or
(ii) a single error, omission or failure, or a series of interrelated errors, omissions or failures, by a person or a Computer System that is external to the Insured Company,

which constitutes or causes a Cyber Incident and/or Business Interruption and/or Cyber Extortion Event and/or Privacy and Network Security Event, and also constitutes or causes an incident within a Computer System of any person or entity outside the Limited Impact Group.

However, the term *Widespread Cause* does not include an act that requires the malicious manipulation of the actions of an Authorized User in order to bring about or cause such Cyber Incident and/or Business Interruption and/or Cyber Extortion Event and/or Privacy and Network Security Event.

3.2 Multimedia Content: electronic media distributed by or on behalf of the Insured on the internet, including social media websites.

3.3 Indecent Content: words, phrases, online publications, images, advertisements or any other material that:
A. is sexually explicit and in breach of a law prohibiting such content;
B. is sexually explicit and published online without the consent of the individual(s) depicted in the material;
C. encourages, facilitates, incites, or threatens abuse, harassment or sexual exploitation, including human trafficking and/or trafficking for sexual exploitation; or
D. encourages, facilitates, incites, or threatens physical violence, self-inflicted violence or any similar physical harm, including terrorism.

3.4 Policyholder: the entity indicated in Section 1 of the Policy Schedule that enters into this contract.

3.5 Improvement Costs (applicable only to the coverage set out in Section 2.2 of Art. 2 "Subject of Insurance: Coverage Extensions"):
A. costs to replace or restore software or applications within an Insured Computer System with newer, updated and/or improved versions of such software or applications; and
B. reasonable costs incurred for cybersecurity consulting following a breach and for improvements or preventive remedies.

Improvement Costs are deemed to be part of, and not in addition to, the Policy Period Limit stated in the Policy Schedule for the coverage "Data and Systems Recovery Costs" pursuant to Section 1.3 of Art. 1 "Subject of Insurance: Basic Coverages", and shall reduce such limit.

3.6 Loss Preparation Expenses: reasonable and necessary costs incurred by the Insured, with the prior consent of the Insurer, to prepare, certify details and verify particulars of the incident as required by the Insurer, and to appoint a third-party forensic accounting firm, including Aon Global Risk Consulting, in order to obtain assistance in calculating Business Interruption Losses, Extra Expenses, Incident Response Costs, Emergency Incident Response Costs, Hardware Replacement Costs, Reputational Damage Loss and Improvement Costs, where applicable.

3.7 Data and Systems Recovery Costs: reasonable and necessary costs:
A. to recover or reconstruct Data that have been damaged, compromised or lost. Costs to recover or reconstruct Data are covered only if and to the extent that a third-party computer forensics firm engaged to recover the lost Data determines that such Data can be recovered or reconstructed; and
B. to repair or restore software or applications within an Insured Computer System or a Shared Computer System, but only to the extent necessary to restore such system to a condition or functionality equal or equivalent to that existing prior to the Business Interruption; and
C. to identify and remedy the cause of the Business Interruption; and
D. with the Insurer's prior written consent, which shall not be unreasonably withheld or delayed:
i. to update, upgrade, replace or improve an Insured Computer System or a Shared Computer System, but only where the cost of upgrading, enhancing, replacing or improving the damaged or compromised software or applications to a newer or updated standard, condition, functionality or version is reasonably assessed by the Insured to be less than or equal to the cost of repairing, correcting or restoring the same; or
ii. to update, upgrade, replace or improve an Insured Computer System, but only where Improvement Costs are applicable; and
iii. any other reasonable and necessary cost to restore the Insured's operations to full operating capacity, but only to the extent that the Business Interruption alone created or caused the impediment or issue preventing full operational capacity; and
iv. Loss Preparation Expenses.

The term *Data and Systems Recovery Costs* does not include:
(a) costs or expenses incurred to identify or remedy software vulnerabilities;
(b) costs to replace any hardware or tangible property;
(c) costs incurred for the research and development of Data, including Trade Secrets;
(d) the economic or market value of Data, including Trade Secrets;
(e) any other indirect damage or loss;
(f) Incident Response Costs;
(g) costs to update, upgrade, replace, maintain or improve any Data or Computer System beyond what is provided for in items (i) and (ii) of letter D above.

3.8 Hardware Replacement Costs: reasonable costs incurred with the Insurer's prior written consent to repair, restore or replace Hardware, where such costs represent a more time-efficient and cost-effective solution than the recovery, reconstruction, repair or restoration of the Insured's Data within the Insured's existing Hardware.
Repair, restoration and/or replacement are limited to Hardware of equivalent condition or functionality to that existing prior to

the Network Security failure and do not apply to Hardware that was not part of the Insured Computer System immediately prior to the Network Security failure.

3.9 Damages: compensation for damages (including non-pecuniary damages), payment of interest accrued before or after judgment, settlements and the claimant's costs that the Insured is legally obligated to pay as a consequence of a Loss Event covered under this Policy.
The term *Damages* includes punitive and exemplary damages, but only to the extent that such damages are insurable under the laws of the applicable jurisdiction.
Solely in relation to coverage 1.5 of Art. 1 "Subject of Insurance: Basic Coverages", the term *Damages* also includes the Consumer Redress Fund, Payment Card Losses and Supervisory Authority Fines.
Each Damage is subject to the Policy Period Limit or Sublimit stated in the Policy Schedule in relation to the applicable coverage.

The term *Damages* does not include:
i. any amount the Insured is not legally obligated to pay;
ii. matters that are uninsurable under the law governing this Policy;
iii. the cost of complying with injunctive or other non-monetary relief or declaratory relief, including specific performance and any agreement to provide such relief;
iv. except as covered under Section 1.2 of Art. 1 "Subject of Insurance: Basic Coverages", the Insured's loss of fees or profits, or the return of fees or commissions;
v. royalties or the repetition of services by or under the supervision of the Insured;
vi. the return of profits, remuneration or economic benefits to which the Insured is not legally entitled;
vii. any other consequential loss or damage.

In relation to the coverage set out in Section 1.5 of Art. 1 "Subject of Insurance: Basic Coverages", the term *Damages* does not include any consideration due or paid to or by an Insured (including royalties or the return, reduction, surrender or refund of any payment, charge or fee) or costs to correct or repeat services relating to Products, including recall, loss of use or removal of Products.

3.1 Property Damage: physical damage to, or loss or destruction of, tangible property, including loss of use thereof. The term *Property Damage* does not include any damage to, loss, destruction or loss of use of Data.

3.2 Personal Injury: any injury arising out of one or more of the following:
A. wrongful arrest, detention or imprisonment;
B. legal action commenced in bad faith and with gross negligence;
C. libel, slander or any other defamatory or disparaging material;
D. publications or statements in violation of an individual's right to privacy; and
E. trespass, wrongful eviction, or any other invasion of the right of private occupancy.

3.3 Retroactive Date: the date stated in Section 4 of the Policy Schedule.

3.4 Data: any software or other information in electronic form stored on an Insured Computer System or on a Shared Computer System. The term *Data* includes the capability of an Insured Computer System or a Shared Computer System to store information, process information and transmit information via the Internet.

3.5 Personal Data:
A. the name of an individual, identity document or tax identification number, health or healthcare data, other confidential medical information, driver's license number, credit or debit card number, VAT number, address, telephone number, e-mail address, bank account number and transaction history, or passwords; and
B. any other personal information protected as defined by Privacy and Network Security Regulations, in any format.

3.6 Telecommunications Data: software or other information in electronic form stored on an Insured Telecommunications System or a Shared Telecommunications System. The term *Telecommunications Data* includes the capability of an Insured Telecommunications System or a Shared Telecommunications System to store, process and transmit information via the Internet, but does not include any hardware or tangible property.

3.7 Money: cash, coins, banknotes, bullion, checks, traveller's cheques, cashier's checks, postal orders, payment orders held for sale to the public, or funds, in tangible or electronic form. The term *Money* does not include cryptocurrencies, goods or tangible property.

3.8 Programming Error: an error:
A. by the Insured, or by an external service provider administering the Insured Computer System solely for the benefit of the Insured pursuant to a written agreement or contract with the Insured, occurring during the development or coding of a program, application or operating system on an Insured Computer System and which, once operational, would cause malfunctioning and/or interruption of operation and/or an incorrect result of such Insured Computer System;
B. by the external service provider administering the Shared Computer System for the benefit of the Insured pursuant to a written agreement or contract with the Insured, occurring during the development or coding of a program, application or operating system on a Shared Computer System and which, once operational, would cause malfunctioning and/or interruption of operation and/or an incorrect result of such Shared Computer System.

The term *Programming Error* does not include the integration, installation, updating or patching of any software, hardware or firmware of an Insured Computer System or a Shared Computer System, unless the Insured can demonstrate that the Programming Error arises from an Accepted Program.

3.9 Human Error: an operational error or omission, including the choice of program used, an error in setting parameters or any single inappropriate intervention on:
A. the Insured Computer System by the Insured or by the external service provider administering such Insured Computer System solely for the benefit of the Insured pursuant to a written agreement or contract with the Insured; or
B. the Shared Computer System by an external service provider administering such Shared Computer System for the benefit of the Insured pursuant to a written agreement or contract with the Insured,
resulting in loss, alteration or destruction of Data.

3.10 Loss Event: any actual or alleged Privacy and Network Security Event, Media Wrongful Act, Malicious Computer Act, Fraudulent Use or Access, Cyber Extortion Event, Cyber Incident or Business Interruption.

3.11 Widespread Impact Event: a Cyber Incident and/or Business Interruption and/or Cyber Extortion Event and/or Privacy and Network Security Event arising from a Widespread Cause.

3.12 Limited Impact Event: a Cyber Incident and/or Business Interruption and/or Cyber Extortion Event and/or Privacy and Network Security Event not arising from a Widespread Cause.

3.13 Cyber Extortion Event: a credible threat or a related series of credible threats made against the Insured with the express intent to carry out or cause, or the actual act of carrying out or causing:
A. the release, disclosure, dissemination, destruction or use of confidential, sensitive or protected information, or personally identifiable information, stored on an Insured Computer System or a Shared Computer System;
B. the failure of Network Security of an Insured Computer System or a Shared Computer System;
C. the introduction or insertion of a Malicious Computer Act into an Insured Computer System or a Shared Computer System;
D. the alteration, corruption, destruction, misappropriation, manipulation or damage of Data, instructions or electronic information transmitted or stored on an Insured Computer System or a Shared Computer System; or
E. the denial of or inability to access an Insured Computer System or a Shared Computer System,

for the purpose of demanding Money or cryptocurrencies from the Insured or otherwise requiring the Insured to satisfy a demand in exchange for the mitigation or removal of such threat or related series of threats, or the cessation or conclusion of the actual act of carrying out such threat or related series of threats.

The term *Cyber Extortion Event* does not include any threat or related series of threats against the Insured with the express intent to carry out or cause the foregoing, if originating from, approved by or ordered by a member of the Control Group.

3.14 Reputational Event: any negative publication, including print media, television, radio and social media, in relation to a Cyber Incident discovered by a member of the Control Group during the Policy Period and reported to the Insurer pursuant to Art. 5.8 “Claims Notification – Insureds’ Obligations”.

3.15 Cyber Extortion Funds: Money and cryptocurrencies paid by the Insured, where legally permitted and insurable, in an attempt to terminate or end a Cyber Extortion Event. The valuation of Cyber Extortion Funds shall be determined in accordance with Art. 5.10 “Loss Quantification”.

3.16 Consumer Redress Fund: an amount of money that the Insured is legally required to deposit into a fund as equitable relief for the payment of Privacy and Network Security Claims or Media Claims by consumers in the event of an adverse judgment or settlement in connection with a Supervisory Authority Proceeding. The term *Consumer Redress Fund* does not include amounts paid as taxes, duties, penalties, fines, injunctions or sanctions.

3.17 Deductible: the portion of Damages and Expenses and any other covered indemnifiable amount that remains the responsibility of the Insured, the amount of which is stated in the Policy Schedule with reference to the applicable coverage. The Deductible shall apply in accordance with Art. 5.4 “Deductible”.

3.18 Theft (applicable only to the coverage set out in Section 2.3 of Art. 2 “Subject of Insurance: Coverage Extensions”): a fraudulent and unlawful act by a Third Party whereby Money or Securities of an Insured Company are taken with the intent permanently to deprive the Insured Company thereof and to obtain a financial benefit for the perpetrator.

3.19 Control Group: the Chief Financial Officer, Chief Executive Officer, General Manager, Head of Legal Affairs, Risk Manager, Head of Information & Communication Technology, Chief Information Security Officer, Chief Technology Officer, Data Protection Officer, Insurance Manager, or the position within the Insured Company equivalent to the above-listed corporate roles.

3.20 Limited Impact Group: collectively:
(i) an Insured;
(ii) a person or entity having a direct business relationship with the Insured Company (a "Relationship"):

1. which, solely as a result of such Relationship, is affected by the Cyber Incident and/or Business Interruption and/or Cyber Extortion Event and/or Privacy and Network Security Event; or
2. through which, solely as a result of such Relationship, a Cyber Incident and/or Business Interruption and/or Cyber Extortion Event and/or Privacy and Network Security Event occurs;
   (iii) any other person or entity that is consequently affected by the Cyber Incident and/or Business Interruption and/or Cyber Extortion Event and/or Privacy and Network Security Event solely as a result of a direct or indirect business relationship with a person or entity described in item (ii)1 above; and
   (iv) solely with reference to coverage 1.1 "Incident Response Costs" of Art. 1 "Subject of Insurance: Basic Coverages" and 1.5 "Privacy and Network Security Liability" of Art. 2 "Subject of Insurance: Coverage Extensions", any "Impacted Party", meaning any person or entity that has a direct business relationship with a data custodian that falls within the definition of Third Party where such data custodian suffers a Data Custody Breach, provided that:
3. such Data Custody Breach results in:
   – a Breach Notification; and
   – the "Impacted Parties" incur similar notification expenses in compliance with Privacy Regulations; and
4. such act, error, omission or failure (or a series of interrelated acts, errors, omissions or failures) constituting or causing such Data Custody Breach does not result in further data breaches involving other Third Parties beyond the "Impacted Parties".

3.21 Hardware: desktop computers, laptop computers, mobile devices, servers, or network devices, including individual components thereof, owned or operated by the Insured or leased or rented by the Insured from third parties pursuant to a written contract.
The term does not include:
i. SCADA or ICS;
ii. servers or network devices;
iii. telecommunications systems or equipment;
iv. equipment connected with the operation, maintenance or provision of infrastructure, such as electrical, water-treatment or control equipment;
v. any other critical machinery or similar equipment.

3.22 Cyber Incident: any actual:
A. Malicious Computer Act, Human Error, Programming Error, Network Security failure, Unauthorized Use or Access or any other threat or action against an Insured Computer System or a Shared Computer System, including threats or actions in the commission of a Cyber Extortion Event;
B. Privacy and Network Security Event; or

C. power outage, power surge or voltage drop of an electrical system controlled by the Insured that gives rise to the need to incur Incident Response Costs.

3.23 Infrastructure: any of the following services, operated or provided by Third Parties:
A. electricity, gas, fuel, energy, water, telecommunications or similar services;
B. Internet infrastructure, including any Domain Name System ("DNS"), Certification Authority or Internet Service Provider ("ISP");
C. satellite services; or
D. financial transaction or payment processing platforms, including stock exchanges.

3.24 Business Interruption: inability to access, interruption or disruption of:
(i) an Insured Computer System or access to, deterioration of or destruction of Data contained therein; or
(ii) a Shared Computer System or access to, deterioration of or destruction of Data contained therein,
as the sole and direct result of:
A. a Malicious Computer Act;
B. Unauthorized Use or Access;
C. a Human Error;
D. a Network Security failure;
E. a Programming Error;
F. the reasonable and necessary shutdown of all or part of the Insured Computer System or the Shared Computer System in an effort to mitigate the effects of one of the events listed in A, B, C, D or E above; or
G. solely in relation to item (i) above, a power outage, power surge or voltage drop of an electrical system controlled by the Insured resulting from one of the events listed in A, B or D above.

3.25 Bodily Injury: bodily injury, sickness, illness or death. The term *Bodily Injury* also includes mental injury, mental anguish or tension, emotional distress, affliction, pain or shock, regardless of how caused or manifested. The term *Bodily Injury* does not include any mental injury, mental anguish or tension, emotional distress, affliction, pain or shock arising out of a Privacy and Network Security Event or a Media Wrongful Act covered pursuant to Sections 1.5 and 1.6 of Art. 1 "Subject of Insurance: Basic Coverages".

3.1 Aggregate Policy Limit: the amount stated in the Policy Schedule representing the maximum total amount payable by the Insurer under this Policy for each Policy Period, regardless of the number of Claims, Sublimits, Policy Period Limits, third parties seeking compensation, Insureds reporting a Claim, applicable coverages and/or any other element, whether considered separately or jointly.

3.2 Policy Period Limit: the amount stated in the Policy Schedule which forms an integral part of the Aggregate Policy Limit and represents the maximum total amount indemnifiable by the Insurer for each Policy Period for Damages and Expenses and other indemnifiable amounts under each coverage set out in Art. 1 "Subject of Insurance: Basic Coverages" and Art. 2 "Subject of Insurance: Coverage Extensions", regardless of the number of Claims, Sublimits, third parties seeking compensation, Insureds, applicable coverages and/or any other element, whether considered separately or jointly.

3.3 Operating Margin: the operating margin generated by the Insured's business net of all fixed costs.

3.4 Privacy and Network Security Regulations: regulations requiring commercial entities to publish privacy policies, adopt and enforce specific privacy or network security controls, or implement and enforce responsible management procedures,

including notification, protection, collection, custody, control, use or disclosure of Personal Data or other non-public third-party business information, including Data governed by the General Data Protection Regulation (GDPR).

3.5 Breach Notification: written communication from the Insured to an individual, sent voluntarily with the Insurer's prior consent or in order to comply with consumer notification obligations under Privacy Regulations, regarding any actual or reasonably suspected improper activity by the Insured, or by any external party for whose actions the Insured is legally responsible, in the handling, management, storage, destruction, protection or other control of:
(i) the Personal Data of such individual; and/or
(ii) confidential or proprietary information of such individual, where such individual is a Third Party and the Insured is legally required to maintain such information confidential.

3.6 Direct Financial Loss (applicable only to the coverage set out in Section 2.3 of Art. 2 "Subject of Insurance: Coverage Extensions"): the replacement value of Money or the market value of Securities at the time the Theft was first discovered by a member of the Control Group during the Policy Period. Direct Financial Loss shall be calculated in accordance with Art. 5.10 "Loss Quantification".

3.7 Payment Card Losses: monetary assessments, fines, penalties, chargebacks, refunds and fraud recoveries that the Insured is legally obligated to pay as a consequence of a Privacy and Network Security Event, where such amount is due to the Insured's failure to comply with the Payment Card Industry Data Security Standard (PCI-DSS).
The term *Payment Card Losses* does not include:
A. fines or monetary assessments resulting from continued non-compliance with PCI-DSS beyond a period of three (3) months from the date of the initial fine or monetary assessment; or
B. costs or expenses incurred to update or otherwise improve privacy or network security policies, procedures or controls.

3.8 Reputational Damage Losses:
A. the Insured's Operating Margin, before income taxes, that would have been generated had the Reputational Event not occurred, less the Operating Margin actually generated before income taxes, as a result of:
I. termination, cancellation or suspension by the Insured's customers of existing service contracts; or
II. any decrease in the volume or value of the Insured's customers' transactions;
B. with the Insurer's prior consent, reasonable and necessary costs to engage a third-party forensic accounting firm to calculate the amount of Reputational Damage Losses.

Reputational Damage Losses form part of, and not in addition to, the applicable Policy Period Limit stated in the Policy Schedule for Business Interruption and shall reduce such limit.
Reputational Damage Losses shall be calculated in accordance with Art. 5.15 "Calculation of Reputational Damage Losses".

3.9 Business Interruption Losses: the Insured's Operating Margin before income taxes that would have been generated had the Business Interruption not occurred, less the Operating Margin actually generated before income taxes.
The term *Business Interruption Losses* does not include amounts incurred during the Waiting Period. The Deductible applicable to Business Interruption Losses shall be calculated in accordance with Art. 5.4 "Deductible", letter D.

3.10 Policy Period: the period of time stated in Section 2 of the Policy Schedule, subject to termination pursuant to the Policy or applicable law.

3.11 Reduced Activity Period: the continuous period of time commencing immediately after the first date attributable to a Reputational Event and ending on the earlier of:
A. the date on which the Insured's customer accounts and seasonally adjusted daily revenue return to the level they would have been at had the Reputational Event not occurred; or
B. sixty (60) days after the commencement of the Reduced Activity Period.

3.12 Waiting Period: the number of hours stated in Section 3 under "Business Interruption" of the Policy Schedule following the occurrence of a Business Interruption.
Intermittent, partial or temporary restoration of functionality of the Insured Computer System or Shared Computer System shall not interrupt the running of the Waiting Period.

3.13 Indemnity Period: the period stated in Section 5 of the Policy Schedule during which the Insured sustains Business Interruption Losses or Data and Systems Recovery Costs, commencing when the Business Interruption occurs.

3.14 Extended Reporting Period: the period of extended coverage, where applicable, as described in Arts. 5.6 "Corporate Transactions" and 5.14 "Extended Reporting Period for Non-Renewal of the Policy".

3.15 Insured Person:
A. any past, present or future partner, director, supervisory board member, executive officer or employee (including temporary or fixed-term workers) of the Insured Company, while acting on behalf of or under the direction and control of the Insured Company; and
B. individuals engaged under a service contract with the Insured Company, while acting on its behalf.

The term *Insured Person* also includes:
i. the spouse (by marriage or civil union) of a partner, director, executive officer or employee, but only where a third-party claim that would have been covered under this Policy if brought against such partner, director, executive officer or employee is instead brought against such spouse;
ii. the heir, legal representative or successor in interest of a partner, director, executive officer or employee who is deceased, but only where a third-party claim that would have been covered under this Policy is brought against such individual.

The term *Insured Person* does not include any auditor, receiver, liquidator, extraordinary or judicial administrator, bankruptcy trustee, mortgagee or pledgee, or other similar role, nor any of their employees.

3.16 Individual: a person who can be identified, directly or indirectly, by reference to an identifier such as a name, tax identification number or other identification number issued by a State, location data, an online identifier such as an IP address, or one or more factors specific to the physical, cultural or social identity of that person.

3.17 Policy: this insurance contract, including the Policy Schedule and any endorsements issued thereto. It is specified that the proposal/questionnaire completed at inception also forms part of the contract.

3.18 Unlawful Employment Practices: any actual or alleged violation of employment or labor laws or other regulations relating to the actual or potential employment relationship of an individual with the Insured, including:
A. workplace violations of privacy, except to the extent such violations relate to a Privacy and Network Security Claim arising from the loss of Personal Data otherwise covered under Section 1.5 of Art. 1 "Subject of Insurance: Basic Coverages";
B. unlawful infliction of emotional distress in the workplace, except to the extent such distress relates to a Privacy and

Network Security Claim arising from the loss of Personal Data otherwise covered under Section 1.5 of Art. 1 “Subject of Insurance: Basic Coverages”.

3.19 Reward Payment (applicable only to the coverage set out in Section 2.4 of Art. 2 “Subject of Insurance: Coverage Extensions”): the reasonable amount or other reasonable security paid by an Insured Company, with the Insurer’s prior written consent (which shall not be unreasonably withheld or delayed), to an individual third party who is not affiliated with or employed by the Insured Company and who provides otherwise unavailable information leading to the arrest and conviction of the person responsible for a Cyber Extortion Event.
The term *Reward Payment* does not include any Incident Response Costs or Cyber Extortion Expenses.
Reward Payment forms part of, and not in addition to, the Policy Period Limit stated in the Policy Schedule for “Cyber Extortion” pursuant to coverage Section 1.4 of Art. 1 “Subject of Insurance: Basic Coverages”, and shall reduce such limit.

3.20 Supervisory Authority Proceeding: a request for information, complaint, action, investigation or civil proceeding by or on behalf of an administrative authority, commenced by the filing of a complaint or similar allegation asserting a violation of Privacy Regulations. The term *Supervisory Authority Proceeding* does not include any action, proceeding or lawsuit based on or relating to a criminal violation of Privacy Regulations, nor any portion of an action, proceeding or lawsuit based on or relating to such violation.

3.21 Products: anything the Insured sells, designs, creates, develops, assembles, manufactures, supplies, installs, disposes of, leases or licenses to third parties, or that is distributed by or on behalf of the Insured, including related repair or maintenance.

3.22 Accepted Program: a program that has been fully developed, successfully tested and proven effective in an equivalent operating environment prior to release.

3.23 Any Other Widespread Impact Event: a Widespread Impact Event not arising from Exploitation of Known Vulnerabilities, Exploitation of Software Supply Chain Vulnerabilities or Exploitation of Zero-Day Vulnerabilities.

3.24 Ransomware: any extortionate demand for Money or cryptocurrencies received by the Insured in connection with:
A. a Cyber Incident and/or Business Interruption and/or Cyber Extortion Event and/or Privacy and Network Security Event involving the introduction of malicious code for the purpose of blocking access to a Computer System or Data, or altering, corrupting, damaging, manipulating, misappropriating, encrypting, deleting or destroying Data; and/or
B. a credible threat, or a related series of credible threats, to release, disclose, disseminate or use Data exfiltrated in connection with one of the events described above.

3.25 Insurance Manager: the individual(s) employed by the Insured Company responsible for purchasing and maintaining the Insured Company’s insurance policies.

3.26 Privacy and Network Security Claim:
A. a written demand for monetary damages made against the Insured;
B. a civil proceeding against the Insured for monetary damages commenced by service of a summons, complaint or similar pleading;
C. an arbitration proceeding against the Insured for monetary damages; or
D. a Supervisory Authority Proceeding.

3.27 Media Claim:
A. a written demand for monetary damages made against the Insured;
B. a civil proceeding against the Insured for monetary damages commenced by service of a summons or similar pleading; or
C. an arbitration proceeding against the Insured for monetary damages.

3.28 Supervisory Authority Fines: civil monetary fines imposed by a government or public administrative authority, including an entity acting as a regulatory or supervisory body within its powers in a Supervisory Authority Proceeding. The term *Supervisory Authority Fines* does not include any civil monetary fines that are uninsurable by law, nor criminal fines or penalties, disgorgement of profits or multiple damages.

3.29 Additional Coinsurance: the percentage stated in Section 3 of the Policy Schedule applicable to the coverages set out in Art. 1 “Subject of Insurance: Basic Coverages” and Art. 2 “Subject of Insurance: Coverage Extensions”, representing the portion of each Damage or Expense for each Single Claim that, after application of the Deductible, remains the responsibility of the Insured and is not covered by this Policy. The Additional Coinsurance is subject to the terms set out in Art. 5.3 “Limits of Indemnity” of the “General Conditions Applicable to All Coverages”.

3.30 Trade Secret: information, including a formula, pattern, compilation, program, device, method, technique or process, that derives independent actual or potential economic value from not being generally known or readily ascertainable by others who could obtain economic value from its disclosure or use, provided that reasonable efforts have been made to maintain its secrecy.

3.31 Multimedia Services: the publication, distribution or dissemination of Multimedia Content.

3.1 Exploitation of Neglected Software: the exploitation of a vulnerability in software, firmware or hardware where, as of the first known date of exploitation:

1. such software, firmware or hardware has been withdrawn, is no longer available, is no longer supported by, or has reached end-of-life or end-of-support status with the vendor that developed it; or
2. such vulnerability has been listed as a Common Vulnerability and Exposure (“CVE”) in the National Vulnerability Database maintained by the National Institute of Standards and Technology, and a patch, fix or mitigation technique for such vulnerability was available to the Insured but was not applied by the Insured,

for a number of days falling within the ranges indicated with reference to the Sublimits for Exploitation of Neglected Software set out in Section 3 of the Policy Schedule.

3.2 Exploitation of Known Vulnerabilities: a Widespread Cause involving the exploitation of a software, firmware or hardware vulnerability which, as at the date of the first confirmed exploitation:
(i) is listed as a Common Vulnerability and Exposure (“CVE”) in the National Vulnerability Database maintained by the National Institute of Standards and Technology; and
(ii) has been assigned a Base Score or Overall Score of 8.0 or higher under version 2.0 or later of the Common Vulnerability Scoring System (“CVSS”).

3.3 Exploitation of Zero-Day Vulnerabilities: a Widespread Cause involving the exploitation of a software, firmware or hardware vulnerability (that is not an Exploitation of Known Vulnerabilities) which, within 45 days from the time the related

Cyber Incident and/or Business Interruption and/or Cyber Extortion Event and/or Privacy and Network Security Event is reported to the Insurer:
(i) is listed as a Common Vulnerability and Exposure ("CVE") in the National Vulnerability Database maintained by the National Institute of Standards and Technology; and
(ii) has been assigned a Base Score or Overall Score of 8.0 or higher under version 2.0 or later of the Common Vulnerability Scoring System ("CVSS").

3.4 Exploitation of Software Supply Chain Vulnerabilities: a Widespread Cause involving the insertion of malware, backdoors or other vulnerabilities into an Insured Computer System or a Shared Computer System through the malicious alteration of the source code of software, firmware or hardware that:
(i) is distributed by the software, firmware or hardware developer to more than one customer;
(ii) is not developed specifically for a single customer, including the Insured; and
(iii) is identified as secure by a digital certificate, such as a Software Publisher Certificate ("SPC").

3.5 Network Security: the activities performed by the Insured, or by others on behalf of the Insured, to protect against Malicious Computer Acts or Unauthorized Uses or Accesses to an Insured Computer System or a Shared Computer System.

3.6 Claim: a Privacy and Network Security Claim, a Media Claim and/or a Loss Event.

3.7 Single Claim: all Claims, Supervisory Authority Proceedings or other matters giving rise to a request for indemnification under this Policy that relate to the same originating source or cause or the same underlying source or cause, regardless of whether such Claims, Supervisory Authority Proceedings or other matters involve the same or different claimants, Insureds, events or legal grounds.

3.8 Insured Telecommunications System (applicable only to the coverage set out in Section 2.5 of Art. 2 "Subject of Insurance: Coverage Extensions"): the Insured's fixed-line telecommunications system or a fixed-line telecommunications system administered by an external service provider exclusively for the benefit of the Insured pursuant to a written agreement or contract.

3.9 Shared Telecommunications System: a fixed-line telecommunications system managed for the benefit of the Insured by a Third Party pursuant to a written agreement or contract with the Insured. The term *Shared Telecommunications System* does not include any Infrastructure.

3.10 Computer System: hardware, software, firmware and the Data stored thereon, including associated mobile devices, input and output devices, data storage devices, network equipment and local storage networks and other electronic data backup equipment, including SCADA and ICS systems.

3.11 Insured Computer System: a Computer System:
A. owned by, or administered or leased by, the Insured; or
B. administered exclusively for the benefit of the Insured by an external service provider pursuant to a written agreement or contract with the Insured.

3.12 Shared Computer System: a Computer System, other than an Insured Computer System, managed for the benefit of the Insured by a Third Party pursuant to a written agreement or contract with the Insured for the provision of data hosting,

cloud, co-location, data backup, data storage, data processing, Platform-as-a-Service, Software-as-a-Service, Infrastructure-as-a-Service or other similar outsourced services. The term *Shared Computer System* does not include any Infrastructure.

3.13 Insured Company: the Policyholder and each Subsidiary.

3.14 Subsidiary: a company, other than a partnership or joint venture, in which, as at the inception date of the first Policy Period, the Policyholder directly or indirectly:
A. owns more than 50% of the voting rights;
B. has the right to appoint or remove more than 50% of the members of the board of directors; or
C. controls, alone pursuant to a written agreement with other shareholders, more than 50% of the voting rights,

and only:
i. with respect to Privacy and Network Security Wrongful Acts and Media Wrongful Acts occurring after the Retroactive Date and while such company was a Subsidiary; and
ii. with respect to Cyber Incidents, Business Interruptions, Cyber Extortion Events and Thefts discovered by a member of the Control Group while such company was a Subsidiary.

3.15 Pollutants: any solid, liquid, gaseous or thermal irritant or contaminant, including smoke, vapor, soot, fumes, acids, alkalis, chemicals, asbestos, asbestos-containing products or waste (including materials to be recycled, reconditioned or remediated).

3.16 Expenses: Privacy and Network Security Claim Expenses, Media Claim Expenses, Cyber Extortion Expenses, Cyber Extortion Funds, Business Interruption Losses, Data and Systems Recovery Costs and Incident Response Costs. The term *Expenses* also includes, if the applicable coverage is operative, Improvement Costs, Loss Preparation Expenses, Emergency Incident Response Costs, Direct Financial Loss, Reward Payment, Hardware Replacement Costs, Reputational Damage Losses and/or Telecommunications Expenses.

3.17 Extra Expenses: reasonable costs and expenses incurred in an effort to avoid, mitigate or reduce the duration or extent of a Business Interruption, or to reduce the loss of Gross Operating Margin as a consequence of a Business Interruption.
The term *Extra Expenses* includes, by way of example only:
A. the use of external equipment, whether by engaging a third party or by renting such equipment;
B. the adoption of an alternative working method in accordance with a business continuity plan;
C. subcontracting costs incurred with an external service provider; and
D. increased labor costs.

Extra Expenses do not include Incident Response Costs or Data and Systems Recovery Costs.

3.18 Emergency Incident Response Costs (applicable only to the coverage set out in Section 2.1 of Art. 2 “Subject of Insurance: Coverage Extensions”): reasonable and necessary expenses:
A. to engage the services of a cyber incident response service provider in order to coordinate the response to a confirmed Cyber Incident or confirmed Business Interruption of the Insured;
B. to engage the services of a forensic computer firm to determine the cause and scope of a confirmed Cyber Incident or

confirmed Business Interruption of the Insured and to initiate the process necessary to stop, reverse or remedy the effects of such Cyber Incident or Business Interruption.

Emergency Incident Response Costs form part of, and not in addition to, the Policy Period Limit stated in the Policy Schedule for "Incident Response" pursuant to Section 1.1 of Art. 1 "Subject of Insurance: Basic Coverages", and shall reduce such limit and may exhaust it entirely.

3.19 Incident Response Costs: reasonable and necessary expenses:
A. to engage incident response services to coordinate the response to a Cyber Incident or Business Interruption;
B. to engage the services of a forensic computer firm to determine the cause and scope of a Cyber Incident or Business Interruption;
C. to comply with consumer notification obligations under applicable Privacy and Network Security Regulations, to the extent insurable, where such compliance is required as a result of a Cyber Incident, including by way of example:
i. costs to engage a notification service provider or call center; and
ii. costs to engage legal counsel to determine applicability of and actions required to comply with Privacy and Network Security Regulations;
D. to engage legal counsel to manage and respond to investigations initiated by a regulatory or supervisory authority, or equivalent administrative body, regarding an alleged violation of Privacy and Network Security Regulations, or to communicate with such authority to determine applicability of and actions required to comply with such regulations, expressly excluding costs to represent or defend the Insured in a Supervisory Authority Proceeding;
E. to engage a public relations firm, law firm or crisis management firm for publicity or similar communications, solely for the purpose of protecting or restoring the Insured's reputation as a consequence of a Cyber Incident or Business Interruption;
F. to engage legal counsel solely to obtain preliminary legal advice regarding the Insured's rights and alternatives in connection with reasonable and necessary legal issues arising from a Cyber Incident or Business Interruption, including determination of potential indemnification rights under a supplier contract and preparation for and mitigation of potential third-party litigation;
G. to engage a licensed private investigator or credit specialist to provide fraud consultation, for a period not exceeding one (1) year, to individuals whose Personal Data have been unlawfully disclosed or otherwise compromised, and to engage identity restoration services for individuals confirmed by such investigator or specialist to be victims of identity theft as a direct and exclusive result of the Cyber Incident;
H. for credit monitoring, identity theft monitoring, social media monitoring, credit freezes, fraud alert services or other fraud prevention software for the benefit of individuals whose Personal Data have been unlawfully disclosed or otherwise compromised as a result of the Cyber Incident; and
I. with the Insurer's prior written consent:
i. to voluntarily notify individuals whose Personal Data have been unlawfully disclosed, including the use of notification services or support call centers; and
ii. any other reasonable and necessary expense, which may include reasonable costs to prevent, limit or mitigate third-party liability.

The term *Incident Response Costs* does not include:
(a) costs or expenses to update or otherwise improve privacy or network security controls, policies or procedures beyond the level existing prior to the Loss Event, or to comply with Privacy and Network Security Regulations, except to the extent Improvement Costs apply;
(b) taxes, duties, fines, penalties, injunctions or sanctions;
(c) Supervisory Authority Fines;

(d) Data and Systems Recovery Costs;
(e) Business Interruption Losses;
(f) Money or cryptocurrencies paid by the Insured to terminate or end a Cyber Extortion Event;
(g) Cyber Extortion Expenses;
(h) internal salaries, wages, expenses or operating costs of the Insured;
(i) costs to respond to, initiate or defend third-party litigation relating to the Cyber Incident or Business Interruption; or
(j) Loss Preparation Expenses.

3.20 Telecommunications Expenses (applicable only to the coverage set out in Section 2.5 of Art. 2 "Subject of Insurance: Coverage Extensions"): the invoiced amount for unauthorized voice or data line charges or unauthorized bandwidth. Telecommunications Expenses do not include any fraudulent charges that are cancelled, refunded or recovered by or on behalf of the telecommunications provider, nor any voice, data or bandwidth charges arising from voluntary, negligent or unlawful abuse or excessive use of an Insured Telecommunications System or a Shared Telecommunications System by employees or authorized third parties with legitimate access.
Telecommunications Expenses form part of, and not in addition to, the Policy Period Limit stated in the Policy Schedule for "Telecommunications Fraud" pursuant to Section 2.5 of Art. 2 "Subject of Insurance: Coverage Extensions", and shall reduce such limit.

3.21 Cyber Extortion Expenses: reasonable and necessary expenses to engage an external consultant solely for the purpose of managing negotiation and payment of Cyber Extortion Funds in order to terminate or end a Cyber Extortion Event.

3.22 Privacy and Network Security Claim Expenses:
A. reasonable and necessary legal fees, expert witness fees and other fees and costs incurred by the Insured, with the Insurer's prior written consent (not to be unreasonably withheld or delayed), in the investigation, settlement, defense and appeal of a covered Privacy and Network Security Claim; and
B. in jurisdictions where applicable, reasonable and necessary bond premiums for appeal bonds, attachment bonds or similar bonds, provided that the Insurer shall have no obligation to furnish or post any bond.

3.23 Media Claim Expenses:
A. reasonable and necessary legal fees, expert witness fees and other fees and costs incurred by the Insured, with the Insurer's prior written consent (not to be unreasonably withheld or delayed), in the investigation, settlement, defense and appeal of a covered Media Claim;
B. in jurisdictions where applicable, reasonable and necessary bond premiums for appeal bonds, attachment bonds or similar bonds, provided that the Insurer shall have no obligation to furnish or post any bond; and
C. with the Insurer's prior written consent, reasonable and necessary fees incurred for public relations and crisis communications services.

3.24 Third Party: any person or entity that does not fall within the definition of Insured under this Policy.

3.25 Securities (applicable only to the coverage set out in Section 2.3 of Art. 2 "Subject of Insurance: Coverage Extensions"): negotiable or non-negotiable instruments or contracts, including any security, share, bond, evidence of debt or other instrument representing equity or debt, representing money or property. The term *Securities* does not include Money, cryptocurrencies, goods or tangible property.

3.26 Corporate Transaction: any of the following events:
A. the Policyholder or all of its assets are acquired by another entity;
B. the Policyholder merges with or is consolidated into another entity;
C. any person, entity or connected group acquires the right or power to elect, appoint or designate at least 50% of the members of the board of directors;
D. any person, entity or connected group acquires 50% or more of the share capital of the Policyholder; or
E. a liquidator, receiver, trustee or judicial administrator (or equivalent role appointed by a court in insolvency, debt restructuring or recovery proceedings), an extraordinary administrator or a fiduciary is appointed to assume management, administration, liquidation, supervision or other form of control over the Policyholder.

3.27 Malicious Use or Access:
A. prohibited, illegal and unauthorized entry, use of or access to an Insured Computer System or a Shared Computer System; or
B. prohibited, illegal and unauthorized entry, use of or access to an Insured Telecommunications System or a Shared Telecommunications System.

3.28 Unauthorized Use or Access: entry or access to an Insured Computer System or a Shared Computer System by an unauthorized person, including an employee or authorized party acting in excess of their authorization.

3.29 Authorized User: an individual authorized by the Insured Company to access an Insured Computer System or a Shared Computer System.

3.30 Personal Data Custody Breach:
(i) unlawful or unauthorized access to, exposure, disclosure, loss, alteration or destruction of Personal Data and/or confidential or proprietary information of a Third Party for which the Insured is legally responsible to maintain confidentiality; and/or
(ii) a data breach as defined by Privacy Regulations, involving Data stored in a Computer System managed by a Third Party acting as data custodian or data processor pursuant to a written agreement or contract with the Insured.

4. GENERAL EXCLUSIONS

The Insurer shall not indemnify any **Damages or Expenses** arising out of a **Claim**:

4.1 Known facts that alleges, is based upon, arises out of or is attributable to a Loss Event actually or allegedly occurring prior to the inception date of the first Policy Period if, as of that date (or, if earlier, as of the inception date of any other policy issued by the Insurer of which this Policy is a renewal or replacement), a member of the Control Group was aware of, or could reasonably have foreseen, that such Loss Event had given rise to or could give rise to Damages and/or Expenses.

4.2 Prior or pending litigation that alleges, is based upon, arises out of or is attributable to:
A. any prior or pending litigation, Privacy and Network Security Claim, Media Claim, demand, arbitration, administrative or regulatory proceeding or investigation which, as of the inception date of the first Policy Period (or, if earlier, the inception date of any other policy issued by the Insurer of which this Policy is a renewal or replacement), had been filed or commenced against the Insured and of which the Insured had received notice, or that contests or arises out of the same or substantially the same facts, circumstances or situations underlying the foregoing; or
B. any Loss Event reported under any other policy prior to the inception date of the first Policy Period; or
C. any other Loss Event occurring at any time which, together with a Loss Event reported under any other policy prior to the inception date of the first Policy Period, would constitute a Single Claim.

4.3 Intentional acts directly or indirectly caused by, arising out of, or in any way connected with conduct of the Insured whereby:
A. any knowing or intentional unlawful act, breach of duty, or violation of any law or regulation is committed or permitted; or
B. any criminal act or any intentionally fraudulent or intentionally dishonest act or omission is committed or permitted; or
C. the Insured obtains or seeks to obtain a personal profit, gain or advantage to which it is not legally entitled; or
D. there is intentional and unauthorized, undisclosed or unlawful use or collection of Personal Data by the Insured.

This exclusion applies only if such conduct has been established by a final judgment (after exhaustion of all appeals) or by written admission.
Pursuant to Art. 1900 of the Italian Civil Code, this exclusion does not apply to intentional acts of persons for whom the Insured is legally liable.
No conduct of an Insured Person shall be imputed to any other Insured Person or Insured Company. However, conduct committed by or with the knowledge of a past, present or future member of the Control Group shall be imputed to the relevant Insured Company.

4.4 Discrimination and unlawful employment practices that alleges, is based upon, arises out of or is attributable to:
A. discrimination of any nature;
B. humiliation, harassment or any improper conduct based on, arising out of or related to discrimination of any nature; or
C. Unlawful Employment Practices.

However, this exclusion shall not apply to the portion of a Privacy and Network Security Claim alleging invasion of privacy in the workplace or infliction of emotional distress in the workplace, where such claim arises from a loss of Personal Data otherwise covered pursuant to Section 1.5 of Art. 1 “Subject of Insurance: Basic Coverages”.

4.5 Insured vs. Insured brought or maintained by or on behalf of the Insured, or by any other person or entity for whom the Insured is legally responsible, arising from a Privacy and Network Security Claim or a Media Claim.
However, this exclusion shall not apply to a Privacy and Network Security Claim brought against the Insured by an Insured Person alleging the commission by the Insured of a Privacy and Network Security Event pursuant to letters B and C of the relevant definition, expressly covered under Section 1.5 of Art. 1 “Subject of Insurance: Basic Coverages”.

4.6 Contractual obligations for breach of any contract, commitment, warranty or promise (including quasi-contracts under common law jurisdictions and equivalent obligations under civil law jurisdictions), including liquidated damages clauses and any obligation assumed by the Insured.
This exclusion shall not apply to:
A. liability that would have attached to the Insured in the absence of such contract, commitment, warranty, promise or agreement; or
B. indemnities provided by the Insured under a written contract or agreement with a customer of the Insured relating to a Privacy and Network Security Event that results in failure to maintain the confidentiality or privacy of Personal Data of that customer’s clients; or
C. with respect to coverage under Section 1.5 of Art. 1 “Subject of Insurance: Basic Coverages”, Payment Card Losses.

4.7 Fees and remuneration solely with respect to coverages under Sections 1.5 and 1.6 of Art. 1 “Subject of Insurance: Basic Coverages”: that alleges, is based upon, arises out of or is attributable to any fee, charge or cost paid to or charged by the Insured.

4.8 Bodily injury and property damage that alleges, is based upon, arises out of or is attributable to any Bodily Injury or Property Damage.
However, this exclusion shall not apply to Hardware Replacement Costs.

4.9 Infrastructure

that alleges, is based upon, arises out of or is attributable to any failure, interruption, disturbance, degradation, corruption, deterioration or inactivity of Infrastructure.
However, this exclusion shall not apply to a Limited Impact Event.

4.10 Natural perils

that alleges, is based upon, arises out of or is attributable to fire, smoke, explosion, lightning, wind, flood, earthquake, volcanic eruption, electromagnetic impulse or radiation, tidal wave, landslide, hail, or any natural event (other than an intentional act) or any other physical event of whatever cause.

4.11 War

that alleges, is based upon, arises out of or is attributable to:

1. any Malicious Computer Act and/or Unauthorized Use or Access, committed in whole or in part by or on behalf of a sovereign state or a state-supported actor or group, giving rise to or cited as the basis for:
   A. an order by a G7 member state, or any governmental body of any sovereign state, involving the use of force against a sovereign state; or
   B. a resolution or other formal action of the United Nations Security Council authorizing the use of force or economic sanctions against a sovereign state, or involving the use of force by NATO or any equivalent international intergovernmental military or political alliance against a sovereign state; or
2. any Malicious Computer Act and/or Unauthorized Use or Access, or any hostile act or event, or series of related acts or events (each a “Hostile Act”), committed or occurring in whole or in part by or on behalf of a sovereign state

or state-supported actor or group:
A. giving rise to or cited as the basis for a formal declaration of war by the United States Congress or by any governmental body of any other sovereign state against a sovereign state; or
B. following any of the acts or events described in items 1 and 2.A above, where such act or event has the same originating or underlying source or cause as the Malicious Computer Act and/or Unauthorized Use or Access and/or Hostile Act described therein; or

3. civil war, rebellion, revolution or insurrection.

4.12 Commercial hardware

that alleges, is based upon, arises out of or is attributable to any damage to, loss or destruction of Hardware that:
A. is intended by the Insured for sale, lease, rental or loan to third parties; or
B. has already been sold, leased, rented or loaned to third parties by the Insured.

4.13 Pollution

that alleges, is based upon, arises out of or is attributable to the actual or threatened discharge, release, escape, seepage, migration or disposal of Pollutants, or any order, directive or formal demand that the Insured test, monitor, remediate, remove, contain, treat, detoxify or neutralize Pollutants, or any voluntary decision to do so.

4.14 Wear and tear and deterioration

solely with respect to coverages under Sections 1.1, 1.2 and 1.3 of Art. 1 “Subject of Insurance: Basic Coverages” and Sections 2.1, 2.2 and 2.5 of Art. 2 “Subject of Insurance: Coverage Extensions”: that alleges, is based upon, arises out of or is attributable to normal wear and tear or gradual deterioration of an Insured Computer System, a Shared Computer System, an Insured Telecommunications System, a Shared Telecommunications System, Data or Telecommunications Data, including any data processing media.

4.15 Patents and trade secrets

that alleges, is based upon, arises out of or is attributable to any claim, dispute or litigation regarding the validity, invalidity, infringement, misappropriation or misuse of any patent or Trade Secret by or on behalf of the Insured.
However, this exclusion does not apply to Incident Response Costs, Data and Systems Recovery Costs or Cyber Extortion coverage.

4.16 Intellectual property

that alleges, is based upon, arises out of or is attributable to any infringement, misappropriation or violation by the Insured of any copyright, service mark, trademark, trade name or other intellectual property right of a third party.
However, this exclusion does not apply to a Privacy and Network Security Event or a Media Wrongful Act expressly covered under Sections 1.5 or 1.6 of Art. 1 “Subject of Insurance: Basic Coverages”.

4.17 False or misleading advertising

solely with respect to coverage under Section 1.6 of Art. 1 “Subject of Insurance: Basic Coverages”: that alleges, is based upon, arises out of or is attributable to goods, Products or services described, depicted or referenced in Multimedia Content.

4.18 Products

arising out of the performance or safety of any Product, any Product recall, or any liability arising from Products.

4.19 Financial transactions

that alleges, is based upon, arises out of or is attributable to any:

A. financial loss due to inability to trade, invest, divest, purchase or sell securities or financial assets of any nature; however, solely with respect to Business Interruption Losses covered under Section 1.2 of Art. 1 “Subject of Insurance”, this exclusion does not apply to the Insured’s loss of fee or commission income;
B. fluctuations in the value of assets;
C. financial value of any account held by the Insured with a financial institution; or
D. inability to realize interest or capital gains on any asset.

4.20 Cyber crime acts

solely with respect to coverage under Section 2.3 of Art. 2 “Subject of Insurance: Coverage Extensions”, the Insurer shall not pay any Direct Financial Loss that consists of or results from:
A. any act of the Insured’s employees or external contractors, including acts involving collusion with any employee or contractor;
B. any act of the Insured’s directors, general managers or executive officers, including acts involving collusion with such persons;
C. any administrative seizure of the Insured’s Money or Securities;
D. any fluctuation in the value of Money or Securities;
E. indirect or consequential damages or losses, including by way of example income and profits; or
F. recall costs.
The Insurer shall not indemnify any **Damages or Expenses** arising out of a **Claim**:

4.1 Apache Log4j

that alleges, is based upon, arises out of or is attributable to the presence of, or vulnerability in, any Log4j software version earlier than v2.15.0 on any Computer System.

4.2 Public Authorities

that alleges, is based upon, arises out of or is attributable to any public or administrative authority, foreign enemy, military power or coup d’état:
A. giving rise to the seizure or confiscation of an Insured Computer System, Shared Computer System, Insured Telecommunications System, Shared Telecommunications System, Data or Telecommunications Data; and/or
B. imposing restrictions on operations, closure or shutdown of:
(i) any entity or person managing a Computer System; and/or
(ii) any Computer System.
However, this exclusion shall not apply to such actions if taken by a public or administrative authority directed exclusively against an Insured Computer System or an Insured Telecommunications System in response to a Malicious Computer Act, Unauthorized Use or Access, or Malicious Use or Access, also directed exclusively against such Insured Computer System or Insured Telecommunications System.

4.3 Antitrust or Unfair Trade Practices

that alleges, is based upon, arises out of or is attributable to price fixing, restraints of trade, monopolies, interference with economic relations (including interference with contractual relations or prospective economic advantage), unfair competition, unfair business practices or unfair trade practices, or any violation of the Federal Trade Commission Act, the Sherman Antitrust Act, the Clayton Act, or any other antitrust, monopoly, price-fixing, price-discrimination, predatory-pricing, restraint-of-trade, unfair competition or unfair trade practice law in force in the United States (and any amendments thereto), or any related statute or regulation (and amendments thereto), or any similar federal, state or common law of the United States.

However, with respect to coverage 1.5 “Privacy and Network Security Liability” under the Policy, this exclusion shall not apply to Privacy and Network Security Claims arising directly from a violation of a Privacy Regulation.

4.4 Indecent Content

that alleges, is based upon, arises out of or is attributable to failure by the Insured, or by any other person or entity for whom the Insured is legally responsible, to prevent the publication or dissemination of Indecent Content.

4.5 Gambling or Games of Chance

solely in relation to coverage 1.6 “Media Liability”: that alleges, is based upon, arises out of or is attributable to any gambling, contest, wager, game of chance or skill, lottery or promotional game, including tickets, coupons, vouchers or similar items.

4.6 Inaccurate Prices, Costs or Estimates

solely in relation to coverages 1.5 “Privacy and Network Security Liability” and 1.6 “Media Liability”: that alleges, is based upon, arises out of or is attributable to guaranteed costs, representation costs, contractual prices, guaranteed prices, estimates of probable costs or cost overruns, or any other warranty or promise regarding cost reductions, return on investment or profitability of the Insured.

4.7 Violation of Laws of the United States of America

that alleges, is based upon, arises out of or is attributable to:
A. a Claim brought in the United States of America; or
B. a Claim based on any action or liability arising out of the following:
(i) **Consumer Protection Laws:** that alleges, is based upon, arises out of or is attributable to any violation by the Insured of the Truth in Lending Act, the Fair Debt Collection Practices Act, or the Fair Credit Reporting Act (and any amendments thereto), or any related statute or regulation (and amendments thereto), or any similar federal, state or common law of the United States. However, with respect to coverage 1.5 “Privacy and Network Security Liability”, this exclusion shall not apply to Privacy and Network Security Claims arising directly from the actual or alleged disclosure or theft of Personal Data directly resulting from a Cyber Incident;
(ii) **ERISA or Securities Laws:** that alleges, is based upon, arises out of or is attributable to any violation by the Insured of the following laws in force in the United States:
a. the Employee Retirement Income Security Act of 1974 (ERISA), as amended;
b. the Securities Act of 1933, the Securities Exchange Act of 1934, the Investment Company Act of 1940;
c. the Investment Advisors Act, or any other federal, state or local securities law of the United States;
and any amendments thereto, or any related statute or regulation (and amendments thereto), or any similar federal, state or common law of the United States.
However, with respect to coverages 1.1 “Incident Response Costs” and 1.5 “Privacy and Network Security Liability”, item (a) above shall not apply;
(iii) **Unsolicited Communications:** that alleges, is based upon, arises out of or is attributable to any unsolicited electronic dissemination of faxes, emails or other communications by or on behalf of the Insured, including actions brought pursuant to the Telephone Consumer Protection Act or any federal or state anti-spam law in force in the United States, or any similar federal, state or common law relating to the right to privacy of individuals or legal entities. However, with respect to coverage 1.5 “Privacy and Network Security Liability”, this exclusion shall not apply to Privacy and Network Security Claims arising from a Privacy and Network Security Wrongful Act as defined in item C of the relevant definition;
(iv) **Foreign Corrupt Practices Act:** that alleges, is based upon, arises out of or is attributable to any violation of the U.S. Foreign Corrupt Practices Act (as amended), or any related statute or regulation (and amendments thereto), or any similar federal, state or common law of the United States;

(v) **False Claims Act** (solely in relation to coverages 1.5 "Privacy and Network Security Liability" and 1.6 "Media Liability"): that alleges, is based upon, arises out of or is attributable to any actual or alleged violation by the Insured of the False Claims Act (31 U.S.C. §§ 3729–3733), as amended, or any related statute or regulation, or any similar federal, state or common law of any country worldwide.

5. GENERAL CONDITIONS APPLICABLE TO ALL COVERAGES

5.1 Territorial Scope Coverage

To the extent permitted by law (including applicable trade or economic sanctions) and subject to the terms and conditions of this Policy, the insurance provided under this Policy applies to Claims occurring anywhere in the world, with the exception of Privacy and Network Security Claims, Media Claims and Supervisory Authority Proceedings brought or originating in the United States of America or Canada, or in any territory subject to the jurisdiction thereof, which are therefore excluded from coverage.

5.2 Temporal Validity of Liability Coverages (Claims Made)

With reference to the third-party liability coverages set out in Sections 1.5 and 1.6 of Art. 1 "Subject of Insurance: Basic Coverages", this Policy is issued on a claims-made basis. It therefore covers Privacy and Network Security Claims and Media Claims first made against the Insureds during the Policy Period or, where applicable, during the Extended Reporting Period, provided that such Claims arise from Privacy and Network Security Wrongful Acts or Media Wrongful Acts occurring after the Retroactive Date and before the expiry of the Policy Period.

5.3 Limit of Indemnity

A. The Policy Period Limits, Deductibles and Sublimits stated in the Policy Schedule in relation to the coverages set out in Art. 1 "Subject of Insurance: Basic Coverages" and Art. 2 "Subject of Insurance: Coverage Extensions" shall apply separately to each coverage.

B. The total amount payable by the Insurer (including Damages and Expenses) under this Policy in relation to each Single Claim and in the aggregate shall not exceed the Policy Period Limit and the Aggregate Policy Limit.

C. The total amount payable by the Insurer (including Damages and Expenses) under this Policy in relation to each coverage set out in Art. 1 "Subject of Insurance: Basic Coverages" and Art. 2 "Subject of Insurance: Coverage Extensions" shall not exceed the applicable Policy Period Limit or Policy Period Sublimit, which shall be deemed an integral part of the Aggregate Policy Limit.

D. The total amount payable by the Insurer (including Damages and Expenses) under this Policy for each Policy Period shall not exceed the Aggregate Policy Limit.

E. Each coverage under Art. 2 "Subject of Insurance: Coverage Extensions", as well as any other Sublimit indicated in the Policy Schedule, shall be deemed part of, and not in addition to, the Policy Period Limit applicable to the coverage under Art. 1 "Subject of Insurance: Basic Coverages" to which it refers, which in turn forms part of the Aggregate Policy Limit. Sublimits shall not be reinstated once exhausted or reduced.

F. Any payment made by the Insured for Damages or Expenses by way of Additional Coinsurance shall not reduce the applicable Sublimit, Policy Period Limit or Aggregate Policy Limit. Only the portion of Damages or Expenses paid by the Insurer shall reduce the applicable limits. Where Additional Coinsurance applies to more than one coverage under Art. 1 or Art. 2 or to the related Sublimits, such Additional Coinsurance shall be calculated on the lesser of the Sublimit and the Policy Period Limit.

G. Where a Widespread Impact Event, Exploitation of Neglected Software or Ransomware is covered under more than one coverage under Art. 1 or Art. 2, only the lowest applicable Policy Period Sublimit, together with the corresponding Additional Coinsurance and Deductible, shall apply.

H. Limits of Indemnity for Widespread Impact Events: the Sublimits for Widespread Impact Events shall be deemed part of, and not in addition to, the applicable Policy Period Limits indicated in Section 3 of the Policy Schedule and shall not increase such limits or render operative coverages for which no Policy Period Limit is stated. Such Sublimits also form part of, and not in addition to, the Aggregate Policy Limit. All covered Damages or Expenses arising from a Single Claim shall be subject to the applicable Deductible, Additional Coinsurance and Sublimit.

I. Ransomware Sublimit: all covered Damages or Expenses arising from a Single Claim in connection with a Cyber Incident and/or Business Interruption and/or Cyber Extortion Event and/or Privacy and Network Security Event resulting from Ransomware shall be subject to the applicable Ransomware Sublimit, Deductible and Additional Coinsurance indicated in Section 3 of the Policy Schedule.

J. Exploitation of Neglected Software Sublimit: all covered Damages or Expenses arising from a Single Claim in connection with a Cyber Incident and/or Business Interruption and/or Cyber Extortion Event and/or Privacy and Network Security Wrongful Act resulting from Exploitation of Neglected Software shall be subject to the applicable Sublimit, Deductible and Additional Coinsurance indicated in Section 3 of the Policy Schedule..

5.4 Deductible

A. The Insurer shall be liable only for that portion of a Claim, and of any other covered indemnifiable amount arising from a Claim, which exceeds the Deductible. The Deductible shall remain the responsibility of the Insured and is not covered under this Policy.

B. Only one Deductible shall apply to each Single Claim. However, the Deductible applicable to coverage under Section 2.2 of Art. 2 “Subject of Insurance: Coverage Extensions” shall apply separately to each Single Claim.

C. If a Single Claim is subject to multiple Deductibles, each Deductible shall apply separately to the relevant portion of Damages and Expenses, provided that the aggregate shall not exceed the highest Deductible. However, the Deductible applicable to coverage under Section 2.2 of Art. 2 shall apply separately and in addition.

D. With reference to coverage under Section 1.2 of Art. 1 “Subject of Insurance: Basic Coverages”, the Insurer shall pay Business Interruption Losses actually incurred by the Insured:
i. after expiration of the applicable Waiting Period;
ii. in excess of the Deductible stated in Section 3 of the Policy Schedule.

Business Interruption Losses shall not include any losses incurred during the Waiting Period.

E. The total amount payable by the Insurer in relation to each Single Claim arising from Ransomware shall not exceed the “Ransomware” Sublimit stated in the Policy Schedule, which forms an integral part of the applicable Policy Period Limit and the Aggregate Policy Limit. Such Sublimit shall not be reinstated once exhausted or reduced.

5.5 Claims and Related Facts

A Single Claim shall be relevant for the purposes of this Policy only if notice of the first Claim, or of any other matter giving rise to a Claim that subsequently became such Single Claim, is provided by the Insured during the Policy Period.

5.6 Corporate Transactions

In the event that a Corporate Transaction occurs during the Policy Period, the Insurer shall indemnify only Damages and/or Expenses relating to Loss Events covered under this Policy that occurred prior to the Corporate Transaction, provided that such Loss Events are reported in accordance with Art. 5.8 "Claims Notification – Insureds' Obligations".

The Policyholder may, however, up to 45 days following a Corporate Transaction, request the Insurer to activate an Extended Reporting Period of a maximum duration of 84 months from the expiry date of the Policy Period during which the Corporate Transaction occurred. Following such request and upon receipt of any information the Insurer may require, the Insurer shall be free to submit an offer for a duration it determines, not exceeding 84 months, subject to payment of an additional premium and on such terms and conditions as the Insurer may determine at its sole discretion. The additional premium shall not be refundable.

5.7 Acquisitions and Creations of New Subsidiaries

The definition of Subsidiary under this Policy includes any company that becomes a Subsidiary during the Policy Period, provided that:

A. the new Subsidiary does not increase the aggregate turnover of the Insured Company by more than 20%, based on the latest certified consolidated financial statements;

B. the new Subsidiary is not domiciled in the United States of America, Canada or territories subject to their jurisdiction;

C. the new Subsidiary does not provide financial advisory or brokerage services and is not registered as an Investment Advisor with the U.S. Securities and Exchange Commission; and

D. the activities of the new Subsidiary are not materially different from those of the Insured Company.

With respect to any new Subsidiary not meeting the above conditions, the Policy shall nevertheless automatically extend coverage to such company for a period of 60 days from the date of acquisition or incorporation. Coverage may be extended beyond 60 days subject to the Insurer's written approval, under such terms and conditions as the Insurer may determine.

With respect to each new Subsidiary, insurance coverage shall apply solely to Claims first made or first discovered during the Policy Period, provided that they relate to Loss Events committed or occurring after the acquisition or creation of such new Subsidiary.

5.8 Claims Notification – Insureds' Obligations

A.

The Insured shall notify the Insurer in writing of any **Claim** as soon as reasonably possible after a member of the Control Group has reason to believe that such Claim may reasonably give rise to a loss or liability (including claim expenses) equal to or greater than 50% of the applicable Deductible, and in any event no later than sixty (60) days from the earlier of:

i. the date on which a member of the Control Group first becomes aware of the Claim; or

ii. in the event of non-renewal of the Policy, the expiry date of the Policy Period or of the Extended Reporting Period, where applicable.

B.

All notifications under this Policy shall be sent to the Insurer or to the intermediary entrusted with the administration of the Policy.

C.
Each notification shall include detailed information. In particular:

i. the following shall be provided:
a) a detailed description of the alleged Claim, Damage or Expense and any other relevant element;
b) details of all parties involved, including names and contact information;
c) a copy of the Privacy and Network Security Claim or Media Claim brought by the third party and all notices and documents relating to a Supervisory Authority Proceeding;
d) comprehensive details of the alleged Damage and/or Expense; and
e) any other information reasonably requested by the Insurer.

ii. claims for indemnity submitted by the Insured to the Insurer in relation to **Business Interruption Losses** shall be accompanied by a calculation of such losses, setting out in detail how the losses were calculated and the underlying assumptions. The Insured shall provide all documentary evidence reasonably requested by the Insurer, including accounts, accounting records, statements, invoices, registers or other documents, or copies thereof.

D.
If, during the Policy Period or the Extended Reporting Period (where applicable), the Insured:
i. following discovery by any member of the Control Group, becomes aware of any circumstance that may give rise to a Claim and reports such circumstance to the Insurer; or
ii. receives a written request asking the Insured to waive a limitation period, or to suspend the running of the remaining time before expiry of a limitation period for the commencement of civil proceedings against the Insured arising from a Loss Event occurring prior to the expiry of the Policy Period, and reports such request and such Loss Event in writing to the Insurer,

any Claim subsequently arising from such circumstance or request shall be deemed to have been first reported during the Policy Period.

E.
The Insured shall report any **Ransomware** event to the competent authorities as soon as reasonably possible.

F. Additional obligations in the event of a Cyber Incident and/or Business Interruption and/or Cyber Extortion Event and/or Privacy and Network Security Event:

1) Mitigation and preservation of evidence.
The Insured shall take all reasonable steps to mitigate loss, continue operations, preserve any contractual rights or remedies, and protect and retain property, Computer Systems, log files, books and records, reports or evidence (collectively, the “Evidence Items”) reasonably necessary for the determination of Damages and Expenses arising from a Cyber Incident and/or Business Interruption and/or Cyber Extortion Event and/or Privacy and Network Security Event. Any costs incurred to protect or preserve Evidence Items shall be covered as Incident Response Costs, subject to the Insurer’s prior consent.

2) Cooperation in claim adjustment.
Upon request, the Insured shall provide the Insurer with a proof of loss, setting out full details of the Cyber Incident and/or Business Interruption and/or Cyber Extortion Event and/or Privacy and Network Security Event as soon as possible after notification pursuant to paragraph A above. Where requested, such proof shall include written reports from all service providers involved in the investigation or response, and any written reports or correspondence to or from law enforcement

agencies, public bodies or authorities, regulatory or supervisory authorities, or similar entities.
The proof of loss shall provide full details of each amount claimed, including the calculation method, underlying assumptions and all relevant documentary evidence. The Insured shall cooperate fully with the Insurer and provide all additional information reasonably requested for the investigation and shall allow and facilitate the Insurer's examination of any relevant Evidence Item. The Insured shall not be required to disclose information subject to a court-ordered non-disclosure; however, once such order ceases to apply, the Insurer shall be entitled to request such information as part of the proof of loss.

3) Right of inspection.
The Insurer, and any Third Party acting on its behalf, shall have the right, but not the obligation, to inspect, assess and verify any Evidence Items relevant to the assessment of Damages and Expenses. Such right shall not constitute any undertaking on behalf of, or for the benefit of, the Insured. Any inspection-related costs shall be borne by the Insurer and shall not erode any Sublimit, Policy Period Limit or Aggregate Policy Limit.

4) Loss assessment and indemnification.
In determining whether a Cyber Incident and/or Business Interruption and/or Cyber Extortion Event and/or Privacy and Network Security Event constitutes a **Limited Impact Event** or a **Widespread Impact Event**, the Insurer may rely on the proof of loss and Evidence Items provided by the Insured and/or on any independent evidence, including public information or non-public information obtained during the Insurer's investigation, such as third-party reports (e.g., from public authorities, IT service providers or forensic firms). Any costs incurred in obtaining such independent evidence shall be borne by the Insurer and shall not erode limits.

Incident Response Costs and Emergency Incident Response Costs shall be covered pursuant to Art. 1.1 and Art. 2.1, respectively, up to the applicable Sublimit or Policy Period Limit for a Limited Impact Event, until the earlier of:
– the time when the Insured obtains, or should reasonably obtain, facts or evidence indicating that the event is a Widespread Impact Event; or
– the time when the Insurer determines, based on the available evidence, that the event is a Widespread Impact Event.

Thereafter, such costs shall be covered up to the Policy Period Limit applicable to a Widespread Impact Event.
If it is impossible or impracticable to determine the classification, the Insurer may, at its sole discretion, treat the event as a Limited Impact Event.

The Insurer shall pay covered Damages and Expenses after receipt of a complete proof of loss, provided the Insured has complied with all Policy obligations and the parties agree on the amounts payable. If relevant information is subject to a non-disclosure order, loss assessment shall be suspended until disclosure is permitted. Any disagreement shall be resolved pursuant to Art. 6.17 "Governing Law and Jurisdiction".

5)
If the Insured elects not to provide the proof of loss or Evidence Items required to determine event classification, the Insured agrees that the event shall be deemed a Widespread Impact Event. Such failure shall not constitute a breach of the Policy. Failure to provide notice in accordance with this section shall relieve the Insurer of liability only to the extent it demonstrates material prejudice arising from such failure; the burden of proof rests with the Insurer.

5.9 Calculation of Business Interruption Losses and Reputational Damage Losses

A. Calculation of Business Interruption Losses

In assessing the losses, the Insurer shall take into account trends and circumstances relating to the twelve (12) months immediately preceding the Business Interruption which affected, or would have affected, the profitability of the business had the Business Interruption not occurred, including any material change in market conditions that would have affected the Operating Margin generated.

However, the Insurer's assessment shall not include any increase in income that would presumably have been achieved as a result of increased business volume due to favorable market conditions.

Such calculation must be supported by **Loss Preparation Expenses**.

B. Calculation of Reputational Damage Losses

The Insurer shall calculate Reputational Damage Losses giving full and due consideration to the following:

i. the Insured's proof of loss;

ii. forensic accounting analysis relating to Reputational Damage Losses, pursuant to subsection B;

iii. any past or future trends or circumstances that affected, or would have affected, the Insured's business profitability;

iv. any material changes in market conditions or adjustment expenses that would impact the Operating Margin generated; and

v. any income derived from substitute methods, facilities or personnel used by the Insured to maintain its revenue stream.

Such calculation must be supported by **Loss Preparation Expenses**.

5.10 Loss Quantification

For the purpose of quantifying:

A. Direct Financial Loss indemnifiable by the Insurer, the following valuation criteria shall apply:

i. for foreign currencies, the value in Euro based on the exchange rate published by *Il Sole 24 Ore* on the date on which the Theft was first discovered by a member of the Control Group;

ii. for Securities indemnifiable by the Insurer, the lesser of:

a) the closing price of the Securities on the business day immediately preceding the date on which the Theft was first discovered by a member of the Control Group; or

b) the replacement cost of the Securities.

B. Cyber Extortion Funds and/or Reward Payments reimbursable by the Insurer shall be quantified as follows: where Cyber Extortion Funds and/or Reward Payments are paid in a currency, including cryptocurrencies, other than the Euro or the local currency of the place in which this Policy was issued, reimbursement shall be subject to submission of evidence of the method used to calculate the applicable exchange rate for converting such currency into Euro or into the local currency of the place in which this Policy was issued, as at the date on which such Cyber Extortion Funds and/or Reward Payments were actually paid.

Reimbursement by the Insurer of Direct Financial Loss and/or Cyber Extortion Funds and/or Reward Payments shall be made in the local currency of the place in which this Policy was issued, upon submission of the relevant supporting evidence by the Insured. The Insurer reserves the right to challenge or adjust the calculation where the evidence provided is based on an incorrect or inflated exchange rate.

5.11 Allocation of Loss

Where a Claim involves both matters covered and matters not covered under this Policy, the Insured and the Insurer agree to make a fair and proper allocation of Damages and Expenses, taking into account the relative legal and financial exposure attributable to the covered and uncovered matters.

5.12 Management of Legal Proceedings

A. With respect to the coverages set out in Sections 1.5 and 1.6 of Art. 1 "Subject of Insurance: Basic Coverages", the Insurer may assume and conduct, in the name of the Insured, the defense of Privacy and Network Security Claims and Media Claims for which the Insurer may be required to indemnify the Insured.

B. The Insured undertakes not to take any action that may prejudice or potentially prejudice the Insurer in connection with covered Privacy and Network Security Claims or Media Claims.

C. The Insured further undertakes not to admit liability in respect of, or agree to settle, any Privacy and Network Security Claim or Media Claim, including any related Expense, without the Insurer's prior written consent (which shall not be unreasonably withheld or delayed), and to consult the Insurer before initiating any investigation, defense or settlement thereof.

At its own expense, the Insured shall provide the Insurer and any investigator or legal representative appointed by the Insurer with all information reasonably requested and shall fully cooperate and assist the Insurer in investigating, defending, settling, avoiding or limiting Claims, Damages and Expenses, whether actual or potential.

5.13 Disputes Regarding Defense and Settlement of Claims

If a dispute arises between the Insured and the Insurer as to whether to settle a Privacy and Network Security Claim or Media Claim, or to appeal a judgment or decision relating thereto, the Insurer may seek the opinion of a legal adviser of proven experience selected by the Insurer.

If such adviser recommends, taking into account all circumstances, attempting settlement, the Insurer—after consulting with the Insured and obtaining the Insured's written consent (which shall not be unreasonably withheld or delayed)—shall attempt settlement in accordance with that recommendation. Should such settlement attempt be unsuccessful, the Insurer shall continue to indemnify the Insured in accordance with all terms, conditions, exclusions and limitations of this Policy.

The Insured shall not be required to accept the adviser's recommendation.

5.14 Extended Reporting Period in the Event of Non-Renewal of the Policy

If, upon expiry of the Policy Period, this Policy is not renewed or replaced by another policy issued by a different insurer covering, in whole or in part, the same risk, the Insureds shall automatically benefit from a sixty (60)-day Extended Reporting Period at no additional premium.

Furthermore, except where a Corporate Transaction has occurred, coverage may be extended for the Extended Reporting Period upon payment of the additional premium stated in Section 6 of the Policy Schedule, commencing from the expiry of the last Policy Period.

Coverage during the Extended Reporting Period shall operate as follows:

A. for coverages under Sections 1.1, 1.2, 1.3 and 1.4 of Art. 1 and the coverages under Art. 2, solely with respect to Loss Events occurring prior to the expiry of the most recent Policy Period and reported before expiry of the Extended Reporting Period;

B. for coverages under Sections 1.5 and 1.6 of Art. 1, solely with respect to Privacy and Network Security Wrongful Acts and Media Wrongful Acts entirely committed prior to expiry of the Policy Period and reported before expiry of the Extended Reporting Period.

To obtain the Extended Reporting Period described above, the Policyholder must, within sixty (60) days of expiry of the last Policy Period:

i. notify the Insurer in writing of its intention to exercise the option; and

ii. pay the additional premium.

The additional premium shall be fully earned and non-refundable.

The right to an Extended Reporting Period shall cease if, and from the time when, the Policyholder obtains insurance

coverage covering, in whole or in part, the same risk as this Policy. Any Extended Reporting Period already purchased shall automatically terminate, and the premium shall be deemed fully earned and non-refundable.
No Extended Reporting Period shall apply or be activated where the Policy is not renewed due to non-payment of premium, termination for wilful misconduct, or cancellation or annulment for any other reason.
For clarity, an offer by the Insurer to renew the Policy on different terms, conditions, limits or premiums shall not constitute a refusal to renew.

6. GENERAL PROVISIONS APPLICABLE TO THE INSURANCE CONTRACT

6.1 How to Read the Policy

In this Policy, unless the context requires otherwise:
A. the singular includes the plural and vice versa;
B. headings are for convenience only and shall not affect interpretation;
C. any position, office, legal status, concept or legal basis includes the equivalent in any other jurisdiction;
D. any law or regulation includes any subsequent amendment or re-enactment thereof; and
E. words shown in **bold** have the meaning set out in Art. 3 “General Policy Definitions” and in the Policy Schedule.

6.2 Statements Relating to Risk Circumstances

Any misstatements or omissions by the Policyholder or the Insured relating to circumstances affecting risk assessment may result in total or partial forfeiture of the right to indemnity and may also lead to termination of the Policy pursuant to Articles 1892, 1893 and 1894 of the Italian Civil Code.

6.3 Increase of Risk

The Policyholder or the Insured shall notify the Insurer in writing of any increase of risk. Increases of risk not known to or accepted by the Insurer may result in total or partial forfeiture of the right to indemnity and may also lead to termination of the Policy pursuant to Art. 1898 of the Italian Civil Code.

6.4 Decrease of Risk

In the event of a decrease of risk, the Insurer shall reduce the premium or subsequent premium instalments following notification by the Policyholder or the Insured, pursuant to Art. 1897 of the Italian Civil Code.

6.5 Payment of Premium and Inception of Coverage

Coverage shall incept at 12:00 midnight on the date stated in the Policy if the premium or first instalment has been paid; otherwise, coverage shall incept at 12:00 midnight on the date of payment.
If the Policyholder fails to pay subsequent premiums or instalments, coverage shall be suspended from 12:00 midnight on the 30th day after the due date and shall resume at 12:00 midnight on the date of payment, without prejudice to subsequent due dates (Art. 1901 of the Italian Civil Code).
Premiums shall be paid to the intermediary appointed to manage the Policy or directly to the Insurer.

6.6 Taxes

All taxes relating to the Policy shall be borne by the Policyholder.

6.7 Policy Term and Automatic Renewal

Where the law or the Policy refers to the insurance period, it shall be deemed to be twelve (12) months, unless the Policy is entered into for a shorter or longer term, in which case it shall coincide with the duration of the contract.

6.8 Ownership of Rights Arising from the Policy

Actions, claims and rights arising from this Policy may be exercised only by the Policyholder and the Insurer. In particular, the Policyholder is entitled to perform the acts necessary for loss assessment and settlement.
Loss assessment and settlement carried out in this manner shall also be binding on the Insured, who shall have no right of

challenge.
Indemnity determined in accordance with the Policy shall be payable only to, or with the consent of, the holders of the insured interest.

6.9 Authorization Clause
The Policyholder agrees to act on behalf of the Insureds in connection with this Policy.

6.10 Subrogation
The Insurer shall be subrogated, up to the amount paid, to the rights of each Insured against third parties liable for the loss. Each Insured shall be liable to the Insurer for any prejudice caused to such right (Art. 1916 of the Italian Civil Code).

6.11 Amendments to the Insurance
Any amendments to the insurance shall be evidenced in writing.

6.12 Other Insurance
If multiple insurance policies are taken out separately with different insurers for the same risk, the Insured shall notify each insurer of all such policies. If the Insured wilfully fails to provide such notice, the insurers shall not be obliged to pay indemnity. In the event of a loss, the Insured shall notify all insurers, indicating the names of the others (Art. 1910 of the Italian Civil Code).

6.13 Form of Communications to the Insurer
Communications pursuant to Art. 5.8 “Claims Notification – Insureds’ Obligations”, notice of cancellation and any other communication resulting in termination of coverage shall be sent to the Insurer by registered letter with return receipt or by certified electronic mail (PEC).
All other communications may be sent, by any other valid documentary means, to the Policyholder or the intermediary managing the Policy, but in the latter case they shall take effect only if promptly forwarded to the Insurer.

6.14 Fraudulent Exaggeration of Loss
The Policyholder or the Insured shall forfeit the right to indemnity if they wilfully exaggerate the amount of a Claim, Expense or Damage, declare destroyed property that did not exist at the time of the loss, conceal, remove or tamper with salvaged or undamaged property, use false or fraudulent documents, wilfully alter traces or remnants of the loss, facilitate its progression, or alter material evidence of a crime.

6.15 Economic and Trade Sanctions
The Insurer shall not be liable to provide coverage, pay any indemnity or compensation, or grant any benefit under this Policy if doing so would expose the Insurer, or its parent/controlling company, to sanctions, prohibitions or restrictions under United Nations resolutions or under trade or economic sanctions imposed by the European Union or its Member States, the United Kingdom or the United States of America.

6.16 Confidentiality Undertaking
Each Insured shall undertake not to disclose to any third party information relating to Deductibles, Sublimits, Policy Period Limits, the Aggregate Policy Limit and the premium under this Policy, nor to disclose such information in the financial statements of the Insured Company, unless:
i. the Insurer has given prior written consent; or
ii. the Insured is required to provide, or procure the issuance of, an insurance certificate to a customer; or
iii. disclosure is required by court order.

6.17 Governing Law and Jurisdiction
This Policy shall be governed by Italian law, which shall apply to all matters not expressly regulated herein. Any dispute relating to its validity, interpretation or performance shall be subject to the exclusive jurisdiction of the courts of Milan.

6.18 Broker Clause

The Policyholder declares that it has entrusted the management of this Policy to **ALPHA International Insurance Brokers S.r.l.**, with registered office in Florence, Viale Don Giovanni Minzoni No. 44, acting as Broker pursuant to Legislative Decree No. 209/2005.

The parties acknowledge that all communications relating to the performance of this insurance shall be made also through the appointed Broker. Accordingly, any communication made by the Policyholder and/or the Insured to the Broker shall be deemed made to the Insurer and vice versa, and any communication made by the Broker to the Insurer shall be deemed made by the Policyholder and/or the Insured. Any communication involving contractual amendment shall bind the Insurer only upon written consent.

Exclusively for notices of termination, the parties (Policyholder and Insurer) shall send such notice directly to each other, copying the appointed Broker.

In the event of inconsistency between communications made by the Broker and those made directly by the Policyholder to the Insurer, the latter shall prevail.

By virtue of the authority granted by the Insurer to collect premiums, payment made in good faith to the Broker or persons for whom it is responsible shall be deemed payment made directly to the Insurer pursuant to Art. 118, paragraph 2, of Legislative Decree No. 209/2005, with full discharge also for the purposes of Art. 1901 of the Italian Civil Code.

The Broker's remuneration shall not be borne by the insurers awarded the contract, as such fees shall be borne by the Procuring Institute in accordance with procedure No. **NP/EUI/REFS/2025/005** for the provision of Insurance Brokerage Services.

6.19 Tax Exemption

The Policyholder declares that it is exempt from payment of taxes due to the Italian State pursuant to the agreements between the Government of the Italian Republic and the European University Institute, as set out in Presidential Decree No. 990 of 13 October 1976, published in the Official Gazette on 19 December 1977.

The Policyholder **The Company**

INSURANCE POLICY TABLE

Aggregate Policy Limit

€ 1,000,000

Policy Period Limits and Deductibles

First-Party Damage Coverages

Incident Response Costs

- in relation to an **Insured Computer System**
  - Limit per Policy Period: **100% of the indemnity limit**
  - Deductible: **€35,000**
- in relation to a **Shared Computer System**
  - Limit per Policy Period: **100% of the indemnity limit**
  - Deductible: **€35,000**

Business Interruption Losses

- in relation to an **Insured Computer System**
  - Limit per Policy Period: **100% of the indemnity limit**
  - Deductible: **€35,000**
  - Waiting Period: **24 hours**
- in relation to a **Shared Computer System**
  - Limit per Policy Period: **100% of the indemnity limit**
  - Deductible: **€35,000**
  - Waiting Period: **24 hours**

Data and Systems Recovery Costs

- in relation to an **Insured Computer System**
  - Limit per Policy Period: **100% of the indemnity limit**
  - Deductible: **€35,000**
- in relation to a **Shared Computer System**
  - Limit per Policy Period: **100% of the indemnity limit**
  - Deductible: **€35,000**

Cyber Extortion Losses

- in relation to an **Insured Computer System**
  - Limit per Policy Period: **100% of the indemnity limit**
  - Deductible: **€35,000**
- in relation to a **Shared Computer System**
  - Limit per Policy Period: **100% of the indemnity limit**
  - Deductible: **€35,000**

Third-Party Liability Coverages

Privacy and Network Security Liability

- Limit per Policy Period: **100% of the indemnity limit**
- Deductible: **€35,000**

Media Liability

- Limit per Policy Period: **100% of the indemnity limit**
- Deductible: **€35,000**

Coverage Extensions

Emergency Incident Response Costs

- in relation to an **Insured Computer System**
  - Sublimit per Policy Period: **€50,000**
  - Deductible: **€35,000**
- in relation to a **Shared Computer System**
  - Sublimit per Policy Period: **€50,000**
  - Deductible: **€35,000**

Improvement Costs

- Sublimit per Policy Period: **€50,000**
- Deductible: **€35,000**

Cyber Crime

- in relation to an **Insured Computer System**
  - Sublimit per Policy Period: **€25,000**
  - Deductible: **€35,000**
- in relation to a **Shared Computer System**

  - Sublimit per Policy Period: **€25,000**
  - Deductible: **€35,000**

Reward Payment

- Sublimit per Policy Period: **€50,000**
- Deductible: **€0**

Telecommunications Fraud

- in relation to an **Insured Computer System**
  - Sublimit per Policy Period: **€25,000**
  - Deductible: **€35,000**
- in relation to a **Shared Computer System**
  - Sublimit per Policy Period: **€25,000**
  - Deductible: **€35,000**

Sublimits

Consumer Redress Fund

- Sublimit per Policy Period: **100% of the indemnity limit**
- Deductible: **€35,000**

Payment Card Losses

- Sublimit per Policy Period: **100% of the indemnity limit**
- Deductible: **€35,000**

Supervisory Authority Fines

- Sublimit per Policy Period: **100% of the indemnity limit**
- Deductible: **€35,000**

Additional Sublimits

Ransomware

- Additional Coinsurance: **0%**
- Sublimit per Policy Period: **50% of the indemnity limit**

- Deductible: **€35,000**

Exploitation of Neglected Software

- **0–45 days:**
  - Additional Coinsurance: **0%**
  - Sublimit per Policy Period: **100%**
  - Deductible: **€35,000**
- **46–90 days:**
  - Additional Coinsurance: **5%**
  - Sublimit per Policy Period: **50%**
  - Deductible: **€35,000**
- **91–180 days:**
  - Additional Coinsurance: **10%**
  - Sublimit per Policy Period: **25%**
  - Deductible: **€35,000**
- **181–365 days:**
  - Additional Coinsurance: **25%**
  - Sublimit per Policy Period: **10%**
  - Deductible: **€35,000**
- **Over 365 days:**
  - Additional Coinsurance: **50%**
  - Sublimit per Policy Period: **5%**
  - Deductible: **€35,000**

Sublimits for Widespread Impact Events

- **Exploitation of Known Vulnerabilities**
  - Additional Coinsurance: **0%**
  - Sublimit per Policy Period: **100%**
  - Deductible: **€35,000**
- **Exploitation of Software Supply Chain Vulnerabilities**
  - Additional Coinsurance: **0%**
  - Sublimit per Policy Period: **100%**
  - Deductible: **€35,000**
- **Exploitation of Zero-Day Vulnerabilities**
  - Additional Coinsurance: **0%**
  - Sublimit per Policy Period: **100%**
  - Deductible: **€35,000**
- **Any Other Widespread Impact Event**
  - Additional Coinsurance: **0%**
  - Sublimit per Policy Period: **100%**

- Deductible: **€35,000**

Special Conditions

It is agreed as follows:

Policy Schedule – Section 3

Section 3 of the Policy Schedule is supplemented with the following **Sublimit**:

Coverage Extensions	Limit per Claim	Limit per Policy Period	Deductible per Claim
2.6 Hardware Replacement	100% of the Indemnity Limit	100% of the Indemnity Limit	Policy Deductible

---

Amendment to Art. 2 – "Subject of Insurance: Coverage Extensions"

Article 2 "Subject of Insurance: Coverage Extensions" is supplemented with the following paragraph, to be read at the end of the article:

First-Party Damage Coverages

The Insurer shall pay on behalf of the Insured:

2.6 Hardware Replacement
Hardware Replacement Costs arising exclusively and directly from a Network Security failure that results in Hardware being rendered electrically inoperable, reduced in its functionality or rendered unusable for its intended purpose, provided that such Network Security failure is discovered by a member of the Control Group during the Policy Period and is reported to the Insurer in accordance with Art. 5.8 "Claims Notification – Insureds' Obligations".

Amendment to Art. 3 – "General Definitions"

Article 3 "General Definitions" is supplemented with the following definitions:

3 Hardware:**
desktop computers, laptop computers, mobile devices, servers, or network devices, including individual components thereof, owned or operated by the Insured or leased or rented by the Insured from third parties pursuant to a written contract.

The term does not include:
i. SCADA or ICS;
ii. telecommunications systems or equipment;
iii. equipment connected with the operation, maintenance or supply of infrastructure, such as electrical, water-treatment or

control equipment;
iv. any other critical machinery or similar equipment.

3 Hardware Replacement Costs:**
reasonable costs incurred with the Insurer's prior written consent to repair, restore or replace Hardware, where such costs represent a more time- and cost-efficient solution than the recovery, reconstruction, repair or restoration of the Insured's Data within the Insured's existing Hardware.
Repair, restoration and/or replacement shall be limited to Hardware of equivalent condition or functionality to that existing prior to the Network Security failure and shall not apply to Hardware that did not form part of the Insured Computer System and/or a Computer System managed for the benefit of the Insured by a Third Party pursuant to a written agreement or contract immediately prior to the Network Security failure.

Replacement of Existing Definitions

The following definitions in Art. 3 "General Definitions" are deleted and replaced as follows:

3.81 Expenses:
Privacy and Network Security Claim Expenses, Media Claim Expenses, Cyber Extortion Expenses, Data and Systems Recovery Costs and Incident Response Costs.
The term *Expenses* also includes, where the applicable coverage is operative, Improvement Costs, Emergency Incident Response Costs, Reward Payment, Telecommunications Expenses and/or Hardware Replacement Costs.

3.75 Computer System:
Hardware, software, firmware and the Data stored thereon, including associated mobile devices, input and output devices, data storage devices, network equipment and local storage networks and other electronic data backup equipment, including SCADA and ICS systems.

Amendment to Art. 4 – "General Exclusions"

Replacement of Exclusion 4.8

Exclusion 4.8 in Art. 4 "General Exclusions" is deleted and replaced as follows:

4.8 Bodily Injury and Property Damage
that alleges, is based upon, arises out of or is attributable to any Bodily Injury or Property Damage.
However, this exclusion shall not apply to Hardware Replacement Costs.

Additional Exclusions

Art. 4 "General Exclusions" is supplemented with the following exclusion:

4. Commercial Hardware**

that alleges, is based upon, arises out of or is attributable to any damage to, loss or destruction of Hardware that:

A. is intended by the Insured for sale, lease, rental or loan to third parties; or

B. has already been sold, leased, rented or loaned to third parties by the Insured.

Art. 4 “General Exclusions” is further supplemented with the following exclusion:

4.xx Professional Civil Liability

solely in relation to the coverages under Art. 1.5 “Privacy and Network Security Liability” and Art. 1.6 “Media Liability”, that alleges, is based upon or arises out of:

a) acts, errors or omissions giving rise to civil liability in the provision of Professional Services;

b) breach of duties, false or misleading statements, or negligent misrepresentations in the provision of Professional Services;

c) any unintentional contractual breach with a client in the provision of Professional Services;

d) fraudulent or dishonest acts or omissions by an employee of the Insured Company during the provision of Professional Services;

e) unintentional infringement of intellectual property rights;

f) any civil liability arising from failure to provide Professional Services due to a Cyber Incident, Cyber Extortion Event, Malicious Use or Access or Business Interruption.

Additional Definition

Article 3 “General Policy Definitions” is supplemented with the following definition:

1.1 Professional Services:

any service or good provided in the ordinary course of business, whether or not pursuant to a written contract, in the name and on behalf of the Insured.

All other terms and conditions remain unchanged.