Mosaic Business Solutions Limited, Data Breach Notification Policy

Document Control

Document ref	ISMS202104
Version	1
Dated	22/12/2020
Document author	Russell Fielding
Document owner	Mike Stobbs, Mosaic FSI
Approved by	Mike Stobbs
Confidentiality level	Internal

Revision History

Date	Version	Description	Author
25/01/21	1.1	Q/A	Mike Stobbs

Distribution

Name	Title

Table of Contents

Introduction

FSI Mosaic FSI data breach notification plan covers responsibilities in the case of a data breach incident under the EU General Data Protection Regulation (GDPR) and NZ privacy act 2020.

Regulations and Legislation Background

NZ Privacy Act 2020

Under the NZ privacy act 2020, organisations must notify the Privacy Commissioner (the Commissioner) and the affected individual(s) as soon as practicable after becoming aware of a notifiable privacy breach.

A notifiable privacy breach means a breach that has caused severe harm to an affected individual or is likely to do so.

Mosaic FSI defines harm as including:

1. Specific damage such as financial loss, loss of employment, physical injury, or other forms of harm.
2. Loss of benefits which include any adverse effect on the rights, benefits, privileges, obligations, or interests of the individual.
3. Emotional harm such as significant humiliation, significant loss of dignity or considerable injury to feelings.

For the harm to be considered serious harm depends on the unique circumstances of a privacy breach and requires an assessment on a breach-by-breach basis.

The Privacy Act states that the assessment must include consideration of the following factors:

1. Nature of information - is the nature sensitive such as credit card details or health information.
2. Recipient of personal information course by the breach - The risk of serious harm is likely to be greater if personal data is in the hands of people with unknown or malicious intentions.
3. Mitigation depending on what action has been taken after the breach - cancelling or changing computer access codes, disabling the system, and trying to get lost information back.
4. Nature of harm - The nature of the harm that may be caused to affected individuals.
5. Security measure - Whether a security measure protects personal information. For example, encryption or other security measures.
6. Other relevant factors will depend on the circumstances of the breach, such as how many individuals are affected, how widespread is the breach, and how long has it been occurring.

EU General Data Protection Regulation (GDPR)

When Mosaic FSI are dealing with potential new employees or clients within the EU, Mosaic FSI follows the EU General Data Protection Regulation (GDPR), specifically, regarding data breach Article 33 and Article 34.

Mosaic FSI commits to reporting any data breach involving the personal data of European Union residents within 72 hours if possible.

If the breach is not reported within this time, Mosaic FSI will report possible reasons for the delay.

If a data processor suffers a data breach, Mosaic FSI would inform the data controller immediately.

Within the notification Mosaic FSI would describe the nature of the data breach, contact information for Mosaic FSI the likely consequences of the data breach, and which measures are taken to address and mitigate the data breach.

If the data breach is considered a high risk to the rights and freedoms of data subjects, Mosaic FSI would inform the data subjects of the matter as soon as possible.

Mosaic FSI would create the notification to be easy to understand and contain specific information about the data breach.

Overriding Guidelines

Mosaic FSI follow both data privacy act 2020 and the GDPR and will follow these three overriding guidelines.

1. Are individuals at real risk of harm? If so, notify the individuals as soon as possible, and assist in mitigating the risk. Notify regulators and others (such as law enforcement agencies, payment card fraud teams, etc.) as appropriate or necessary. (if there is a real risk, individuals are notified even if there is no legal obligation to do so.)
2. If individuals are not at real risk of harm, provide notifications as may be required by law.
3. If there is no risk of harm and no legal obligation to notify anyone, document the findings and implement any organisation learning needed to reduce the likelihood of this incident reoccurring.

Mosaic FSI is fully committed to protecting the security and confidentiality of all the personal information that is entrusted to us.

To show this commitment Mosaic FSI has documented and implemented this data breach notification plan.

The notification plan will guide our internal handling of events and incidents that may impact “Personal Data,”.

Personal data is any information that can be used to identify, locate, or contact an individual.

Including:

1. Name,
2. Identification number
3. Location data
4. An online identifier

Or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Personal data breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Mosaic FSI defines a privacy event as any occurrence that could compromise the privacy, confidentiality, security, or integrity of personal data. Privacy events include any deviation from Mosaic FSI privacy or security policies, loss of personal data as well as any unauthorised use or disclosure of personal data.

Examples of Privacy Events:

1. A lost or stolen device containing personal data.
2. Misdirected package, email containing personal data.
3. Presence of malware on a computer or device containing personal data.
4. Transmission of personal data other than as permitted by company policy.

Mosaic FSI requires all employees and contractors to report privacy events via an established process. Mosaic FSI investigate all privacy events, to determine what happened, establish if personal data were compromised, and (if so) evaluate the risk of harm that could result from the situation.

In many cases, privacy events do not expose any personal data to any unauthorised individuals. For example, personal data on a lost laptop may have been encrypted so that any unauthorised person could not view it.

In some cases, privacy events do impact personal data. For example, a lost device may contain unencrypted information. Or an employee may have accidentally transmitted a file containing personal data to the wrong recipient.

If the recipient was able to view the personal data in the file, that information, it is an unauthorised disclosure.

These events are personal data breaches.

In responding to personal data breaches, it is essential that Mosaic FSI quickly and accurately assess the risk of harm. If individuals are at risk of harm, Mosaic FSI policy is to notify the individuals as soon as possible and to help them mitigate the harm. If individuals are a risk, we notify them even if there is no specific legal obligation to do so. If individuals are not a real risk of harm, Mosaic FSI policy is to provide notification as may be required by law.

If there is a high, real risk of harm, Mosaic FSI must take the following steps immediately: Time is of the essence.

Mosaic FSI must notify the Commissioner immediately. If applicable and appropriate, a notification may also need to be made to

1. Law enforcement
2. Other regulatory agencies
3. PCI fraud teams
4. The company insurance carrier.

Mosaic FSI must notify the affected individual as quickly as possible.

The notification letter should alert individuals about the possible harm as well as steps that the individuals should take to minimise the risks.

The notification letters must fully comply with all Privacy Act 2020 requirements as well as any other applicable legal requirements, depending on the residency location of the data subject:

Personal Data Breach Notification Form

Part One -Notification Details

Name:	Mike Stobbs
Title	Partner, DPO
Name of the organisation	Mosaic Business Solutions Limited
NZBN number	9429031749442
Sector	Financial
Industry classification	Consultant
Organisation Address:	Level 15, 51 Shortland St Auckland New Zealand 1010
Phone Number	0800 667 242
Email	mike.stobbs@mosaicfsi.com
Date and Time Notification Submitted	[insert what data and time notification submitted]
Date and Time of Detection of the Data Breach:	[insert what data and time detection of the breach happen]
Elapsed Time Between Detection and Notification:	[insert the difference in time between detection and notification]
Is the problem that caused the breach ongoing	Yes/ No [delete one]

Part Two -Description of the Nature of the Personal Data Breach

How many people were affected (if known)?
The type of personal information involved in the breach.
The type of breach (i.e. what caused it)
If you know where the information has gone, and if so, where?

Part Three - Likely Consequences of the Data Breach

Indicate how serious the privacy breach was by answering the following:
How sensitive is the information that is involved in the breach?
Who has obtained or may obtain the information?
How likely is it that someone will be harmed because of this breach?
Depending on the answers to the above questions, you might also need to include:
Is someone's physical safety in immediate danger?
Is someone's psychological safety at immediate risk?
Is someone at immediate risk of serious financial harm?
Were any other organisations affected by the breach? If yes, explain who, and explain how they were affected.

Part four - Measures Already Taken to Address the Breach

What steps have been taken to reduce the risk of harm from this breach?
Are there security measures in place that protect the information from being accessed?
Have you notified the people affected by the breach? what have you done to notify the people affected.
Has the breach been reported to other authorities?
– If yes, what authorities has the breach been reported to?

Part five - Measures Proposed to be Taken to Further Address the Breach

Have you contacted any organisations (such as CERT, ID Care, Netsafe, or any other) that might be able to provide support to your organisation or people affected by the breach?

What new measure will you be putting in place? Do you plan to implement an Information security management system? Will you be recruiting further employees dedicated to maintaining your information security?

Part Six -Reasons for Delay in Notification, if applicable

Include any reasons for delay, if not applicable just put in N/A