Altro Group

Data Security Incident Breach Management Policy

December 2020

1. Scope

1.1 This Data Security Incident Breach Management Policy applies to all Altro Group companies and provides a framework to assist the Company in responding effectively and quickly in the event of a Security Incident.

2. Definitions

"Business & Customer Data" means data that the Company processes on behalf of its business partners, suppliers and customers, such as individuals' contact details, and includes their Personal Data.

"Employee" or **"you"** means all managers, board members, secondees, officers, directors, agents, employees, consultants, contractors, trainees, home workers, part-time and fixed-term workers, casual and agency staff.

"Employee Data" means data that the Company processes about its staff, such as HR records, and includes Personal Data.

"Personal Data" means any information (which may include an opinion, whether true or not, and whether recorded in a material form or not) relating to an identified or reasonably identifiable natural person; a reasonably identifiable natural person under Australian Privacy Law is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more specific factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. It includes name, address, date of birth, contact details, account details etc. Under New Zealand Privacy Law it is simply information about an identifiable individual but it is not necessary to be able to identify the individual from the information itself. You should assume that all information relating to individuals that you deal with at the Company will be 'Personal Data', including information about individuals within companies and other organisations.

"Sensitive Data" means:

(a) information or an opinion about an individual's:

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual orientation or practices; or

(ix) criminal record;

that is also Personal Data; or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information; or

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates.

3. What is a Security Incident?

3.1 A **"Security Incident"** means any unauthorised use of Business & Customer Data or Employee Data, or any other Personal Data or Sensitive Data, whether by an Employee or a third party. It includes any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, data. In New Zealand under applicable Privacy Laws it means any unauthorised or accidental access to, or disclosure, alteration, loss or destruction of, Personal Data held by the Company, or an action that prevents the Company from accessing the Personal Data on either a temporary or permanent basis.

3.2 A Security Incident can occur in a number of ways, including through:

(a) loss, theft or failure of equipment on which data are stored;

(b) physical or IT/IS security breaches;

(c) intentional or accidental access to or misuse of data by Employees or third parties;

(d) inadvertent disclosure of Personal Data due to 'human error', for example an email sent to the wrong person or an employee accidentally publishes a confidential data file containing Personal Data on the internet;

(e) inappropriate disposal or return of devices/paper;

(f) 'force majeure', e.g. fire or flood;

(g) equipment failure or human error; or

(h) hacking or deception ('blagging' or 'phishing') offences by third parties.

4. Why is it important to respond effectively to a Security Incident?

4.1 A Security Incident may have serious consequences, including:

(a) loss or compromise of the Company's confidential information or intellectual property;

(b) adverse publicity, brand damage and ultimately loss of trust by our customers and partners; and

(c) in severe cases (such as Security Incidents that result in the loss of Personal Data and/or Sensitive Data) serious harm to individuals whose Personal Data has been compromised, and regulatory investigation, enforcement action (e.g. fines) and regulatory and legal liability.

4.2 The Company has a business interest in protecting its data, and in certain circumstances is under legal obligations to do so. This extends to being able to respond quickly and effectively in the event of a Security Incident.

4.3 Prompt Security Incident management will mitigate potential harm to the Company and others, including individuals if personal information is affected, and will limit adverse PR and any regulatory and legal liability consequences for us.

5. Security Incident Management Team

5.1 The Data Protection Steering Group will act as the "Security Incident Management Team" in the UK. The Altro NZ SIMT will act as the "Security Incident Management Team" in relation to Security Incidents involving Personal Data for individuals in New Zealand. All Security Incidents reported to the Altro NZ SIMT must also be immediately reported to the Data Protection Steering Group in the UK. All references to the Data Protection Steering Group in this Policy include, where applicable. the Altro NZ SIMT.

5.2 Individual contact details for members of The Data Protection Steering Group are available on Apex. The Group can also be contacted on **mydata@altro.com** or **mydata@autoglym.co.uk**. The

contact details for the Altro NZ SIMT are available via email and the Altro NZ SIMT can also be contacted on **tim@asf.com.au** and **siva@asf.com.au**

6. When and how to report a Security Incident

6.1 If an individual suspects a Security Incident (no matter how minor it is) they should *immediately* contact a member of the Data Protection Steering Group (contact details available on Apex). The Data Protection Steering Group is responsible for the effective management of any data security incident and Security Incident. The notification should include the time and date the suspected Security Incident was discovered, the type of information involved, the cause and extent of the suspected Security Incident, and the context of the affected information of the suspected Security Incident.

6.2 The Data Protection Steering Group will investigate the Security Incident and whether a Security Incident has occurred and, where necessary, implement an appropriate Security Incident containment plan.

6.3 The Data Protection Steering Group will determine the exact steps of the Security Incident containment plan in each particular case. The steps that should be covered in the containment plan are set out at a high level in the remainder of this Policy.

6.4 Apart from notifying the Data Protection Steering Group, the Security Incident must be kept strictly confidential – confidentiality is important to avoid anybody taking advantage of any particular weaknesses in our systems.

7. Investigation and containment

7.1 The Data Protection Steering Group will co-ordinate the Security Incident investigation and will manage the local Company's response in a timely manner. It will document all relevant issues identified and containment actions taken.

7.2 In particular, the Data Protection Steering Group will investigate:

(a) whether a genuine Security Incident has occurred;

(b) if so, the nature and cause of that Security Incident and the sensitivity of the affected information;

(c) where Personal Data may have been affected, the identity of the data controller (if not the Altro Group), the number of individuals affected and the possibility of harm or distress caused to individuals;

(d) the risk involved (see paragraph 9);

(e) whether any back-ups of the data exist and, if so, how easily we can recover the data;

(f) whether to inform or consult other parts of the business to contain the risk or limit potential harm; and

(g) whether to inform or consult any external third parties to contain the risk or limit potential harm (such as external lawyers, IT forensics and security experts, PR/media, credit card companies, regulators, the police, individuals, insurers or financial institutions).

7.3 The Data Protection Steering Group will only involve and inform people who need to be informed and share information about the suspected Security Incident on a need-to-know basis and with appropriate confidentiality and data protection measures in place (such as Non-Disclosure Agreements or Data Processing Agreements).

7.4 Where the Data Protection Steering Group establishes that a genuine Security Incident has occurred, it will promptly draw up and implement a plan to contain it and mitigate actual or potential harm that may result from the Security Incident.

7.5 The Data Protection Steering Group will also liaise with Marketing, especially when it has reason to believe that the Security Incident may come or already is in the public domain.

8. Response and reporting

8.1 Immediately upon becoming aware of a Security Incident, the Data Protection Steering Group will:

(a) find and contain the source of the breach (at least in a general sense);

(b) take action to limit the Security Incident and any risk to individuals (e.g. stop the unauthorised practice, recover the records, change passwords, address weaknesses in physical or electronic security, reconfigure firewalls, or shut down the system that was breached. If it is not practical to shut down the system, or if it would result in loss of evidence, then revoke or change computer access privileges); and

(c) gather and evaluate as much information about the Security Incident as possible, in order to decide whether affected individuals must be notified.

8.2 The Data Protection Steering Group should preserve all evidence and facts associated with the Security Incident, such as system or activity logs, document all actions taken, by whom, and the exact time and date. No Employee should attempt to contaminate (or destroy) any evidence to hinder ability to investigate the Security Incident.

9. Risk assessment

9.1 When conducting its investigation and implementing a containment plan, the Data Protection Steering Group will have due regard to specific risks presented by the nature and scope of the Security Incident. Corruption of data caused by a computer virus will, for example, carry different risks to those associated with theft of a Company laptop.

9.2 The Data Protection Steering Group will assess the risks involved by reference to a number of factors, including:

(a) the nature of the data affected (e.g. Personal Data, legally sensitive Personal Data, or commercially sensitive data);

(b) how third parties could use the affected data and what the business can do to mitigate any adverse effects of such use;

(c) whether we have applied technological security measures (e.g. encryption, hashing or password protections) to protect the affected data; and

(d) how much data are involved and, if it is Personal Data, whether the Security Incident will affect a large number of individuals.

9.3 In assessing the risks, the Data Protection Steering Group will have regard to any applicable local laws and regulatory guidance. Where the Security Incident affects our operations in multiple countries, the Data Protection Steering Group will coordinate efforts.

9.4 When conducting an investigation of a Security Incident with an Australian connection, the Company must take all reasonable steps to complete the assessment within 30 calendar days, and otherwise in an expeditious manner. When conducting an investigation of a Security Incident with a New Zealand connection, the Company must take all reasonable steps to complete the assessment as soon as practicable.

10. Notification

10.1 The Data Protection Steering Group will decide whether it is necessary or advisable to notify the Security Incident to regulators, affected individuals and other parties.

10.2 Notification (or lack of notification when there is a requirement to do so) may have serious consequences. No Employee should contact any regulator or individuals directly. Security Incident notifications will be the responsibility of the nominated person from the Data Protection Steering Group.

10.3 The Data Protection Steering Group will decide the timing and content of any notifications. The exact content may vary depending on the circumstances and the persons to whom the notification is addressed, however as a general rule the notification may include information concerning the nature of the Security Incident, its consequences, any measures taken to address it, and the steps that affected parties (in particular individuals) can take to mitigate adverse effects.

10.4 It is a legal requirement in some countries to inform data protection authorities or individuals (or both) if Personal Data are lost or unlawfully accessed. In that event, the Data Protection Steering Group will act immediately to comply with applicable notification periods and mitigate further data losses, harm to individuals and damage to the Company.

10.5 For Security Incidents concerning individuals in the EU, the law is stricter. Our obligations differ depending on whether we are the controller (i.e. it is making decisions about how the data are processing) or processor (i.e. it is processing data on another company's instructions).

Notification to the relevant Australian data protection authority

10.6 If the Data Protection Steering Group has reasonable grounds to believe that the Security Incident involves Personal Data for individuals in Australia, and is likely to result in serious harm to one or more individuals, the Company must, as soon as possible, notify the Australian Information Commissioner. This includes where:

(a) there is unauthorised access to, unauthorised disclosure of, or loss of, Personal Data held by the Company; and

(b) the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the Personal Data relates.

10.7 'Serious harm' in the context of a Security Incident, may include serious physical, psychological, emotional, financial, or reputational harm. In assessing the likelihood of serious harm, the Company must consider the kind of information and its sensitivity, the persons or kinds of persons who have obtained or could obtain the information, and whether the information is protected by security measures.

10.8 The notification to the Australian Information Commissioner must include:

(a) details of the Company and a contact person;

(b) a description of the Security Incident, which may include:

(i) the date or date range of the unauthorised access or disclosure;

(ii) the date the Company detected the data breach;

(iii) the circumstances of the data breach (such as any known causes for the unauthorised access or disclosure, or loss);

(iv) who has obtained or is likely to have obtained access to the Personal Data (not necessarily specific individuals, could be general, like 'external third party' or 'former employee'); and

(v) relevant information about the steps the Company has taken to contain or remediate the Security Incident;

(c) an explanation of the types of information that were involved in the Security Incident;

(d) a list of steps the Company recommends that individuals take to reduce the risk that they experience serious harm as a result of the Security Incident; and

(e) details of any other entities involved in the Security Incident (if any, for example, cloud service providers).

10.9 In addition, the Company may choose to provide the following information to the Australian Information Commissioner, voluntarily:

(a) description of any action the Company has taken, or intends to take, to assist individuals whose personal information was involved in the Security Incident;

(b) description of any action the Company has taken, or intends to take, to prevent reoccurrence;

(c) details of how the company intends to notify individuals who are likely to be at risk of serious harm as a result of the Security Incident, and when this will occur; and

(d) a list of any other data protection authorities, law enforcement bodies or regulatory bodies to whom the Company has reported this data breach.

Notification to the relevant New Zealand Privacy Commissioner

10.10 If the Data Protection Steering Group has reasonable grounds to believe that the Security Incident involves Personal Data for individuals in New Zealand, and is likely to result in serious harm to one or more individuals, the Company must, as soon as practicable, notify the New Zealand Privacy Commissioner. This includes where:

(a) there is unauthorised or accidental access to, or disclosure, alteration, loss or destruction of, Personal Data held by the Company, or an action that prevents the Company from accessing the Personal Data on either a temporary or permanent basis (**"breach"**); and

(b) it is reasonable to believe the breach has caused serious harm to any of the individuals to whom the Personal Data relates, or is likely to do so (a **"notifiable privacy breach"**).

10.11 In assessing the likelihood of serious harm, the Company must consider:

(a) any action taken by the Company to reduce the risk of harm following the breach;

(b) whether the Personal Data is sensitive in nature;

(c) the nature of the harm that may be caused to affected individuals;

(d) the person or body that has obtained or may obtain personal information as a result of the breach (if known);

(e) whether the Personal Data is protected by a security measure; and

(f) any other relevant matters.

The notification of a notifiable privacy breach to the New Zealand Privacy Commissioner should be done through the *Notify Us* tool on the Office of the Privacy Commissioner's website (accessible here). The form captures the information required under Section 117 of the NZ Privacy Act, which sets out the legal requirements on how privacy breaches must be notified to the Privacy Commissioner. The Company may provide information required under the mandatory privacy breach requirements incrementally. However, any information that is available at any point in time must be provided as soon as practicable after that point in time. Updates to a previously submitted report can also be submitted via NotifyUs.

Notification to the relevant customer

10.12 In relation to Business & Customer Data where we are acting as a processor, we must notify the relevant customer without undue delay (unless otherwise agreed in the customer contract). We must assist our customers to meet their own notification obligations.

10.13 The notifications in paragraphs 10.6, 10.10 and 10.12 must, as a minimum:

(a) describe the nature of the Security Incident (e.g. the categories and number of individuals affected, the number of records affected, the type of data, the likely consequences etc.);

(b) communicate an appropriate contact point (a member of the Data Protection Steering Group); and

(c) describe any steps taken or proposed to address or mitigate the effects of the Security Incident.

10.14 This information can be notified in phases if the Company cannot provide it all immediately.

Notification to affected individuals

10.15 Where Security Incidents involving Personal Data for which the Company is a controller (e.g. Employee Data) are likely to result in high risk to the rights and freedoms of Employees in Europe, the Company must notify the affected individuals (e.g. Employees) without undue delay. Such notifications must be in plain language and contain at least the information in paragraph 10.13. If the Company implements suitable security measures (e.g. encryption) so that any Personal Data can no longer be accessed, it does not need to notify the employees.

10.16 For other Security Incidents where Personal Data are involved, the Data Protection Steering Group will consider whether the affected individuals should be informed, even if not legally obliged to do so. In considering this, it will take the following factors into consideration:

(a) how many individuals have been affected;

(b) whether the individuals are identifiable and whether the Company can contact them personally; and

(c) the nature of the data affected, the risk of actual or potential harm to individuals, and the urgency of the situation.

10.17 Where the Data Protection Steering Group has reasonable grounds to believe there has been a Security Incident involving Personal Data for individuals in Australia and there is a risk of serious harm, the Company must, as soon as practicable:

(a) make a decision about which individuals to notify; and

(b) notify individuals of the contents of this statement, by doing whichever of the following is practicable for the Company:

(i) notifying all individuals to whom the relevant information relates; or

(ii) notifying only those individuals at risk of serious harm;

(c) if neither option (i) or (ii) above is practicable (for example, the Company does not have up to date contact details for individuals), publish a copy of the statement to the Australian Information Commissioner on its website and take reasonable steps to publicise the contents of the statement, to increase the likelihood that the Security Incident will come to the attention of individuals at risk of serious harm. The Australian Information Commissioner recommends that this statement be available for at least 6 months.

10.18 Where the Data Protection Steering Group has reasonable grounds to believe there has been a Security Incident involving Personal Data for individuals in New Zealand and there is a risk of serious harm (i.e. there is a notifiable privacy breach), the Company must, as soon as practicable:

(a) notify the affected individuals (unless an exception under the Privacy Act applies[1] or a delay is permitted[2]; or

(b) if it is not reasonably practicable to notify an affected individual or each member of a group of affected individuals, instead give public notice of the breach[3]

---

[1] See *section 116* of the Privacy Act.

[2] Under *section 116(4)*.

[3] Under *section 115*.

The notification to the affected individual(s) must:

(a) describe the notifiable privacy breach and state whether the Company has or has not identified any person or body that the Company suspects may be in possession of the affected individual's Personal Data (but, except as provided in section 117(3), must not include any particulars that could identify that person or body); and

(b) explain the steps taken or intended to be taken by the Company in response to the privacy breach; and

(c) where practicable, set out the steps the affected individual may wish to take to mitigate or avoid potential loss or harm (if any); and

(d) confirm that the Commissioner has been notified under section 114; and

(e) state that the individual has the right to make a complaint to the Commissioner; and

(f) give details of a contact person within the Company for inquiries.

When providing information to affected individuals, the Company must ensure that it does not disclose information about any other affected individuals.

There is no prescribed medium that must be used to provide notifiable privacy breach notifications to affected individuals. Typically, notification should be direct and using the Company's usual method of communicating with that individual. The preferred method of notification is direct – by phone, letter, email or in person – to affected individuals. Depending on the circumstances, using multiple methods of notification may be appropriate.

10.18.2 If giving public notice, the notice must:

(a) be published on an Internet site that is maintained by or on behalf of the Company and is publicly accessible free of charge at all reasonable times (i.e. Company's website);

(b) also be published in at least one other medium (whether electronic or non-electronic) that the Company considers is most likely to bring the notice to the attention of the greatest number of affected individuals;

(c) describe the notifiable privacy breach without identifying any affected individual;

(d) state any steps that an affected individual may take to mitigate or avoid potential loss or harm;

(e) confirm that the Privacy Commissioner has been notified of the privacy breach;

(f) state that an affected individual has the right to make a complaint to the Commissioner about the privacy breach; and

(g) state the contact details of a person within the Company to whom inquiries may be made in respect of the privacy breach.

In addition to the above, if the Company elects to give public notice or an exception is relied upon, it must notify the affected individual at a later time if:

(a) circumstances change so that it is now reasonably practicable to notify those affected individuals or the exception no longer applies; and

(b) at that later time, there is or remains a risk that the privacy breach will cause serious harm to the affected individual(s).

Notification to other parties

10.19 In particular circumstances it may be necessary or advisable to notify other parties such as the police, insurers, our customers, vendors or business partners.

10.20 Insurance policies should also be consulted at the point of discovery of a data security breach to ascertain whether and when the insurers need to be notified.

11. Evaluation and review

11.1 Following a Security Incident, the Data Protection Steering Group will consider the adequacy of the Company's systems, policies and procedures to protect company data and whether any improvements are needed to prevent such a Security Incident from reoccurring.

11.2 Where a Security Incident arose due to a failing by any of the Company's third party service providers, the Data Protection Steering Group will advise whether the Company should seek contractual redress against that service provider.

11.3 The Data Protection Steering Group will also advise, having taken HR and/or legal advice, whether the Company should consider disciplinary proceedings against any employees whose actions or negligence caused (or contributed to) the Security Incident.

12. Questions?

12.1 If you have any questions or require further guidance in relation to this Policy please contact a member of the Data Protection Steering Group by contacting **mydata@altro.com** or **mydata@autoglym.co.uk.**

To be completed and returned to your line manager.

I acknowledge receipt and accept the contents of the Security Incident Data Breach Management Policy

Signed……. Date……

Name……