



CyberContract

General terms & conditions

Version: 2018.3.0 EN

Communication

In consideration of the payment of the annual premium and subject to all the provisions of this policy, the **insurers** and the **insured** agree as follows:

Any **claim, breach of data security, breach of retention, newsworthy event, extortion, cyber theft, network interruption** or claim under the legal protection coverage must be reported to the relevant **insurer** or to CyberContract in its capacity of insurance broker during the term of the policy in accordance with the provisions of this policy.

Insurers

Cyber
AIG Europe SA (Belgian branch)
Boulevard de la Plaine 11 –
1050 Brussels Belgium
RPM: 0682.816.659
FSMA : 0976

Option Legal protection
Euromex SA
Generaal Lemanstraat 82 – 92
2600 Berchem
Belgium
RPM: 0404.493.859
FSMA : 0463

Table of contents

SECTION 1. Definitions for the Cyber-guarantees.....	8
1.1 Administrative fines	8
1.2 Administrative investigation/regulatory investigation	8
1.3 Annual premium.....	8
1.4 Board Member, Member of the board/Family Member	8
1.5 Breach Notice Law	8
1.6 Breach of personal information	8
1.7 Breach of the company data	8
1.8 Breach of the data security	9
1.9 Claim	9
1.10 Company.....	9
1.11 Company data.....	9
1.12 Company's' Computer System.....	10
1.13 Computer assets.....	10
1.14 Control.....	10
1.15 Cyber-incident	10
1.16 Cyber-terrorism	10
1.17 Damages	10
1.18 Data.....	11
1.19 Data protection officer.....	11
1.20 Data Protection Regulation/Privacy Legislation	11
1.21 Data Subject.....	11
1.22 Data Subject Access Request	11
1.23 Defence costs.....	12
1.24 Digital media	12
1.25 Discovery period	12
1.26 Enforcement Notice.....	12
1.27 Expenses for the reduction of network interruption	12
1.28 External IT specialist.....	12
1.29 Identity theft insurance (ID theft insurance).....	12
1.30 Inception date	13
1.31 Information Commissioner, Data Protection Officer	13
1.32 Information holder.....	13
1.33 Insured	13
1.34 Insured event	13
1.35 Insured period.....	13

1.36	Insurer(s).....	13
1.37	Legal specialist	14
1.38	Limit(s) of Liability	14
1.39	Loss.....	14
1.40	Multimedia activities	15
1.41	Newsworthy event.....	15
1.42	Outsourcer	15
1.43	Personal information.....	15
1.44	Policyholder.....	15
1.45	Professional expenses	15
1.46	Regulator	15
1.47	Responsible Officer	15
1.48	Retention.....	15
1.49	Security failure	16
1.50	Settlement agreement	16
1.51	Subsidiary	16
1.52	System failure	16
1.53	Third parties.....	16
1.54	Third party data	17
	SECTION 2. Cyber Insurance Covers.....	18
2.1	Liability for data- and network security	18
2.1.1	Loss of personal data	18
2.1.2	Loss of company data	18
2.1.3	Data liability and network security.....	18
2.1.4	Outsourcing	18
2.1.5	Information holder of personal information or company data.....	18
2.1.6	Failure to notify	19
2.1.7	Multimedia liability.....	19
2.2	Damages and expenses	20
2.2.1	Urgent professional expenses	20
2.2.2	Legal services under the cyber coverages	21
2.2.3	IT services and forensic services.....	22
2.2.4	Notification Costs	23
2.2.5	Credit and ID monitoring	23
2.2.6	Recovery of data	23
2.2.7	Reputational damage restoration	24
2.2.8	Board members	25
2.2.9	Administrative obligations.....	26

2.3	Loss of profit due to network interruption.....	26
2.3.1	Cover of the loss of profit due to network interruption	26
2.3.2	Extension network interruption of a cloud provider.....	26
2.3.3	Extension network interruption of an outside service provider	26
2.3.4	Specific definitions.....	26
2.3.5	Notification	30
2.4	Cyber criminality.....	32
2.4.1	Cyber-extortion	32
2.4.2	Cyber theft.....	33
2.4.3	Telephone system hacking	33
SECTION 3. Exclusions of Cyber-guarantees		34
3.1	Anti trust law	34
3.2	Contractual liability	34
3.3	Claims and previous circumstances.....	34
3.4	Monetary value.....	34
3.5	Intellectual property.....	34
3.6	Bodily Injury and property damage.....	35
3.7	Illegally or illicitly collected data.....	35
3.8	Uninsurable loss	35
3.9	Conduct.....	35
3.10	Pollution	35
3.11	Securities Claims	36
3.12	Systems.....	36
3.13	Terrorism / War	36
3.14	Employment practices violations.....	36
SECTION 4. Claims.....		37
4.1	Notification of claims and circumstances that may lead to a claim.....	37
4.2	Circumstances.....	37
4.3	Related claims	38
4.4	Fraudulent claims	38
SECTION 5. Defence and settlement.....		39
5.1	Defence.....	39
5.2	Insurer's consent.....	39
5.3	Insured's consent	39
5.4	Subrogation and recovery	39
SECTION 6. Insured amount and waiver.....		40
6.1	Insured amount	40
6.2	Retention.....	40

SECTION 7. Optional guarantee for cyber legal protection	41
7.1 Insurer for legal protection	41
7.2 Other provisions relating to legal protection	41
7.2.1 Claim	41
7.2.2 Guarantee limit.....	42
7.2.3 Waiting period	42
7.2.4 The threshold.....	42
7.2.5 Premiums.....	42
7.2.6 Euromex commitment.....	43
7.2.7 Obligation of the insured.....	43
7.2.8 Obligation of limitation of damage	44
7.2.9 Free choice of expert lawyer	45
7.3 The insured	46
7.4 Application scope.....	46
7.5 Guarantee area	46
7.6 Guarantee table	47
7.7 General cover of legal protection	47
7.7.1 Payment of RC waiver	47
7.7.2 Advance payment in case of material damage.....	47
7.7.3 Surety bond.....	47
7.8 cover of legal cyber protection	48
7.8.1 Penal defence	48
7.8.2 Salduz assistance.....	48
7.8.3 Civil recourse for extra-contractual damage.....	49
7.8.4 Personal professional conflict	49
7.8.5 Civil defence.....	49
7.8.6 Dispute with insurer for cyber risk.....	49
7.8.7 Dispute with administrative authorities	50
7.8.8 Contractual law	50
7.9 Never guaranteed	50
SECTION 8. Common general provisions	51
8.1 Collaboration	51
8.2 Maintenance of technology	51
8.3 Sanctions.....	51
8.4 Acquisition of cover	51
8.5 Assignment	51
8.6 Duration of insurance and termination.....	52

8.7	Termination after a claim.....	52
8.8	Insolvency	52
8.9	Plurals, sections and titles.....	52
8.10	Applicable law	52
8.11	Complaints	53
8.11.1	Complaints addressed to CyberContract:	53
8.11.2	Complaints addressed to AIG Europe	53
8.11.1	Complaints addressed to Euromex	53
8.11.4	Ombudsman	53
8.12	Privacy Policy	54
8.12.1	Common provisions	54
8.12.2	Privacy policy of CyberContract:	56
8.12.3	Privacy policy of AIG Europe SA:	56
8.12.4	Privacy policy of Euromex SA:	56
8.13	Discovery Period.....	56

SECTION 1. Definitions for the Cyber-guarantees

1.1 Administrative fines

Any lawfully insurable fine and/or penalty imposed by a **regulator** to be payable by an **insured** for a breach of **data protection legislation**.

Administrative fines do not include any other type of civil or criminal fines and penalties.

1.2 Administrative investigation/regulatory investigation

Any formal or official action, investigation, inquiry or audit by a **regulator** against an **insured** once the **insured** is identified in writing by the **regulator** arising out of the use or suspected misuse of **personal information** or any aspects of the control or processing of **personal information** or delegation of data processing to an **outsource service provider** which is regulated by **data protection legislation**, but shall not include any industry-wide, non-firm specific, inquiry or action.

1.3 Annual premium

The amount indicated in the specific conditions.

1.4 Board Member, Member of the board/Family Member

Boardmember is defined as :

(i) a natural person holding an active position as a member of the management committee, director, CEO or partner of the **company**;

(ii) a member of the **family member** of a member of the management committee, a director, a partner, a partner of the **company** in office.

A **family member** within the meaning of the definition of **board member** means:

(i) dependent children or children in any form of joint parenthood;

(ii) any natural person officially residing in the same household.

1.5 Breach Notice Law

Any **data protection legislation** that creates a legal obligation to give notice in respect of an actual or potential qualifying **breach of data security**.

1.6 Breach of personal information

The unlawful disclosure or transmission of **personal information** for which the **insured** is responsible, in accordance with any applicable **data protection legislation**.

1.7 Breach of the company data

An unlawful publication or transfer of **company information** by an **insured** or a **third party**, for which the **insured** is responsible.

1.8 Breach of the data security

(i) The illegitimate access of a **third party** to the **company's computer system** or the use of access to the **company's computer system** outside the authorities given by the insured

(ii) An unauthorised publication or transfer of **personal information** or **company data** for which the **insured** is responsible.

1.9 Claim

The receipt by or service upon the **insured** of:

(i) an **enforcement notice**;

(ii) a written demand seeking a legal remedy for **loss**;

(iii) a demand or notification of civil, regulatory, administrative or criminal proceedings seeking legal remedy, compliance or other sanction; or

(iv) a written demand by a **regulator** in connection with a **regulatory investigation** (in respect of Insurance cover B (Administrative Obligations) only) These **professional expenses** will only be paid by the **insurer** to the extent that they arise after the date of notification to the **insurer** in accordance with SECTION 4 Claims.

(v) Administrative obligations

Claim shall not include any (i) **data subject access request** by a **data subject**; nor (ii) allegation brought by or on behalf of any director, partner, principal, Chief Compliance Officer, **data protection officer** or General Counsel of the **insured** unless they are a **data subject** and only in their capacity as **data subject**.

1.10 Company

The **policyholder** and each subsidiary.

1.11 Company data

(i) Any type of confidential information which is the exclusive intellectual property of a **third party**, including, but not limited to, budgets, customer lists, marketing plans and other information the disclosure of which may be of interest to a third party and which is not available to the public;

(ii) Any type of confidential or privileged information to which a third party is entitled, including, but not limited to, confidential information provided to a lawyer, accountant or other adviser in the performance of his or her professional duties and which would not otherwise be made public; or

(iii) Any type of information which has been lawfully disclosed to the **company** and which has been lawfully obtained by the **company** under conditions which include a legal obligation to treat such information as confidential or which is provided to the **company** after the signing of a written non-disclosure agreement.

(iv) **Personal information**

1.12 Company's Computer System

Information technology and communication systems, networks, services and solutions (including **computer assets**) that either (a) are part of those systems and networks, or (b) are used to provide such services and solutions that are leased, available or accessible to the **company** or that are supplied to the **company** for exclusive, secure and professional use.

1.13 Computer assets

Any item or part of the hardware, software or equipment that is or may be used to create, access, process, protect, control, store, request, display or transmit electronic **data** of any kind (including voice technology).

1.14 Control

of the securing of affairs of an entity by means of: (i) controlling of the composition of the Board of Directors of such entity; (ii) controlling more than half of the shareholder- or equity voting power at the general assembly of such entity; or (iii) holding more than half of the issued shares or equity capital of such entity.

1.15 Cyber-incident

An incident, event, **newsworthy event**, episode, circumstance or suspicion of which, upon further investigation, is reasonable to assume will become apparent that it relates to an **insured event**.

1.16 Cyber-terrorism

The premeditated use of disruptive activities against any **company's computer system, outsource service provider's** computer system or network, or the explicit threat to use such activities, with the intention to cause harm and further social, ideological, religious, political or similar objectives, or to intimidate any person(s) in furtherance of such objectives.

Under no circumstances shall **cyber terrorism** include any such activities which are part of or in support of any military action, war or warlike operation.

1.17 Damages

- (i) Any amount that an **insured** shall be legally liable to pay to a **third party** in respect of judgments or arbitral awards rendered against an **insured**;
- (ii) monies payable by an **insured** to a **third party** pursuant to a **settlement agreement** negotiated by an **insured** and which is approved by the **insurer**; including but not limited to punitive, exemplary or multiple damages, where insurable by law and ensuring the most advantageous cover.

Damages shall not mean and this policy shall not cover any: (i) non-compensatory damages (unless they are covered under (iii) above), including liquidated damages; (ii) costs and expenses of complying with any order for, grant of or agreement to provide injunctive or other non-monetary relief; (iii) costs or other amounts that the **insured** are responsible for under a merchant services agreement; or (iv) discounts, service credits, rebates, price reductions, coupons, prizes, awards or other contractual or non-contractual incentives, promotions or inducements offered to the **insured's** customers or clients

1.18 Data

Electronically stored digital or digitalised information or media.

1.19 Data protection officer

A person who is designated by the **company** as the person responsible to implement, monitor, supervise, report upon and disclose the **company's** regulatory compliance standards with respect to data collection, data processing and delegation of data processing

1.20 Data Protection Regulation/Privacy Legislation

The Privacy Act of 8 December 1992, the Act of 30 July 2018 on the protection of privacy in relation to the processing of personal data and any subsequent legislation that alters, repeals or replaces such data protection act, and all other equivalent laws and regulations relating to the regulation and enforcement of protection of **personal information** and privacy in any country.

1.21 Data Subject

Any natural person whose **personal information** has been collected or processed by or on behalf of the **company**.

Any past, present or future directors, officers or employees, past, present and future will be considered a third party for any **claim** based or arising out of a qualifying resulting from a **breach of personal information**.

1.22 Data Subject Access Request

A written request from a **data subject** to a **company** regarding the mandatory production of:

- (i) **personal information** held which identifies such individual person;
- (ii) the reason such **personal information** has been collected or processed;

- (iii) the recipients or classes of recipients to whom such **personal information** has been or may be disclosed; and
- (iv) the source of such **personal information**

1.23 Defence costs

All reasonable and necessary legal fees, costs and expenses which the **insured** incurs, with the prior written consent of the **insurer**, in relation to the investigation, response, defence, appeal and/or settlement of a **claim** or **regulatory investigation** made against the **insured**.

Defence costs shall not include any internal costs of the **insured** (e.g. wages, salaries or other remunerations).

1.24 Digital media

Any digitised content, including text, graphics, audio, and video, that can be transmitted over the internet or computer networks.

1.25 Discovery period

The extra period of time, specified in article 3.2 during which the **insured** may give the **insurer** written notice of a **claim** first made during such period of time, but only in respect of **losses** which occurred during the **policy period**.

1.26 Enforcement Notice

A notice from a **regulator** requiring the **insured** to:

- (i) confirm compliance with the applicable **data protection legislation**;
- (ii) take specific measures to comply with the applicable **data protection legislation**; or
- (iii) refrain from processing any specified **personal information** or **third party data**; within a specified time period.

1.27 Expenses for the reduction of network interruption

The reasonable and necessary costs and expenses that the **insured** incurs to reduce the duration of a **business interruption**, excluding the cost of any legal or IT consultant.

1.28 External IT specialist

The IT company designated by the **insured** after prior agreement of the **insurer** or without such prior agreement in the context of point 2.2.1 Urgent professional expenses.

1.29 Identity theft insurance (ID theft insurance)

An identify theft policy issued by the **insurer** or by another carrier with the **insurer's** prior written consent, to be offered to **data subjects** whose **personal information** has been compromised

1.30 Inception date

The date indicated in the specific conditions.

However, it can never be earlier than the date on which the respective insurers or CyberContract received the first premium paid into their respective bank accounts.

1.31 Information Commissioner, Data Protection Officer

A member of, or expert designated by the Commission for the Protection of Privacy (Belgium) or position that replaces such role under the laws and regulations relating to the regulation and enforcement of data protection and data privacy in any other jurisdiction.

1.32 Information holder

A **third party**:

- (i) to which an **insured** has provided **personal information** or **company data**; or
- (ii) who has received **personal information** or **company data** on behalf of an **insured**; including an **outsourcer**.

1.33 Insured

refers to:

- (i) The **company**;
- (ii) any natural person who is or has been a director, principal, partner or officer (including but not limited to any Chief Compliance Officer, **data protection officer** or General Counsel) of the **company** to the extent such person is acting in such capacity;
- (iii) any employee of the **company**; and
- (iv) any estates or legal representatives of any **insured** described in (i), (ii) and (iii) of this Definition to the extent that a **claim** is brought against them in respect of an act, error or omission of such **insured**.

1.34 Insured event

An matter or event triggering cover under this policy.

1.35 Insured period

The period from the **inception date** to **expiration date** as specified in the specific conditions

1.36 Insurer(s)

Unless explicitly stated otherwise in the text, the term insurer means:

Regarding the guarantees of SECTION 7 Optional guarantee for legal cyber protection: Euromex

Regarding all the other guarantees: AIG Europe SA (Belgian branch) is an insurer under Luxembourg law (RCS n° B 218806). Registered office at 35 D Avenue John F. Kennedy, L-1855 Luxembourg. AIG Europe S.A. is an insurance company approved by the Luxembourg Ministry of Finance and under the supervision of the Commissariat aux Assurances 7, boulevard Joseph II, L-1840 Luxembourg, GH Luxembourg, tel: (+352) 22 69 11 - 1, caa@caa.lu, <http://www.caa.lu/>.

AIG Europe S.A., Belgian branch, is located at Boulevard de la Plaine 11, 1050 Brussels, Belgium. RPM Brussels - VAT number: 0692.816. 659. AIG Europe S.A., Belgian branch, is registered with the National Bank of Belgium (BNB) under number 3084.

Where the text mentions the **insurers**, reference is made to both insurers jointly and to each separately.

1.37 Legal specialist

The law firm appointed by the **insured** after prior agreement by the **insurer** or without such prior agreement in the context of point 2.2.1 Urgent professional expenses

1.38 Limit(s) of Liability

The Amount(s) indicated in the specific conditions

1.39 Loss

- (i) **Compensation, defence costs, professional expenses, administrative fines;**
- (ii) **Extortion Loss**
- (iii) **Network interruption loss;**
- (iv) **Cyber theft loss.**
- (v) **loss** due to multimedia liability and **loss** due to **hacking of the telephone system**, if this option has been selected by the **insured** and as such communicated in the specific conditions by defining a specified insured amount.

Loss do not include compensation, internal or overhead costs of an **insured**, a **subcontractor** or an information holder, or time compensation of the **insured**, **subcontractor** or **information holder**, except for the provisions referred to under the cover provided for in Section 1 - Network Interruption and in point 2.1.3 - Data Liability and Network Security.

Loss shall not mean any compensation, internal or overhead expenses of any **insured**, **outsourcer** or **information holder** or the cost of their time, unless for the cover provided in Section 1 – Network Interruption and in point 2.1.3 – Data Liability and Network Security.

1.40 Multimedia activities

Relate to the publication or broadcast of **digital media content**

1.41 Newsworthy event

Actual or threatened public revelations in the media which arises directly out of an actual or potential or alleged breach of **data protection legislation** or a **breach of data security** that could bring the **company** into disrepute or tarnish its reputation and damage its goodwill towards the community of people or business. The latter includes customers, suppliers and any person with whom the **insured** habitually deals in the course of its business.

1.42 Outsourcer

A natural person or entity that collects or processes **personal information** or **company data** on behalf of the **company**, either on the basis of an express contractual agreement or on the basis of a legal obligation (including, but not limited to, web hosting, payment processing and IT-security, data collection, data processing, delegation of data processing, data storage and/or data deletion or destruction).

1.43 Personal information

All personal information concerning a **data subject** which has been lawfully collected and maintained by or on behalf of the **company**.

1.44 Policyholder

The entity specified in the specific conditions.

1.45 Professional expenses

Reasonable and necessary fees, costs and expenses for the benefit of experts engaged by the **insured** in accordance with the terms of this policy and with the prior written consent of the **insurer**, except for the provisions referred to under the cover provided for in point 2.2.1 Urgent professional expenses.

1.46 Regulator

An **information commissioner** or statutory body established pursuant to **data protection legislation** in any jurisdiction and which is authorised to enforce statutory obligations in relation to the processing or control of **personal information** (or, where relevant, **corporate information**).

1.47 Responsible Officer

Any Chief Executive Officer (CEO), Chief Financial Officer, Chief Compliance Officer, Chief Information Officer, **Data Protection Officer**, Risk Manager or General Counsel (or equivalent positions).

1.48 Retention

The Amount indicated in the specific conditions.

1.49 Security failure

Any interference or intrusion due to the failure of the security of the **company's computer system**, including that which results in or fails to mitigate any unauthorised access, unauthorised use, denial of service attack or denial of access or receipt or transmission of a 'malicious code'.

Security failure also means:

(i) Any possible interference or intrusion resulting from the physical theft of a password or network access code from:

- a. the **insured's** premises;
- b. a **company's computer system**;
- c. an officer, director or employee of an **insured**;

which represents a direct violation of the specific, written safety policy or safety procedures of the **insured**;

(ii) the disclosure of **data** due to the physical theft or loss of hardware controlled by the **insured**, or components thereof;

(iii) the disclosure of **data** by an employee of the **insured**.

1.50 Settlement agreement

Any agreement made by the **company** (with the prior written consent of the **insurer**) and a **third party** in order, to set aside permanently any potential or actual litigious matter or disagreement between the **insured** and the third **party**.

1.51 Subsidiary

Any entity in which the **insured**, directly or indirectly through one or more other entities:

- (i) determines the composition of the board of directors;
- (ii) holds more than half of the voting rights; or
- (iii) holds more than half of the issued capital or share capital.

For any **subsidiary** or **insured** of such entity, this policy covers only a **breach of data protection law** or an act, error or omission leading to a breach of data protection where the entity is a **subsidiary** of the **insured**.

1.52 System failure

An unintentional and unplanned failure of **the company's computer system**

1.53 Third parties

Any entity or natural person not **controlled** by the **insured** and which does not **control** the **insured** except: (i) the **insured**; (ii) any other entity or natural person having a financial interest or executive role in the operation of the **insured**; (iii) any person or entity who can by virtue of any legal, equitable or commercial right or interest control or influence the board of directors or the management of the **insured** or which can be influenced or controlled by the **insured** in a similar manner.

1.54 Third party data

(i) Company data

(ii) Any personal information about a natural person that has been lawfully collected and stored by or on behalf of a **third party**;

(iii) Other data of a commercial, professional or operational nature belonging to a **third party**,

and which are in the possession of the **company** by virtue of a contractual obligation between the **company** and a **third party** for the duration of the service.

SECTION 2. Cyber Insurance Covers

2.1 Liability for data- and network security

2.1.1 Loss of personal data

The insurer shall pay to or on behalf of the **insured** all **damages** and **defence costs** arising from any claim by a **data subject** or a **third party** against the **insured** in respect of an actual or alleged **breach of personal information**.

2.1.2 Loss of company data

The **insurer** shall pay to or on behalf of the **insured** all **damages** and **defence costs** arising from any claim by a **third party** against the **insured** relating to an actual or alleged **breach company data**.

2.1.3 Data liability and network security

The **insurer** shall pay to the **insured** or on his behalf all **damages** and **defence costs** arising from a claim by a **third party** against the **insured** in respect of a **security failure** in the **company's computer system**, including:

- (i) the installation of any unauthorised software, the receipt of computer code or a virus;
- (ii) blocking access by an authorised **third party** to his own **data**; unauthorised appropriation of an access code to the **company's** network;
- (iii) the destruction, alteration, disruption, corruption or deletion of **third party data** stored on any computer system;
- (iv) the physical theft or loss of **computer assets** by a **third party**;
- (v) the disclosure of **third party data** by an employee of the **company**.

2.1.4 Outsourcing

The **insurer** shall pay to or on behalf of the **company** all **damages** and **defence costs** arising from a claim by a **third party** against an **outsourcer** (if the **company** is contractually obliged to compensate them) and arising from an actual or alleged breach by the **outsourcer** with regard to the processing of **personal information and/or company data data** on behalf of the **company** (and for which the **company** is liable).

2.1.5 Information holder of personal information or company data

The **insurer** shall pay to or on behalf of the **insured** all **damages** and **defence costs** arising from a claim by a **third party** against the **insured** in respect from an actual or alleged breach of the obligations of the **information holder** in connection with the processing on behalf of the **company** of **personal information and/or company data** (for which the **company** is liable).

2.1.6 Failure to notify

The **insurer** will pay to or on behalf of any **insured** all **damages** and **defence costs** arising from any **claim** against the **insured** in respect of a failure by the **company** to notify a **data subject** and/or any **regulator** of a **breach of personal information** in accordance with the requirements of **data protection legislation**.

2.1.7 Multimedia liability

The **insurer** will pay to or on behalf of any **company** all **damages** and **defence costs** which arise out of a **claim** by a **third party** against the **company** with respect to the following alleged or actual wrongful acts, solely in the performance of **multimedia activities**:

- (i) defamation, including but not limited to libel, slander, or disparagement of trade reputation or the character of any person or organization, or infliction of emotional distress or mental anguish arising from the foregoing;
- (ii) unintentional infringement of copyright, title, slogan, trademark, trade name, trade dress, mark, service mark, service name or domain name;
- (iii) plagiarism, piracy or misappropriation or theft of ideas or information;
- (iv) invasion, infringement or interference with rights of privacy or publicity, false light, public disclosure of private facts, intrusion and commercial appropriation of name, persona or likeness;
- (v) liability resulting from the negligence of the insured in respect of any digital media content.
- (vi) the negligent correction or masking of one of the actions (i) to (v) above

2.1.7.1 Specific exclusions for multimedia liability

2.1.7.1.1 Product Descriptions

Excluded are damages resulting from, based on or attributable to the actual or presumed incorrect, inadequate or incomplete description of the price of the goods, products or services, cost guarantees, cost descriptions or price estimates established in contracts, the authenticity of the goods, products or services and non-compliance with the quality or performance standards offered by the goods or services.

This exclusion will not apply if such changes were made by a **third party** by means of an unauthorised access.

2.1.7.1.2 Financial data

Excluded is the **loss** arising-out of, based upon or attributable to errors in any financial data the **company** publishes, including, but not limited to, the **company's** annual report and annual accounts and any communications to the stock market.

This exclusion will not apply if such changes were made by a **third party** by means of an unauthorised access.

2.1.7.1.3 Software copyrights

Excluded are **damages** resulting from, based on or attributable to a breach of copyrights relating to software, source codes or software licences.

2.2 Damages and expenses

2.2.1 Urgent professional expenses

In the event of a **cyberincident** reported by the **insured** to or on behalf of the **company**, the **insurer** pays all **urgent professional expenses** relating to an actual or presumed **breach of personal information or company data**, an actual or presumed **security failure** or **system failure**.

Such **urgent professional expenses** include the use of:

- (i) an **external IT specialist** for the provision of urgent **IT and forensic** services;
- (ii) a **legal specialist** for the provision of **legal services in the context of the cyber-coverages**.

These **urgent professional expenses** will be borne by the **insurer** up to a maximum amount of 25,000 EUR without prior agreement of the **insurer**, it being understood that the **cyber incident** will be reported by telephone as soon as possible to CyberContract and consequently to the **insurer**.

No **retention** applies to the cover of **urgent professional expenses**.

If the **cyber incident** concerns an insured claim, the cover is provided according to the insurance covers and the **limit of liability** mentioned in the specific conditions.

2.2.2 Legal services under the cyber coverages

The **insurer** will pay to or on behalf of the **company** the **professional expenses** of the **legal specialist** in providing **legal services** in connection with a **breach of personal information, breach of company data, a security failure** or a **system failure**. These **legal services** include:

- (i) taking instruction regarding the factual background of the **breach of personal information, breach of corporate data, security failure** or **system failure** and co-ordinating the external **IT specialist** and/or **crisis consultants**
- (ii) advising on the requirement to notify, notifying and corresponding with any relevant **regulator**;
- (iii) advising on **data subject** notifications;
- (iv) monitoring complaints raised by **data subjects** and advising the **insured** on responding to questions raised by **data subjects**;
- (v) advising the company on the company's response to the **breach of personal information, breach of corporate data, security failure** or **system failure**.

Such **professional expenses** will only be paid by the **insurer** to the extent that they are incurred after the moment of notification to the insurer in accordance with SECTION 4 Claims or after the date of notification in accordance with the insurance cover provided 2.2.1 Urgent professional expenses.

2.2.3 IT services and forensic services

The insurer will pay to or on behalf of the company all professional expenses of the external IT specialist in connection with an **insured event**, including the following services:

- (i) investigating whether a **security failure** or **system failure** has occurred, how it occurred and whether it is still occurring; and
- ii) identify whether such a **security failure** or **system failure** has resulted in a **breach of personal information** or a **breach of corporate data** and establishing the extent of the **personal information** or **company data** that may have been compromised;
- (iii) containing a **security failure or system failure**, including containing a denial of service attack;
- (iv) resolving a denial of service attack and removing any malicious software, computer code or virus from the **company's computer system** and/or identifying any compromised **data**; and
- (v) examining the **company's computer system** to determine the remediation actions that are required in order to comply with an **enforcement notice**;
- (vi) verifying whether a **breach of data protection** has occurred/is occurring, and
- (vii) determining the cause of the breach, and
- (viii) make recommendations to avoid or reduce the risk of such breach;
- (ix) giving the necessary advice and provide the necessary services and benefits to minimise the adverse and negative consequences of the **cyber incident** to the extend possible;
- (x) to provide the necessary advice and services to restore the **company's IT system** to the same or an equivalent operational state as before the **cyber incident** as soon as reasonably possible;
- (xi) to provide the necessary advice and services to make the **company's** data available to the **insured** via the **company's IT system** so that it is complete, intact, legible and ready for use again.

Such **professional expenses** will only be paid by the **insurer** to the extent that they are incurred after the moment of notification to the **insurer** in accordance with SECTION 4 Claims, or after the moment of notification in accordance with the insurance cover Section 2.2.1 Urgent professional expenses.

2.2.4 Notification Costs

The **insurer** will pay to or on behalf of the **insured** all **professional expenses** (not exceeding the **limit(s) of liability** stipulated in the specific conditions), including costs associated with setting up call centres in relation to the investigation, collection of information, preparation for and notification to **data subjects** and/or any relevant **regulator** of any actual or suspected **breach of data protection, breach of personal information, breach of company data** or breach of **data protection regulation**.

2.2.5 Credit and ID monitoring

Following notification to **data subjects** under the insurance cover referred 2.2.4 Notification Costs, **the insurer** will pay to or on behalf of the **company**:

- (i) all **professional expenses** for credit or identity theft monitoring services to identify possible misuse of any **personal information** as a result of an actual or suspected **breach of personal information**;
- (ii) the reasonable and necessary premium for any **ID theft insurance**.

Such fees, costs and expenses (including premium) will only be paid by the **insurer** for the **data subjects** who within 90 days following receipt of the notification in accordance with insurance cover referred 2.2.4 Notification Costs and this insurance cover 2.2.5 Credit and ID monitoring, request and/or activate the credit and identity theft monitoring services and **ID insurance**.

Credit and identity monitoring will only be provided to **each data subject** for a period of two years from the date of activation.

2.2.6 Recovery of data

The **insurer** will pay to the **company** or on its behalf all **professional expenses** (not exceeding the **limit of liability** stipulated in the specific conditions) in order to:

- (i) determine whether or not **data**, including **data** held by the **company** on behalf of a **third party**, can be restored, recovered or recreated; and
- (ii) recreate or recover **data** held by the **company** including **data** held on behalf of a **third party**, when backup systems are unable to recover these **data** or when these **data** are damaged or lost or are not machine legible.
- (iii) reload and re-customise licensed software operated by the **company** at the time of the **security failure or system failure**, where the licensed software is not -readable.

2.2.7 Reputational damage restoration

2.2.7.1 *Company reputational damage restoration*

The **insurer** will pay to or on behalf of the **company** all **professional expenses** (not exceeding the limit of liability stipulated in the specific conditions) for advice and support from independent advisors (including, but not limited to, legal advice concerning media strategy, crisis consulting and independent public relations services) responsible for the development of actions reasonably necessary to prevent or mitigate the potentially adverse effect of a **newsworthy event**, including the design and implementation of a communications strategy.

Such **professional expenses** may only be incurred from the date of notification to the **insurer** in accordance with SECTION 4 Claims until the 185th day following such notification.

2.2.7.2 *Personal reputational damage restoration*

The **Insurer** will pay to or on behalf of the directors, partners, associates, chief compliance officer, **data protection officer** or legal representative of a **company** all **professional expenses** (not exceeding the limit of liability stipulated in the specific conditions) for advice and support by an independent public relations consultant, in order to limit or prevent damage to their individual (personal and professional) reputation due to an actual or alleged **breach of data protection** or breach of **data protection regulation**.

Such **professional expenses** may only be incurred from the date of notification to the **insurer** in accordance with SECTION 4 Claims until the 185th day following such notification.

2.2.8 Board members

If a **board member** or **family member** is a victim of one of the following **cyber incidents**:

(i) He or she is the subject of defamatory messages on social media, web pages or other digital forums (such as, but not limited to, hate sites, harassment sites, voting sites, blogs, chatrooms, e-mails, mobile phones, text messages...).

(ii) the unjustly damaging their reputation via social media, web pages or other digital forums (such as, but not limited to, hate sites, harassment sites, voting sites, blogs, chatrooms, e-mails, mobile phones, text messages...).

(iii) Sexual grooming; the online process by which an adult approaches and manipulates a child/adolescent for the purpose of sexual contact and sexual acts (e.g. via webcam, chat messages, e-mails...), including the creation and distribution of photographs over the Internet.

(iv) Sextortion; any sexual blackmail, including the creation and distribution of photographs on the Internet.

(v) Cyber-bullying and cyber-stalking; the repeated harassment, abuse, insults, humiliation or threats over the Internet or via other electronic means of communication (e.g. via mobile phone, SMS, e-mail or other Internet technology).

(vi) Any unauthorised disclosure or transfer of **their personal information** by a **third party** in violation of the **data protection regulation** and any related misuse of their **personal information**

The **insurer** will pay **professional expenses** up to a maximum of € 3.000 incurred in connection with the following services:

(i) restoration of reputation, including, but not limited to, the deletion of the incriminating messages or the publication of these messages with new content, etc. (**IT services**)

(ii) Computer forensics concerning the identification of the author, including, but not limited to, the discovery of the author's IP address, etc. (**IT services**)

(iii) Assistance in formulating a complaint and claiming compensation, including but not limited to: a formal notice from the author, a formal notice from the website... etc. (**legal services**)

Such **professional expenses** will only be paid by the **insurer** to the extent that they arise after the date of notification to the **insurer** in accordance with SECTION 4 Claims.

2.2.9 Administrative obligations

2.2.9.1 *Administrative investigations*

The **insurer** will pay to or on behalf of the **insured** all **professional expenses** (not exceeding the limit of liability stipulated in the specific conditions) incurred for legal advice and in respect of a **regulatory investigation**.

2.2.9.2 *Administrative fines*

The **insurer** will pay to or on behalf of the **insured** all **administrative fines** (not exceeding the limit of liability stipulated in the specific conditions) which are legally insurable in the most favourable jurisdiction, , and that the **insured** is legally liable to pay upon the conclusion of a **regulatory investigation** by a regulator for an infringement of the **data protection legislation**.

2.3 Loss of profit due to network interruption

2.3.1 Cover of the loss of profit due to network interruption

The **insurer** will pay for any **network loss** (not exceeding the **limit of liability** stipulated in the specific conditions) in respect of a **network interruption** incurred by the **insured** which exceeds the **waiting period** and which is the exclusive result of a **security failure** or **system failure**.

2.3.2 Extension network interruption of a cloud provider

The cover **network interruption** is extended to **network loss** following a **network interruption of a cloud provider** incurred by the **company** which exceeds the **waiting period** and this during the **network interruption of a cloud provider** (but limited to a maximum of 120 days from the expiry of the **waiting period**) and subsequently a maximum period of 90 days after the resolution of the **network interruption of a cloud provider**.

2.3.3 Extension network interruption of an outside service provider

The cover **network interruption** is extended to **network loss** following a **network interruption** of an **outside service providers' computer system** incurred by the **company** which exceeds the **waiting period** and this during the **network interruption of an outside service providers' computer system** (limited to a maximum of 120 days from the expiry of the **waiting period**) and subsequently for a maximum period of 90 days after the resolution of the **network interruption of an outside service providers computer system**.

2.3.4 Specific definitions

2.3.4.1 *Network interruption*

(i) Any suspension, including degradation, of the service provided by the **company's computer system** solely caused by a **security failure** or **system failure**

(ii) The inability of the **insured** to access **data** due to such data being deleted, damaged, corrupted, altered or lost, but only where such deletion, damage, corruption, alteration or loss is solely cause by a **security failure** or **system failure**.

2.3.4.2 Security defect/security failure

Refers to any interference or intrusion due to the failure of security of the **company's computer system**, including that which results in or fails to mitigate any, unauthorised access, unauthorised use, "denial of service" attack or denial of access or receipt or transmission of a "malicious code".

In addition to the above, a **security failure** also means:

(i) any possible interference or intrusion resulting from the physical theft of a password or network access code from:

- a. the **insured's** premises,
- b. a **company's computer system** or,
- c. an officer, director, member of management or employee of an **insured**,

which represents a direct violation of the specific written safety policy or safety procedures of the **insured**;

(ii) the disclosure of **data** due to the physical theft or loss of hardware controlled by the **insured**, or components thereof;

(iii) disclosure of **data** by an employee of the **insured**.

2.3.4.3 Cloud service

Any "on-demand" access to hosted computer infrastructure or computing platforms, including cloud computing services provided on an "Infrastructure as a Service (IaaS)" or "Platform as a Service (PaaS)" model, provided by any person or entity not owned, operated or controlled by an **insured** for a fee.

2.3.4.4 Network interruption of a cloud provider

(i) the suspension of the services of the **cloud provider** used by the **company** caused solely by a **cloud service failure**; or

(ii) the inability of the company to access data due to such data being deleted, damaged, corrupted, altered or lost, but only where such deletion, damage, corruption, alteration or loss is solely as a result of a.

2.3.4.5 Cloud service failure

An unintended and unplanned failure of a **cloud service** to give an **insured** to access IT-modalities defined in the service agreement and which is caused by:

(i) the failure of any computer or telecommunications hardware under control of the **cloud service**

(ii) a interruption or intrusion in the **cloud services' computer system** that, in including but not limited to, results in, or cannot limit the consequences of, an unauthorised access, an unauthorised use, a denial of service attack or the reception or sending of malicious code or a virus.

(iii) insolvency of the cloud service

(iv) a legal, regulatory or judicial order which interrupts the cloud service.

2.3.4.6 Cloud provider's computer system

Any computer, hardware, software, or any components thereof that are linked together through a network of two or more devices accessible through the Internet or internal network or that are connected through data storage or other devices that are owned, operated, controlled or leased by a **cloud service**.

2.3.4.7 Outsource service provider (OSP)

A natural person or entity that collects or processes **personal- or company data** on behalf of the **company**, either on the basis of an express contractual agreement or on the basis of a legal obligation (including, but not limited to, web hosting, payment processing and IT security, data collection, data processing, delegation of data processing, data storage and/or data deletion or destruction).

2.3.4.8 Network interruption of an outside service provider's computer system means:

(i) the suspension, including degradation, of the service provided by an **outside service provider** used by the **company**, caused solely by a **OSP failure** or

(ii) the inability of the **company** to access the **data** due to such **data** being deleted, damaged, corrupted, altered or lost, but only where such deletion, damage, corruption, alteration or loss is solely caused by **OSP failure**.

2.3.4.9 *OSP failure*

Includes:

2.3.4.9.1 *OSP security failure*

(i) an intrusion or unauthorised access (including unauthorised access by a person using authorised access), in the **outside service provider's computer system** which, including, but not limited to, results in or cannot limit the consequences of unauthorised access, unauthorised use, denial of service attack or unauthorised reception or sending of malicious code or a virus.

(ii) A loss of **data** provided by the **company** to an **outside service provider**, resulting from the physical theft or loss of hardware under the control of the **outside service provider**.

2.3.4.9.2 *OSP system failure*

Any unintentional and unplanned failure of an **outside service provider's computer system** such that the **outside service provider** is unable to provide to the **company** the services described in a vendor agreement.

2.3.4.10 *Outside service provider's computer system*

Any computer, hardware, software, or parts thereof, which are interconnected through a network of two or more devices, accessible through the Internet or the internal network, or which are connected through the storage of data or other devices which are the property of, used by, controlled by or rented by an **outside service provider**.

2.3.4.11 *Network loss*

(i) A reduction in the net operational profit that the **company** would have been earned or incurred had **network interruption** not occurred.

(ii) A reduction in profit due to a contractual reduction in payments for services or service credits on at the expense of the **insured**.

(iii) Contractual penalties insofar as they are not of a punitive nature, but are a reflection of the actual evaluated damage.

(iv) The expenses of the **insured**, including salaries, necessary to ensure the continuation of the business as usual of the **insured**.

(vi) **Expenses for the reduction of network interruption**

2.3.4.12 *System failure*

An unintentional and unplanned failure a computer system

2.3.4.13 *Waiting period*

Refers to the number of hours determined in the specific conditions commencing at the beginning of a **network interruption** that must pass before **network loss** can be incurred .

2.3.5 Notification

In addition to the requirements to give notice to the **insurer**, the **company** must also:

- (i) complete and sign a written, detailed and affirmed proof of loss within one hundred and eighty (180) days after the resolution of the **material interruption** (unless this period is otherwise extended in writing by the **insurer**) which will include a full description of the **network interruption costs** or **network loss** and the circumstances of such **network interruption costs** or **network loss**, a detailed calculation of any **network loss**; and all underlying documents and materials that reasonably relate to or form a part of the basis of the proof of the **material interruption**;
- (ii) upon the **insurer's** request promptly respond to requests for information.

All adjusted **claims** are due and payable forty five (45) days after:

1. the presentation of the satisfactory written proof of **network loss** and **network interruption costs** as provided for in (i) and (ii) above; and
2. the subsequent written acceptance thereof by the **insurer**.

2.3.6 Appraisal

If the **company** and the **insurer** disagree on the extent of **network loss** or **network interruption costs**, either may make a written demand for an appraisal of such **network loss** or **network interruption costs**. If such demand is made, each party will select a competent and impartial appraiser. The appraisers will then jointly select an expert who has not less than ten (10) years' standing and who is a partner in a major international accounting firm, experienced in assessing loss of this nature. Each appraiser will separately state the extent of **network loss** or **network interruption costs**. If they fail to agree, they will submit their differences to the expert. Any decision by the expert will be final and binding.

The **company** and the **insurer** will (i) pay their own costs, including the costs of their respective chosen appraiser and (ii) bear the expenses of the expert equally. Any evaluation of the **network loss** will be calculated according to all provisions, conditions and exclusions of this policy.

2.3.7 Specific exclusions of profit loss due to network interruption

This coverage section shall not cover **network loss** arising out of, based on or attributable to any of the following:

2.3.7.1 Costs of proof of damage

The costs and expenses of establishing or proving incurred damage suffered by the **company** under this coverage section, such as your auditor's fees, including but not limited to the costs associated with preparing proof of loss, shall be the responsibility of the **company** and are not covered under this policy.

This exclusion does not apply to the reasonable expenses of the **company's** accountants or external accountants in attending meetings and interviews and in providing information at the **insurer's** request.

2.3.7.2 Administrative service or local authority

Any seizure, confiscation, nationalization or destruction of a **company's computer system** by order of any government entity or public authority, except where this occurs as a result of an **regulatory investigation**.

2.3.7.3 Interruptions

Network- or system interruptions caused by a loss of communication with the computer system of a **third party**, making it impossible for the **insured** to communicate with these systems;

2.3.7.4 Legal costs

Legal costs or expenses of any kind;

2.3.7.5 Betterment

Any updating, upgrading, enhancing or replacing any **company's computer system** to a level beyond that which existed prior to the occurrence of a **network loss** with a system that provides superior performance to that which existed prior to the **damage caused by a network disruption**;

2.3.7.6 Unfavourable market conditions

Unfavourable market conditions; a change in the market situation that has a negative impact on the company results of the **company**.

2.3.7.7 Pre-existing software and infrastructure problems

The removal of software program errors or vulnerabilities that already existed prior to a **network interruption**;

2.3.7.8 Specific exclusion of Interruption of activity in a cloud service:

Not covered are the losses that would have been excluded if the **cloud service** had the status of an **insured**, with the exception of the cover "insolvency of the **cloud service**".

2.3.7.9 specific exclusion of Interruption of activity by a sub-contractor:

Not covered are the losses that would have been excluded if the **subcontractor** had the status of insured.

2.4 Cyber criminality

2.4.1 Cyber-extortion

The **insurer** will pay to or on behalf of the **insured** all **extortion loss** (not exceeding the limit of liability provided for in the specific conditions) which the **insured** incurred as a result of an **extortion threat** alone.

2.4.1.1 Definitions

2.4.1.1.1 Extortion threat

Any threat or connected series of threats, communicated to the **insured**, to cause a **security threat** to the **company**.

2.4.1.1.2 Extortion adviser

The person or entity appointed by the **insurer** to manage an **extortion**.

2.4.1.1.3 Security threat

Any threat to the **company's computer system** that may result in an actual or alleged **breach of data protection**, that causes or might cause financial harm to the **insured**.

2.4.1.1.4 Extortion loss

(i) Monies paid by an **insured** with the **insurer's** prior written consent to prevent or end an **extortion threat** in case the latter is made for the purpose of demanding monies or could cause financial or reputational damage to the **company**;

(ii) **Professional expenses** for independent advisers to an investigation to determine the cause of an **extortion threat** and/or help resolve the an **extortion threat**.

2.4.1.2 Specific conditions

In case of **extortion threat**, the **insured** will immediately inform **CyberContract** by contacting the **hotline** and the **insurer** will then appoint the **extortion adviser**.

The **insured** will immediately provide all information and assistance to the **extortion adviser**.

The **insured** shall use its best efforts at all times to ensure that knowledge regarding the existence of the insurance for **extortion loss** afforded by this policy is kept confidential. If the existence of insurance for **extortion loss** provided by this policy enters into the public domain or is revealed to a person presenting a **security threat** through no fault of the **insurer**, the **insurer** may terminate the insurance provided by this policy for **extortion loss** with immediate effect from the moment this knowledge enters into the public domain or is revealed to any person presenting a **security threat**.

The **insured** shall allow the **insurer** (or the **insurer's** nominated representatives) to notify the police or other responsible law enforcement authorities of any **extortion threat**.

2.4.1.3 Government entity or public authority exclusion

Excluded is any **extortion loss** arising out of, based upon or attributable to any **extortion threat** made by any government entity, public authority or local authority.

2.4.2 Cyber theft

The **insurer** shall pay the **insured** (without exceeding the limit of liability stipulated in the specific conditions) for all **loss** incurred by the **insured** as a result of a **cyber theft**.

2.4.2.1 Definition of cyber theft

- (i) Loss of money, negotiable instruments due to an unauthorised transfer;
- (ii) Loss of tangible goods due to an unauthorised delivery;
resulting from an unauthorised access to the **insured's** computer system by a **third party**.

2.4.3 Telephone system hacking

The **insurer** shall pay the **company**, any phone call expenses, to the exclusion of any other damage, for which the **company** is responsible as a result of unauthorised access and use of the **telephone system** of the **company**.

This cover also applies to new telephone systems put into service by the **insured** after the start of the policy, provided that they have at least the same level of security as the replaced systems.

2.4.3.1 Definition of the telephone system

A private branch exchange (PBX) or electronic key system, with or without peripherals such as voicemail, answering machines and automated calling systems, which are wholly owned, operated, managed, controlled or leased by the **insured**.

SECTION 3. Exclusions of Cyber-guarantees

The **insurer** shall not be liable for damage resulting from, based on or attributable to:

3.1 Anti trust law

An actual or alleged antitrust violation, restraint of trade or unfair competition of anti trust law and legislation concerning trade restrictions and unfair competition.

3.2 Contractual liability

Any warranty, guarantee, contract term or liability assumed or accepted by an **insured** under any contract or agreement (including, but not limited to, service credits, discounts, price reductions, vouchers, prizes, awards or other non-contractual incentives, promotions or stimuli offered by the **insured** to its customers), except to the extent such liability would have attached to the **insured** in the absence of such contract or agreement;

This exclusion shall not apply to the cover provided in Section 1 Network Interruption; in addition, claims by a **third party** against the **insured** are covered, to the extent that they are claims relating to a loss actually suffered as a result of a cyberincident due to a **security failure**.

3.3 Claims and previous circumstances

Any circumstance that as of the **inception date** of this policy may reasonably have been expected by any **insured** to give rise to a **loss** or **claim**; or any circumstance, **claim** or **insured event** of which notice has been given under any policy of which this policy is a renewal or replacement or which it may succeed in time.

3.4 Monetary value

A monetary loss or monetary liability, loss of money or securities, the monetary value of an electronic funds transfer or transaction by or on behalf of the **insured** that is lost, diminished or damaged in the course of a transfer from, to or between accounts.

However, this exclusion will not apply when such monetary loss or monetary liability is due to a **security failure**;

3.5 Intellectual property

(i) Any infringement of patents or misappropriation of trade secrets or loss of the rights to secure registration of patents due to unauthorised disclosure.

This exclusion shall not apply to a **claim** against an **insured** based on loss of **company data** and **multimedia activities**;

(ii) Any actual or alleged obligation to make licensing fee or royalty payments.

3.6 Bodily Injury and property damage

(i) Any physical injury, sickness, disease or death; and if arising out of the foregoing nervous shock, emotional distress, mental anguish or mental injury, with the exclusion of psychological suffering or mental trauma resulting from the violation by the **company** of the **data protection regulation**.

(ii) Loss or destruction of tangible property, other than **data**, or the loss of their use.

(iii) Fire, smoke, explosion, lightning, wind, water, flood, earthquake, volcanic eruption, tidal wave, landslide, hail, act of God or any other physical event, however caused;

3.7 Illegally or illicitly collected data

Illegal or unlawful collection of **data** from a **third party** by the **company**.

This exclusion does not apply to acts committed by employees of the **insured** without the knowledge, approval or cooperation of the directors, partners, associates, compliance officer, **data protection officer** or legal representative of the **company**;

3.8 Uninsurable loss

Any matters which the **insurer** is prohibited from paying by the law of this policy or the jurisdiction where a **claim** is made or where an **insured event** first arises.

3.9 Conduct

(i) Any wilful disregard or non-compliance with a ruling, direction or injunction by a court, tribunal, arbitrator or a **regulator** within the jurisdiction;

(ii) any intentional criminal breach of law or regulation; or

(iii) any deliberate, intentional or reckless act by any **insured**;
if committed by the **company's**:

a. directors, principals, partners or **data protection officer** whether acting on their own or in collusion with others; or

b. employees acting in collusion with any of the **company's** directors, principals, partners or **data protection officer**.

3.10 Pollution

Any impact on air, soil or water resulting from the discharge, dispersal, seepage, release or escape of solid, liquid, gaseous, biological, radioactive or thermal irritant or contaminant, whether natural or unnatural, including smoke, vapour, soot, fibres, germs, moulds, viruses, fumes, acids, alkalis, chemicals, waste and other toxic or hazardous substances, sound, noise, smell, vibrations, waves or changes in temperature;

3.11 Securities Claims

Any actual or alleged violation of any law, rule or regulation (whether statutory or common law) relating to the ownership, purchase, sale or offer of, or solicitation for an offer to purchase or sell securities.

3.12 Systems

(i) Electrical or mechanical failure of infrastructure, with the exception of a computer system, whether or not under the control of the **insured**, including a power interruption, surge, brownout or blackout.

(ii) Failure of telephone lines, data transmission lines or other telecommunications or networking infrastructure not under the control of an **insured**.

However, this exclusion does not apply to: a **security failure**; a **system failure**; a failure to protect **personal information or company data**; a breach of any **data protection regulation** which results in a **claim** caused by such failure for telephone lines, data transmission lines or other infrastructure comprising or supporting the Internet.

(iii) Satellite failure;

3.13 Terrorism / War

Strikes or similar labour action, war, invasion, act of a foreign enemy, hostilities or warlike operations (whether declared or not), civil war, mutiny, civil commotion assuming the proportions of or amounting to a popular uprising, military rising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against these actions. This exclusion does not apply to actual, alleged or threatened **cyber-terrorism**.

3.14 Employment practices violations

Disputes related to employment practices such as wrongful dismissal, discharge or termination of a contract, discrimination, harassment, retaliation or other employment practices related claims, unless covered under **breach of personal information**.

SECTION 4. Claims

4.1 Notification of claims and circumstances that may lead to a claim

This policy affords covers solely with respect to:

- (i) **claims** which are first made against the **insured** during the **policy period**; or during the **discovery period**, if applicable, and
- (ii) **insured events** which occur during the **policy period**,
- (iii) and that the **insured** communicates in writing to the **insurers**, or in any equivalent manner whatsoever to CyberContract, as soon as practicable and in any case during the **policy period** or during the **discovery period**, if applicable.

4.2 Circumstances

If, during the **policy period**, any **insured** becomes aware of a fact, circumstance, breach of data protection, breach of **data protection regulation**, a **newsworthy event**, **extortion**, **cyber-theft** or **network interruption** that an informed person operating within the same type of business as the **company** would reasonably believe is likely to give rise at a later date to a **claim**, the **insured** shall promptly inform the **insurer** about those circumstances. Such notification must be presented in chronological order and must detail the facts or matters which have or may give rise to a **claim** which should include at a minimum the following information:

- the nature and circumstances of the facts;
- the alleged, supposed or potential breach;
- the date, time and place of the alleged, supposed and potential breach;
- the identity of the potential claimants and all other potentially involved persons and/or entities;
- an estimate of possible loss;
- the potential consequences

All notifications regarding **claims**, circumstances, **breach of data protection**, breach of **data protection regulations**, **newsworthy events**, **extortion**, **cyber theft** or **network interruptions** must be made through the following channels:

(i) by telephone, by contacting CyberContract

(ii) in writing, by contacting CyberContract or the **insurer** by e-mail, fax or mail or by telephone at the address of:

CyberContract SCRL

Tel. Claims: 0800 260 21

AIG Europe SA (Belgian branch)

Prins Boudewijnlaan 7D 0101

Tel. Contact : 03 369 09 68

Boulevard de la Plaine 11

2550 Kontich

1050 Bruxelles

info@cybercontract.eu

4.3 Related claims

Upon notification of a **claim**, circumstance, **breach of data protection, breach of data protection regulation, newsworthy events, extortion, cyber theft or network interruption** or other **insured event** to the **insurer** in accordance with the terms and conditions of this policy, will result in in this case too:

- (i) each subsequent **claim**, circumstance, **breach of data protection, breach of the data protection regulation, newsworthy events, extortion, cyber theft or network interruption** or other **insured event** alleging, arising out of, based upon or attributable to the facts alleged in that previously notified **claim**, circumstance, **breach of data protection, breach of the data protection regulation, newsworthy events, extortion, cyber theft or network interruption**; and
- (ii) any subsequent **claim**, circumstance, **breach of data protection, breach of violation of the data protection regulations, newsworthy event, extortion, cyber theft or network interruption** or **insured event** that claims identical or related to the damage that was reported in that previous **claim**, circumstances, **breach of data protection, breach of data protection regulations law , newsworthy events, extortion, cyber theft or network interruption**

shall be considered made against the **insured** and reported to the **insurer** at the time notice was first given

Any **claim**, circumstance, **breach of data protection, breach of data protection regulation, newsworthy events, extortion, cyber theft or network interruption** or other **insured event** arising out of, based upon or attributable to:

- (i) single cause; or
- (ii) a single **loss**; or
- (iii) a series of continuous, repeated or related **losses**;

is considered for the purposes of this policy to be a single **claim** for compensation, circumstance, **breach of data protection, breach of the data protection regulation, newsworthy event, extortion, cyber theft or network interruption**.

4.4 Fraudulent claims

If any **insured** shall give any notice or **claim** cover for any **loss** under this policy knowing such notice or **claim** to be false or fraudulent as regards amounts or otherwise, such **loss** shall be excluded from cover under the policy, and the **insurer** shall have the right, in its sole and absolute discretion, to avoid its obligations under or void this policy in its entirety, and in such case, all cover for **loss** under the policy shall be forfeited and all premium deemed fully earned and non-refundable

SECTION 5. Defence and settlement

5.1 Defence

The **insured** must render all reasonable assistance to the **insurer** and take all reasonable measures to mitigate or avoid the **loss** or to determine the **insurer's** liability under the policy.

5.2 Insurer's consent

As a condition precedent to cover under this policy, no **insured** shall admit or assume any liability, enter into any **settlement agreement**, consent to any judgment, or incur any **defence costs** or **professional fees** without the prior written consent of the insurer.

Only those settlements, judgments and defence costs or **professional fees** consented to by the **insurer**, and judgments resulting from **claims** defended in accordance with this policy, shall be recoverable as **loss** under this policy. The **insurer's** consent shall not be unreasonably withheld, provided that the **insurer** shall be entitled to exercise all of its rights under the policy. Compliance with a **breach notice law** will not be considered as an admission of liability for the purposes of this clause.

5.3 Insured's consent

The **insurer** may make any settlement of any **claim** or **insured event** it deems expedient with respect to any **insured**, subject to such **insured's** written consent (which shall not be unreasonably withheld or denied). If any **insured** withholds consent to such settlement, the **insurer's** liability for all **loss** on account of such **claim** or **insured event** shall not exceed the amount for which the **insurer** could have settled such **claim** or **insured event**, plus **defence costs** incurred as of the date such settlement was proposed in writing by the **Insurer**, less coinsurance (if any) and the applicable **retention**.

5.4 Subrogation and recovery

If the **insurer** makes any payment under this policy, it shall be subrogated to the extent of such payment to all of the **insured's** rights of recovery and shall be entitled to pursue and enforce such rights in the **insured's** name, even if the **insured** is compensated for such **loss**.

Subrogation against employees (including directors, officers, partners or principals) of the **insured** shall be limited to cases where such employees have been found guilty of an intentional, fraudulent or criminal act by any court or government entity.

The **insured** shall provide the **insurer** with all reasonable assistance and shall do everything that may be necessary to secure any rights including the execution of documents necessary for the **insurer** to bring suit in the **insured's** name. Any amount recovered in excess of the **insurer's** total payment shall be restored to the **insured** less the recovery cost.

SECTION 6. Insured amount and waiver

6.1 Insured amount

The total amount payable by the **insurer** under this policy shall in principle not exceed the **limit of liability**. Sub-limits of Liability, Extensions and **professional fees** and **defence costs** are part of that amount and are not payable in addition to the **limit of liability**.

If the **limit of liability** is exhausted by payment of **loss**, then the **limit of Liability** will be increased, but solely for **defence costs**, salvage costs and statutory interest incurred by the **insured** in accordance with article 106 and 146 of the Belgian Law of 4 April 2014 on Insurances. Such increase will be limited to the amounts mentioned in article 4 and article 6 ter of the Royal Decree of 24 December 1992 on the execution of the law of 25 June 1992 on non marine insurance contracts or any other decree that will be enacted to execute the law of 4 April 2014 on insurances or any other legislation/regulation.

The inclusion of more than one **insured** under this policy does not operate to increase the total amount payable by the **insurer** under this policy.

In the event that another insurance is provided by the **insurer** or any member company or affiliate of the **insurer**, then the maximum amount payable by the **insurer** under all such policies shall not exceed the Limit of Liability of that policy referred to above which has the highest applicable Limit of Liability. Nothing contained herein shall be construed to increase the **limit of liability** of this policy. To the extent that another insurance policy imposes upon the **insurer** a duty to defend a claim, defence costs arising out of such a claim shall not be covered under this policy.

6.2 Retention

With respect to all **claims** or **breaches of data protection, breaches of the data protection regulation, network interruption, extortion** or **cyber theft**, the **insurer** will only pay the amount of the **damage** that exceeds the **retention** referred to in the specific conditions.

The amount of the **retention** is borne by the **company** and remains uninsured.

A single **retention** shall apply to **loss** arising from **claims** or **breaches of data protection, breaches of the data protection regulation, network interruption, extortion** or **cyber theft** or other **insured events** which are considered related **claims** or other **insured events** pursuant to 5.3 "Related Claims or Insured Events".

In the event that a **claim, breach of data protection, breach of the data protection regulation, network interruption, extortion** or **cyber theft** triggers more than one of the **retention** amounts, then, as to that **claim** or **breach of data protection, breach of the data protection regulation, network interruption, extortion** or **cyber theft** or other **insured event** the highest of such **retention** amounts shall be deemed the **retention** applicable to **loss damages** (to which the **retention** applies under the provisions of this policy) arising from such **claim** or **breach of data protection, breach of the data protection regulation, network interruption, extortion** or **cyber theft** .

SECTION 7. Optional guarantee for cyber legal protection

7.1 Insurer for legal protection

Euromex NV, Generaal Lemanstraat 82-92, B-2600 Berchem, insurance company authorised under code no. 00463 to practise branch 17 Legal protection (Royal Decree of 4 July 1979 - MB of 14 July 1979, RPM Antwerp, VAT BE 0.400.048.883.

CyberContract acts as an authorised intermediary and can grant, modify or terminate the guarantee on behalf of Euromex, and also collect the premiums on behalf of Euromex.

7.2 Other provisions relating to legal protection

If the other provisions of this optional guarantee deviate from the general terms and conditions, the other provisions shall prevail.

7.2. 1 Claim

An event or circumstance for which one or more **insured** may call upon the services and/or financial intervention of Euromex. A claim occurs when you objectively know or need to know that you are in a conflict situation and that you can assert rights or claims as a claimant or defendant.

This is not necessarily the time when the **third party** takes action.

In a situation of conflict with an authority that imposes sanctions, the claim relates to the application of all guarantees at the time of the alleged offence(s).

In a situation of conflict with an administrative authority, the claim arises at the latest when you have been able to gain knowledge of the decision you wish to contest. It must be a circumstance, condition or action that commenced while the contract was in force.

If Euromex can prove that you knew or should reasonably have known of the conflict situation before entering into the contract, no cover will be provided.

Cover is available for claims which occur during the term of the contract and which arise after the start of the contract and after the end of the waiting period specified in the Special Conditions, even if they are reported after the end of the contract.

7.2.2 Guarantee limit

The maximum financial intervention per claim, regardless of the number of **insured**.

This limit is indicated in the table of cover per guarantee.

If several coverages apply in a conflict situation, the maximum financial intervention is that of the coverage with the highest limit.

If several **insured** request assistance and the guarantee is insufficient, priority is given first to the **insured**.

Priority is also given to persons who live with the **insured** in a family relationship.

Only then is it granted on an equal footing with the other **insured**.

The maximum intervention for facts causing identical damage with a causal link and occurring within 30 days, involving several **insured** with different Euromex contracts, is equal to five times the highest amount provided for such a claim. An event or circumstance involving one or more **insured**

7.2.3 Waiting period

The period during which you must be insured before you can benefit from a guarantee.

This period begins on the date the guarantee begins, when the contract is extended or immediately after the end of the suspension of the contract. The waiting period is indicated per guarantee in the Table of guarantees.

If a waiting period has already elapsed for identical cover with a previous **insurer** and Euromex cover follows, without interruption, on this previous contract, the waiting period will not be applied.

7.2.4 The threshold

For certain guarantees, a threshold applies. The applicable threshold is indicated in the guarantee table.

This means that you cannot get a refund from Euromex for the **insured** costs if your initial claim or that of the **third party** is below the threshold amount.

(*) For "Civil Protection" cover, the threshold is equal to the **waiver** provided for in your civil liability policy.

7.2.5 Premiums

The premium, including taxes and contributions, is payable on the due date.

Euromex may change the rate. CyberContract sends you a notice of the due date for payment.

If you do not pay, CyberContract will send you a reminder.

If you still do not pay, CyberContract will send you a reminder by registered letter.

If the premium is not paid within 30 days following the day following the service or the day following the delivery of the registered letter, your policy will be cancelled.

You are no longer insured from the day following the expiry of the above-mentioned thirty-day period.

7.2.6 Euromex commitment

In the contract, Euromex undertakes to provide services and to bear the costs enabling you to assert your rights in an amicable, judicial, extrajudicial or administrative settlement.

In the event of a claim, Euromex gives the order to first seek a settlement out of court.

Euromex will:

- * inform you of the extent of your rights and how the dispute will be settled;
- * guarantee the free choice of the expert in an amicable, judicial or administrative settlement procedure;
- * guarantee the free choice of lawyer in case of disagreement, conflict of interest, and with regard to the timing of legal proceedings, arbitration proceedings or legally regulated administrative proceedings.

In the event of an insured claim, Euromex pays:

- the costs of proceedings and legal costs;
- the costs of enforcement proceedings by way of an enforcement order;
- the fees and expenses of the lawyer, the judicial or extra-judicial expert, the bailiff and the mediator, as a result of the mission entrusted to them under the guarantee;
- the costs of arbitration or a recognised form of out-of-court dispute settlement;
- proven costs for the necessary translation of procedural documents;
- justified travel and accommodation costs if you have to appear in person at the request of a foreign court.

If these costs can be recovered from a third party, they will be reimbursed to Euromex.

Procedural fees are also paid to Euromex.

For this reason, you are not allowed to come to an agreement with the third party for these costs and procedural costs without prior agreement with Euromex.

If you or your lawyer believe that the third party is insolvent, you must first consult Euromex before taking enforcement measures.

VAT is not compensated if there is a possibility of having it refunded.

7.2.7 Obligation of the insured

7.2.7.1 *During the guarantee:*

You must inform CyberContract as soon as possible if you become aware of new or changed circumstances that permanently increase the risk insured by Euromex in the guarantee.

If you fail to do so, with fraudulent intent, there will be no cover for claims arising from the increased risk.

7.2.7.2 *In case of claim:*

You must inform CyberContract of any claim as soon as possible. You must inform CyberContract and Euromex of all useful information, the correct circumstances and the desired solution. You must also communicate to CyberContract and Euromex all useful information and documents such as proofs of damages, summonses and subpoenas as soon as possible, both when filing and when processing a claim.

There is no cover for claims reported more than three years after their occurrence.

Euromex may refuse cover if you fail to comply with these obligations with fraudulent intent.

If you have not fulfilled these obligations and a disadvantage results for Euromex, Euromex has the right to reduce the intervention in the event of a claim to the extent of this disadvantage.

Never give an assignment to a lawyer before you have reported the claim to CyberContract or Euromex.

If Euromex is unable to make a useful attempt at an amicable settlement due to the premature intervention of a lawyer, you will have to bear the lawyer's costs and fees yourself.

7.2.8 **Obligation of limitation of damage**

Despite the intervention of Euromex in the costs and fees, you are the client and therefore the debtor of the costs and fees.

The lawyer, adviser or expert chosen by you has no direct right of action against Euromex.

Euromex actually pays the justified and fair fees and costs, provided that you:

- do not agree on the calculation of fees and costs without the express prior agreement of Euromex;
- do not make any payment to a lawyer, adviser or expert without the agreement of Euromex;
- if requested by Euromex, include the fees and costs in your claim against the **third party**(ies).

If Euromex considers that the fees and costs claimed have not been calculated correctly, you agree that Euromex - in your name and on your behalf - may challenge the statement of fees.

If you are summoned for non-payment of a statement of fees, Euromex will have you defended by its lawyer and you will be fully compensated within the financial limits of the guarantee(s) provided in respect of the claim, and in full with regard to defence costs and expenses.

7.2.9 Free choice of expert lawyer

If, in the absence of an amicable solution, it is necessary to proceed to a legally regulated judicial, arbitration or administrative procedure, you choose your lawyer or any other person who, according to the law applicable to the procedure, is qualified to defend your interests.

In the absence of a solution for another recognised out-of-court form of dispute resolution (mediation, voluntary arbitration, etc.), you may choose any person who, under the law applicable to the procedure, is qualified to defend your interests.

You also choose your expert (e.g. an accountant, auditor, etc.) if the assistance of this person is appropriate to reach a solution.

If you choose a lawyer, adviser or expert who does not reside in the country where your mission is to be carried out, Euromex's intervention is limited to the normal costs in the case of appointment of a lawyer, adviser or expert from the country where your mission is to be carried out.

Euromex only pays the costs and fees resulting from the intervention of a lawyer, adviser or expert. Whenever a lawyer, adviser or expert has a successor, the intervention of Euromex is limited to the costs and fees of the subsequent lawyer or expert from the time of the continuation of the case. Costs and fees resulting from a follow-up (study file, opening costs, notification of intervention to other parties, ...) are not covered.

This restriction does not apply if you are obliged to engage another lawyer, adviser or expert without your supervision.

7.2.10 Conflict of interest

A conflict of interest arises if you and Euromex have conflicting interests.

This is also the case if Euromex provides assistance to a **third party** who asserts an interest contrary to yours.

Whenever a conflict of interest arises, you choose your lawyer or any other person qualified under applicable law to defend your interests.

7.2.11 Dispute settlement

If you disagree with Euromex on the chances of success, the reasonableness of your position or the reasonableness of any proposed solution, you may seek advice from a lawyer of your choice as soon as Euromex communicates its position.

- If the lawyer confirms your position, Euromex will provide full cover and pay all additional costs and fees (including the costs and fees of the counsel). This does not depend on the final result obtained. Euromex will also pay if the court finally finds you wrong;
- If the lawyer confirms Euromex's position, you have to pay half of the costs and fees of the lawyer yourself;
- If you nevertheless initiate proceedings, at your own expense, against the lawyer's advice, and you are successful, Euromex will continue to cover you (including the costs and fees of the consultation). You must, however, inform Euromex.

This regulation does not apply in case of disagreement with the expert you have chosen, when it concerns a technical determination, the assessment of the **damage** and the costs of its repair. Euromex cannot be required to go beyond the settlement notice of the expert appointed by you or at your request.

However, if you obtain, at your own expense, a better final result than that resulting from the first advice of your own expert, you can always obtain reimbursement from Euromex for the justified costs and fees.

7.3 The insured

- The insured or the manager(s);
- Family members who cooperate and cohabit with the manager(s) who have taken out the guarantee on behalf;
- The legal and statutory representatives of the insured in the exercise of their mandate as a natural person;
- Your employees, assistants, volunteers, trainees and temporary staff deployed in the performance of their employment contract or mission.

The heirs are also insured, but only as heirs. They are not insured for their personal damage.

All other (legal) persons are third parties.

An insured person cannot invoke the guarantee if his interests may conflict with those of the insured.

7.4 Application scope

The conflict situations guaranteed in the guarantee table must be related to the use of computers, the Internet, networks, electronic data, multimedia or damage to the company's reputation and image in a cyber-environment.

7.5 Guarantee area

Cover applies in the Benelux, Europe or worldwide.

In the table of guarantees, you can see which area of guarantee applies to the different guarantees.

7.6 Guarantee table

This table presents an exhaustive list of disputes covered by a guarantee. Conflicts not mentioned are never insured. A specific conflict is always settled according to the provisions of the most specific guarantee for the risk encountered.

Risks	Guarantes	Guarantee limits	Waiting time	Threshold	Area	Article
General	Waiver payment RC	€ 50.000, -			Worldwide	7.7.1
	Advance payment in case of material damage	€ 20.000, -			Worldwide	7.7.2
	Surety bond	€ 20.000, -			Worldwide	7.7.3
Cyber	Penal defence	€ 50.000, -			Worldwide	7.8.1
	Salduz Assistance	€ 375,-				7.8.2
	Civil recourse	€ 50.000, -			Worldwide	7.8.3
	Personal professional conflict	€ 18.000, -			Benelux	7.8.4
	Civil defence	€ 50.000, -		see 7.2.4 (*)	Worldwide	7.8.5
	Dispute with insurer for cyber risk	€ 25.000, -	3 months		Europe	7.8.6
	Dispute with administrative authorities	€ 18.000, -	6 months	€ 1.000, -	Europe	7.8.7
	Contractual law (**)	€ 18.000, -	3 months	€ 1.000, -	Benelux	7.8.8

(**) outside dispute with insurer for cyber risk

7.7 General cover of legal protection

Additional payments obtained in the case of legal protection for guaranteed claims.

7.7.1 Payment of RC waiver

Euromex will advance the waiver when you provide Euromex with an original signed release of indemnity, issued by an insurer or an insurer-approved claims handler.

As soon as the liability insurer of the third party pays the compensation for the damage, Euromex will pay the waiver, which still has to be paid by that third party.

7.7.2 Advance payment in case of material damage

Euromex advances compensation for material damage, insofar as an agreement has been reached with the identified liable third party or the insurer of this third party for the assessment of this damage.

The advance can be requested as soon as the full liability of the third party is established.

7.7.3 Surety bond

Euromex pays the deposit required by the authorities after an accident. The refund of the deposit is due to Euromex. You assign all your rights in this respect to Euromex. You will complete all formalities to obtain the refund of the deposit. If the authorities only partially release the deposit, you will reimburse Euromex in full .

7.8 cover of legal cyber protection

7.8.1 Penal defence

We provide legal protection if you have to appear before an investigating court, a criminal court or a sanctioning official.

It concerns the defence against violations due to negligence or carelessness concerning national and European regulations relevant to the cyber-environment and the use of multimedia.

These include, in particular, privacy legislation, rules on spam, electronic advertising, remote selling and telesales. However, this list is not exhaustive.

If you are brought to court for an intentional offence, your **defence costs** will be reimbursed provided you are finally acquitted or dismissed for reasons other than a prescription or procedural error.

An intentional offence is any punishable act that is known or ought to be known to be prohibited and that is committed deliberately and not accidentally.

If you are summoned only as civilly liable for the acts of a subordinate, the guarantee is not acquired if you do not contest this civil liability.

7.8.2 Salduz assistance

This guarantee relates to possible violations due to negligence or carelessness concerning national and European regulations relevant to the cyber-environment and the use of multimedia.

These include in particular the protection of **personal data**, rules concerning spam, electronic advertising, remote selling and telephone sales. This list is not exhaustive.

Euromex provides legal protection if you are questioned as a suspect for acts for which your arrest may be ordered, but in which you are not involved or which you did not commit intentionally.

Euromex's intervention is limited to the reimbursement of the costs and fees you have paid to your preferred personal lawyer for the confidential consultation prior to your first interrogation. The reimbursement amounts to a maximum of € 375. Reimbursement will be made in case of suspicion of an intentional crime, as long as you are no longer considered a suspect because you did not commit the acts. This determination may be made on the basis of all the supporting documents (a decision to suspend proceedings, the reasons given by a criminal court judge...). Contrary to the general conditions, the request for this assistance is made on the day of the first hearing or the invitation to do so.

7.8.3 Civil recourse for extra-contractual damage

Euromex provides legal protection if you wish to recover cyber-damages from an identified **third party** with whom you have no contractual relationship.

This also applies to physical damage to your computers, servers and data lines and indirect non-material damage.

Euromex also takes over other damages caused by a **third party** through malicious manipulation of data, websites, multimedia messages (e-mails, SMS, etc.).

In addition, Euromex will take recourse against an identified **third party**, with whom you do not have a contractual relationship, who can be held liable for damage to reputation or loss of image.

Euromex also covers assistance in the event of a dispute in which a **third party** has illegally registered a domain name, as a result of which damage to your business occurs or may occur.

7.8.4 Personal professional conflict

Euromex provides legal protection in the event of a conflict with an employee if the origin of the conflict concerns the processing of data, software and hardware in violation of regulations, (labour) rules and company policy.

This also applies to conflicts in which an employee damages the company's reputation by using any multimedia.

7.8.5 Civil defence

Euromex provides legal protection if a **third party** with whom you do not have a contractual relationship accuses you of an error or negligence for which they claim compensation.

You are not entitled to legal protection if the defence against the **third party's** claim must be carried out by your liability insurer and if there is no conflict of interest with the latter. As soon as you receive the formal notice, you must immediately inform your liability insurer.

If the latter refuses or expresses reservations, you will immediately contact Euromex so that Euromex can take over the defence or advise you on the chances of successfully opposing the **claim** and avoiding a conviction and unnecessary legal costs.

You are not entitled to legal protection if:

- you do not have a liability insurer or if the liability insurer has suspended cover due to non-payment of the premium;
- you do not contest the **third party's** claim;
The defence may also consist of the involvement by Euromex of a **third party**, or your cyber-risk **insurer**, in the dispute.

7.8.6 Dispute with insurer for cyber risk

Euromex provides legal protection in the event of a dispute with the **insurer** of your cyber-risks, with the exception of the actual non-payment of a premium due.

7.8.7 Dispute with administrative authorities

With the exception of disputes falling within the scope of the guarantee referred to in point 7.7.3 Guarantee, Euromex assists you whenever you wish to contest a decision of an administrative authority (e.g. the Belgian Data Protection Authority...), and insofar as this decision concerns the Cybersphere.

7.8.8 Contractual law

With the exception of disputes falling within the scope of point 7.8.6 Dispute with the cyber-risk insurer, Euromex will assist you if, as a claimant, you wish to file a claim for cyber-damage caused by a **third party** with whom you have a contractual relationship.

The damage may include network interruption, loss of data or damage caused by illegal copying of data. Physical damage to computers, servers and data lines is also covered.

If the damage consists exclusively of a work stoppage, recourse is only guaranteed if the work stoppage has lasted more than 8 hours.

7.9 Never guaranteed

You never have legal protection for:

- amounts to be paid in principal and any additional amounts you are ordered to pay;
- criminal and administrative fines, contributions, penalties and settlements with the Public Prosecutor's Office;
 - the defence if you are prosecuted for misdemeanors or crimes under criminal law, or have attempted to commit them. These are the crimes for which, in principle, the assize court has jurisdiction;
- the recovery of damages, if no firewall or basic virus protection is provided;
- the defence of the interests of an insured in the event of a conflict of interest with the insured;
- the complaint against another insured, unless the damage is actually borne by the civil liability insurer and the liable insured does not oppose his intervention;
- conflicts resulting from wars and riots, political or civil unrest in which you yourself participated;
- conflicts resulting directly or indirectly from floods and the ownership of nuclear products, nuclear fuels, radioactive or ionizing products and exposure to non-medical radiation. This restriction does not apply to a conflict with the fire insurer;
- conflicts with Euromex concerning the application of this policy, unless they are explicitly declared as insured;
- the costs of a forensic investigation to identify a **liable third party**;
- costs or fees paid by you or to whose payment you have committed yourself prior to the declaration of the claim or without the agreement of Euromex, except in the case of precautionary or urgent measures;
- disputes resulting from the following acts of gross negligence: fraud, swindling, theft or illegal copying or reproduction of data or software, misuse of licences;
- the defence of the interests **of third parties** or interests transferred to you by waiver of disputed rights or conventional subrogation.

SECTION 8. Common general provisions

8.1 Collaboration

The **insured** shall:

- (i) provide all reasonable support to **insurers** and cooperate in the defence against any possible **claims** and the exercise of its rights to **compensation** and payment;
- (ii) exercise due diligence and do everything possible to avoid or mitigate any damage under this policy;
- (iii) provide **insurers** with all information and support that **insurers** reasonably consider necessary to investigate any damage and determine the liability of the **insured** under this policy.

8.2 Maintenance of technology

The **insured** will take all reasonable steps to maintain data and information security procedures to no lesser standard than disclosed in the proposal form.

The **insured** will ensure that back-up systems and processes are maintained to no lesser standard than disclosed in the proposal form and that the ability to restore such data is regularly tested.

8.3 Sanctions

The **insurer** shall not be deemed to provide cover and the **insurer** shall not be liable to pay any **claim** or provide any benefit hereunder to the extent that the provision of such cover, payment of such **claim** or provision of such benefit would expose the **insurer**, its parent company or its ultimate controlling entity to any sanction, prohibition or restriction under United Nations resolutions or the trade or economic sanctions, laws or regulations of the European Union, Belgium or the United States of America.

8.4 Acquisition of cover

In granting cover to the **insured**, the **insurer** has relied upon the material statements and particulars in the proposal together with its attachments and other information supplied. These statements and information are the base of the cover and are considered an integral part of the present policy.

In the event of the **insurer** being entitled to avoid this policy from the **inception date** or from the time of any variation in cover, the **insurer** may at its discretion maintain this policy in full force, but exclude the consequences of any **claim**, circumstance or **breach of data protection, breach of data protection regulations, newsworthy event, cyber theft** or **business interruption** relating to any matter which ought to have been disclosed before the **inception date** or before any variation in cover.

8.5 Assignment

This policy and any rights hereunder or in respect of it cannot be assigned without prior written consent of the **insurer**.

8.6 Duration of insurance and termination

This insurance contract applies during the **policy period** indicated in the special conditions as possibly modified by later additional clauses, and is automatically extended tacitly with a new **policy period** added to this and any following **policy period**, unless the **company** or the **insurer** terminates this insurance contract at least 3 months prior to the end of the **policy period** by registered letter, by bailiff's writ or delivery of a termination letter with proof of receipt to the other party.

The **company** and the **insurers** may shorten this period of notice by mutual agreement.

8.7 Termination after a claim

After each notification of **claim**, but one month at the latest after payment or the refusal of payment of the compensation the **insurer** and **policyholder** have the right, without indication of reasons, to terminate the insurance with a notice period of three months from the day after the notification, the day after the date of the proof of receipt, or, in case of a registered letter, from the day after its delivery.

8.8 Insolvency

In case of bankruptcy of the **insured's** the policy continues to exist for the benefit of the mass of the creditors who are responsible to the **insurer** for the payment of the premiums to be expired after the declaration of bankruptcy.

Nevertheless, the **insurer** and the liquidator of the bankruptcy have the right to terminate the agreement. However, the termination of the insurance by the **insurer** may only occur three months after the bankruptcy at the earliest, while the liquidator of the bankruptcy may only do so during the three months after bankruptcy declaration.

8.9 Plurals, sections and titles

The titles of paragraphs in this policy are for convenience only and do not lend any meaning to this contract. Words and expressions in the singular shall include the plural and vice versa.

In this policy, words in **bold** have a meaning that is defined or specifically stated in the specific conditions and general conditions.

Words which are not expressly defined in this policy have the meaning normally attributed to them.

8.10 Applicable law

All interpretations of this policy relating to its construction, validity or operation will be made in accordance with Belgian law.

The courts of Brussels have exclusive jurisdiction in this respect.

This last provision does not apply to the application of the "legal protection" guarantee.

8.11 Complaints

CyberContract and the **insurers** are working hard to find a suitable solution to your complaints. You can always report any complaint, to us or to the respective **insurers**, depending on the service you are not satisfied with.

If no solution is found to your complaint, you can always turn to the mediator.

Filing a complaint with one of these parties does not prevent the **insured** from taking legal action.

8.11.1 Complaints addressed to CyberContract:

- by e-mail to info@cybercontract.eu;
- phone number 03 369 09 68;
- a letter to CyberContract;

8.11.2 Complaints addressed to AIG Europe

- an e-mail to info.belgium@aig.com;
- phone number 03 369 96 20;
- a letter to AIG Belgium;

8.11.1 Complaints addressed to Euromex

- an online complaints form www.euromex.be;
- by e-mail to klachtenbehandeling@euromex.be;
- phone number 03 451 44 45;
- a letter to the internal complaints department of Euromex;

8.11.4 Ombudsman

Any complaint relating to the contract may be addressed to the Ombudsman des assurances, Square Meeûs 35, 1000 Brussels or to the Banking, Finance and Insurance Commission, 12-14, rue du Congrès, 1000 Brussels.

As AIG Europe S.A. is an **insurer** based in Luxembourg, you also have access to the competent Luxembourg authorities for any claim concerning the "cyber" cover you may have under this policy. The contact details of these authorities can be found on the AIG Europe S.A. website. <http://www.aig.lu/>.

8.12 Privacy Policy

8.12.1 Common provisions

How insurers and CyberContract use personal information

CyberContract SCRL and the **insurers** are committed to protecting the privacy of customers, claimants and other business contacts

CyberContract SCRL and the insurers are separately responsible for their treatment within CyberContract.

Whenever "we" or "our" is used in this document, it refers only to CyberContract SCRL

“Personal Information” identifies and relates to you or other individuals (e.g. your partner or other members of your family). If you provide Personal Information about another individual, you must (unless we agree otherwise) inform the individual about the content of this notice and our Privacy Policy and obtain their permission (where possible) to share their Personal Information with us and the insurers

The types of Personal Information insurers collect and why - Depending on our relationship with you, Personal Information collected may include: contact information, financial information and account details, credit reference and scoring information, sensitive information about health or medical conditions (collected with your consent where required by applicable law) or (where we require it and are legally permitted to collect it) information about criminal convictions, as well as other Personal Information provided by you or that we obtain in connection with our relationship with you. Personal Information may be disclosed to insurers for the following purposes:

- Insurance administration, e.g. communications, claims processing and payment
- Assessments and decisions about the provision and terms of insurance and the settlement of claims
- Assistance and advice on medical and travel matters
- Management of our business operations and IT infrastructure
- Prevention, detection and investigation of crime, e.g. fraud and money laundering
- Establishment and defence of legal rights
- Legal and regulatory compliance (including compliance with laws and regulations outside your country of residence)
- Monitoring and recording of telephone calls for quality, training and security purposes
- Market research and analysis
- (Internal) audit

Sensitive Personal Information – In connection with the provision of insurance and the assessment of a claim, we will collect, use and disclose certain Sensitive Personal Information concerning your health and medical conditions. Where we do this, we will do so with your explicit consent and as otherwise permitted by law.

Sharing of Personal Information - For the above purposes, Personal Information may be shared with our group companies and third parties (such as brokers and other insurance distribution parties, insurers and reinsurers, credit reference agencies, healthcare professionals and other service providers). Personal Information will be shared with other third parties (including government authorities) if required by laws or regulations. Personal Information (including details of injuries) may be recorded on claims registers shared with other insurers. Personal Information may be shared with prospective purchasers and purchasers, and transferred upon a sale of our company or transfer of business assets.

International transfer - Due to the global nature of our business, Personal Information may be transferred to parties located in other countries (including the United States, China, Mexico Malaysia, Philippines, Bermuda and other countries which may have a data protection regime which is different to that in your country of residence). When making these transfers, we will take steps to ensure that your Personal Information is adequately protected and transferred in accordance with the requirements of data protection law. Further information about international transfers is set out in our Privacy Policy (see below).

Security of Personal Information – Appropriate technical and physical security measures are used to keep your Personal Information safe and secure. When we provide Personal Information to a third party (including our service providers) or engage a third party to collect Personal Information on our behalf, the third party will be selected carefully and required to use appropriate security measures.

Your rights – You have a number of rights under data protection law in connection with our use of your Personal Information. These rights may only apply in certain circumstances and are subject to certain exemptions. These rights may include a right to access Personal Information, a right to request that we correct inaccurate data, erase data, or suspend our use of data. These rights may also include a right to transfer your data to another organisation, a right to object to our use of your Personal Information, a right to request that certain automated decisions we make have human involvement, a right to withdraw consent and a right to complain to the data protection regulator in your country. Further information about your rights and how you may exercise them is set out in full in our Privacy Policy (see below).

8.12.2 Privacy policy of CyberContract:

In addition to the purposes stated above, your personal data may be used by CyberContract for direct marketing purposes.

You have the right to access and rectify your personal data and the right to freely object to the processing of your personal data for direct marketing purposes.

You will find more information about your rights and the way CyberContract SCRL collects, uses and discloses your personal data in the complete privacy policy of CyberContract SCRL at the following address:

<https://www.cybercontract.eu/over-ons/disclaimer> or ask a copy by writing to: CyberContract, Prins Boudewijnlaan 7D 0101 – 2550 Kontich, or send an e-mail to to: info@cybercontract.eu.

8.12.3 Privacy policy of AIG Europe SA:

More details about your rights and how we collect, use and disclose your Personal Information can be found in our full Privacy Policy at <http://www.aig.be/privacy> or you may request a copy by writing to: Data Protection Officer, AIG Europe, Pleinlaan 11, 1050 Brussels or by email at: dataprotectionofficer.be@aig.com.

8.12.4 Privacy policy of Euromex SA:

For more information about your rights and the manner in which Europe SA collects, uses and discloses your personal information, please consult Euromex SA's full Privacy Policy at the following address: <https://www.euromex.be/disclaimer-en-privacybeleid> or ask a copy by writing to: Data protection officer, AIG Europe, Boulevard de la Plaine 54, 2650 Bruxelles, or send an e-mail to: privacy@euromex.be.

8.13 Discovery Period

The liability cover is extended to **claims** raised against the **insured** or the **insurer** and notified to the **insurer** during the period of 36 months after the end of this policy, but only for:

- **loss** occurred during the **policy period** if at the end of the policy the risk is not covered by another **insurer**;
- actions that could lead to **loss** and that occurred during the period the cover applied.
This extension does not apply
 - (i) in case of cancellation or non-renewal due to non-payment of the premium; or
 - (ii) in case of replacement of the policy by a policy with the same or similar cover.