CARIBBEAN INSURERS GROUP

Data Privacy Breach Policy

Updated on June 17, 2021

Introduction

The Caribbean Insurers Group ("us", "we", "our") comprises the following British Virgin Islands companies:

- Caribbean Insurers Ltd.
- Caribbean Insurers (Health) Limited
- Caribbean Insurers Marine Limited
- Caribbean Adjusters Ltd
- Caribbean Financing Services Limited

This Data Privacy Breach Policy sets out the steps that should be taken when dealing with a data breach.

What is a data privacy breach?

A data privacy breach refers to the unauthorised access and retrieval of information that may include corporate and personal data. Managing data breaches is very important to protect the personal data of our clients should a data breach occur.

How could a data privacy breach occur?

A data breach, which may or may not involve personal data, can take many forms. A data breach may be caused by employees, external parties to the organisation or by computer system errors. Some examples of possible ways in which a data breach can occur are as follows:

Human error

- Loss of laptop, phone, data storage devices or paper records containing personal data;
- Sending personal data to a wrong e-mail or physical address or disclosing data to the wrong recipient;
- Unauthorised access or disclosure of personal data by employees;
- Improper disposal of personal data that may have been included on a hard drive, storage media or paper documents containing the personal data.

Malicious activities

- Hacking incidents or other illegal access to databases containing personal data;
- Theft of laptop, phone, data storage devices or paper records containing personal data;
- Scams that trick employees or companies into releasing personal data.

Computer System Errors

- Error or bugs in programming code of websites, databases or other software which may be exploited to gain access to personal data.

Data Breach Management Plan

Should there be a data breach, the following management plan is to be strictly adhered to:

Identification and classification

Should a data breach occur, the incident should be reported immediately to the Data Protection Officer or the Managing Director. The following details should be documented:

- Date;
- Time;
- Who reported the breach?
- Description of the breach;
- Details of any IT systems involved;
- Corroborating material or evidence such as error messages or log files;
- A description of the immediate actions taken.

Containment and recovery

The following containment and recovery measures should be considered immediately, where applicable:

- Shut down the compromised system that led to the data breach;
- Prevent further unauthorised access to the system;
- Reset passwords if user accounts or passwords have been compromised;
- Establish whether steps can be taken to recover lost data and limit damage caused by the data breach;
- Isolate the causes of the data breach in the system and change the access rights to the compromised system if applicable and remove external connections to the system;
- Notify the police if criminal activity is suspected and preserve evidence for investigation;
- Notify the British Virgin Islands Financial Services Commission within seven (7) days of the suspected or actual breach and provide and explanation of the steps taken or to be taken to address the breach;
- Put a stop to practices that led to the data breach;
- Address lapses in processes that led to the data breach.

Risk assessment

Knowing the risks and the impact of a data breach will assist in determining the consequences to the affected organisations and individuals. For each data breach, the following should be assessed:

- How many people were affected?
- Whose personal data has been breached?
- To whom does the personal data belong? (clients, employees, vendors or other third parties)
- What types of personal data were involved?
- Is there a risk to reputation, identity theft, safety concerns or financial loss implications to the affected organisations and individuals?
- How sensitive is the information?
- Do any additional measures need to be put in place to minimise the impact of the data breach?
- What caused the data breach?
- When and how often did the data breach occur?
- Who might gain access to the compromised personal data?
- Will the compromised personal data affect transactions with other third parties?
- Who needs to be notified of the data breach?

Reporting of the breach

Clients or individuals affected by the data breach should be notified as follows:

- We will notify organisations and individuals whose personal data breach has been compromised;
- We will notify other third parties such as banks, credit card companies or the police, where relevant;
- We will notify the British Virgin Islands Financial Services Commission within seven (7) days of the breach;
- We will notify the affected individuals immediately if a data breach involves sensitive personal data to allow them to take any necessary actions to avoid potential abuse of the compromised data;
- We will notify affected individuals or organisations when the data breach has been resolved;
- Notifications will be easy to understand, specific and provide clear instructions on what the individuals can do to protect themselves and will include the following:
    - How and when the data breach occurred?
    - The types of personal data involved in the data breach;
    - What we have done or will be doing in response to the risks brought about by the data breach?
    - Specific details on the data breach where applicable and the actions individuals can take to prevent the data from being misused or abused;
    - Contact details of how affected individuals can reach us for further information or assistance.

Evaluation of the response and recovery to prevent future breaches

After the above steps have been taken to resolve the data breach, the cause of the data breach must be reviewed and an evaluation made as to whether the existing protection and prevention measures are sufficient to prevent similar breaches from occurring.

The assessment and evaluation will include whether:

- Audits were regularly conducted on both physical and IT-related security measures;
- There are processes that can be streamlined or introduced to limit the damage if future data breaches should occur or to prevent a re-occurrence;
- There were weaknesses in existing security measures and protection measures or weaknesses in the use of portable storage devices or connectivity to our servers via the internet;
- The methods for accessing and transmitting personal data were sufficiently secure;
- Support services from external parties such as vendors or insurance companies should be enhanced;
- The responsibilities of vendors and insurance companies is clearly defined in relation to the handling of personal data;

- There is a need to develop new data-breach scenarios;
- There are enough resources to manage the data breach;
- Key personnel were given sufficient resources to manage the data breach incident;
- Employees were aware of security-related issues;
- Training was provided on personal data protection matters;
- Employees were informed of the data breach and the lessons learned from the incident;
- Management was involved in the management of the data breach;
- There was a clear line of responsibility and communication during the management of the data breach.

Changes to this data privacy breach policy

We may modify this policy from time to time. When we make changes, we will revise the date at the top of this Data Privacy Breach Policy.