# CyberQuick

## General Conditions of Cyber Insurance

DK 2024.08

**Contents** **Page:**


1 Cover for liability claims and other specified claims made by third parties ..... 3
2 Cover for own losses ..... 3
3 Cover for business interruption/loss of income ..... 6
4 General exclusions ..... 7
5 General conditions and claims conditions ..... 10
6 Definitions ..... 13
7 Complaints procedure ..... 18
8 GDPR Privacy Notice ..... 18

# 1 Cover for liability claims and other specified claims made by third parties

## 1.1 Information security breach

This policy covers the **insured companies** or **additional insured persons** against a **third-party claim** during the **policy period** for **financial loss** arising from an **information security breach** occurring after the inception of the insurance.

## 1.2 Defence of data protection proceedings; reimbursement of administrative fines resulting from a data protection breach

This policy covers the defence of civil or administrative investigations or proceedings, brought before national courts, data protection authorities or equivalent EU GDPR or data privacy regulator, against **insured companies** or **additional insured persons** due to **data protection breaches**.

A condition precedent for such cover is that the **data protection breach** must have occurred, and the civil or administrative investigation or proceedings must also have been initiated during the **policy period**.

This policy shall cover any liability to pay a fine imposed upon **insured companies** or **additional insured persons** by national courts or data protection authorities, as a result of **data protection breaches**, subject to such cover being legally permissible.

## 1.3 Indemnity payments

The cover under Section 1 encompasses assessment of liability, the defence costs and covered **third party claims**. Unless otherwise agreed, the insurer shall be under an obligation to defend **third party claims** within the deductible specified in the policy schedule.

Admissions and settlements that the **insured company** or an **additional insured person** has made without the prior approval of the insurer shall only be binding on the insurer insofar as the **third-party claim** would have been sustained in the absence of an admission or settlement.

The insurer is authorised to take all reasonable steps in the handling or defence or settlement of a covered **third-party claim** including in the conduct of any proceedings in respect of such **third-party claim**.

# 2 Cover for own losses

## 2.1 Insurance cover

Cover is provided pursuant to Sections 2.1.1 to 2.1.6 for the reimbursement of reasonable and necessary costs and expenditure incurred by an **insured company** arising from an insured event during the **policy period** in connection with the services specified.

### 2.1.1 Forensic investigations

In the event of an **information security breach** first discovered during the **policy period** by an **insured company** or an **additional insured person**, cover is provided for reasonable and necessary costs and expenditure incurred by a consultancy firm named in the policy schedule for forensic investigations, to determine how the **information security breach** was caused and to make recommendations to prevent or respond to **information security breaches** of this kind.

Expenditure for determining whether **data** and **software** that were located in **IT systems** can be recovered shall solely be insured under Section 2.3.

### 2.1.2 Data protection notification

In the event of a **data protection breach** first discovered during the **policy period** by an **insured company** or an **additional insured person**, cover is provided for reasonable and necessary costs and expenditure incurred by **insured companies** to notify the competent data protection authorities and the affected parties, if there is an obligation under **data protection law** to notify them.

Costs and expenditure in connection with the appointment of external service providers, such as call centres/hotlines, shall be reimbursed, provided that their appointment is required to ensure the proper and timely compliance under **data protection law** to notify the parties affected and the insurer has approved their appointment.

The cover also includes reasonable and necessary legal advice in connection with the notification of the competent data protection authorities and the parties affected.

### 2.1.3 Public relations crisis management

In the event of an actual or suspected **information security breach** suffered and first discovered during the **policy period** by **insured companies** or an **additional insured person** is reasonably expected to result in **insured companies** or **additional insured persons** suffering reputational damage, cover is provided for:

- the reasonable and necessary costs and expenditure of the consultancy firm named in the policy schedule or of a firm that an **insured company**, with the prior agreement of the insurer, appoints to prepare and execute a public relations crisis strategy, to uphold or restore its reputation;
- for the reasonable and necessary costs and expenditure for the placing of corresponding notices, representations and advertisements in the media in the context of the public relations crisis strategy, provided that such measures have been agreed in advance with the public relations consultancy firm and the insurer;
- for reasonable and necessary legal advice on the public relations crisis strategy.

Cover shall be provided for costs and expenditure incurred in the six months after the onset of the **information security breach** or, if later, its discovery by the **insured company**.

### 2.1.4 Identity and credit monitoring services

In the event of an **information security breach** suffered and first discovered during the **policy period** by **insured companies** or an **additional insured person** that contains **personal data** which is subject to confidentiality, cover is provided for the reasonable and necessary costs and expenditure for monitoring services to protect the individuals against the misuse of **personal data** and for verification purposes and notification in the event of identity theft, and credit monitoring.

Cover is to be provided for monitoring services:

- where the **insured company** is under an obligation under **data protection law**, reasonably required, or subject to a direction from the competent data protection authority, to provide such service; and
- within a period of twelve months from the time at which the **information security breach** was first discovered.

### 2.1.5 Cyber extortion management

In the event of a **cyber threat** suffered and first discovered by an **insured company** or an **additional insured person** during the **policy period**, the insurer shall reimburse the reasonable and necessary costs and expenditure of the consultancy firm named in the policy schedule, or of another independent company appointed with the prior approval of the insurer, that are incurred for the duration of the **cyber threat** to prevent or mitigate a claim or loss arising from an **information security breach**.

The **insured companies** shall:

- immediately inform the insurer and the consultancy firm named in the policy schedule of the **cyber threat** and provide relevant information and documents; and
- notify the police or similar authorities of the **cyber threat** and authorise the consultancy firm named in the policy schedule to pass on relevant information and documents; and
- keep the insurer and the consultancy firm named in the policy schedule fully and promptly informed with regard to all developments relating to the **cyber threat**.

### 2.1.6 Cyber threat

In the event of a **cyber threat** first discovered by an **insured company** or an **additional insured person** during the **policy period** (insured event), insurance cover shall be provided for the reimbursement of the costs and expenditure listed below.

### 2.1.6.1 Indemnities

**a) Indemnities in accordance with Sections 1 to 3 in connection with cyber threats**

The insurance cover shall include indemnities by the insurer in accordance with any other coverage module in connection with a **cyber threat** or with the underlying **information security breach** specified in any other coverage module. Any other coverage module within the meaning of this Section shall refer to Sections 1 to 3 except for Sections 2.1.1, insofar as the Section is included in the coverage.

**b) Fees and expenses of the consultancy firm**

The insurer shall reimburse the reasonable and necessary fees and disbursements of the consultancy firm named in the policy schedule or of another independent company appointed with the prior consent of the insurer in written or electronic form, that are incurred during a **cyber threat** for purposes such as travel, accommodation, translation and communication costs, as well as payments to informants.

**c) Reimbursement of extortion monies**

In so far as permitted by law, the insurance cover shall include the reimbursement of extortion monies paid directly by an **insured company** due to a **cyber threat**.

### 2.1.6.2 Deductible

Section 5.3.6 shall apply.

### 2.1.6.3 Shared sub-limit

The indemnity provided by the insurer under Sections 1 to 3 in connection with **cyber threats** shall be limited to the amount stated in the policy schedule within the scope of the sum insured.

If the insurer's indemnity for any other coverage module is limited by a lower sub-limit than the shared sub-limit for this Section, the lower sub-limit amount in connection with **cyber threats** shall apply. All indemnities made by the insurer for other cover modules in connection with **cyber threats** shall be offset against the shared sub-limit for this Section. For insured events not in connection with **cyber threats**, the unused part of the sub-limits for any other cover module is available.

### 2.1.6.4 Duties

The policyholder shall be obliged,

- to immediately inform the insurer and the consultancy firm named in the policy schedule of the **cyber threat** without delay and to place all of the required information at their disposal, and
- to notify the investigative authorities of the **cyber threat** or to authorise the consultancy firm named in the policy schedule to pass on that information; in the case of events occurring in another country, the competent investigative authority must be selected in agreement with the insurer and/or the consultancy firm named in the policy schedule, and
- to inform the insurer and the consultancy firm named in the policy schedule and keep them up to date with regard to all developments and
- to make all reasonable efforts to keep the existence of the insurance cover of this Section 2.1.6 confidential. The policyholder shall oblige the persons informed of the existence of this insurance cover to maintain confidentiality and duly document their names including the date of their information and to be able to make this documentation available to the insurer upon request.

In the event of a breach of these duties, the legal consequences set out in Section 5.4 shall apply.

### 2.1.6.5 Specific exclusions

In addition to the exclusions set out under Section 4, the insurance cover shall not extend to

- a **cyber threat** pronounced by an authority or another state institution;
- ransom payments handed over within the scope of kidnapping following or during the use or threat of violence towards persons or other dangers to life or limb;
- ransom payments that are lost, destroyed or stolen as a result of fraudulent or criminal action of an **insured company**, of their supervisory boards, directors, board members, managers, employees or representatives, irrespective of whether they act alone or jointly with others;

– ransom payments, where there is an unlawful threat to contaminate, pollute or render inferior those products manufactured, marketed or processed by **insured companies** or to arrange publication thereof (product blackmail).

### 2.2 Indemnity payments

The cover within Sections 2.1.1 to 2.1.6 includes the reasonable and necessary costs and expenditure specified in those Sections.

For losses within Sections 2.1.2 and 2.1.3, the **insured companies** shall seek the prior approval of the insurer for the choice of lawyer and the applicable hourly rates.

### 2.3 Recovery of data, software and IT systems

#### 2.3.1 Insurance cover

In the event of a **network security breach** first discovered by an **insured company** or an **additional insured person** during the **policy period**, cover is provided for the reasonable and necessary costs and expenditure within Sections 2.3.1 to 2.3.2.

– for the recovery of **data**, **software** and **IT systems** within Section 2.3.2;
– for the removal of **malware** from **IT systems**.

Cover shall solely be provided for the interest of the **insured company** concerned.

In assessing the extent of any cover under this Section 2.3.1, account shall be taken of any contributory causes of direct or indirect losses of **data**, **software** and **IT systems** due to physical damage or destruction of data storage and/or **IT systems** which shall be excluded under Section 4.14.

#### 2.3.2 Data and software

Cover is provided for **data** and **software** that the **insured company** is entitled to use, provided that they are stored within the **IT systems**.

## 3 Cover for business interruption/loss of income

### 3.1 Insurance cover

In the event that the operations of **insured companies** during the **policy period** are completely or partially interrupted or impaired due to the non-availability of the **IT systems** resulting from an **Interruption event**, the insurer shall cover any resulting Loss of Income during the Period of Indemnity subject always to the provisions of this Section and Sections 5.3.4 and 5.3.6.

### 3.2 Loss of income

Loss of Income shall mean the revenue that could reasonably have been expected to be obtained from the operation of the business of the **insured company** during the Period of Indemnity had the **Interruption Event** not occurred less the variable charges and expenses of the business (and any other costs) not incurred.

In calculating Loss of Income, such adjustment shall be made as may be necessary to provide for the trend of the business and for variations in or other circumstances affecting the business either before or after the interruption or interference which would have affected the business had the **Interruption Event** not occurred. The figures so adjusted shall represent, as nearly as may be reasonably practical, the results which would have been achieved by the business during the same period had the **Interruption Event** not occurred. In particular, operating profit and costs shall not be indemnified if they would not have been generated or incurred in any event due to planned or necessary overhauls, maintenance work or modifications.

### 3.3 Increased cost of working

Cover is provided for the increased cost of working incurred during the Period of Indemnity.

Increased Cost of Working shall mean costs and expenditure reasonably and necessarily incurred during the Period of Indemnity to maintain and continue the normal business operations of the **insured company** for the sole purpose

of avoiding or diminishing the Loss of Income which would otherwise be suffered not exceeding the amount of Loss of Income thereby avoided.

Expenditure for the recovery of **data, software** and **IT systems** shall not be regarded as increased cost of working and shall solely be insured under Section 2.3.

### 3.4 Period of Indemnity

The Period of Indemnity is the period specified in the policy schedule for which insurance cover is provided for Loss of Income. The Period of Indemnity shall commence at the time the **Interruption Event** occurs for the first time.

Section 5.3.4 (series loss clause) shall apply.

### 3.5 Scope of indemnity

#### 3.5.1 Calculation of indemnity

Coverage for loss of income is only provided if the insured loss resulting from an **Interruption Event** is identified, or reasonably should have been identified, by or on behalf of the **insured company** during the **policy period**.

The insurer shall not cover any loss of income caused or increased by:

– events occurring during the period of indemnity which are not a direct consequence of the **Interruption Event**; or
– recovery or operational restrictions imposed by any statutory or governmental authority, provided that they are not directions for the suspension of business from data protection authorities within Section 3.1.

#### 3.5.2 Waiting period

In respect of each **Interruption Event**, the **insured companies** are not covered for any loss during the waiting period as specified in the policy schedule. The waiting period shall commence at the time an **Interruption Event** occurs and if exceeded the deductible within Section 5.3.6 shall apply.

### 3.6 Voluntary shutdown

#### 3.6.1 Insurance cover

In the event that the operation of the business of an **insured company** is interrupted or impaired during the **policy period** due to a voluntary shutdown of the **IT systems** at an insured location, other than due to a measure within Section 2.1.1, the insurer shall cover the resulting loss of income arising during the period of indemnity and any increased cost of working.

It shall be a condition precedent to the provision of cover under Section 3.6.1 that there shall have been onset of a **network security breach** during the **policy period** which has not led to an **Interruption Event** within Section 3.1.

Any voluntary shutdown of the **IT systems** must, in the reasonable opinion of the Chief Information Security Officer of the **insured company** or of a person holding a corresponding position, represent a suitable and appropriate measure to prevent the further compromise of the availability, integrity and/or confidentiality of **data** and/or **IT systems** of **insured companies**; this must be confirmed in written or electronic form to the insurer by the Chief Information Security Officer of the **insured company** or a person holding a corresponding position immediately after voluntary shutdown, stating the reasons on which the decision is based.

Each voluntary shutdown of the **IT systems** shall be reported to the insurer in written or electronic form within the waiting period.

#### 3.6.2 Period of indemnity and sub-limit

Notwithstanding any other provision of this policy, the period of indemnity shall commence when the voluntary shutdown of the **IT systems** first commences but all cover shall be subject to the sub-limit specified in the policy schedule.

## 4 General exclusions

Unless stated to the contrary in a Section, the general exclusions apply to the policy as a whole.

The policy does not cover **third party claims**, losses, costs and expenditure or expenses arising from, directly or indirectly caused, or contributed to, by the following:

### 4.1 Conduct

Insured events or losses arising from or in connection with the wilful

- causation of the insured event,
- breach of duty,
- failure to adhere to statutory or official regulations or instructions.
- criminal, fraudulent dishonest and malicious acts or omissions

If it is disputed whether the above conduct, breach of duty or act or omission has occurred, the insurer shall temporarily provide cover for the costs of defence of a **third-party claim** within Section 1. The insurer shall be released retroactively from the duty to provide cover for defence costs if the above conduct, breach of duty or act or omission is finally established by settlement, court order or arbitration award. In such cases, the payments made by the insurer shall be repaid in full.

Only the conduct of the **control group** shall be attributed to the policyholder and **additional insured companies**.

### 4.2 Products and services

Products or services designed, manufactured or distributed by **insured companies**.

Any product liability including but not limited to any alleged inaccurate description, misrepresentation, failure to perform or failings in quality.

### 4.3 Contractual liability

Any liability or obligation assumed under the terms of a contract; this shall not apply to any liability or obligation which exists independently of such contract.

### 4.4 Claims by insured parties or beneficial owners

Any liability or obligation between **insured companies** and/or **additional insured persons** or owed to shareholders of partners of **insured companies** or the liquidators, official receivers or insolvency administrators of **insured companies**.

This shall not apply if **additional insured persons** bring a **third-party claim** against **insured companies** for **data protection breaches** and in that regard constitute **third parties**.

### 4.5 Intellectual property

The infringement of intellectual property rights including (without limitation) copyrights, patents or the loss of patentability.

Any obligation or liability to pay royalties, or licences, including the payment of licence fees; this shall not apply to expenditure for the purchase of new licences that arises because insured **data** and **software** are secured by copy protection, access control or similar protection measures.

### 4.6 Company or trade secrets

The infringement of **company or trade secrets**; this shall not apply if cover is provided under Sections 1.1.

### 4.7 Competition law

The breach of antitrust or competition law

### 4.8 Known losses, circumstances and pending proceedings

Circumstances, **third party claims** or losses, including proceedings before courts or arbitral or other tribunal or regulatory bodies known to members of the **control group** prior to the **policy period**.

### 4.9 War, sovereign interventions or civil commotion

- **War**;
- a **sovereign intervention** (this shall not apply regarding the cover provided under Section 3.1, third bullet point (business interruption/loss of income due to an immediately enforceable order from a competent data protection authority in relation to the suspension of operations at the insured locations due to a **data protection breach**));
- a **cyber operation** that is carried out as part of **war** or a military operation by one **state** against another **state** (whether declared or not) or the immediate preparation for a **war** or military operation by one **state** against another **state** (whether declared or not);
- a **cyber operation** that causes a **state** to become an **impacted state** (this shall not apply to the direct or indirect effect of a **cyber operation** on a **computer system** used by the insured companies or third party service providers to insured companies that is not physically located in an **impacted state** but is affected by a **cyber operation**).

For the purposes of this definition:

- **Cyber operation** means the use of a **computer system** by, at the direction of, or under the control of a **state** to disrupt, deny access to or degrade functionality of a **computer system** or copy, remove, manipulate, deny access to or destroy information in a **computer system**.
- **Computer system** means any computer, hardware, software, communications system, electronic device (including but not limited to smart phone, laptop, tablet, wearable device), server, cloud infrastructure or microcontroller including any similar system or any configuration of the aforementioned and including any associated input, output, data storage device, networking equipment or backup facility.
- **Sovereign intervention** means expropriation, nationalisation, seizure, appropriation or any other act by, on behalf or on the orders of a **state**, government, corporation under public law, authority or another (de facto) sovereign institution.
- **Supply infrastructure** means any service that is critical to the effective functioning of a **state** including, but not limited to, financial institutions and associated financial market infrastructure, health services or utility services.
- **Impacted state** means any **state** where a **cyber operation** has a significant negative impact on the functioning of that **state** due to the availability, integrity or delivery of **supply infrastructure** in that **state** or on the security or defence of that **state**.
- **State** means sovereign state.
- **War** means armed conflict involving physical force by a **state** against another **state**, or as part of a civil war, rebellion, revolution, insurrection, military action or usurpation of power, whether **war** be declared or not.

### 4.10 Interruption or disruption of supply infrastructures

Any interruption or disruption of a **supply infrastructure** if the **supply infrastructure** is not within the control of **insured companies.**

### 4.11 Financial transactions

Proprietary trading or trading liabilities or obligations of **insured companies**.

Payment transactions;

The purchase, sale or trading of shares or other securities, including the use of confidential information or the breach of laws or regulations applicable thereto.

Liability to shareholders or holders of other securities in the **insured companies** arising from an **information security breach** that affects the share price of **insured companies** or other companies.

The misrepresentation of the financial standing of **insured companies**.

### 4.12 Claims against members of management

Any liability or obligation of any directors or officers of **insured companies** in their capacity as such.

### 4.13 Fines and penalties, non-compensatory damages

Fines, penalties, liquidated damages or contractual penalties. This shall not apply for insurance cover within the terms of Section 1.2 subject to such cover being legally permissible.

Punitive, multiple or exemplary damages awarded by a court or tribunal or reflected in a settlement.

### 4.14 Bodily injury or property damage
**Bodily injury** to any natural person or **property damage**.

### 4.15 Nuclear energy
Ionising radiation or contamination by radioactivity from any nuclear waste from the combustion of nuclear fuel, or the radioactive, toxic, exposure or other hazardous properties of any explosive nuclear assembly or nuclear component thereof.

### 4.16 Ransom and cyber threat
Any payment of a ransom in response to a **cyber threat.** This shall not apply for insurance cover within Section 2.1.6.

### 4.17 Sanctions
No (re)insurer shall be deemed to provide cover and no (re)insurer shall be liable to pay any claim or provide any benefit to the extent that the provision of such cover, payment of such claim or provision of such benefit would expose that (re)insurer to any sanction, prohibition or restriction under sanction law applicable to the (re)insurer.

### 4.18 Pornographic content, advertising, competition or games of chance
Pornographic content, advertising, competition or games of chance.

### 4.19 Money
Loss, destruction of or damage to money, including cryptocurrency.

### 4.20 Employees
Any obligation owed by the **insured companies** as an employer or potential employer to any employee, director, officer, partner, **additional insured person** or applicant for employment. This shall not apply to a **data protection breach** to the extent that this affects any employee, director, officer, partner, **additional insured person** or applicant for employment.

### 4.21 Data and software, IT processes and IT systems
Costs and expense arising from changes or improvements beyond recovery (also known as betterment).

## 5 General conditions and claims conditions

Unless stated to the contrary in a Section, the general conditions apply to the Policy as a whole.

### 5.1 Insured companies/additional insured companies and additional insured persons
Cover shall be provided to the insured(s) specified in the policy schedule **additional insured companies** and **additional insured persons**.

### 5.1.1 Newly acquired companies (subsidiary companies)
In the event that subsidiary companies are first acquired or founded by the **insured companies** after inception of the **policy period**, cover shall be provided for an insured event due to an **information security breach** occurring after the date of takeover or founding.

A company is not covered under this Section when newly acquired after the inception of the Policy and the activity is different from that of the **insured companies**, and:

- it does not comply with the information security standards and the technical and organisational measures established within the **insured companies'** organisation;
- its consolidated balance sheet total or consolidated turnover exceeds 10% of the **insured companies'** most recent consolidated balance sheet total or most recent consolidated turnover;
- its business falls within the **financial industry** or telecommunications;

– its registered office is outside of EU/EEA

In the event of a breach of the duties set out in this Section 5.1.1, the newly acquired or founded company shall not be covered by this Policy.

### 5.1.2 Withdrawing companies (subsidiary companies)

In the event that an **additional insured company** is liquidated or ceases to be an **additional insured company** after the inception of the **policy period**, the cover for the subsidiary company in question shall only extend to **information security breaches** that occur up to the time at which the liquidation is completed or prior to the time it ceases to be an **additional insured company**.

## 5.2 Change of control or insolvency of insured companies

### 5.2.1 Change of control

In the event that the insured(s) named in the policy schedule undergo(es) a change of control, cover shall only be provided for **information security breaches** prior to the change of control becoming effective.

A change of control occurs when a controlling influence over the company within Section 6.2 is acquired by **third parties**.

### 5.2.2 Insolvency of insured companies

In the event that an **insured company** becomes insolvent, cover shall be provided for **information security breaches** prior to its insolvency.

Insolvency refers to the commencement of insolvency proceedings affecting the assets of an **insured company** under the Danish Insolvency Act or comparable laws in other countries.

## 5.3 Provisions regarding the scope of the indemnity

### 5.3.1 Sum insured

Notwithstanding Section 53 subclause 2 of the Danish Insurance Contracts Act the sum insured specified in the policy schedule is the maximum amount payable by the insurer for any one insured event.

The annual limit of indemnity specified in the policy schedule is the maximum amount payable by the insurer for all insured events in any one **policy period**.

The sub-limits specified in the policy schedule shall be the maximum amounts payable by the insurer in respect of the cover to which sub-limits apply and shall erode the sum insured and the annual limit of indemnity.

The amounts payable by the insurer shall be denominated in the currency mentioned in the schedule.

### 5.3.2 The inclusion of costs

Reimbursement of expenditure and costs in connection with own losses, indemnity for loss of income and defence costs, excluding the insurer's own costs, and interest payable after the due date of the indemnity payment, shall form part of the sum insured and shall erode the sum insured.

### 5.3.3 Settlement of a claim

If the insurer requests that a **third party claim** under Section 1 be settled and the **insured company** does not comply, the insurer shall not be under an obligation to pay any additional amount in respect of the indemnity payment, interest and defence costs subsequent to the request.

### 5.3.4 Series losses

Multiple insured events during the **policy period** shall be regarded as a single insured event that occurred at the time that the first of the insured events took place, if these arise from, or are attributable to, the same originating cause.

The deductible shall only apply once to each such event.

With regard to cover for business interruption/loss of income within Section 3, the period of indemnity shall only apply once to each such event.

If an insured event extends over more than one **policy period**, the **insured companies** and **additional insured persons** shall be covered solely under the **policy period** in which the insured event first occurs.

### 5.3.5 Other insurance

Where any coverage under this Policy is also insured under another policy, such other policy shall apply in priority to this policy.

If the other policy has been taken up with HDI Global SE or any of its subsidiaries, the total sum insured, whether under this policy or all policies, shall be limited to the highest sum insured under any policy which responds to the claim, liability, loss or defence costs or other amount payable.

### 5.3.6 Deductible

All payments made by the insurer shall be reduced by the amount of the deductible per insured event, as specified in the policy schedule.

If different deductibles apply to individual parts of a loss or claim, then the deductibles shall be limited in total to the amount of the highest applicable deductible.

## 5.4 Fair presentation of risk, non-disclosure and misrepresentation

### 5.4.1 Legal consequences of a breach of the duty of fair presentation

The **insured companies** and **additional insured persons** are under a duty at inception, renewal and upon any variation of the Policy to make a fair presentation of the risk including to disclose to the insurer all material facts and circumstances in a clear and accessible manner and not to misrepresent to the insurer any material facts and circumstances.

### 5.4.2 False and fraudulent claims

If any claim under this policy is in any respect fraudulent, or if any fraudulent means or devices are used by an **insured company** or **additional insured person** or anyone acting on their behalf to obtain any benefit under this policy, or if any benefit under this policy is obtained by the wilful act or with the connivance of the **insured company** or **additional insured person**:

1) the insurer will be entitled to refuse to pay the whole of the claim and recover any sums that the insurers have already paid in respect of the claim;
2) the insurer may terminate the policy with effect from the date of any fraudulent or wilful act and the **insured companies** or **additional insured person** will have no cover under this policy for any event loss damage incident or act after the date of termination:
3) the **insured companies** and **additional insured persons** shall not be entitled to any refund or return of premium.

## 5.5 Inception of the cover, policy period, cancellation

Cover shall incept at the time and date stated in the policy schedule, subject to late payment or non-payment of the premium. It is warranted that the premium will be paid in full within the period mentioned in the invoice.

### 5.5.1 Policy period and extension

The Policy shall initially be for the **policy period** specified in the policy schedule, subject to earlier termination as provided herein.

## 5.6 Premium

The premium is specified in the policy schedule.

## 5.7 Duties prior to the occurrence of an insured event

The **insured companies** and **additional insured persons** shall take reasonable steps to prevent or minimise any **third-party claim**, circumstance, expense or loss under this Policy.

### 5.8 Claims conditions

#### 5.8.1 Notification of an insured event

All insured events shall be notified to the insurer as soon as a member of the control **group** becomes aware of an insured event.

The same applies for **third party claims** if court, arbitration or other proceedings are commenced against the **insured companies** or **additional insured persons**.

#### 5.8.2 Duty to cooperate

The **insured companies** and **additional insured persons** shall comply promptly with reasonable requests made by the insurer following notification of an insured event. The **insured companies** and **additional insured persons** shall provide the insurer with information and documents relating to the claim or loss and assist with the investigation and settlement of a claim or loss.

#### 5.8.3 Subrogation

The **insured companies** and **additional insured persons** shall take reasonable steps to preserve rights to recover a claim or loss covered under this policy from a **third party** and shall provide all reasonable assistance to the insurer to enforce such rights. On request from the insurer, the **insured companies** and **additional insured persons'** rights in respect of **third parties** shall be assigned to the insurer if it has made any payment under this policy.

### 5.9 Increase in risk

The **insured companies** shall notify the insurer of an increase in risk that occurs after commencement of the **policy period**, as soon as they become aware of the increase in risk. The insurer shall be entitled to increase the premium payable for the cover provided by this policy following such increase in risk.

An increase in risk may in particular, but not exclusively, occur if a material fact changes about which the insurer inquired before the policy was effected. An increase in risk shall not have occurred if the risk has only increased to an insignificant degree or, given the circumstances, should be deemed to have been accepted.

### 5.10 Territorial limits

Cover shall be provided worldwide insofar as it is legally permissible.

### 5.11 Legal status

The duties of disclosure and other duties specified in this Policy shall apply to the **insured companies**.

No payment or indemnity due under this policy may be assigned without the approval of the insurer.

### 5.12 Jurisdiction and applicable law

Unless otherwise agreed by the **insured company** and the insurer, this policy shall be governed by and construed solely in accordance with the law set forth in the schedule. The Courts of the country set forth in the schedule shall have exclusive jurisdiction over the parties on all matters relating to this policy.

## 6 Definitions

The definitions below apply to the policy as a whole and are highlighted in bold.

### 6.1 Additional insured persons

**Additional insured persons** means all:

- employees working for **insured companies** on the basis of an employment or service contract in fulfilment of their working activities;
- duly appointed members of the members of the Board of Directors and Board of Management in fulfilment of their working activities;
- employees and the members of the Board of Directors and Board of Management who have left the **insured company** concerned

### 6.2 Additional insured companies

**Additional insured companies** are, unless expressly stated otherwise, subsidiary companies in the EU and EEA of the insured(s) named in the policy schedule. Subsidiary companies are companies that are affiliated to the insured(s) named in the policy schedule within the definition of the applicable company law, over which direct or indirect controlling influence may be asserted by virtue of either:

- the majority of voting rights;
- the right to appoint and dismiss members of the **control group**, where the insured(s) named in the policy schedule is at the same time a shareholder;
- the right to exercise a controlling influence; or
- it bears the majority of the risks and opportunities from a financial point of view, where the company acts to achieve a limited and defined objective of the parent company (special purpose company).

A company that becomes or is intended to become a subsidiary company shall also be deemed to be a subsidiary company while it is in the process of being founded.

### 6.3 Bodily injury

**Bodily injury** means injury, disease or death and shall include (without limitation) mental injury anguish, shock, false arrest or invasion of the right of privacy. This shall not include mental anguish or emotional distress resulting from a **data protection breach**.

### 6.4 Cloud service

A **cloud service** refers to the provision of **hardware**, **software** or infrastructure to the **insured companies** utilising the internet and operated by **third party**.

The **cloud service** must be provided by a **third party** in a direct business relationship, based on a written agreement, with an **insured company**, in return for payment.

The term **cloud service** shall not include the provision of services relating to **supply infrastructure** or to the provision of banking and financial services, including debt collection services.

### 6.5 Company or trade secrets

**Company or trade secrets** are all confidential information relating to an **insured company** not publicly known, or generally known or readily accessible to persons within circles that normally deal with the kind of information in question, which an **insured company** wishes to be kept secret on grounds of commercial value or sensitive nature.

### 6.6 Control group

**Control group** means:

- the members of the Board of Directors or the senior management team, and
- the head of the legal department, and
- the Chief Information Security Officer, and
- the head of the risk management department, and
- data protection officers, and
- the insurance or risk manager

or equivalent of the **insured companies**.

### 6.7 Cyber threat

**Cyber threat** means an **information security breach** threatened by a **third-party**.

**Cyber threat** shall also include:

- the threatened unauthorised disclosure, use or trading of **personal data** or **company or trade secrets** of **insured companies**, if obtained through an **information security breach**;
- the threatened unauthorised encryption, the threatened rendering unusable or threatened other impairments of the availability, integrity or confidentiality of **IT systems** or **data** of **insured companies** by **malware**;
- the continuation of a **cyber threat** following an **information security breach**;

- the ongoing encryption of **data** of **insured companies** following an **information security breach**;
- the refusal by a **third party** to whom an **information security breach** is attributed to provide a decryption key or other means to enable **insured companies** to regain use of their **data** following an **information security breach**.

### 6.8 Data

**Data** means information, facts, concepts or code that the **insured companies** are legally permitted to use and which is digitalised, machine-readable or readable in another technical manner, is electronically stored on data storage or processed by **IT systems**. **Data** does not constitute objects in any physical form.

### 6.9 Data confidentiality breach

A **data confidentiality breach** is a violation of the confidentiality of **data**. A **data confidentiality breach** is deemed to have occurred if **data** ceases to be subject to the control of an **insured company** or **additional insured persons** in breach of a duty of confidentiality and is made available to unauthorised **third parties** or in the public domain.

### 6.10 Data protection breaches

A **data protection breach** is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, **personal data** transmitted, stored or processed or any other action concerning the collection, processing or use of **personal data** by **insured companies** or **additional insured persons** in breach of **data protection law**.

### 6.11 Data protection law

**Data protection law(s)** mean(s) all applicable data protection and privacy legislation, regulations and guidance including Regulation (EU) 2016/679 (the "EU GDPR") and comparable laws in other countries, each as supplemented updated or amended from time to time.

### 6.12 Financial industry

**Financial industry** means banks, savings banks, investment management companies, funds, insurance companies and other companies subject to supervision by the Financial Supervisory Authority in the country set forth in the schedule, including equivalent companies and supervisory authorities in other states.

### 6.13 Financial loss

**Financial loss** means:

- Losses arising from the loss, alteration or unavailability of **data** belonging to a **third-party**;
- Non-material damage suffered by a **third-party** natural person as a result of **data protection breaches**.

### 6.14 Information security breach

An **information security breach** means an impairment of the availability, integrity or confidentiality of **data** and/or **IT systems** in the form of:

- a **data protection breach**;
- a **data confidentiality breach**; or
- a **network security breach;**

### 6.15 Insured companies

**Insured companies** mean the insured(s) named in the policy schedule and the **additional insured companies**.

### 6.16 Interruption event

**Interruption event** means

- a **network security breach**;
- a forensic investigation agreed with the insurer under Section 2.1.1; or
- an immediately enforceable order from a competent data protection authority in relation to the suspension of operations due to **a data protection breach**

### 6.17 IT service

**IT service** means the provision of a service:

– for the maintenance, administration or control of **IT systems**; or
– for the hosting of the web presence of an **insured company**.

The **IT service** must be provided by a **third party** in a direct business relationship, based on a written agreement with an **insured company**, in return for payment.

**IT service** shall not include the provision of services relating to **supply infrastructures**, or to the provision of services to the **financial industry**, including debt collection services.

### 6.18 IT systems

**IT systems** means

– **hardware** and **software** systems operated by **insured companies**, including network components and **networks** (including virtual networks) and end-user devices (including mobile devices, such as laptops, tablets and smartphones); and
– **hardware** and **software** systems for the control of technical production processes, such as embedded systems, SCADA (Supervisory Control And Data Acquisition) systems or other industrial automation systems

used for processing **data**. **IT systems** include **cloud services** or **IT services** provided to the **insured companies** by **third parties**. No insurance cover is provided if the recovery of **data** is technically impossible or the consultancy firm named in the policy schedule is not provided with the necessary technical access required for the recovery of **data**.

### 6.19 Network security breach

**Network security breach** means

– any unauthorised access to, processing of, use of and or operation of any **IT system,**
– the unauthorised deletion, suppression, rendering unusable or alteration of **data** stored in **IT systems,**
– a transfer of any type of **malware** via the **IT system of insured companies** to a **third-party IT system**,
– the theft or loss of **hardware** belonging to **insured companies** for information processing purposes (including laptops, tablets and smartphones). Theft or loss shall not be deemed to arise from **sovereign intervention**.

### 6.20 Personal data

**Personal data** means any information which relates to an identified or identifiable natural person, being a person who can be directly or indirectly identified from such information including but not limited to any information protected by EU Regulation 2016/679 (the “GDPR”) and comparable laws in other countries, each as supplemented updated or amended from time to time.

### 6.21 Policy period

**Policy period** means the period of time this policy is in force as specified in the policy schedule, or another policy is or was in force, as the context requires.

### 6.22 Property damage

**Property damage** means damage to loss of or destruction of tangible property.

### 6.23 Software

**Software** means **programs** or code used for the operation of **IT systems** and which the **insured companies** are legally permitted to use.

### 6.24 Supply infrastructure

**Supply infrastructure** means the supply of:

– electricity, gas, oil, water and/or other forms of energy

– internet, cable, satellite and/or telecommunications services
– financial market infrastructure, securities trading platforms and payment systems including banking, financial and debt collection services

or any component thereof.

### 6.25 Third parties

**Third parties** mean all legal entities or natural persons not being the insurer or **insured companies** or, save as provided in this Section, **additional insured persons**.

**Third parties** shall include (without limitation) affected persons covered by **data protection law**, clients or parties contracting with **insured companies**. **Additional insured persons** shall only be deemed to be **third parties** if they make a **third-party claim** as affected persons against **insured companies** as a result of a **data protection breach**.

### 6.26 Third party claim

**Third party claim** means an assertion of legal liability made in writing against the **insured companies** and/or **additional insured persons** by a **third party** during the **policy period** or extended reporting period whether in a pleading, letter of claim, correspondence or otherwise, whether or not including a demand for **financial loss**.

## 7 Complaints procedure

If the policyholder does not believe to have received the benefit that was agreed upon or is entitled to, or if the case processing drags on unnecessarily, the policyholder has the right to complain.
This can be done by writing to:

HDI Denmark
Langebrogade 3F, 1.
DK-1411 Copenhagen K
Phone number: +45 3336 9595
Email: info.dk@hdi.global

We will acknowledge your complaint in writing within five working days of receipt.

We will endeavour to send a final response to you within eight weeks of receipt of your complaint. If we are unable to provide you with a final response within this time frame, we will write to you explaining the delay and advise you when you can expect a final response.

## 8 GDPR Privacy Notice

The insured is hereby made aware that the insurance company carries out electronic data processing of the **personal data** of the insured and other persons mentioned in the insurance conditions, which is obtained by the policyholder, the insurance company or an external claims adjuster regarding the insurance cover, the treatment thereof and of damages covered by the insurance. The insured declares when applying for or joining the insurance as having agreed to this.

Pursuant to the General Data Protection Regulation (EU) 2016/679, the insured is expressly made aware that the provision of **personal data** is necessary to obtain coverage and for processing according to the insurance program, and that this **personal data** may be passed on to or processed for HDI in countries outside Denmark and the EU. This information is intended exclusively for the policyholder, the insurance company and their partners for the purpose of fulfilling tasks in accordance with the insurance program and for use by authorities for any supervisory tasks. Individuals have a right to access their information and can also request a copy of them.

You can also find more information on our handling of privacy information on our website; https://www.hdi.global/legal/privacy/