General Insurance Conditions (GIC)

Cyber Insurance Companies

Version 06.2024

15967EN – 2024-06 D

Contents

Part E
Definitions

Key Points at a Glance

This overview provides you with information about the key content of the insurance contract in accordance with Article 3 of the Federal Act on Insurance Contracts (ICA). The rights and obligations of the contracting parties arise on conclusion of the insurance contract, in particular on the basis of the application, the policy, the insurance conditions and the statutory provisions.

Who is the insurance carrier?

The insurance carrier is AXA Insurance Ltd, General-Guisan-Strasse 40, 8401 Winterthur (hereinafter referred to as "AXA"), a joint stock company with registered office in Winterthur and a subsidiary of the AXA Group.

What is insured?

This is indemnity insurance pursuant to the Insurance Contract Act.

First-party cyber event:
The insurance covers the restoration of your own electronic *data* caused by a *first-party cyber event*.

The insurance also covers loss of earnings and additional costs arising from a business interruption due to insured loss or damage.

Cyber liability event:
The insurance covers claims for damages due to *financial loss* that are brought against the *policyholder* or an *insured* based on statutory liability provisions. These include claims due to

- destruction of, damage to, modification, non-availability or loss of a *third party's data* which was in the possession of the *policyholder* or of a party to whom the *policyholder* had entrusted such data,
- destruction of, damage to, modification, non-availability or loss of *data* on *IT systems* of a *third party*,
- *breaches of data protection*,
- the breach, theft or loss of confidential information.

E-banking, online shop and shipment of goods (optional):
The insurance covers financial loss incurred due to the manipulation of e-banking transactions, the online shop or the shipment of goods.

Online payment system (optional):
The insurance covers *financial loss* incurred due to the manipulation of online banking or an online payment system.

Social engineering (optional):
The insurance covers *financial loss* incurred in connection with social engineering attacks.

Phone hacking (optional):
Under phone hacking, the unauthorized use of the telephone system by *third parties* following *first-party cyber damage* is insured.

What does the insurance not cover?

The insurance does not cover, among other things, claims arising from:

- loss or damage due to warlike events, civil unrest or terrorism,
- loss or damage in connection with the deliberate use of pirated copies by the *policyholder* or an *insured*,
- *bodily injury and property damage*,
- loss in connection with virtual currencies.

The precise scope of coverage is specified in the policy and these GIC.

What benefits does AXA provide?

In connection with an insured *first-party cyber event*, AXA indemnifies the costs of restoring the insured *data*, the costs of removing *malware* from the *policyholder's IT system*, as well as insured loss of earnings and additional costs.

In connection with an insured *cyber liability event*, AXA indemnifies the amount that the *policyholder* must pay to the injured party as indemnity within the scope of the insurance and the statutory liability provisions.

The indemnity is limited to the sum insured specified in the application and in the policy for each group or coverage module.

Any applicable deductible and any indemnity limits are specified in the application and the policy.

How much is the premium and when is it due?

The premium as well as its due date are set out in the application and/or the policy.

What are the policyholder's main obligations?

Among other things, the *policyholder* must:

- perform a full *data* backup at least once a week,
- store data backups, programs and licenses in such a way that they cannot be damaged or destroyed together with the originals,
- use protective systems (e.g. internet protection programs, antivirus software, firewalls) and keep them updated.

When does the notice of claim need to be filed?

If an insured event occurs, the *policyholder* must file the notice of claim as quickly as possible.

When does the insurance begin and end?

The insurance begins on the date specified in the policy. AXA may reject the application up until the date on which it issues the policy or a definitive cover note. The insurance is valid for the period specified in the policy.

Unless terminated on expiry, the insurance contract is automatically renewed for another year. If the insurance contract is concluded for less than one year, it expires on the date specified in the policy.

How to exercise the right of withdrawal

The *policyholder* may withdraw from the contract with AXA within 14 days of their acceptance. This deadline will be met if the withdrawal is communicated to AXA in writing or another form of text (e.g. by email or letter).

In the event of withdrawal, any benefits already received must be paid back.

Special information for the Principality of Liechtenstein

The applicant is bound by the application to conclude an insurance contract within two weeks of submitting or sending the application.

If AXA breaches the duty to provide information pursuant to the Liechtenstein Insurance Contract Act or the Liechtenstein Insurance Supervision Act, the *policyholder* will have the right to withdraw from the contract within four weeks of receipt of the policy.

The responsible supervisory authority is the Swiss Financial Market Supervisory Authority FINMA, 3000 Bern.

What definitions apply?

The key terms are explained in Part E under “Definitions.”

What data does AXA use and how?

AXA uses data in compliance with the applicable statutory provisions. More information may be found at AXA.ch/data-protection.

Part A
Underlying Provisions of the Insurance Contract

A1 Scope of the insurance contract

The policy specifies what insurance has been taken out. The policy, these General Insurance Conditions (GIC), and any Special Insurance Conditions (SIC) provide information about the scope of the insurance.

A2 Territorial scope

The insurance covers claims arising from damage that occurs anywhere in the world. The insurance does not cover liability claims that are judged in accordance with any state, provincial or federal law of the USA or Canada. Likewise, the insurance does not cover costs incurred in the USA or Canada, or enforcement orders or settlements in those countries. The territorial scope also applies with respect to coverage of costs.

A3 Trigger

A3.1 First-party cyber event

The insurance covers *first-party cyber events* that are discovered for the first time and reported during the term of the contract.
If it is found that the *first-party cyber event* occurred before the start of the contract, insurance coverage is valid only if the *policyholder* and *insureds* were unaware of this.

A3.2 Cyber liability event

The insurance covers damage and claims brought against the *policyholder*, an *insured* or against AXA as their liability insurer while the policy is in force. The policy period is deemed to be

- the term of the contract as specified in the policy
- the term of any contracts with AXA replaced by this policy
- any extended coverage period granted by AXA

A3.2.1 **Date of assertion of claim**

The date on which a claim is asserted is deemed to be:

- the date on which the *policyholder* or an *insured* first becomes aware of circumstances pursuant to which it must be assumed that a claim will be brought against the *policyholder*, an *insured* or against AXA as their liability insurer. If there are no such circumstances, the date on which the claim is made is deemed to be the date of verbal or written notice that a claim for damages falling under this insurance contract will be brought.
- the date on which the *policyholder*, an *insured*, or AXA as their liability insurer, first becomes aware that criminal, administrative, supervisory or investigative proceedings have been initiated against the *policyholder* or an *insured* that could lead to an insured claim.

If multiple criteria apply for the same event, the earliest date applies.

A3.2.2 **Prior acts coverage**

The insurance also covers claims arising from loss or serial loss incurred as a result of acts or omissions that took place prior to the date on which this insurance contract was first concluded. The insurance will only cover these, however, if the *policyholder* or the *insured* was unaware of any act or omission that could give rise to liability prior to the date on which this contract was first concluded.

A3.2.3 **Extended coverage period**

a) During the term of the contract

If, during the term of the contract, an *insured* leaves the group of *insureds*, or if an insured business or a part of it is excluded or discontinued, coverage will remain in effect. This will only be the case, however, if any acts or omissions giving rise to liability occurred prior to this. If this is the case, the day of leaving, of exclusion or of discontinuation will be deemed to be the date of the claim.

b) On expiry of the insurance

After expiry of the insurance, coverage also extends to claims arising from damage that are only made after expiry of the insurance and within the statutory limitation periods, provided that such damage was caused prior to expiry of the insurance. There is no extended coverage if the insurance contract was canceled due to late payment of a premium. Claims which are made during such extended coverage periods and which are not part of a serial loss are considered to have been asserted on the day on which the contract ended.

A3.2.4 **Statutory provisions**

Mandatory statutory provisions governing the extended coverage period that go beyond A3.2.3 take precedence over these provisions.

A3.2.5 **Loss prevention costs**

A claim for loss prevention costs is deemed to be asserted on the date on which the *policyholder* or an *insured* first determines that a loss is imminent.

A3.2.6 **Serial loss**

The total of all the claims arising from the same cause and the consequences of several acts or omissions in the same matter are considered to be one event (serial loss). The number of injured parties, claimants or persons entitled to claim is irrelevant.

A4 Term of the insurance contract

The insurance contract begins on the date specified in the policy. It is concluded for the term specified in the policy, after which it is automatically renewed for another year. If the insurance contract is concluded for less than one year, it expires on the date specified in the policy. Any provisional insurance coverage that may be in place expires once the policy is issued.

AXA may reject the application. Any provisional insurance that may be in place expires three days following receipt of the notice of rejection by the applicant. In this case, the applicant shall owe the pro rata premium for the period of coverage.

A5 Termination of the insurance contract

A5.1 **Termination effective at the end of the insurance year**
Either contracting party may terminate the insurance contract in writing or in another form of text as of the end of any insurance year, subject to compliance with a period of notice of three months (annual right of termination).

A5.2 **Termination in the event of a claim**
After a loss event for which AXA provides indemnity, the insurance contract may be terminated as follows:
- By the *policyholder*, no later than 14 days after they become aware of the payment of the indemnity, with coverage expiring 30 days following receipt by AXA of the notice of termination.
- By AXA, at the latest when the indemnity payment is made, with coverage expiring 30 days following receipt by the *policyholder* of the notice of termination.

A5.3 **Termination in the event of an increase in risk**
A13.5 applies.

A6 Premiums

The premium specified in the policy is due on the first day of each insurance year; the due date for the first premium is specified on the invoice. In the case of payment in installments, the installments due during the insurance year are deemed to be deferred. AXA may add a surcharge to each installment.

A7 Sum insured and indemnity limits

The sum insured or indemnity limits constitute a single aggregate per insurance year.
If the claims, losses and costs per event (including claims and costs in connection with risks to which indemnity limits apply) exceed the sum insured specified in the policy, AXA will pay no more than the sum insured (maximum compensation).

A8 Deductible

The deductible specified in the policy applies.
The deductible is deducted from the calculated loss or damage. It also applies to costs such as those for the defense against unjustified claims or crisis management.
If multiple coverages are triggered for the same loss event, the deductible will only be subtracted once. In this case, the highest deductible applicable to the coverages triggered will be the one subtracted.

A9 Cyber insurance takes precedence

In the event of a cyber loss, this cyber insurance takes precedence over any other insurance policies taken out with the AXA Group by the *policyholder* or an *insured* .

A10 Cumulation clause

If a claim affects more than one policy (insurance contract) concluded by the *policyholder* or an *insured* with the AXA Group, the maximum benefit payable by the AXA Group is limited to the highest sum insured specified in any of these policies per insured event and insurance year. If benefits are claimed under more than one policy, the deductible is deducted separately for each policy.

A11 Duty of care and other obligations

A11.1 **Duty of care when handling data**
The *policyholder* is obliged to exercise a duty of care. In particular, it must take the measures required by the circumstances in order to protect insured *data* against the insured risks.

A11.2 **Measures**
The *policyholder* must take the following measures:
- A backup of all *data* must be performed at least once a week. By way of an amendment to E5 (Data), operating systems and programs (apart from programs produced within the company) do not fall under the definition of data. This requirement does not apply to operating systems or to programs not produced within the company.
- At least one weekly backup of data must be stored separately from the network of the *policyholder*. In addition, the network-independent data backup as well as programs and licenses must not be stored in such a way that they could be damaged, destroyed or lost together with the originals.

The obligation to perform a backup does not apply to the use of an external *cloud computing system* that is not operated by the *policyholder* or an *insured*, as long as the provider of the *cloud computing system* has agreed by contract to perform the data backup. The data backup must meet the above-mentioned requirements.

A11.3 **Protective systems**
The *policyholder* must
- use a manufacturer-supported operating system that comes with security updates and must use protective systems (such as internet protection programs, antivirus software and firewalls).
- apply security patches for software and operating systems within 30 days of their release in the event that critical security vulnerabilities (zero-day exploits) are identified.
- apply the manufacturer-recommended security updates (patches) to operating systems, protective systems, user programs and software in connection with online shops and websites in a timely manner after the release date.

A11.4 Breach of duty of care

If any duty of care, security regulations or other obligations are culpably breached, the indemnity may be reduced commensurately with the degree to which the breach affected the occurrence or extent of the loss or damage.

If it is discovered in the event of a claim that, for example,

- the last data backup was performed more than one week ago, only the costs that would have been incurred if the data backup had been performed as required will be taken into account for calculation of the compensation.
- no usable data backup is available, only the costs of establishing this fact are covered.

A12 Duty to provide information

A12.1 Communication with AXA

The *policyholder* must address all communications to the relevant branch office or registered office of AXA.

A12.2 Claims

D1 applies.

A12.3 Termination of the insurance contract

A5 applies.

A13 Increase or decrease in risk

A13.1 Contingent insurance for new risks and changes in material circumstances

If a new risk presents a significant increase in risk (e.g. changed or new activities) or there is a change in a material circumstance relevant to the assessment of the risk, the scope of which was determined by the contracting partners when replying to the questions in the application, the insurance also covers the new risk or changed circumstance within the scope of the contractual conditions (contingent insurance).

A13.2 Duty to notify

By the end of the insurance year at the latest, the *policyholder* must notify AXA, in writing or in another form that allows proof by text, of the increase in risk pursuant to A13.1, and include the following information:

- the change in circumstances that is of significance for assessing risk. An increase in risk is deemed to be, for example, an increase of more than 25% in the amount of webshop sales than were determined at the time the contract was concluded .

A13.3 Contingent insurance for new companies

Newly added companies (acquired or newly founded) domiciled in Switzerland or the Principality of Liechtenstein are also co-insured on a provisional basis within the scope of this insurance contract, provided that the *policyholder* directly or indirectly holds more than 50% of their capital. The underinsurance clause of the contractual provisions underlying the policy does not apply if the cause of underinsurance can be attributed to the new companies.

For companies that are acquired, contingent insurance applies only if they are not otherwise insured for the same interests or the same risks and their area of activity corresponds to the insured risk listed in the policy.

The *policyholder* is required to notify AXA of the following no later than three months after the end of the financial year in which new companies are added:

- Name, domicile, legal form, business purpose, size of shareholding
- Date on which operations commenced or on which the new company was founded or acquired (= commencement of risk)
- Sales of the new company or new total sales as a result of these changes

A13.4 Rights of AXA

In respect of the newly added companies or a change in risk, AXA reserves the right:

- to redefine the premium and conditions retroactively
- to reject their inclusion
- to terminate the contract within 14 days of receipt of the notification

If AXA refuses to accept the new company or the changed risk, or if it terminates the insurance contract, the contingent insurance or the insurance contract will expire 30 days following receipt by the *policyholder* of the written rejection or notice of termination.

AXA is entitled to the premium corresponding to the risk from the date when coverage begins until the date when the contingent insurance or the insurance contract expires.

A13.5 Policyholder's right of termination

The *policyholder* can terminate the insurance contract within 14 days if no agreement is reached on the new premium or the new provisions. The insurance contract ends 30 days following receipt of the notice by the other party.

AXA is entitled to the premium corresponding to the risk from the date when coverage begins until the date when the contingent insurance or the insurance contract expires.

A13.6 Decrease in risk

In the event of a significant decrease in risk, the *policyholder* is entitled to terminate the insurance contract, in writing or in another form that allows proof by text, by giving four weeks' notice, or to request a reduction in premium.

If the *policyholder* requests a reduction in premium, AXA will reduce the premium correspondingly from the date on which it receives notification from the *policyholder*.

If the *policyholder* is not in agreement with the reduction in premium, it may terminate the insurance contract within four weeks of receipt of notification of the new premium by giving four weeks' notice in writing or in another form that allows proof by text.

A14 Principality of Liechtenstein

If the *policyholder* has their domicile or registered office in the Principality of Liechtenstein, the references to provisions of Swiss law contained in the insurance contract documents shall be construed as referring to the corresponding provisions of Liechtenstein law.

A15 Applicable law and place of jurisdiction

A15.1 Applicable law

This insurance contract is governed by Swiss law. For contracts that are governed by Liechtenstein law, the binding provisions of the Liechtenstein law take precedence if they differ from these General Insurance Conditions (GIC).

A15.2 Place of jurisdiction

The ordinary courts of Switzerland and, in the case of *policyholders* having their domicile or registered office in the Principality of Liechtenstein, the ordinary courts of Liechtenstein, have exclusive jurisdiction over any disputes arising out of or in connection with the insurance contract, including any lawsuits filed by *insureds* or *third parties* for indemnification for liability claims.

A16 Place of performance

Compensation paid to the *policyholder*, *insureds* or *third parties* under this insurance contract is to be paid exclusively to the registered office of the *policyholder* or to the registered office of AXA.

A17 Sanctions

AXA will not provide insurance cover, claims payments or other benefits to the extent that the provision of such benefits would expose AXA to any sanction, prohibition or restriction under any UN resolution or any trade or economic sanctions, laws or regulations of the European Union, the United Kingdom, the United States of America or Switzerland.

A18 Assignment of claims for compensation

Claims for compensation to which the *policyholder* or an *insured* is entitled against *third parties* devolve to AXA to the extent of the benefits paid by AXA. The *policyholder* or the *insured* is liable for all acts or omissions that could negatively affect the rights of recourse. Coverage will lapse if any *third parties* are released from liability without the consent of AXA.

Part B
Scope of Insurance

B1 First-party cyber event

B1.1 Costs of restoration

B1.1.1 **Subject of the insurance**

The insurance covers the policyholder's own *data*. The policyholder's own *data* is defined as data created or purchased by the policyholder itself, used for its own purposes and located on the *policyholder's IT system* or on *cloud computing systems*. The insurance also covers *data* from *third parties* that is located on the policyholder's IT system and managed by the *policyholder*.

The insurance also covers the cost of restoring private *data* of the insureds, provided that such data was permitted to be present on a device of the *policyholder* in accordance with the internal guidelines. For private *data*, the maximum compensation per device affected is limited to CHF 5,000 per insurance year within the scope of the sum insured applicable to this insurance contract.

B1.1.2 **Insured risks**

The insurance covers the destruction, impairment, loss, modification or non-availability of *data* according to B1.1.1.

The insurance also covers the costs of restoration in the event of extortion, e.g. via ransomware.

B1.1.3 **Compensation**

For a maximum of one year after the loss occurrence, AXA covers the costs of restoring *data* to the condition it was in immediately prior to the loss that the *policyholder* suffered as a result of a *first-party cyber event* (exhaustive list):

- costs of restoring the *data* from backup
- reconstruction of the *policyholder's* physical documents for the last seven days prior to the loss assessment
- the costs of removing *malware* from the *policyholder's IT system*
- reinstalling and configuring the *policyholder's* operating systems and user programs
- the costs to the *policyholder* of acquiring new licenses if their acquisition is unavoidable and the obligations pursuant to A11.2 have been met

If the *first-party cyber event* occurred on a *cloud computing system* rather than on the *policyholder's* system, the *policyholder's* costs of restoration are covered on a subsidiary basis in amendment of A9.

B1.2 Business interruption

B1.2.1 **Subject of the insurance**

The insurance covers:

- Loss of earnings
  Revenue is covered as loss of earnings. Revenue is defined as:
  - for trading businesses: the proceeds from the sale of traded goods
  - for service sector businesses: the proceeds from the services rendered
  - for manufacturing businesses: the proceeds from the sale of goods produced
- Additional costs
  AXA covers additional costs actually incurred, i.e. extraordinary expenses which, due to the circumstances and for operational reasons, are necessary and cost-effective to maintain operations to the expected extent for the duration of the interruption. Additional costs are deemed to include loss mitigation costs, in particular costs incurred by the eligible claimant to mitigate loss during the indemnity period in compliance with the obligation to mitigate loss in pursuant to D1.4.

B1.2.2 **Insured risk**

The insurance covers loss or damage due to an interruption that occurs if it is temporarily impossible to continue the operation insured under the policy, or if such operation can only be continued in part.

The interruption must have been caused by a *first-party cyber event*. The *policyholder* must prove that there is an adequate causal connection between the insured damaging event and the loss or damage resulting from the interruption.

B1.2.3 **Compensation**

AXA is liable for the loss or damage for a maximum of one year calculated from the date of the occurrence of the loss event (indemnity period).

If, in the event of a claim, it is discovered that there is no functional data backup that is more than one week old, AXA will be liable for the loss or damage resulting from the interruption only to the extent that it would have been liable if there had been a functional backup.

The waiting period is twelve hours. Any business interruptions of less than twelve hours are not insured. The waiting period is not deducted from business interruptions lasting more than twelve hours.

Compensation includes

- **Loss of earnings**
  AXA compensates the difference between the revenue generated during the indemnity period and the revenue expected without the business interruption, minus the difference between the assumed costs and the costs actually incurred.
  AXA indemnifies unproductive expenses if the loss or damage occurs in an associated maintenance facility or in a research or development laboratory. These expenses are calculated on the basis of the costs that are charged to this facility during the interruption, but not past the indemnity period.
- **Additional costs**
  AXA compensates additional costs in accordance with B1.2.1.
  Supplements for shift and night work, overtime allowances, or the employment of additional staff (temporary employees) are compensated if AXA provided its agreement in advance.
  Any costs saved are deducted.
- **Special circumstances**
  The calculation of the loss must take account of circumstances that would have influenced revenue during the indemnity period even if the interruption had not occurred.

If operations are not resumed after the loss event, AXA will only cover the effective ongoing running costs to the extent that they would have been covered by gross profit had there been no interruption. The calculation is based on the presumed length of the interruption during the indemnity period.
The loss assessment is based on the numbers provided by the companies insured under the policy that are directly and indirectly affected by the loss. If a loss of gross profit can be fully or partially offset by additional income or reduced costs at another insured company, this will be taken into account (interdependency losses).
Circumstances not insured pursuant to B1.2.3, point six, letters b and c, are not taken into account when calculating the loss.

- **Underinsurance**
  If the insurance contract is based on revenue that is too low, the loss will be reimbursed only in the ratio of the declared amount to the assessed amount. In this case, the financial year specified in the policy applies.
- **Provisional revenue**
  The provisional revenue specified in the policy serves as the basis. The *policyholder* must report the definitive amount of revenue no later than six months after the end of the financial year specified. If this report is not submitted, the provisional revenue taken as the basis will be deemed definitive.
  If this amount proves to be too low, compensation will be reduced in accordance with the aforementioned point four, Underinsurance.
- **AXA accepts no liability for any increase of the loss or damage:**
  a) that is attributable to contributory causes that are not sufficiently causally related to the first-party cyber event, such as delays in the delivery of spare parts or property damage
  b) in connection with changes to, expansions of or upgrades to the IT system that were carried out after the loss event
- **Contingent business interruption loss**
  The insurance does not cover contingent business interruption loss due to third-party companies. Contingent business interruption loss is deemed to include, in particular, damage or loss in third-party companies which leads to an interruption of the policyholder's own business although none of the policyholder's own *data* is affected.

B1.3 Breaches of data protection

B1.3.1 Insured risks and losses

The insurance covers *breaches of data protection* caused by a *first-party cyber event*.

B1.3.2 Subject of the insurance

The insurance covers expenses incurred by the *policyholder* or an *insured* following a breach of data protection laws in order to inform authorities, the public and potential data subjects, as required by law (first-party loss). Claims by *third parties* arising from *breaches of data protection* are not covered by the insurance.
The insured costs include (exhaustive list):

- legal advice from an external lawyer specializing in IT/data protection law, if this service cannot be provided by AXA
- identification of the data subjects in the event of *breaches of data protection*. These costs also include the costs of their being notified by the *policyholder* itself or notified by a notification service. The costs of communicating with the competent authorities are also insured
- setting up a telephone hotline (call center) and an internet portal in order to answer inquiries from data subjects
- credit monitoring services performed as a direct consequence of a *breach of data protection* for a period of up to twelve months following an actual *breach of data protection*, provided these are necessary because of the type of *data* that has fallen into unauthorized hands or because of legal requirements
- the costs (such as lawyer's fees, investigation expenses, court costs and fees for expert opinions) that the *policyholder* or insureds incur in connection with criminal, regulatory or administrative proceedings brought against the *policyholder* or an *insured* by an authority. If a decision by a court of first or second instance is appealed, AXA may refuse to pay further benefits if the appeal seems unlikely to succeed. AXA will appoint a lawyer to represent the *policyholder*, with their agreement. If none of the lawyers proposed by AXA is accepted, the policyholder must suggest three lawyers from different law firms, from which AXA will select the lawyer to be retained. Any non-court costs and lawyer's fees awarded to the *policyholder* must be transferred to AXA to the extent of the benefits it has paid, as long as they are not compensation for personal efforts and expenses of the *policyholder*. The *policyholder* must inform AXA immediately about any information with respect to the legal proceeding and follow AXA's instructions.

B1.3.3 Requirement for the assumption of costs

The insured costs set out under B1.3.2 must be reasonable and should be agreed with AXA in advance (insofar as this is not already a legal requirement) and approved by AXA.
If *data* is stored with an external service provider (e.g. cloud provider), the policyholder must ensure by means of contract that the external service provider will comply with the applicable data protection laws. A11.4 is applicable.

B1.4 Loss assessment

Both the *policyholder* and AXA may request that the loss be assessed immediately. The loss must be assessed either by the parties themselves, by a jointly appointed expert, or through a loss adjustment procedure. Each party may request that a loss adjustment procedure be conducted pursuant to B1.6.
The *policyholder* must provide proof of the event and of the amount of damage at its own expense.
In the case of insurance on third-party account, AXA reserves the right to assess the damage only with the *policyholder*.
AXA may decide which companies should rectify the damage.
Business interruption loss is determined at the end of the indemnity period. It may be ascertained earlier, however, if both parties agree.
The measures ordered by AXA or by *third parties* engaged by AXA in order to ascertain, mitigate or prevent a loss, or to preserve or assert rights of recourse, in no way constitute acknowledgment of the obligation to pay benefits.

B1.5 Payment of compensation

Compensation is due four weeks from the date on which AXA is in possession of all the information necessary to determine the insurance benefit.

Four weeks after the occurrence of the loss, the *policyholder* may request a first part payment in an amount determined on the basis of the current status of the loss assessment.

AXA's obligation to pay will be deferred as long as the amount of the indemnity cannot be determined or paid due to culpable conduct on the part of the *policyholder*. In particular, no payment will be due as long as

- it is unclear to whom the insurance benefit is lawfully to be paid
- police or investigating authorities are investigating circumstances in connection with the event
- criminal proceedings against the *policyholder* are still in progress

B1.6 Expert loss adjustment procedure

The following principles apply to the loss adjustment procedure:

1. Each party must appoint an expert in writing. Before the loss assessment begins, the experts select an umpire in writing. If a party fails to appoint its expert within 14 days after having been requested to do so in writing, the competent judge will appoint one at the request of the other party; the same judge will also appoint the umpire if the experts are unable to agree on one.
2. Persons who lack the necessary expertise or who are related to one of the parties or are otherwise biased may be rejected as experts. If the reason for rejection is in dispute, the decision will rest with the competent judge, who will then appoint the expert or umpire if the objection is justified.
3. The experts determine the cause, detailed circumstances and amount of the loss or damage. If there are any discrepancies between the assessments, the umpire decides on the remaining points in dispute within the upper and lower limits of both assessments.
4. The assessments made by the experts within the scope of their competence are binding unless proven by one party to vary significantly from the actual circumstances.
5. Each party pays for their own expert. Each party pays half the costs of the umpire.

B2 Cyber liability event

B2.1 Subject of the insurance

AXA offers coverage against claims for damages arising from a *cyber liability event* that are brought against the *policyholder*, an *insured* or AXA as their liability insurer, for *financial loss* on the basis of statutory liability provisions.

The insurance also covers claims brought against the *policyholder* or *insureds* for any loss or damage caused by auxiliaries. Companies and independent professionals (subcontractors) engaged by the *policyholder* or insureds are considered to be auxiliaries.

The insurance does not cover the personal liability of these companies and professionals.

The insurance covers claims of *third parties* arising from

- destruction of, damage to, loss, modification or non-availability of *data* of a *third party* that was in the possession of the *policyholder* or of a party to whom the *policyholder* had entrusted such data
- destruction of, damage to, loss, modification or non-availability of *data* on the *IT systems* of a *third party*
- *breach of data protection*
- breach, theft or loss of confidential data. This includes the unauthorized publication or any breach of copyright, rights to a name and trademark rights in connection with data that was in the possession of the policyholder or of a party to whom such *data* was entrusted by the policyholder.

B2.2 Insured benefits

B2.2.1 **Compensation for justified claims**

AXA will pay the amount that the *policyholder*, an *insured* or AXA as their liability insurer, is required to pay to the injured party as compensation within the scope of the coverage and the statutory liability provisions. AXA may pay compensation to the injured party directly.

B2.2.2 **Defense against unjustified claims**

In the case of an insured event, AXA will cover the costs of defending against unjustified or excessive claims for damages that are brought against the *policyholder*, an *insured* or against AXA as their liability insurer.

B2.2.3 **Scope of indemnity**

In the case of *cyber liability events*, AXA's indemnity for all claims is limited to the sum insured specified in the policy. This includes interest on damages, loss mitigation costs, attorney fees, court costs, costs of expert opinions, arbitration and mediation, loss prevention costs and other costs, such as indemnification of the opposing party's legal expenses. Certain risks included in the insurance may be subject to an indemnity limit specified in the policy (limit within the sum insured).

Indemnity and limits are governed by the contractual provisions (such as provisions relating to sums insured or deductibles) that were in effect at the time the claim was first asserted pursuant to A3.2.1.

If the insured indemnity or the scope of insurance is expanded, insurance coverage is provided under the new agreements only if the *policyholder* or the *insured* was unaware of any act or omission that could give rise to their liability prior to the date on which the contract amendment entered into effect.

B2.2.4 **Responsibility for claims handling**

AXA will handle claims asserted if they exceed the deductible, up to the amount of the sum insured. It will conduct negotiations with the injured party at its own expense. In this regard, it acts as representative of the *policyholder* or the insured. Settlement by AXA of the claims of the injured party is binding on the *policyholder* or the *insured*.

B2.3 Legal action

If no understanding is reached with the injured party and if this party takes legal action, the following applies:

B2.3.1 **Lawsuit against the policyholder or an insured**

AXA, in consultation with the *policyholder* or the *insured*, appoints the trial lawyer and determines the trial strategy, the outcome of the proceeding (acknowledgment, settlement or judgment) and all other procedural steps. In this regard, it acts as representative of the *policyholder* or the insured. AXA will assume the costs of litigation and attorney fees incurred by the *policyholder* or the *insured*. It is authorized to reach an agreement with the trial lawyer regarding fees. AXA is entitled to any legal expenses awarded to the *policyholder* or the *insured*. However, the *policyholder* or the *insured* may retain any personally awarded compensation for their efforts.

B2.3.2 **Lawsuit against AXA**
AXA appoints the trial lawyer, determines the trial strategy, the outcome of the proceeding (acknowledgment, settlement or judgment) and all other procedural steps. AXA will assume the litigation expenses and attorney fees incurred as part of the insured benefits. AXA will keep the *policyholder* or the *insured* informed about the proceeding.

B2.3.3 **Lawsuit against an insured**
AXA decides, if possible and after consultation with the *policyholder* or the *insured*, on a trial lawyer to jointly represent the *policyholder* or the *insured* and AXA. B2.3.1 and B2.3.2 apply in all other respects.

B2.4 Arbitration proceedings
Settlement of insured claims in proceedings before an arbitration tribunal will not affect coverage, provided that the proceedings are conducted in accordance with the rules of the Swiss Civil Procedure Code and the Federal Act on International Private Law.

B2.5 Contractual fidelity
The *policyholder* and the *insured* are required to respect contractual fidelity. They may not, without the consent of AXA, conduct any direct negotiations with the injured party, acknowledge any liability or claims, enter into any settlement or pay any compensation. They may not assign coverage claims without the consent of AXA.

B2.6 Lawsuit against the policyholder or the insured
AXA has a right of recourse against the *policyholder* or the *insured*, provided that it would be entitled, pursuant to the provisions of the insurance contract or the Federal Act on Insurance Contracts (ICA), to refuse or reduce its insurance benefit.

B3 Crisis management

B3.1 Incident response
The insurance covers the costs of *incident response* measures incurred when an insured risk pursuant to B1.1.2 occurs. A reasonable belief that such an event has occurred is also sufficient.
In particular, the insurance covers the costs of an expert provided to the *policyholder* by AXA for the purpose of *incident response*.
In the event of a critical security incident, the *policyholder* may contact the expert provided by AXA and instruct them to take *incident response* measures, without having to obtain consent from AXA in advance. AXA will pay a maximum of CHF 5,000 per claim for this, without the requirements in B3.4 having to be met.
The *incident response* measures are not charged against the deductible or the sum insured for *cyber events*. This also applies if the event does not turn out to be an insured loss event.

B3.2 Crisis consulting
In the case of an insured event, AXA will pay the costs of
- experts to identify security gaps in the *IT system* of the *policyholder*,
- advice to the *policyholder* regarding the prevention of any other loss events of a similar kind.

B3.3 Crisis communication
If the *policyholder* is faced with the risk of critical media reporting due to an event insured under these GIC, AXA will pay the costs of a PR agency to support and assist the *policyholder* in order to promptly prevent or mitigate any potential reputational damage.

B3.4 Requirement for the assumption of costs
According to B3.1 to B3.3, a requirement for the assumption of costs is that the expenses are agreed with AXA in advance and AXA has issued a confirmation of coverage in text form. This does not apply to a critical security incident as described in B3.1.
However, in this case too the claim must be reported immediately. AXA must agree to any continuation of activities by an expert.

B4 Manipulation of e-banking, the online shop or the shipment of goods

If specified in the policy, the insurance covers:

B4.1 Subject of the insurance
The insurance covers *financial loss* suffered by the *policyholder* or an *insured due to a cyber event*. The *financial loss* must have been caused due to intentional manipulation within the scope of the respective application and/or associated databases pursuant to B4.1.1 to B4.1.4.

B4.1.1 Manipulation of e-banking (electronic payments)
The insurance covers applications (such as e-banking, accounting programs, etc.) which the policyholder or an insured uses and which facilitates the outgoing, electronic payments. A requirement of the insurance coverage is that the *policyholder or an insured follow the recommendations of their financial institution and use the most secure option for online banking offered by that financial institution.* This must, in every case, include two-factor authentication. The insurance also covers manipulation of payment orders that are scanned into e-banking systems. *If the financial institution covers the loss in full or in part, AXA will bear the loss, within the framework of the indemnity limit, to the extent that this must be borne by the policyholder or the insured.*
C1.13 does not apply as part of this supplementary coverage.

B4.1.2 **Manipulation of the online shop and the shipment of goods**
The insurance covers applications used by the *policyholder* or an *insured* and which serve to operate an online shop or similar internet portal. A requirement for insurance coverage is that the online shop software transmits all data in encrypted form. The insurance also applies if goods ordered from the *policyholder* are delivered or diverted incorrectly as a result of data manipulation.

B4.1.3 **Manipulation of the website**
The insurance covers applications used by the *policyholder* and which serve to create and operate a website. A requirement for insurance coverage is that the website uses encrypted protocols.

B4.1.4 **Manipulation of online shopping orders**
The insurance covers applications that are used by third parties and used by the *policyholder* to order goods from these third parties. For online shopping, a requirement for insurance coverage is that all online shop data be transmitted in encrypted form and that the offer by the third party is a legal one. If the online retailer covers the loss entirely or in part, AXA will bear the loss, within the framework of the indemnity limit, to the extent that this must be borne by the *policyholder*.

B4.2 Compensation in the event of first-party loss
Payment of compensation requires that the *policyholder* prove the occurrence and the amount of the loss. The comparison of a current state with an envisioned state without further information about how the differences arose or statistically derived *data* does not constitute adequate proof.

B4.3 Compensation for liability claims
Compensation is governed by B2.

B5 Phone hacking and misuse of the IT system

If specified in the policy, the insurance covers:

Phone hacking or misuse of the IT system or the unauthorized use of the telephone equipment or the IT system by third parties as a result of a first-party cyber event. The resulting financial loss due to the increased telephone or electricity bill is compensated.
Under this supplementary coverage, C1.16 does not apply.

B6 Social engineering

If specified in the policy, the insurance covers:

financial loss incurred in connection with social engineering attacks. Social engineering occurs when third parties make personal contact with the policyholder or an insured (by telephone or electronically, for example) in order to exploit, under false pretenses, their willingness to help, good faith or uncertainty, and to induce them to disclose confidential data such as user names or passwords orally or in writing to the third parties, or to perform certain actions (such as a transfer of monetary assets or a delivery of goods, for example). Financial transactions are required to be checked for new or changed payment coordinates. In the case of new or changed payment coordinates, their accuracy and allocation to the correct payee must be verified by means of additional traceable authentication (telephone callback, for example) and the authenticity of the transaction order must be ensured. The review must be documented in writing. If this requirement is breached, insurance coverage under this supplementary coverage will lapse. This supplementary coverage does not extend to expenses and costs incurred as a result of acts that predated the social engineering attack and represent a cyber event. No coverage exists if the social engineering attack was carried out in cooperation with an insured. C1.11 does not apply as part of this supplementary coverage.

Part C
General Exclusions

C1 General exclusions

The insurance does not cover:

C1.1 Losses, damage, liability, costs or expenses of any kind as a result of war, cyber operations and comparable acts.

C.1.1.1 War: Warlike events, violations of neutrality, revolution, rebellion, uprising, civil unrest and the measures taken to counteract these;

C.1.1.2 Cyber operations and comparable acts that are carried out as part of a war;

C.1.1.3 Cyber operations that cause significant adverse effects on the vital functions, security or defense of a sovereign state;
or

C.1.1.4 Cyber operations that result in or form the basis of a response by a sovereign state that include the following:
- use of force or
- a cyber operation that impacts another sovereign state in such a way that is the equivalent to the use of force.

C.1.1.5 Insurance coverage is provided if the policyholder can prove that the loss is in no way related to the events described in C1.1.1 to C1.1.4.

C1.2 losses, damage, liability, costs or expenses of any kind that can be traced directly or indirectly to terrorism, regardless of any contributory causes. Terrorism is defined as any act of violence or threat of violence to achieve political, religious, ethnic, ideological or similar objectives designed to spread fear and terror among the population or parts of it, or to influence a government or state institution.

C1.3 loss or damage in connection with the deliberate use of pirated copies by the *policyholder* or an *insured.*

C1.4 loss or damage in connection with contractual penalties, fines and financial penalties or compensation of a punitive nature.

C1.5 loss or damage in connection with public law orders

C1.6 *bodily injury and property damage* including the resulting loss of asset value, loss of earnings and compensation for pain and suffering.

C1.7 loss or damage arising from a contractually assumed liability that goes beyond liability in law.

C1.8 loss or damage in connection with nuclear damage as defined in the Swiss legislation on nuclear energy liability, and the associated costs, or in connection with asbestos and with the action of ionizing and non-ionizing radiation and of electromagnetic fields (EMF).

C1.9 loss or damage due to further acts by employees after the persons entrusted with the management or supervision of the insured companies became aware of an intentional or deliberate act that had previously been committed by these employees.

C1.10 loss in connection with virtual currencies such as Bitcoin

C1.11 loss arising from the fraudulent use of credit, bank, customer identification or other cards (card fraud).

C1.12 loss in connection with the failure, interruption or reduction in services of public utilities and infrastructure or of external service providers (e.g. telecommunications companies). This exclusion does not apply to *cyber events* affecting *cloud computing systems* used under contract by the *policyholder* or *insureds*.

C1.13 payments made in response to blackmail

C1.14 loss in connection with e-banking or electronic payment transactions

C1.15 loss in connection with stock exchange and securities transactions

C1.16 Increased telephone or electricity bills pursuant to B5.

C1.17 Claims
- by natural persons and legal entities, trusteeships and trusts that have a direct or indirect financial interest of at least 30% in the business of the policyholder or an insured.
- by companies under the same management as an insured company (e.g. companies controlled by the same natural person).
- co-insured companies against other co-insured companies or against the policyholder and vice versa.

This exclusion does not apply to claims of an insured as a result of an event pursuant to B2.1, third point, that leads to unauthorized disclosure of personal data.

Part D
Claims

D1 Obligations

D1.1 **If an insured event occurs, the policyholder must**

- notify AXA as quickly as possible
- provide information about the cause, amount and detailed circumstances of the loss or damage. Unless otherwise agreed, this information must be provided in writing
- allow AXA and the experts to conduct any investigation into the cause, amount and detailed circumstances of the loss or damage and the extent of the obligation to pay benefits, and assist AXA with its clarifications. For this purpose, the policyholder is required to submit financial accounting, cost and performance accounting, accounting documents and other information on the course of business for the current financial year and previous years, if applicable, as well as statements with respect to payments from other insurance companies
- provide, at their own expense, the information required to substantiate the claim for compensation and to determine the scope of the indemnity and to submit relevant documents (such as, for example, detailed lists of third-party and in-house services, description of how the loss occurred, including evidence of any compromise of the IT system and relevant log files), in which case AXA may set reasonable deadlines
- make every effort during and after the event in order to mitigate the loss, and follow instructions from AXA or AXA's authorized representative in doing so
- file a criminal complaint at its own expense in consultation with AXA

A11.4 applies to any breach of these duties.

D1.2 **Assessment in the event of a claim**

If, in the event of a claim, it is determined that the IT security precautions or protective systems are inadequate, appropriate measures must be implemented at the expense of the *policyholder*.

D1.3 **Breaches of data protection**

In the case of *breaches of data protection*, the *policyholder* must also

- notify the police immediately and request an official investigation
- collaborate with the investigating authorities and AXA in taking steps to identify the offenders

D1.4 **Business interruption**

In the case of business interruption, the *policyholder* must also

- ensure that the loss or damage is mitigated during the indemnity period. During the indemnity period, AXA has the right to request that all precautions that it considers suitable be implemented, and to examine the measures taken
- inform AXA when full operations are resumed, if this occurs during the indemnity period
- at the request of AXA, provide an interim report at the beginning and end of the interruption or indemnity period. AXA or its experts are authorized to participate in taking the inventory.

D2 Replacement of IT systems

If it transpires that the replacement of an *IT system* or a part thereof is less expensive than the expected compensation, AXA may, in amendment of C1.6, decide to replace the *IT system* (or parts thereof) affected by the *cyber event*.

D3 Limitation period under this insurance contract

Claims arising from the insurance contract become time-barred five years following the occurrence of the event on which AXA's obligation to indemnify is based.

Part E
Definitions

E1 Cloud computing systems

Cloud computing systems make IT infrastructures such as computing capacity, data storage, network capacities or ready-made software available via a network, without the requirement for the installation of such infrastructures on the local *IT system*.

E2 First-party cyber event

A first-party cyber event is a deliberate, damaging attack by third parties or by insureds on the IT system of the policyholder or on cloud computing systems used by the policyholder. A first-party cyber event must be caused by malware, a hacker attack or a denial-of-service attack via networks. An attack using a digital data carrier connected with the IT system of the policyholder is also deemed to constitute a first-party cyber event.

E3 Cyber liability event

A cyber liability event is a deliberate attack by *third parties* on the *IT system* of the *policyholder* or on *cloud computing systems* used by the *policyholder*, which causes damage to other *third parties*. A deliberate attack by *insureds* on the *IT system* of a *third party* is also deemed to constitute a cyber liability event, provided that the *IT system* of the *policyholder* is misused or the attack occurs via a digital data carrier linked with the *IT system* of the *third party*. A cyber liability event must be caused by *malware*, a hacker attack, or a *denial-of-service* attack either via networks or via digital data carriers.

E4 Cyber event

Both *first-party cyber events* and *cyber liability events* are deemed to be cyber events.

E5 Cyber operation

Cyber operation means the use of a computer system by, at the direction or under the control of a sovereign state to change, block, compromise, manipulate, publish or destroy information or access to this information on a computer system of another sovereign state.

E6 Data

Data is information stored electronically on data carriers such as operating systems, programs and user data. Data is not considered to be property.

E7 Breach of data protection

A breach of data protection is the unauthorized acquisition of, access to and use or disclosure of personal data that was in the possession of the *policyholder* or of another party to whom the *policyholder* had entrusted said *data*. A breach of data protection is only deemed to occur if the confidentiality or security of the data is compromised in such a way that the data subjects may suffer *financial loss* or if the *policyholder* thereby becomes legally obligated to disclose this breach to the data subjects and/or to the public.
In the event of any breaches of data protection, *insureds* are deemed to be *third parties*.

E8 Denial of service (DoS)

Denial of service means the disruption of a service as a result of an overload of infrastructure systems, for example. This denial of service must have been caused by a deliberate attack on an *IT system*.

E9 Third parties

Third parties are deemed to be all parties who are neither *policyholders* nor *insureds*.

E10 Hacker attacks

Hacker attacks are deliberate changes to programs and data made with the intention of causing damage. In such an attack, hackers obtain unauthorized access via networks, specifically the internet. Changes to programs and data by *malware* are not considered hacker attacks.

E11 IT system

An IT system includes computer hardware and networks (including software) of any kind that process and store *data*: server systems, storage systems, personal computers, notebooks, tablet computers, smartphones, remote data transmission devices, etc.
IT systems also include computer controls for technical devices, machines and equipment that are integrated into networks.

E12 Bodily injury

Bodily injury is considered to mean the death, physical injury or other damage to the health of persons.

E13 Property damage

Property damage is deemed to be the destruction, damage or loss of movable and immovable property. The death or loss of animals, injury to them or other damage to their health are deemed to be equivalent to property damage.

E14 Malware

Malware, evilware and junkware are terms used to describe computer programs developed in order to perform undesired and damaging functions. "Malware" is therefore a generic term which includes computer viruses, computer worms, Trojan horses, ransomware and the like.
Incorrectly programmed software that can cause damage is not considered malware.

E15 Incident response

Incident response measures encompass the costs of identifying and containing a *cyber event*, including the work undertaken by an expert provided by AXA.

E16 Financial loss

Financial loss is a loss quantifiable in monetary terms which is not attributable to any *bodily injury* or *property damage*.

E17 Insureds

Insureds are deemed to be:

- the representatives of the *policyholder* and the persons entrusted with the management or supervision of the company, in respect of their activities for the insured company
- the employees and other auxiliaries of the *policyholder* (except sub-contractors, etc.), in connection with their activities for the insured company. Members of the Board of Directors or the Board of Trustees are not considered employees
- spouses, registered partners, heirs and legal representatives of insureds, to the extent that claims are asserted against them instead of against the insureds in respect of the insured activities of the latter

E18 Policyholder

The policyholder is deemed to be the natural person or legal entity, partnership, corporation or institution designated as the "policyholder" in the policy. Companies named in the policy as co-insured companies are likewise deemed to be policyholders.
If the policyholder is a partnership or a community of joint owners, the partners or members of the community of joint owners are treated in the same way as the policyholder with regard to rights and obligations.

Want to file a claim?

It's easy and fast – report your claim online at:

AXA.ch/report-claim-companies

by telephone at:

+41 58 218 11 33

AXA
General-Guisan-Strasse 40
P.O. Box 357
8401 Winterthur
AXA Insurance Ltd

AXA.ch
myAXA.ch (customer portal)