

CyberClear by Hiscox
General Terms and Conditions No n°BCR202109



Introduction

Thanks to technology, we can connect with each other in ways that seemed unthinkable not so long ago. Just by pressing a button, we can book medical appointments, order food, shop online, pay with credit cards, etc., leaving our digital fingerprints everywhere. This inevitably creates certain risks.

As a company, you often store and use data that is interconnected and which evolves quickly and significantly.

You have a legal obligation and a social responsibility to process this data securely. More than ever, cunning, crafty cybercriminals know what shortcuts are needed. Legislators, citizens and companies always seem to lag behind when it comes to protecting confidential company information and/or protecting personal data.

CyberClear by Hiscox protects your company against the consequences of computer piracy, data theft, data loss and cyber attacks. CyberClear by Hiscox has been available in Belgium since 2018 and is constantly adapting to rapid digital developments. We have developed this insurance based on our years of experience in both Belgium and abroad. With this insurance, you can focus on your business without worrying about the consequences of this 'new' form of criminality.

We hope you will never experience any damage. But if you do, we will do everything we can to assist you quickly, and in the best way possible.



Robert Childs
Chair of the HISCOX Group

Table of contents

About CyberClear by Hiscox	5
Part 1 – Definitions	6
Part 2 – Description of the cover	10
2.1 Assistance cover	10
2.2 First Party Cover (Damage suffered by you)	11
Section I – Cyberextortion	11
Section II – Investigations and penalties	12
Section III – Breach of personal data	13
Section IV – Breach of your confidential data	14
Section V – Interruption to and interference with your professional activities	14
Section VI – Data recovery	15
Section VII – Improvements	15
Section VIII – Excess charges in invoices	15
2.3 Third-party cover (Damage to third parties)	16
2.4 Mixed cover (Damage suffered by you and by a third party)	18
Part 3 – Cover exclusions	19
Part 4 – Policy management and indemnification	23
Part 5 – In the event of a claim	25
Section I – Declaring a claim	25
Section II – Claims Management	26
Part 6 – Policy administration	28
Section I – Mandatory declaration	28
Section II – Determining and paying out the premium	29
Section III – How the policy works	30

About CyberClear by Hiscox

CyberClear by Hiscox is an insurance policy especially designed by Hiscox to protect professionals against the risks associated with cybercrime and, more generally, from damage to their **computer systems** and/or their data integrity.

The **policy** consists of:

- these Standard Terms and Conditions;
- **your** Special Conditions and any supplementary clauses.

The Standard Terms and Conditions comprise:

- a definition of the words and expressions used in the **policy**;
- a description of what is covered and how this works;
- the general exclusions that apply to the **policy**;
- the general rules in the event of a **claim**;
- the general provisions governing the administration of the **policy**.

The Special Conditions adapt the cover to **your** individual situation. They have been drawn up based on the documents **you** have provided to **us**, and what **you** have declared to **us** when taking out the **policy**, forming an integral part of the policy. **You** will find that they include the amount of cover granted to **you** and the amount of any **excess**. **You** will also find that they include the supplementary clauses to and derogations from these Standard Terms and Conditions applicable to **your policy**.

If there is any discrepancy or ambiguity between the terms of these Standard Terms and Conditions and those of **your** Special Conditions, the latter will take precedence.

FOR YOUR POLICY TO TAKE EFFECT, YOU MUST SEND US A COPY OF YOUR INITIALLED AND SIGNED SPECIAL CONDITIONS AND PAY THE INSURANCE PREMIUM.

We have taken particular care to draft this **policy** in plain language to make it easier to read and understand. If needed, **you** can contact **your** insurance broker, who will explain anything to ensure you are fully informed.

Part 1 – Definitions

For the purposes of this **policy**, certain words and expressions are always used with a specific meaning, as defined below. These words and expressions written in bold font have the following meanings, whether in the singular and/or plural, and regardless of where they are used in the **policy**.

Activities	The activities you carry out as part of running your business, and which are known and accepted by us for the term of the contract.
Assistance	All the assistance benefits described in Part 2, 2.1 below.
Policyholder (you/your)	The legal person referred to in the Special Conditions who has taken out this policy and, where applicable, their affiliated entities and additional policyholders referred to in the Special Terms and Conditions.
Insurer (we/us/our)	The legal entity of the Hiscox group, as specified in the Special Conditions within this policy .
Acquiring bank	Provider of financial services under a service agreement to process transactions.
Director	Any natural person who is a member of a management board or who has day-to-day management responsibilities.
PCI Security Standards Council	Security standards council for the payment card industry, whose founding members are American Express, Discover Financial Services, JCB International, MasterCard and Visa Inc.
Service agreement	Contract signed between you and a payment services provider to enable you to accept and receive credit and debit card payments.
Cyber attack	Act by a hacker .
Hacker	Any person or group of people who threatens you with or succeeds in: <ul style="list-style-type: none"> — fraudulently operating, accessing or using your computer systems or your website; or — fraudulently operating, accessing or using a part of your computer systems to which they do not have legitimate access; or — preventing you or preventing your officials from accessing your computer systems, for example by using denial-of-service attack or encryption solutions; or — accessing, using, destroying, altering or disclosing, without authorisation, data that you hold within your computer systems. <p>The term ‘Hacker’ does not encompass a director of the policyholder.</p>
Denial-of-service (DOS)	An attack on a computer network, website or system that makes the network, website or system unavailable for its intended use.
Damage	<p>Bodily injury, material or non-material damage:</p> <ol style="list-style-type: none"> 1. Bodily injury – means physical or psychological harm caused to a natural person. 2. Material damage – means the destruction, damage to, alteration, disappearance, loss or theft of an object or substance, and any harm to animals. 3. Non-material damage – means a financial loss resulting from the deprivation of a right, the interruption of a service rendered by a person or by movable or immovable property, or the loss of profit. <p>Non-material damage is consequential if it results from an insured bodily injury or material damage. Non-material damage is non-consequential if it does not result from insured bodily injury or material damage, or if it occurs in the absence of bodily injury or material damage.</p>
Confidential data	Any strategic information belonging to or held by the policyholder , including financial or commercial information, which is not accessible to the public and which, if disclosed, would cause financial harm to the policyholder or would incur their liability.

Personal data	Any information relating to an identified or identifiable natural person – an ‘identifiable natural person’ is deemed to be a natural person who can be directly or indirectly identified, for example by reference to an identifier such as a name, ID number, location data, an online username, or to one or more specific elements relating to their physical, physiological, genetic, physical, economic, cultural or social identity, including bank information and sensitive data, and in accordance with the prevailing legislation on the protection of personal data .
Affiliated entity	<ol style="list-style-type: none"> 1. Any legal entity that the policyholder (a) owns on the day this policy takes effect or (b) acquires or directly or indirectly establishes during the period of insurance, provided such legal entity: <ul style="list-style-type: none"> — carries out the same professional activities as the policyholder; and — has an annual turnover of less than 20% of the policyholder’s annual turnover; and — has a registered address within the European Economic Area or in the United Kingdom; and — is not aware of any claim made against them on the date it was acquired. 2. Any legal entity that the policyholder acquires or establishes during the period of insurance with an annual turnover greater than 20% of the policyholder’s annual turnover, and/or carrying out professional activities different from those of the policyholder, and/or with a registered address outside the European Economic Area, provided: <ul style="list-style-type: none"> — the policyholder has informed us in writing about the acquisition and/or establishment of that legal entity within 30 days of the date it took place; — we have agreed to include that legal entity in this policy, where applicable under new conditions. 3. For the purposes of this definition, an entity is considered an affiliate when it is controlled by the policyholder within the meaning of Articles 1:14 et seq of the Companies and Associations Code.
Human error	Handling error due to negligence, carelessness or omission by one of your directors or officials in relation to your computer systems , including a response to a social engineering attempt.
Harmful event	Act, deed or event that gives rise to or is likely to give rise to a claim . A series of harmful events with the same technical cause is treated as a single harmful event .
Excess	The portion of the insured event , excluding assistance (Part 2, 2.1) and defence costs (Part 2, 2.2 Section II and 2.3), that remains payable by the policyholder after the insurer’s cover has been implemented.
Social engineering	Any request sent to your directors or officials with the aim of inducing them, via fraudulent manoeuvres: <ul style="list-style-type: none"> — to disclose personal data or confidential data to which they have access; and/or — to unknowingly hand over valuables belonging to the policyholder to a third party.
Gross operating margin	<p>The amount stipulated per accounting period of the policyholder, corresponding to the difference between:</p> <ol style="list-style-type: none"> 1. Total operating income; and 2. The sum of: <ul style="list-style-type: none"> variable operating costs less discounts, rebates and changes in inventory, plus fixed operating costs covered by the policyholder’s other income and/or not incurred during the period of insurance of a claim. <p>If in doubt, the definition of ‘gross operating margin’ stipulated in Article 3:90 of the Royal Decree of 29 April 2019 implementing the Companies and Associations Code will apply.</p>
Threat	Behaviour by which a third party signals their intention to you : <ol style="list-style-type: none"> 1. to damage, destroy, modify and/or corrupt your computer systems, for example by introducing a virus specifically targeting your system or your data; or 2. to disseminate, disclose and/or use: <ul style="list-style-type: none"> — the personal data that you hold, provided it is data that was not publicly accessible or was not already circulated on the Internet before the threat, and/or — confidential data that you hold, where implementing this threat is likely to cause you commercial damage.

Business partners	Your suppliers, sub-contractors , IT providers, customers and more generally any person with whom you have a business relationship.
Period of insurance	<p>The period between:</p> <ol style="list-style-type: none"> 1. the first effective date of the policy referred to in the Special Conditions and the first renewal date referred to in the Special Conditions; or 2. the first effective date of the policy referred to in the Special Conditions and the date of the policy's expiry before its first annual renewal; or 3. two consecutive annual renewal dates, or; 4. the policy's last annual renewal date and the date of its termination or expiry during the period of cover in place on that date; <p>without prejudice, for 'Damage to third parties' cover only, the 36-month period immediately following the date of termination or expiry of the cover (see Part 4 below).</p>
Withholding period	Waiting period before the cover takes effect. Our cover will be payable as soon as there is a harmful event that continues without having ended during the withholding period .
Cover limit	The maximum amount that we will pay under this policy , as set out in your Special Conditions. Unless otherwise specified in your Special Conditions, the cover limit is agreed per claim and per period of insurance .
Policy	This insurance contract concluded between you and us , including the Standard Terms and Conditions, the Special Conditions and addenda.
Officials	<p>Your employees, apprentices, trainees, and more generally any natural person placed under your authority on a temporary or permanent basis.</p> <p>SELF-EMPLOYED WORKERS AND SUB-CONTRACTORS DO NOT FALL WITHIN THE DEFINITION OF OFFICIALS. PERSONS WHO CARRY OUT THEIR ACTIVITY IN BREACH OF THE LEGAL OR REGULATORY PROVISIONS ON UNDECLARED WORK ARE EXCLUDED.</p>
Ransom	<p>Any sum of money, in cash or otherwise, goods, products and/or services claimed from you by a third party in return for not carrying out a threat.</p> <p>RANSOMS CLAIMED BY A PERSON WHO IS THE SUBJECT OF AN ECONOMIC OR COMMERCIAL SANCTION PROVIDED FOR BY THE UNITED NATIONS, THE EUROPEAN UNION, BELGIUM AND/OR ANY OTHER STATE (INCLUDING THE UNITED STATES), OR WHO IS A MEMBER OF A TERRORIST GROUP WITHOUT PREJUDICE TO SECTION II, PART 2.2, 'INVESTIGATIONS AND SANCTIONS' ARE EXCLUDED.</p>
Complaint	Any written invocation of your liability in connection with a claim .
Outsourced services	Services outsourced by the policyholder to a third party in exchange for remuneration, and corresponding to human resources, payroll, a call centre (sales and assistance), billing, legal, storage and shipping services for finished products.
IT services	<p>Any natural person or legal entity that, under a written agreement, provides you with IT and electronic services, including any of the following services or systems, where hosted by a public cloud service or at a data centre that you do not own:</p> <ol style="list-style-type: none"> 1. Infrastructure as a Service; 2. Platform as a Service; 3. Software as a Service; 4. Hosting services; 5. Email, intranet or extranet services; <p>This does not include Internet service providers and telecommunications services.</p>

Claim or 'insured event'	<ol style="list-style-type: none"> 1. Under the 'Cyberextortion', 'Investigations and penalties', 'Infringement of personal data', 'Interruption of your professional activities', 'Infringement of your confidential data', 'Excess charges in invoices' and 'Cyber fraud' cover: any non-material damage suffered by you as a result of a harmful event or a series of harmful events, as exhaustively listed and described by the cover, as well as material damage included in the 'Perishable foodstuffs' and 'IT equipment' cover as part of the Interruption to your professional activity cover, and loss of physical property included as part of the 'Cyber fraud' cover. 2. Under the 'Damage to third parties' cover: any non-material damage or bodily injury resulting from a harmful event or from a series of harmful events as exhaustively listed and described by the cover, caused to a third party or to an official, for which you may be liable, and which has been the subject of a complaint.
Computer systems	Computer systems that belong to you and over which you have full control.
Sub-limit	The sum insured and indicated as a sub-limit in the policy , and which forms part of the policy without exceeding the cover limit .
Sub-contractor	A natural person or legal entity that is not an affiliated entity of the policyholder and which is instructed to carry out activities or services on behalf of the policyholder , including cloud service providers, web hosts and data controllers.
Third party	Any natural person or legal entity, including your business partners . EXCLUDES THE POLICYHOLDER AND THEIR OFFICIALS .
Valuables	Bank notes, coins, currencies, coins and ingots in precious metals, deposit money, cheques, commercial instruments, money orders and transfer orders, deposit certificates, commercial papers, savings bonds, treasury bonds and other negotiable debt securities, shares and debentures and in general all means of payment and all financial securities. Valuables are either reinstatable or non-reinstatable .
Non-reinstatable valuables	Any valuables – other than bank notes, coins, currency and deposit money – which cannot be reinstated or cancelled, such as precious metal coins and ingots or digital financial securities.
Reinstatable valuables	Any valuables – other than bank notes, coins, currency and deposit money – which can be reinstated or cancelled, such as cheques, commercial instruments or digital financial securities payable to the bearer.
Breach of personal data	The destruction, loss, alteration, disclosure or unauthorised access to personal data (including through a virus) that you hold within your computer systems , resulting: <ol style="list-style-type: none"> 1. from human error; 2. from a cyberattack.

Part 2 – Description of the cover

2.1 Assistance cover

Section I Assistance

We have set up a panel of specialist partners able to intervene to assist **you** in the event of a **cyberattack** and, more generally, in the event of an attack on the integrity of **your computer systems**, as covered by **your policy**, except as a result of a **human error**. **We** will cover, with no **excess**, the fees of these partners instructed by **us** in connection with an **insured event** as described below, provided the **claim** is declared to **us** within 72 hours of its occurrence. It is up to **us** to decide whether to instruct one or more experts from **our** panel, but **we** will make this decision in consultation with **you**. This benefit will always constitute a best endeavours obligation, rather than an absolute obligation.

Up to 72 hours after a **cyberattack**, we will also cover, with no **excess** and beyond the **cover limit**, the reasonable and necessary fees, up to a maximum of €15,000 (non-indexed) per year of insurance, of the specialist service providers listed below that **you** choose to appoint (own service), provided those providers were instructed as soon as **you** became aware of a **cyberattack** or of an attack on the integrity of **your computer systems** and provided the **cyberattack** can reasonably be suppressed within 72 hours.

This **assistance** is designed to be applied regardless of the cover activated in the event of a proven or potential **insured event** with, in the second instance, reliable and concrete evidence of the existence of such an event.

The following specialist providers may be instructed:

A. IT security expert

a consultant specialising in information system security whose work may involve identifying a security breach in **your computer systems**, recommending solutions for remedying the breach, carrying out repair services following the security breach, up to a maximum of €1,000.00 (non-indexed), that are urgent and strictly necessary to prevent an imminent **cyberattack** or to reduce the consequences of an **insured event** that has begun to emerge, identifying the compromised **personal data** or **confidential data**, identifying the author(s) of a **cyberattack**, building a case file for legal action;

B. Lawyer

a lawyer whose work may involve identifying the nature and scope of **your** statutory or regulatory obligations in terms of notifying any **breach of personal data** to the competent authorities and/or to individuals whose **personal data** has been breached, and where applicable to carry out such notifications or to build a case file for legal action;

C. Crisis communication

a communications specialist whose work may involve helping **you** manage **your** external communications to limit the impact of the **insured event** on **your** reputation and/or online reputation.

2.2 First Party Cover (Your own losses)

Section I Cyberextortion

- 1. Scope of the cover** We will cover **you** in the event of:
- a **threat** of extortion by a **hacker** to obtain payment of a **ransom** from **you**;
 - a **ransom** request following damage to, destruction, modification or corruption of **your computer systems** or the disclosure of **confidential** and/or **personal data** by a **hacker**.
- 2. Benefits paid** In the event of an **insured event** covered by this policy, and provided this benefit is legally insurable under the governing law, **we** will cover, in addition to the **assistance** referred to in Part 2.1 above, and under the conditions and limits provided for by the **policy**:
1. the amount of the **ransom** that you have paid to the **hacker**
 - up to its monetary amount; or
 - if it concerns goods, products or services, up to their market value on the day of paying the **ransom**.
 2. operating losses **you** have suffered, where directly caused by the cyberextortion. The operating losses are covered in accordance with the provisions set out in the Special Conditions.
- 3. Conditions of cover** THIS COVER IS SUBJECT TO THE FOLLOWING CONDITIONS:
- **WE** HAVE GIVEN **OUR** PRIOR AGREEMENT FOLLOWING RECEIPT OF AN OPINION FROM **OUR** IT EXPERT PANEL DEMONSTRATING THAT THERE IS NO TECHNICAL AND/OR LEGAL ALTERNATIVE TO PAYING THE **RANSOM**; AND
 - **YOU** DEMONSTRATE TO **US** THAT THE **RANSOM** HAS BEEN PAID TO THE **HACKER** UNDER DURESS; AND
 - **YOU** DEMONSTRATE TO **US** THAT YOU ARE CERTAIN THE **RANSOM** REQUEST WAS A GENUINE **THREAT** AND NOT A HOAX; AND
 - AT LEAST ONE OF **YOUR** CORPORATE OFFICERS HAS GIVEN THEIR PRIOR WRITTEN CONSENT TO PAY THE **RANSOM**.

Section II Investigations and penalties

Following an **insured event** covered under the 'Breach of personal data' benefit (Part 2.2 - Section III), 'Breach of security and/or confidentiality of personal data' (Part 2.3) or 'Breach of third-party confidential data' (Part 2.3), we will cover you in the event of:

- an investigation or action taken against **you** by a competent administrative or government authority concerning the **breach of personal data** concerned, for example, the data protection authority; and/or
- an investigation or action initiated by a member of the **PCI Security Standards Council** or by an **acquiring bank** following an actual or alleged breach on **your** part of the 'PCI-DSS' security rules or the rules laid down by any banking institution or bank card network used by **you** to accept and receive payments by credit card.

If an **insured event** covered by this policy occurs, **we** will cover, in addition to the **assistance** referred to in Part 2.1 above, and under the conditions and limits provided for by the **policy**.

A. Costs of defence

Lawyer's fees incurred with **our** prior written agreement in defending **you** in connection with this investigation or action, within the limits of the rates charged by lawyers on **our** own panel, and provided that:

- **we** are kept strictly informed by **you**, or directly by **your** lawyer, of developments in the case, with enough good time for **us** to be able to present **our** observations (without this being considered as taking charge of the case);
- where **we** have notified **you** of **our** intention to take charge of the case, that these supervisory powers are available to **us**.

This benefit will be paid after the amicable, administrative or judicial settlement or settlement by arbitration of the **claim** has concluded, in the form of reimbursement of the pre-tax cost of the invoices from the relevant law firm duly paid by **you**, and on presentation of the relevant supporting documents. **We** may, if necessary and on request, pay these costs in advance.

B. Fines and penalties

Where applicable, and by partial derogation from the general exclusion of benefit 11 below, fines and penalties that **you** are required to pay in connection with the above investigations and actions, provided they are legally insurable under the governing law. This benefit will take the form of reimbursement of the amount of fines and penalties duly paid by **you**, and on presentation of the supporting documents.

C. Conditions of cover

THIS COVER WILL NOT BE GRANTED TO **YOU** IN CONNECTION WITH INVESTIGATIONS INITIATED BY A MEMBER OF THE **PCI SECURITY STANDARDS COUNCIL** OR BY AN **ACQUIRING BANK**, UNLESS **YOU** HAVE PROVIDED TO **US**, ON THE DATE OF TAKING OUT THE COVER, A DOCUMENT CERTIFYING **YOUR** COMPLIANCE WITH THE APPLICABLE PCI-DSS STANDARD.

Section III Breach of personal data

We will cover **you** in the event of a **breach of personal data** resulting from **human error**, a **cyberattack** committed or suffered by **you** or by a sub-contractor within the meaning of legislation on the protection of **personal data**, including in the absence of a statutory or regulatory obligation incumbent on **you**.

If an **insured event** covered by this policy occurs, **we** will cover, in addition to the **assistance** referred to in Part 2.1 above, and under the conditions and limits provided for by the **policy**:

1. Costs of notification

The costs incurred with **our** prior written agreement, of:

- identifying the nature and scope of **your** statutory or regulatory notification obligations;
- identifying the natural persons and national authorities to whom the **breach of personal data** identified must be notified;
- notifying the **breach of personal data** identified to the natural persons concerned, and to the competent administrative or government authorities, in accordance with **your** statutory or regulatory obligations.

This benefit will be paid in the form of reimbursement of the amount, excluding tax, of invoices issued for notification costs incurred, duly paid by **you** and/or on the basis of supporting documents relating to any other costs associated with this notification. **We** may, if necessary and on request, pay these costs in advance by covering them directly.

2. Call centre

The cost of any external call centre that **you** have commissioned with **our** prior written agreement in order to respond to questions from natural persons whose **personal data** has been compromised, provided **you** do not have the internal resources and facilities required to do so **yourself**.

This benefit will be paid in the form of reimbursement of the amount, excluding tax, of the invoices of the external call centre concerned, duly paid by **you** and on presentation of the relevant supporting documents. **We** may, if necessary and on request, pay these costs in advance by covering them directly.

3. Identity/credit monitoring

The cost of any external provider that **you** have instructed with **our** prior written agreement in order to monitor and prevent any unauthorised use of the **personal data** breached, provided this monitoring relates to:

- a) social security numbers, driving licences, or any other number enabling an individual to be directly or indirectly identified, issued by any organisation and capable of being used, in conjunction with other information, for the purposes of opening bank accounts or taking out insurance; and/or
- b) any other **personal data** for which the prevailing law or regulations require **you** to implement this monitoring.

This benefit will be paid in the form of reimbursement of the amount, excluding tax, of the invoices of the external provider concerned, duly paid by you and on presentation of the relevant supporting documents. **We** may, if necessary and on request, pay these costs in advance by covering them directly.

THIS BENEFIT IS LIMITED TO PAYING IDENTITY OR CREDIT MONITORING SERVICES CARRIED OUT DURING A **12-MONTH** PERIOD AS FROM THE DATE ON WHICH **YOU** BECAME AWARE OF THE **INSURED EVENT**, AND ONLY FOR INDIVIDUALS WHO HAVE REQUESTED IT.

Section IV Breach of your confidential data

We will cover **you** in the event of destruction, loss, alteration, disclosure or unauthorised access to **your confidential data** or the **confidential data of third parties** that **you** hold as a result of **human error** or a **cyberattack**.

If an **insured event** covered by this policy occurs, **we** will cover, in addition to the **assistance** referred to in Part 2.1 above, and under the conditions and limits provided for by the **policy**, the costs of recovering and/or restoring **your confidential data** essential to carrying out **your** professional **activities**.

Section V Interruption to and interference with your professional activities

We will cover **you** in the event of a full or partial interruption to **your** professional **activities**:

- resulting directly from the actions of a **hacker** who has succeeded in hindering or disrupting access to and/or the functioning of all or part of **your computer systems**; or resulting from a **breach of personal data** or **confidential data**; or
- a **denial-of-service** attack, whether or not widespread, and targeting you directly.

If an **insured event** covered by this policy occurs, **we** will cover, in addition to the **assistance** referred to in Part 2.1 above, and under the conditions and limits provided for by the **policy**, and in particular the **sub-limit** per year of insurance provided for in the Special Conditions:

1. What is covered?

1.1. Operating losses

Operating losses will be covered in accordance with the provisions set out in the Special Conditions.

1.2. Additional operating costs

Additional operating costs will be covered in accordance with the provisions set out in the Special Conditions.

1.3. Director

Where a **director** of the **policyholder** or (one of) their children, or one of the persons living with them, is the victim of one or more of the following cyber incidents:

- Publication of defamatory content on social media, an Internet site or any other digital platform (including hate sites, blogs, chatrooms, email, GSM, SMS, etc.);
- Unjustified attack on their personal reputation via social media, an Internet site or any other digital platform (including hate sites, blogs, chatrooms, email, GSM, SMS, etc.);
- Grooming: An online process where an adult approaches a minor and manipulates them for sexual contact or sexual acts (e.g. via webcam, chat or email), including the creation and dissemination of photographic material on the Internet;
- Sextortion: any extortion that is sexual in nature, including the creation and dissemination of photographic material on the Internet;
- Cyberbullying and online harassment: repeatedly harassing, insulting, offending, tormenting or threatening on the Internet or through any other electronic means of communication;
- Any publication, communication or unauthorised use by a **third party** of **personal data** in breach of legislation on the protection of **personal data**;

and where the cyber incidents listed above indirectly harm the reputation of the **policyholder**, **we** will also cover, in addition to the additional operating costs (benefit 1.2 of this section) up to a maximum of €3,000.00 (non-indexed), the costs of rebuilding the policyholder's reputation through, among other things, the deletion or concealment of defamatory content.

2. Period of indemnification

After the retained portion has been converted into a monetary **excess** after the **withholding period**, the indemnification of operating losses and additional operating costs will only be covered for a period of indemnification referred to in the Special Conditions, a period that begins on the day the **insured event** first occurs. It will not be altered if the **policy expires**, is terminated or suspended after the **insured event** occurs.

3. Extensions of cover

The following extensions are only agreed when specifically referred to in the Special Conditions of **your policy**, and within the **sub-limit** set out therein:

3.1. Perishable foodstuffs

Losses resulting from **damage** to stocks of perishable foodstuffs as a direct consequence of changes in temperature and humidity in a controlled environment, due to acts committed by a **hacker**, including the reasonable costs of repairing and replacing such stock

3.2. Computer equipment

Costs relating to the repair or replacement of computer equipment belonging to you following damage to it as a result of acts by a **hacker**, except for theft, vandalism or loss.

- 3.3. IT service providers** Full or partial interruption to **your professional activities** as a direct result of:
- a **cyberattack** suffered by one of **your IT service** providers; or
 - the accidental malfunction or unavailability of **your computer systems** caused by a **human error** by one of **your IT service** providers.
- Our benefit will be payable after the withholding period referred to in the Special Conditions has ended, and for a maximum period of three months. Once the period has ended, we will cover the claim as from its first occurrence, subject to application of the excess.
- 3.4. External service providers** Full or partial interruption to **your professional activities** as a direct result of:
- a **cyberattack** suffered by one of **your external service** providers; or
 - the accidental malfunction or unavailability of **your computer systems** caused by a **human error** by one of **your external service** providers.
- Our** benefit will be payable after the **withholding period** referred to in the Special Conditions has ended, and for a maximum period of three months. Once the **withholding period** has ended, **we** will cover the **claim** as from its first occurrence, subject to application of the **excess**.
- 3.5. Failure of your computer systems due to a human error** Full or partial interruption to **your professional activities** following accidental malfunction or unavailability of **your computer systems** caused by a **human error** by **you** or by one of **your officials**.
- 3.6. Any failure of your computer systems** This benefit covers full or partial interruptions to **your professional activities** following any accidental (understood as unforeseen and unintentional) malfunction or unavailability of **your computer systems**, provided the malfunction originates from the part of the **computer system** or power supply system that is under the sole authority of the **policyholder** or over which the **policyholder** has full control. Malfunctions due to obsolescence or to overload caused by improper scheduling of the **computer systems'** capacity under normal operating **conditions**, or due to increased usage, do not constitute malfunctions of **your computer systems** within the meaning of these Standard Terms and Conditions.
- Section VI**
Data recovery Following an **insured event**, **we** will cover any costs incurred, subject to **our** prior written agreement, by a data recovery expert appointed to recover lost or altered **personal data** and/or **confidential data** from the computer media that **you** have.
- Section VII**
Improvements Following an **insured event**, **we** will cover any costs incurred, subject to **our** prior written agreement, in connection with improving the security level of **your computer systems**, up to a maximum of 10% of the **damage** for which **we** are indemnifying **you**, not exceeding €10,000 (not indexed).
- Section VIII**
Excess charges in invoices
- 1. Scope of the cover** **We** will cover **you** in the event of fraudulent use by a **hacker**:
- of **your** telephone systems; or
 - of **your** Internet connection or cloud service; or
 - of **your** electricity supply point;
- where this use impacts the cost of invoices sent to **you** by **your** operator.
- 2. Benefits paid** If an **insured event** covered by this policy occurs, **we** will cover, up to 60 days after the **cyberattack**, under the conditions set out in the **policy** and within the **sub-limit** indicated in **your** Special Conditions, invoices issued by **your** operator and as a direct result of the actions of a **hacker**.
- 3. Payment arrangements** This benefit will be paid in the form of reimbursement of the amount, excluding tax, of the invoices issued by **your** telecommunications operator and duly paid by **you**, and on presentation of the relevant supporting documents.

2.3. Third-party cover (Damage to third parties)

Section I

Damage to third parties

A. Description of the cover

Under the conditions and limits established by the **policy**, we will cover, for **non-material damage** and **bodily injury**, subject to adhering to the **sub-limit** per **claim** indicated in the Special Conditions, **your** civil liability resulting from a **harmful event** or from a series of **harmful events** as listed exhaustively below.

THIS EXCLUDES ANY **CLAIM** ARISING FROM ACTIVITIES **YOU** CARRY OUT ON BEHALF OF A PRINCIPAL OR FROM NON-COMPLIANCE WITH A LEGAL NOTICE ON THE CONTENT OF AN EMAIL OR OF **YOUR** WEBSITE

1. Breach of the security and/or confidentiality of personal data

We will cover **non-material damage** and **bodily injury** suffered by **third parties**, **your officials** and **your directors** caused by a breach of personal data, in connection with claims made against **you** by natural persons identified or identifiable through **personal data** where you have not ensured the security and/or confidentiality of that data, in breach of your obligation under the prevailing regulations or as a result of an omission, carelessness or negligence on **your** part or that of **your officials** or sub-contractors within the meaning of legislation on the protection of **personal data** or contractual commitments **you** have entered into.

2. Media

We will cover **non-material damage** caused to **third parties** as a result of content published on your Internet site or **your** social media accounts, where this gives rise to a **claim** against **you** during the **period of insurance**, in respect of any:

- infringement of privacy within the meaning of Article 22 of the Belgian Constitution (or its foreign equivalent);
- defamation (damage to the honour or reputation of a **third party**) and/or a smear campaign (discrediting the products or services of the **third party**);
- infringement/breach of the intellectual property rights of a **third party** (copyright, trademarks, designs and models, sui generis rights of database producers);
- cybersquatting, creating hyperlinks or mimicking the standard formats and/or identical or analogous characteristics of a **third-party** website.

THIS EXCLUDES ANY **CLAIM** RELATING TO THE DESCRIPTION, ILLUSTRATION OR PRESENTATION OF PRODUCTS OR SERVICES PROVIDED BY **YOU**.

3. Infringement of third-party confidential data

We will cover **non-material damage** and **bodily injury** caused by the disclosure, as a result of actions by a **hacker**, or resulting from an omission, carelessness or negligence on **your** part or that of **your officials** or sub-contractors within the meaning of legislation relating to the protection of **personal data**, **confidential data** belonging to **third parties**, and which **you** hold within **your computer systems** or the **computer systems** of a sub-contractor within the meaning of legislation on the protection of **personal data**, where such disclosure gives rise to a **claim** against **you** by those **third parties**.

4. Transmission of viruses and cyberattacks via your computer systems

We will cover **you** for **non-material damage** caused to any **third parties** or **officials**, provided a **claim** has been made against **you** by them, invoking **your** liability and resulting:

- from the transmission of a virus from **your computer systems**; or
- from the use of **your computer systems** by a **hacker** for the purposes of a **denial-of-service** attack directed against that **third party**, **official** or **business partner**.

THIS EXCLUDES **CYBERATTACKS** DIRECTED AGAINST **YOUR IT SERVICE PROVIDERS**.

B. What is covered?

If an **insured event** is covered by the '**Damage to third parties**' benefit listed above, **we** will cover, in addition to the **assistance** referred to in Part 2.1 above, and under the conditions and limits provided for in the **policy**:

1. Costs of defence

Lawyer's fees **you** have incurred with our prior written agreement, within the limits of the rates charged by lawyers on **our** own panel, and provided that:

- **we** are kept strictly informed by **you**, or directly by **your** lawyer, of developments in the case, with enough good time for **us** to be able to present **our** observations (without this being considered as taking charge of the case);
- where **we** have notified **you** of **our** intention to take charge of the case, that these supervisory powers are available to **us**.

This benefit will be paid after the amicable, administrative or judicial settlement or settlement by arbitration of the **claim** has concluded, in the form of reimbursement of the pre-tax cost of the invoices from the relevant law firm duly paid by **you**, and on presentation of the relevant supporting documents. **We** may, if necessary and on request, pay these costs in advance.

2. Compensation

- a) **Compensation** that **you** are sentenced to pay by any enforceable arbitration, administrative or judicial decision handed down against **you**;
- b) Where applicable, the amount of compensation charged to **you** under any definitive settlement agreement within the meaning of Sections 2044 et seq of the Civil Code (or their equivalent abroad).

This benefit will be paid:

- i) in the form of reimbursement to **you** of the amount of **compensation** that **you** have paid directly to the beneficiary of this sentence, or the amount of the settlement payment **you** have paid directly to its beneficiary, on presentation of supporting documents as evidence of this payment by **you**; or
- ii) in the form of payment of this **compensation** or this settlement payment paid by **us** directly to the beneficiary of the sentence order or settlement payment.

We will cover **compensation** within the limits provided for in Section II of Part 5 of this **policy**.

3. Retrieval costs

The cost of corrective measures that **you** have implemented, with **our** prior written agreement, with the sole purpose of limiting the financial consequences of the **insured event** with regards to the cover available under this Section, including the repair of **your computer systems**, provided such costs are less than the cost of the **insured event**. **We** will cover retrieval costs within the limits provided for in Section II of Part 5 of this **policy**.

2.4. Mixed cover (Damage suffered by you and by a third party)

Section I

Cyber fraud

- 1. Scope of the cover** We will cover **you** in the event of fraud experienced by **you**, understood as any illegal act carried out by a **hacker** and resulting from their intrusion into **your computer systems** or an act of **social engineering**:
- directly affecting:
 - **valuables** that you own, or which belong to **third parties** and are held by **you** as part of performing **your activities**;
 - physical property that **you** own;
 - goods or services owned by **your business partners**, where the fraudulent act relates to invoices supposedly sent to you by **your business partners**. In this instance, our cover will also be activated when a fraudulent invoice is sent from the computer systems of **your business partner**;
 - **valuables** owed to **you** by **your business partners** but which **you** have never received, due to fraudulent invoices sent by a **hacker** from **your computer systems**;
 - and meeting the definition of one or more of the following offences provided for by Belgian criminal law (or any equivalent offence punishable by the applicable foreign criminal law):
 - Theft (Sections 461 et seq of the Criminal Code);
 - Fraud (Sections 496 et seq of the Criminal Code);
 - Breach of trust (Sections 491 et seq of the Criminal Code);
 - Forgery and use of forgeries (Sections 193 et seq of the Criminal Code);
 - Counterfeiting (Sections 160 et seq of the Criminal Code);
 - Counterfeit or forged cheques (Sections 179 et seq of the Criminal Code).
- 2. Payment arrangements** If an **insured event** covered by this policy occurs, **we** will cover, under the conditions set out in the **policy** and within the **sub-limit** indicated in **your** Special Conditions:
- provided:
 - the existence of this fraud has been established by **you**;
 - a complaint has been filed by **you** with the competent authorities; and
 - the fraud was committed during the **period of insurance**;
 - either the direct financial loss suffered by **you**, consisting of the loss of the **valuables** affected by this fraud;
 - or payment of invoices issued by **your business partner** that are a direct result of the **hacker's** actions.
- 3. What is covered?** For fraud involving banknotes, coins, foreign currency and/or deposit money, **we** will indemnify on the basis of their nominal value on the day the fraud is discovered.
- In the event of fraud involving **reinstatable valuables**, **we** will indemnify on the basis of the lowest sum between (1) their value at their actual market price at the close of the last business day preceding the day of discovering the fraud and (2) the amount of the cancellation or reinstatement costs.
- In the event of fraud involving **non-reinstatable valuables**, **we** will indemnify on the basis of their value at their actual market price at the close of the last business day preceding the day of discovering the fraud.
- In the event of fraud involving goods or services owned by **your business partners**, **we** will indemnify on the basis of the amount, excluding tax, of the invoices issued by **your business partner** and duly paid by **you**, and on presentation of the relevant supporting documents.

Part 3 – Cover exclusions

IN ADDITION TO ANY ADDITIONAL COVER EXCLUSIONS PROVIDED FOR IN **YOUR** SPECIAL CONDITIONS, THE FOLLOWING ARE EXCLUDED FROM THIS **POLICY'S** COVER:

- | | |
|--|---|
| 1. Absence of unforeseeable circumstances | CLAIMS THAT ARE NOT UNPREDICTABLE OR UNFORESEEABLE IN NATURE. |
| 2. Pre-existing Problems | CLAIMS RESULTING FROM ANY FACT, ACT OR EVENT OF WHICH YOU WERE AWARE ON THE DATE THE POLICY OR COVER CONCERNED TOOK EFFECT. |
| 3. Dishonest and criminal acts | <p>CLAIMS RESULTING FROM FACTS OR ACTS:</p> <ul style="list-style-type: none"> — COMMITTED WITH A FRAUDULENT, MALICIOUS OR DISHONEST INTENT; AND/OR — CONSTITUTING INTENTIONAL, FRAUDULENT, TORTIOUS AND/OR CRIMINAL MISCONDUCT; AND/OR — WHETHER THESE FACTS OR ACTS WERE COMMITTED BY YOU, A DIRECTOR OR BY YOUR OFFICIALS AND, IN THE LATTER CASE, PROVIDED THEY HAVE BEEN COMMITTED ON INSTRUCTIONS FROM YOU OR THAT OF A DIRECTOR, OR WERE ALLOWED TO HAPPEN BY YOU OR BY AN ADMINISTRATOR. |
| 4. Claims brought by a related party | ANY CLAIM MADE BY A POLICYHOLDER AGAINST ANOTHER POLICYHOLDER . |
| 5. Material damage and bodily injury | <p>ANY CONSEQUENTIAL NON-MATERIAL OR MATERIAL DAMAGE OR BODILY INJURY SUFFERED OR CAUSED BY YOU.</p> <p><i>This exclusion does not apply to material damage that you suffer under the 'Perishable foodstuffs' or 'Computer equipment' cover listed in Part 2.2 'First party' and in connection with the 'Cyber fraud' cover listed in Part 2.4 as it relates to physical goods. In addition, this exclusion does not apply to psychological or mental harm alleged by a third party natural persons or by officials following a breach of personal data.</i></p> |
| 6. Patents and 'trade secrets' | <p>CLAIMS RESULTING FROM ANY ACTUAL OR ALLEGED INFRINGEMENT:</p> <ul style="list-style-type: none"> — OF PATENTS; AND/OR — TRADE SECRETS, IF THE INFRINGEMENT IS IDENTIFIED IN THE USA OR IN CANADA. |
| 7. Games of chance | CLAIMS RESULTING FROM THE OPERATION OF GAMES OF CHANCE OR CASINO OR BETTING GAMES. |
| 8. Dealings in financial securities | <p>CLAIMS RESULTING FROM:</p> <ul style="list-style-type: none"> I) ANY TRANSFER, ACQUISITION, ISSUE, REDEMPTION OR NEGOTIATION OF SHARES, BONDS, COMPANY SHARES OR RECEIVABLES AND MORE GENERALLY ANY TRANSACTION INVOLVING FINANCIAL SECURITIES; <i>This exclusion does not apply to the 'Infringement of third-party confidential data' cover referred to in Part 2.3 above.</i> II) IN CONNECTION WITH THE 'CYBER FRAUD' COVER (PART 2.4), ANY SPECULATIVE OPERATION OR TRANSACTION CARRIED OUT IN A MARKET AND RELATING TO ANY SECURITY, COMMODITY, FUTURE, OPTION OR FOREIGN CURRENCY. |
| 9. Securities, financial, accounting and tax regulations | <p>CLAIMS RESULTING FROM ANY BREACH BY YOU, WHETHER ACTUAL OR ALLEGED, OF ANY SECURITIES, FINANCIAL, ACCOUNTING AND/OR TAX LEGISLATION AND/OR REGULATIONS.</p> <p><i>This exclusion does not apply to the 'Infringement of third-party confidential data' cover referred to in Part 2.3 above.</i></p> |
| 10. Insolvency proceedings | CLAIMS RESULTING FROM INSOLVENCY STATUS AND/OR THE INITIATION OF INSOLVENCY PROCEEDINGS AFFECTING YOU OR AFFECTING ONE OF YOUR BUSINESS PARTNERS . |

11. Fines, penalties and sanctions

FINES, CHARGES, TAXES, PENALTIES AND/OR ANY OTHER FINANCIAL PENALTIES IMPOSED ON **YOU** BY ANY LEGISLATION, ANY REGULATIONS, ANY CONTRACT, ANY TRANSACTION AND/OR ANY ARBITRATION, ADMINISTRATIVE OR JUDICIAL DECISION, INCLUDING 'PUNITIVE DAMAGES', 'EXEMPLARY DAMAGES', 'LIQUIDATED DAMAGES' AND PROVISIONS IN CRIMINAL LAW.

This exclusion does not apply to the 'investigations and penalties' cover referred to in part 2.2, Section ii above, provided the sums are legally insurable under the governing law.

12. Personal and confidential data of citizens of the USA and Canada and 'Trade secrets' in the USA or Canada

CLAIMS RESULTING FROM ANY ACTUAL OR ALLEGED INFRINGEMENT OF THE PROTECTION OF THE **CONFIDENTIAL** AND **PERSONAL DATA** OF CITIZENS OF THE USA AND CANADA AND OF TRADE SECRETS IDENTIFIED IN THE USA OR CANADA.

13. Orders from public authorities

CLAIMS RESULTING FROM THE ENFORCEMENT OF ORDERS FROM PUBLIC AUTHORITIES SUCH AS DEEDS OF NATIONALISATION, CONFISCATION, REQUISITION, COMPULSORY PURCHASE, APPROPRIATION, SEIZURE OR DESTRUCTION OF PROPERTY.

14. Warfare and Cyber operations

CLAIMS OF ANY KIND DIRECTLY OR INDIRECTLY RESULTING FROM, CAUSED BY, RESULTING FROM, OCCURRING DURING OR AS A CONSEQUENCE OF:

1. A WAR OR **CYBER OPERATIONS** CONDUCTED AS PART OF A WAR; AND/OR
2. **CYBER OPERATIONS** AS REPRISALS BETWEEN **SPECIFIED STATES** LEADING TO TWO OR MORE **SPECIFIED STATES** BECOMING **IMPACTED STATES**; AND/OR
3. **CYBER OPERATIONS** THAT HAVE A MAJOR HARMFUL IMPACT ON:
 - HOW A **STATE** OPERATES, DUE TO THE DIRECT OR INDIRECT EFFECT OF THE **CYBER OPERATIONS** ON THE AVAILABILITY, INTEGRITY OR PROVISION OF AN **ESSENTIAL SERVICE** OR OF **ESSENTIAL SERVICES** IN THAT **STATE**; AND/OR
 - THE SECURITY OF DEFENCE OF A **STATE**.

PARAGRAPH 3 DOES NOT APPLY TO THE DIRECT OR INDIRECT EFFECT OF **CYBER OPERATIONS** ON AN **INFECTED COMPUTER SYSTEM**.

THE FOLLOWING DEFINITIONS APPLY EXCLUSIVELY TO THIS EXCLUSION:

CYBER OPERATIONS

USE OF A **COMPUTER SYSTEM** BY OR ON BEHALF OF A STATE TO DISRUPT, PREVENT ACCESS, DEGRADE, MANIPULATE OR DESTROY INFORMATION ON A **COMPUTER SYSTEM** OF ANOTHER **STATE**.

STATE

MEANS A SOVEREIGN **STATE**.

IMPACTED STATE

IMPACTED STATE MEANS ANY **STATE** WHERE **CYBER OPERATIONS** HAVE HAD A MAJOR ADVERSE IMPACT ON:

- l) HOW THAT **STATE** OPERATES, DUE TO THE DIRECT OR INDIRECT EFFECT OF THE **CYBER OPERATIONS** ON THE AVAILABILITY, INTEGRITY OR PROVISION OF AN **ESSENTIAL SERVICE** IN THAT **STATE**; AND/OR
- l) THE SECURITY OF DEFENCE OF THAT **STATE**.

SPECIFIED STATES

THE **SPECIFIED STATES** ARE CHINA, FRANCE, GERMANY, JAPAN, RUSSIA, THE UNITED KINGDOM AND THE UNITED STATES.

ESSENTIAL SERVICE

REFERS TO A SERVICE THAT IS ESSENTIAL TO MAINTAINING THE VITAL FUNCTIONS OF A **STATE**, INCLUDING ITS FINANCIAL INSTITUTIONS AND THE ASSOCIATED FINANCIAL MARKET INFRASTRUCTURE, HEALTH SERVICES OR PUBLIC SERVICES.

COMPUTER SYSTEM

MEANS ANY COMPUTER, EQUIPMENT, SOFTWARE, COMMUNICATION SYSTEM, ELECTRONIC DEVICE, INCLUDING BUT NOT LIMITED TO SMARTPHONES, LAPTOPS, TABLETS (AND OTHER PORTABLE COMPUTING DEVICES), A SERVER, CLOUD INFRASTRUCTURE OR A MICROCONTROLLER, INCLUDING ANY SIMILAR SYSTEM OR ANY CONFIGURATION OF THE FOREGOING COMPONENTS, AND INCLUDING ANY ASSOCIATED INPUT, OUTPUT, DATA STORAGE DEVICE, NETWORK EQUIPMENT OR ASSOCIATED BACKUP FACILITY.

INFECTED COMPUTER SYSTEM

MEANS A **COMPUTER SYSTEM** USED BY THE POLICYHOLDER OR THEIR **THIRD-PARTY** SERVICE PROVIDERS THAT IS NOT PHYSICALLY LOCATED IN AN **IMPACTED STATE** BUT WHICH IS AFFECTED BY **CYBER OPERATIONS**.

15. Natural events

CLAIMS RESULTING FROM NATURAL EVENTS SUCH AS EARTHQUAKES, VOLCANIC ERUPTIONS, TIDAL WAVES, FLOODING, MAGNETIC POLE REVERSAL, STORMS INCLUDING SOLAR STORMS, SNOW AND HAIL.

16. Nuclear

CLAIMS RESULTING:

- I) FROM ANY TYPE OF NUCLEAR MATERIAL, REACTION OR RADIATION OR FROM ANY RADIOACTIVE CONTAMINATION; OR
- II) FROM ANY SERVICE PROVISION AND/OR SUPPLY OF GOODS THAT INCLUDES, REQUIRES OR WHICH IN ANY WAY RELATES TO WHAT IS DESCRIBED IN (I) ABOVE OR TO THE STORAGE, RETENTION, TRANSFER OR DESTRUCTION OF WHAT IS DESCRIBED IN (I) ABOVE; OR
- III) ANY OPERATION PERFORMED ON A SITE OR IN A BUILDING IN WHICH A SERVICE AND/OR A GOOD DESCRIBED IN (I) AND (II) ABOVE IS CONTAINED/PROVIDED.

17. Electrical fields

CLAIMS RESULTING FROM THE PRODUCTION, BY ANY DEVICE, OF ELECTRICAL OR MAGNETIC FIELDS, OR FROM ELECTROMAGNETIC OR IONISING RADIATION.

**18. Pollution/
contamination**

CLAIMS RESULTING FROM ANY FORM OF POLLUTION OR CONTAMINATION, AND ANY TYPE OF CHEMICAL, BIOLOGICAL OR BACTERIOLOGICAL REACTION OR CONTAMINATION.

19. Infrastructure failure

THE FAILURE, INTERRUPTION OR NON-PERFORMANCE OF SERVICES THAT ARE PROVIDED TO **YOU** BY AN INTERNET SERVICE PROVIDER, AN **IT SERVICE** PROVIDER, A TELECOMMUNICATIONS SERVICE PROVIDER, A PUBLIC UTILITIES PROVIDER OR OTHER INFRASTRUCTURE PROVIDER, UNLESS IT RELATES TO:

- A **BREACH OF PERSONAL DATA** INVOLVING DATA STORED IN THE CLOUD, ON REMOTE SERVERS OR STORED AT A COLOCATION CENTRE OR BY A DATA STORAGE SERVICE. IN THIS INSTANCE **WE** WILL NOT, HOWEVER, COVER **YOUR** OPERATING LOSSES (UNLESS OTHERWISE STATED IN THE SPECIAL CONDITIONS); OR
- A **COMPLAINT** BY THE PRINCIPAL WHEN **YOU YOURSELF** ARE AN INTERNET SERVICE PROVIDER, A TELECOMMUNICATIONS SERVICE PROVIDER, PUBLIC UTILITY PROVIDER OR OTHER INFRASTRUCTURE PROVIDER.

**20. Contractual
civil liability**

CLAIMS RESULTING FROM ANY ACTUAL OR ALLEGED BREACH OF **YOUR** CONTRACTUAL OBLIGATIONS, EXCEPT WHERE **YOU** WOULD HAVE BEEN LIABLE UNDER THE SAME CONDITIONS AND LIMITS IN THE ABSENCE OF CONTRACT.

*This exclusion does not apply to the 'Breach of **personal data** confidentiality and/or security' cover listed in Part 2.3.*

**21. Breach of
Professional Duty**

CLAIMS RESULTING FROM THE SUPPLY BY **YOU** OF PRODUCTS OR SERVICES.

*This exclusion does not apply to the 'Transmission of computer viruses and cyber attacks against **your computer systems**' cover (2.3 Third-party cover, Section I A.4. above).*

**22. Reimbursement for
services provided**

DAMAGES CORRESPONDING TO, OR EQUIVALENT TO, A REIMBURSEMENT, A REFUND OR REDUCTION IN THE PRICE OF **YOUR** SERVICES PAID OR PAYABLE BY **YOUR BUSINESS PARTNERS**.

23. Costs of data recovery	THE COSTS RELATING TO ANY DATA RECOVERY OPERATION THAT WOULD GO BEYOND RECOVERING THAT DATA FROM COMPUTER MEDIA, WHERE BACKUPS OF THAT DATA ARE NOT CARRIED OUT AT LEAST MONTHLY.
24. Direct payment of ransoms	THE INHERENT RISKS OR DAMAGES RESULTING FROM THE IMMEDIATE PAYMENT OF A RANSOM BEFORE ANY CLAIM DECLARED BY THE POLICYHOLDER .
25. Fraud committed by a corporate officer of the policyholder	<p>CLAIMS RESULTING FROM ANY FRAUD COMMITTED OR ABETTED BY:</p> <p>I) ANY MEMBER OF A MANAGEMENT BODY OR MEMBER RESPONSIBLE FOR DAY-TO-DAY MANAGEMENT;</p> <p>II) ANY PERSON WHO CONTROLS OR HAS CONTROLLED MORE THAN 10% OF THE CAPITAL OR VOTING RIGHTS OF THE POLICYHOLDER; AND/OR</p> <p>III) ANY PERSON WITH THE POWER TO FINANCIALLY COMMIT THE POLICYHOLDER BY THEIR SOLE SIGNATURE.</p>
26. Known history	CLAIMS RESULTING FROM ANY FRAUD COMMITTED OR ABETTED BY AN OFFICIAL WHOSE CRIMINAL RECORD WAS KNOWN TO THE POLICYHOLDER .
27. Strikes & industrial disputes	THE INHERENT RISKS OR DAMAGES RESULTING FROM INDUSTRIAL DISPUTES, STRIKES OR LOCK-OUTS.
28. Chargeback	<p>CLAIMS RESULTING FROM ANY CHARGEBACK TO YOU BY A BANKING INSTITUTION OR PAYMENT PROCESSOR, DUE TO THE PARTIAL OR TOTAL NON-FULFILMENT OF A FRAUDULENT TRANSACTION.</p> <p><i>This exclusion does not apply when the transaction follows a breach of personal data held by you or on your behalf.</i></p>
29. Misappropriation of funds	<p>CLAIMS RESULTING:</p> <p>I) FROM ANY MISAPPROPRIATION OR THEFT OF FUNDS, FINANCIAL SECURITIES OR PROPERTY; OR</p> <p>II) FROM ANY LOSS OR ANY TRANSFER OF FUNDS OR FINANCIAL SECURITIES FROM OR TO ACCOUNTS BELONGING TO OR CONTROLLED BY THE POLICYHOLDER, INCLUDING THE ACCOUNTS OF THEIR CUSTOMERS.</p> <p><i>This exclusion does not apply to the 'Cyber fraud' cover referred to in Part 2.4 above.</i></p>
30. Wrongful collection and use of personal data	<p>THE INHERENT RISKS OR DAMAGES RESULTING FROM INFRINGEMENT OF THE STATUTORY OR REGULATORY PROVISIONS RELATING TO DATA PROTECTION, INFRINGEMENT MADE WITH THE KNOWLEDGE, AND/OR ON THE INSTRUCTIONS OF, A DIRECTOR AND/OR FOLLOWING THE LATTER'S NEGLIGENCE, IN CONNECTION WITH:</p> <p>— THE COLLECTION AND PROCESSING OF PERSONAL DATA BY YOU, OR BY ANYONE ACTING ON YOUR BEHALF WITHOUT HAVING FIRST OBTAINED SUFFICIENT CONSENT UNDER THE STATUTORY OR REGULATORY FRAMEWORK;</p> <p>— SENDING COMMERCIAL AND/OR MARKETING COMMUNICATIONS VIA EMAIL, TELEPHONE, FAX AND/OR AUTOMATED DIALERS BY YOU, OR BY ANYONE ACTING ON YOUR BEHALF, WITHOUT FIRST HAVING OBTAINED THE RECIPIENT'S CONSENT.</p>

Part 4 – Policy management and indemnification

I. Point at which the cover is activated and applied

1. The ‘first party’ cover provided for in Parts 2.2 and 2.4 of the **policy** are activated by the occurrence of an **insured event** arising from a covered **harmful event**. The cover will apply if this **insured event** occurs during the **period of insurance**, excluding the suspension of cover period.
2. Except where the **policy** is terminated due to non-payment of premiums, the ‘Third party’ cover provided for in Parts 2.3 and 2.4 above will be triggered by the occurrence of an **insured event** associated with a **complaint** by a **third party**. These two triggering factors for the cover must have occurred during the **period of insurance**.
The **complaint** must also have been notified to **you** in writing, or be addressed to **us** in writing, during the **period of insurance** and must be brought against **you** for the first time. Complaints made in writing against the **policyholder** or the **insurer** in a 36-month period as from the end of the **policy** are also covered, where they relate to:
 - an **insured event** that occurs during the **period of insurance** if, at the **policy**’s expiry, the risk is not covered by another insurer;
 - a **harmful event** that has occurred and been reported to the **insurer** during the **period of insurance**.
3. **We** will not cover the risk of prior claims.

II. Cover limit / Excess

The insurance cannot be a source of profit.

It only guarantees compensation for actual damages that you have suffered and/or for which you are legally liable.

We will indemnify **claims** covered by the cover set out in the second part of the **policy**, within the limits of the insured amounts specified in **your** Special Conditions (limits of cover), less the applicable **excess** provided for in **your** Special Conditions.

1. Unless otherwise specified in your Special Conditions, the **cover limit** is agreed per **claim** and per **period of insurance**.
It represents the maximum amount that **we** are likely to pay under this **policy**, across all cover, for all **policyholders** and for all **claims** within the **period of insurance** concerned. The cover limit is not cumulative from one **period of insurance** to the next (or over the period of subsequent cover granted under the ‘Third party’, ‘**Damage to third parties**’ cover in Part 2.3 of the **policy**), and will be reduced and exhausted by any payment of fees and/or indemnities that **we** would be required to pay under this **policy**, without automatic reimbursement.
If **your** Special Conditions stipulate cover **sub-limits**, these will form an integral part of the **cover limit** granted under this **policy**, rather than being added to it. The cover **sub-limits** work in the same way as the **cover limit**.
The **cover limit** applicable to the subsequent cover granted under the ‘Third party’ and ‘**Damage to third parties**’ cover in Part 2.3 of the **policy** will be unique for the duration of that period of subsequent cover, i.e. for the 36 months following termination or expiry of the **policy**. It is equal to the amount of the **cover limit** applicable to the last **period of insurance** before termination or expiry of the **policy**.
2. The **excess** represents the amount that remains payable by **you** for each **claim**. It is deducted from the **cover limit**.
The Special Conditions may stipulate different **excess** amounts depending on the cover activated.
3. Please note that where a **claim** impacts several areas of insurance cover, the highest **excess** is one applied.

III. Aggregation of claims

Whatever the cover involved, all **damage** resulting from a single **harmful event** will be treated as a single **claim**.

All these **damages** will, on an aggregate basis, be exclusively linked to the **period of insurance** during which the following have occurred:

- the first covered **harmful event** experienced by the **policyholder**, with regard to the cover forming part of the ‘First Party’ component provided for in Part 2.2 above;
- the first **complaint** made against the **policyholder**, with regard to the cover forming part of the ‘Third Party’ component provided for in Part 2.3 above.

IV. Multiple policyholders / multiple insurance policies

Where there are multiple **policyholders**, the amount of the costs and/or benefits that **we** will pay may not exceed the sum due for a single **policyholder**.

In the event of a **claim** indemnifiable by several insurance policies taken out with the **insurer** and/or with any other insurance company in the Hiscox group, the total amount of the insurance benefit that will be paid under all of these policies may not under any circumstances exceed the indemnification limit of the policy providing for the highest indemnification limit.

Part 5 – In the event of a claim

Section I Declaring a claim

Any **claim** must be declared to **us** as soon as possible after **you** become aware of its occurrence, and always within 72 hours thereof.

IN THE EVENT OF FAILURE TO DECLARE, OR A DELAY IN DECLARING THE **CLAIM** NOT ATTRIBUTABLE TO AN UNFORESEEN EVENT OR FORCE MAJEURE, IF IT RESULTS IN A LOSS ON **OUR** PART, **WE** RESERVE THE RIGHT TO REDUCE **OUR** BENEFIT UP TO THE AMOUNT OF THE LOSS INCURRED, OR TO REFUSE **OUR** COVER IF **YOU** HAVE FAILED TO PERFORM **YOUR** OBLIGATION WITH FRAUDULENT INTENT.

You can declare the claim to us:

- by letter sent to:
Hiscox Belgium
Claims Department
Avenue du Bourget 42 bte 8
Airport Building
1130 Brussels
- or by email to: hiscox.claims@hiscox.be

To enable **your** case to be processed quickly, please send **us**, at the same time as your declaration of **claim**, the following information/documents:

- the number of **your** Hiscox **policy** appearing on **your** Special Conditions;
- a document written by **you** stating the causes and circumstances of the **claim** and, where applicable, the amount of any **damages** suffered;
- in the event of a **claim** under the 'Third Party' cover (Part 2.3), a copy of the **complaint** that **you** have received;
- any notice, letter, summons, invitation, and more broadly any judicial or extrajudicial act and procedural document that is sent to **you** or served on **you**;
- any information concerning any other insurance policy that may cover the same risk and that **you** may have taken out.

If the facts forming the object of the **claim** constitutes or are likely to constitute a criminal offence, **you** must file a complaint within 24 hours of the occurrence of such facts and send **us** a copy of the formal complaint **you** have filed when **you** declare the **claim**.

A hotline is available for **you** 24/7 as part of the '**Assistance**' cover of this **policy**.

Section II

Claims management

A. Duty to assist

After declaring the claim, in addition to your obligations under these Special Conditions, you are still required to provide us, at your own expense, with any assistance we request from you in connection with investigating and managing the case, and in particular:

- sending **us** any relevant information and/or documents and responding to requests sent to **you** to determine their circumstances and to determine the extent of the **claim**;
- allowing **us** and any expert and/or lawyer that **we** have appointed to carry out any on-site investigations and/or to meet any person **we** deem likely to provide **us** with useful information about the causes and circumstances of the **claim**;
- take any measures that **we** and **our** experts and/or lawyers deem relevant for defending the case, and/or to prevent the **claim** from occurring or to mitigate its effects, and/or to resolve it amicably.

IF YOU FAIL TO FULFIL **YOUR** DUTY TO ASSIST, IF THIS RESULTS IN A LOSS ON **OUR** PART, **WE** RESERVE THE RIGHT TO REDUCE **OUR** BENEFIT TO THE EXTENT OF THE LOSS SUFFERED OR TO REFUSE **OUR** COVER IF **YOU** HAVE FAILED TO PERFORM **YOUR** OBLIGATION WITH FRAUDULENT INTENT.

B. Choice of providers

As part of the **Assistance** cover, the 'own service' component and the costs of defence, and subject to the provisions of paragraph C below, **you** have free choice in appointing a lawyer, an IT security expert or crisis communications consultant outside **our** panel, provided they offer sufficient guarantees in terms of skills, given the specific nature of the **claim**, and provided they have been approved by **us**.

C. Supervision of the dispute

With regard to civil interests, and to the extent that the interests of the **insurer** and of the **policyholder** coincide, **we** have the right to take over supervision of the case, namely:

- to conduct negotiations on **your** behalf with a view to the amicable settlement of the **claim**, and to decide on the conditions of that amicable settlement;
- to manage **your** defence as part of any arbitration, administrative or civil judicial proceedings.

If **we** deem it necessary, **we** may appoint an expert and/or lawyer of **our** choice. **We** may, but are not obliged to, appoint the lawyer chosen by the **policyholder** in accordance with the provisions of paragraph B above.

D. Retrieval costs

It is **your** responsibility to take any measures requested by **us**, or any urgent and reasonable measures taken at **your** initiative to prevent or mitigate the effects of an existing or imminent **claim**.

We will indemnify **you** for retrieval costs incurred in connection with an **insured event**.

For civil liability insurance, these retrieval costs will be borne entirely by the **insurer**, provided the total compensation and retrieval costs do not exceed, per policyholder and per **claim**, the total sum insured. Beyond the total sum insured, retrieval costs may be limited to:

1. EUR 495,787.05, where the total sum insured is less than or equal to EUR 2,478,935.25;
2. EUR 495,787.05 plus 20% of the portion of the total sum insured between EUR 2,478,935.25 and EUR 12,394,676.24;
3. EUR 2,478,935.25 plus 10% of the portion of the total sum insured that exceeds EUR 12,394,676.24, with a maximum of EUR 9,915,741 in retrieval costs. For property insurance, retrieval costs are equal to the **sum insured**, up to a maximum of EUR 18,592,014.36.

These amounts are linked to changes in the consumer price index, the base index being that of November 1992, i.e. 113.77 (1988 base = 100).

IF **YOU** FAIL TO COMPLY WITH **YOUR** OBLIGATION TO IMPLEMENT THE NECESSARY RETRIEVAL MEASURES, **YOU** ARE LIABLE TO LOSE **YOUR** ENTITLEMENT TO COVER IF THIS FAILURE HAS CAUSED **US** HARM.

E. Legal, judicial and extrajudicial costs and interests

Legal, judicial and extrajudicial costs and interests that **you** must pay to a **third party** are included in **our** cover under the conditions of section 2.3 'Third-party cover (**Damage to third parties**)' above.

If the amount **you** are required to pay to a **third party** in connection with a **complaint** exceeds the **sum insured** per **claim** and/or is only partly covered, the costs and interests will only be paid in proportion to the **sum insured** per **claim**, or in proportion to the amount payable by **you** to the **third party**.

The costs and interests will be paid in full by **us**, provided the total compensation and interests and costs do not exceed, per policyholder and per **claim**, the total sum insured. However, beyond the total sum insured, the costs and interest may be limited to:

1. EUR 495,787.05, where the total sum insured is less than or equal to EUR 478,935.25;
2. EUR 495,787.05 plus 20% of the portion of the total sum insured between EUR 2,478,935.25 and EUR 12,394,676.24;
3. EUR 2,478,935.25 plus 10% of the portion of the total sum insured that exceeds EUR 12,934,676.24, with a maximum of EUR 9,915,741 in costs and interest.

These amounts are linked to changes in the consumer price index, the base index being that of November 1992, i.e. 113.77 (1988 base = 100).

F. Settlement / Recognition of liability

If **you** are approached by the **third party** seeking amicable settlement of the **claim**, **you** must inform **us** immediately. Similarly, **we** must be consulted before any proposed amicable settlement that **you** envisage reaching.

In addition, **you** must not at any time acknowledge **your** liability for the **claim**, whether verbally or in writing.

ANY RECOGNITION OF LIABILITY AND/OR SETTLEMENT WITHOUT **OUR** PRESENCE IS NOT BINDING ON **US**.

In the event that a proposal for a settlement of a **claim** is made to **you/us** and which we wish to accept, but which you reject, **our** cover will then be limited to the settlement of **your** costs incurred up to the date of rejection or expiry of the settlement offer, as well as payment of the excess deducted from a benefit that may not exceed the amount of the rejected or expired settlement offer. In the event of direct action by the third party against us, we may request that you reimburse the sum that we have been required to pay to that third party beyond the amount of the rejected or expired settlement offer.

G. Specific right of the injured party and subrogation of the insurer

We are entitled to pay a benefit directly to the injured party on **your** behalf, or to reach an amicable settlement with them. **Claims** by injured parties for indemnification for **bodily injury** may be processed in accordance with Article 150 of the law of 4 April 2014 on insurance (specific right of the injured party).

If the **insurer** exercises the entitlement described above, by paying the injured party on behalf of the **policyholder**, the **insurer** will have fulfilled their obligations under this **policy**. **We** are subrogated in all **your** rights and actions against any liable **third party** for up to the full amount of the sums **we** have paid under this **policy**, including the costs incurred in **your** defence.

As a result, all sums allocated to **you** by any court of arbitration, administrative or judicial court, or in relation to the costs incurred in **your** defence, will automatically be retained by **us**.

In addition, if the **claim** is attributable to a **third party**, **you** must always preserve any legal recourse **we** may exercise against them, for example by providing **us**, at **your** expense, with any **assistance** that **we** request from **you**, for example by giving **us your** help to initiate the necessary proceedings.

IF **YOUR** ACTIONS PREVENT THE SUBROGATION FROM BEING MADE IN **OUR** FAVOUR, **WE** MAY CLAIM REPAYMENT FROM **YOU** OF THE BENEFIT PAID TO THE EXTENT OF **OUR** LOSS INCURRED (ARTICLE 95 OF THE LAW ON INSURANCE).

Part 6 – Policy administration

Section I Mandatory declarations

A. Key principles

This **policy** is drawn up based on **your** declarations, for the purposes of when the **policy** is first taken out, as well as during its performance, and the premium is set accordingly.

All of these declarations form an integral part of the **policy**.

ANY INTENTIONAL MISREPRESENTATION, ANY RETICENCE, OMISSION OR INTENTIONAL INACCURACY IN THE DECLARATIONS AND ANY FRAUDULENT DECLARATION, RETICENCE, OMISSION OR INACCURACY MAY INVALIDATE THE **POLICY**. THE PREMIUMS DUE UP TO THE TIME **WE** BECOME AWARE OF THE INTENTIONAL OMISSION OR INACCURACY ARE DUE TO **US**. WHERE THE OMISSION OR INACCURACY IN THE DECLARATION IS NOT INTENTIONAL, **WE** MAY TERMINATE THE POLICY WITHIN ONE MONTH AS FROM THE DAY ON WHICH WE BECAME AWARE OF THE OMISSION OR INACCURACY, IF **WE** WOULD NOT OTHERWISE HAVE INSURED THE RISK.

IF THE UNINTENTIONAL INACCURATE DECLARATION OR OMISSION CAN BE ATTRIBUTABLE TO **YOU** AND IF A **CLAIM** ARISES BEFORE THE POLICY IS AMENDED, OR BEFORE TERMINATION HAS TAKEN EFFECT, **WE** ARE ONLY REQUIRED TO PROVIDE A BENEFIT BASED ON THE DIFFERENCE BETWEEN THE PREMIUM PAID AND THE PREMIUM THAT **YOU** SHOULD HAVE PAID IF **YOU** HAD PROPERLY DECLARED THE RISK.

HOWEVER, IF IN THE EVENT OF A **CLAIM**, **WE** PROVIDE EVIDENCE THAT **WE** WOULD NEVER HAVE INSURED THE RISK, **OUR** BENEFIT IS LIMITED TO REIMBURSING ALL OF THE PREMIUMS PAID.

B. Multiple insurance policies

If **you** take out insurance policies with several insurers covering the same risks, **you** must inform each insurer of this. In the event of a **claim**, **we** have the right to reduce the sum insured in accordance with Articles 96 and 99 of the law on insurance.

FRAUDULENTLY OR DISHONESTLY TAKING OUT SEVERAL INSURANCE POLICIES FOR THE SAME PURPOSE AND AGAINST THE SAME RISK WILL RENDER THE **POLICY** NULL AND VOID. IN THIS INSTANCE, **WE** HAVE THE RIGHT TO RETAIN THE PREMIUMS COLLECTED AS COMPENSATION.

C. Change in risk during the period of insurance

Any new circumstances occurring during the **policy's** performance and rendering the declarations of risk made before taking out the **policy** inaccurate or obsolete must be notified to **us** by registered letter within **15 days** of the time that **you** become aware of them.

IN THE EVENT OF A DELAY IN DECLARING THIS NEW CIRCUMSTANCE TO **US**, WITH FRAUDULENT INTENT, **YOU** RISK BEING FULLY OR PARTIALLY DEPRIVED OF **YOUR** RIGHT TO COVER IF THIS FAILURE HAS CAUSED **US** LOSSES.

If the new circumstances that **you** declare to **us** constitute aggravation of risk (Article 81 of the law on insurance), **we** may, beyond any **claim** being made:

- within 30 days as from the day **we** became aware of the aggravation of risk, propose an amendment to the **policy** with retroactive effect backdated to the date of aggravation if the risk of the insured event occurring has increased in such a way that, if the aggravation had existed at the time of taking out the **policy**, **we** would only have agreed to the insurance under different conditions;
- within 30 days as from the day **we** become aware of the aggravated risk, terminate the **policy** if **we** provide evidence that we would never have **insured** the aggravated risk. In this scenario, if **you** do not respond to **our** proposal within 30 days, or if **you** reject it, **we** may automatically terminate this **policy** within 15 days of expiry of the aforesaid period.

If a **claim** arises and where **you** have not fulfilled **your** notification obligation:

- a) **we** will be required to give effect to the agreed benefit where the failure to declare cannot be attributed to **you**;
- b) **we** will only be required to give effect to **our** benefit based on the difference between the premium paid and the premium that **you** should have paid if the increased risk had been taken into consideration, where failure to declare can be attributed to **you**. However, if in this scenario **we** provide evidence that **we** would never have insured the increased risk, our benefit in the event of a **claim** is limited to reimbursing all of the premiums paid;
- c) if **you** have acted with fraudulent intent, **we** may refuse our cover. The premiums due up to the time that **we** become aware of the fraud are due to **us** as compensation.

If the risk is reduced (Article 80 of the law on insurance), **you** have the option of asking **us** to reduce the amount of the premium. If **we** cannot reach an agreement on the new premium amount within 30 days of **your** request for a reduction, **you** may terminate this **policy**.

Section II Determining and paying out the premium

The premium is determined by the year insured on the basis of specific factors such as the **activities** of the company, turnover, quantity of data and the level of security of data and systems. If **we** do not ask **you** for data, or if **you** do not report changes in risk, the current premium will also be valid for the first year following the year insured.

We are entitled but not obliged to ask **you** in writing, three months before the end of the year insured, to provide the necessary information to determine the premium for the next year insured. **You** are required to provide **us** with this information.

You are also required to provide, at **our** request, a declaration from a company auditor concerning the information submitted. The initial premium must be paid by **you** as from the effective date specified in the **policy**. The renewal premiums must be paid by **you** on the effective date of a new year insured.

The premium must be paid by **you** within 30 days of it becoming due. If **you** do not comply with this obligation to pay the premiums and costs, **we** will suspend our cover.

The suspension of cover may only, however, take place after the premium's due date, and only where **you**:

- have been given formal notice by bailiff's writ or by registered letter within 15 days of the day after notification or the day after depositing the registered letter with no response;
- the formal notification states the due date of the premium, the amount of the premium and the consequences, including the possibility of suspending and terminating the **policy** by the insurer, of failure to pay the premium within the stipulated period, and when that period begins. The suspension of cover or termination of the **policy** will take effect from the day after the date when that period ends, without prejudice to cover relating to **damage** that arose previously.

We will not provide cover for **claims** that arose during the suspension of cover period, even if they were notified after that period. From the day after the date when the premium is received by us, the insurance cover will be reinstated for the remaining year insured in respect of **claims** that are made and identified after that date. In this context, **we** deem premium to also mean costs and any insurance taxes.

Section III

How the policy works

A. Effective date, Renewal and Termination

The **policy** will take effect at 00:00 on the first effective date and only as from the date of payment of the first premium. It will remain in effect for the entire **period of insurance**, as indicated in the Special Conditions, not exceeding one year. At the end of the **period of insurance**, the **policy** will be tacitly renewed for the same **period of insurance** of a maximum of one year, with its conditions and premium unchanged, unless terminated in accordance with the conditions stipulated in the policy and otherwise provided for.

The **policy** may be terminated by **you** at the end of its annual term by registered letter or by bailiff's writ, or by delivery of a letter of termination against receipt. The termination will only take effect subject to a three-month notice period as from the day after notification of the letter of termination or, in the case of a registered letter, as from the day after it is filed.

If the **policy** is terminated, **you** have the right to reimbursement of the premium for the period in which this **policy** is no longer in effect.

The **policy** may be terminated by **us** and by **you** at the end of its annual term, or no later than one month after payment or refusal to pay a benefit after a **claim**.

The termination will only take effect after the end of a three-month period as from the day after its notification, or the day after the date of receipt or, in the case of a registered letter, as from the day after it is filed.

Failure to pay the premium when due may give rise to suspension of the cover or termination of the contract. If **we** terminate or suspend the **policy**, this will take effect at the end of a 15-day period as from the day after notification, or the day after filing the registered letter of formal notification.

We will also terminate the **policy** if you have breached any of the obligations arising from the claim arising with the intention of deceiving **us**. **We** may nevertheless terminate the **policy** as soon as **we** have filed a complaint with civil action before an investigating judge or after a summons before the trial court on the basis of Sections 193, 196, 197, 496 or 510 to 520 of the Criminal Code. The termination will take effect, at the earliest, one month from the day after notification, the day after the date of the receipt, or the day after the date the registered letter was filed.

We will reimburse **you** the amount of premiums on a pro-rata basis, unless **we** have agreed to cover a **claim** before termination becomes applicable

B. Non-transferable nature of the policy

This **policy**, and any claim or interest arising from it, may not be transferred without **our** prior written agreement.

C. Valid communications

All communications between the **policyholder** and the **insurer** may be validly made to the insurance intermediary. Communications from the **insurer** are also valid where they are sent to the last address indicated by the **policyholder** or made via the insurance intermediary.

D. Territory of cover and jurisdiction

This **policy** provides cover for the company's **activities** conducted within the countries listed in the 'territory of cover' clause in the Special Conditions.

The condition for **complaints** by **third parties** to be covered is that the governing law is that of one or more countries referred to under the '*jurisdiction*' clause in the Special Conditions.

This also includes proceedings that have been brought within the territory of cover and where the proceedings are based on a decision or on case-law or brought in the context of enforcing a ruling from a court other than the courts referred to in the Special Conditions under the '*jurisdiction*' section.

E. Governing law

The performance and validity of this **policy** are subject to Belgian law.

F. Disputes

The **policyholder** and the **insurer** will do everything possible to attempt to settle disputes arising from this **policy**. Any disputes relating to this policy will be referred to the competent court in Belgium.

Any dispute relating to this **policy**, including any dispute relating to its validity or its interpretation, will fall under the sole jurisdiction of the Belgian courts with territorial competence.

Any complaint or claim under the contract can be addressed to Avenue Bourget 42 B8, Building Airport, B-1130 Belgium, 02 788 26 00, Hiscox.info@hiscox.be.

In addition, **you** may send **your** complaint to the Insurance Ombudsman at Square de Meeûs 35, 1000 Brussels (info@ombudsman.as) without prejudice to your right to take legal action.

G. Financial penalties

ALL COVER GRANTED UNDER THIS **POLICY** WILL HAVE NO EFFECT WHERE THIS COVER, THE ADMINISTRATION OF THE CONTRACT, PAYMENT OF THE BENEFIT AND/OR ANY **ACTIVITY** ARE CONTRARY TO ANY STATUTORY OR REGULATORY PROVISION ON FINANCIAL OR COMMERCIAL PENALTIES PROVIDED FOR BY THE UNITED NATIONS, THE EUROPEAN UNION, BELGIUM AND/OR ANY OTHER **STATE** (INCLUDING THE UNITED STATES).

CLAIMS DIRECTLY OR INDIRECTLY **LINKED** TO SUCH AN INFRINGEMENT, OR WHICH MAY CAUSE SUCH AN INFRINGEMENT, WHERE **WE** MANAGE THE **CLAIM**, ARE EXCLUDED FROM THE COVER.

H. Protection of personal data

HISCOX is the trading name of several companies in the HISCOX group. The company, acting as data controller for your personal data is indicated on the documentation provided to you. If you have any queries or questions, **you** can also contact **us** at any time by telephone on 0032 2 788 26 00, or by sending **us** an email to DataProtectionOfficer@hiscox.com.

We collect and process **your** information for the purposes of offering and providing insurance policies and handling **your** claims. **Your** data is also used for commercial purposes, such as fraud detection and prevention and financial management. This may mean Hiscox has to share **your** information with companies within the group and third parties such as brokers, experts, credit reporting agencies, service providers, professional advisors, our supervisors and fraud prevention agencies. **Your** telephone calls may also be recorded, to help **us** monitor and improve **our** services.

For more information on how **your** data is used, and your rights regarding **your** data, please consult our privacy statement on **our** website: www.hiscox.be.

I. Registered address and Correspondence

Any correspondence or notification addressed to **us** will be deemed validly made if it is sent:

- to **our** address in Belgium, as indicated in the Special Conditions or by subsequent addendum;
- to the address of **your** broker, as indicated in the Special Conditions or by subsequent addendum.

Any correspondence or notification sent to **you** will be deemed validly made, including to your heirs or legal claimants if it is sent to **your** address as indicated in the Special Conditions or by subsequent addendum.

