LSH Auto Australia
Data Breach Response Plan

INDEX

1 Purpose

The purpose of this Data Breach Response Plan (**Plan**) is to set out how LSH Auto (Melbourne) Pty Ltd, LSH Auto (Sydney) Pty Ltd and LSH Auto (Brisbane) Pty Ltd (collectively, **LSH Auto Australia**) will handle a suspected or actual data breach, whether that data breach occurs internally or externally to LSH Auto Australia.

The content of this Plan reflects requirements under applicable legislation, including the requirement to notify particular breaches, known as "eligible data breaches", under the *Privacy Act 1988* (Cth) (**Privacy Act**).

2 Key points

- If you become aware of an actual or suspected data breach, you should report it to the Privacy Officer immediately.
- Examples of data breaches can be found in section 4.5 of this Plan.
- The Privacy Officer and Response Team should respond to an actual or suspected data breach by following the process described in section 7.
- You should fully cooperate with the Privacy Officer and Response Team in their response to a data breach.

3 Responsibility and authority

3.1 Responsibility

All LSH Auto Australia personnel are required to adhere to this Plan.

This Plan is a direction to you as an employee, officer, agent or contractor (**Representative**) of LSH Auto Australia. You must comply with this Plan, however, it does not form part of any contract, including any employment contract. Instead, it sets out the processes you must observe when you become aware of a suspected or actual data breach affecting LSH Auto Australia.

If you do not comply with this Plan (as varied from time to time), LSH Auto Australia may take appropriate disciplinary action against you, which may include potential termination of your employment or engagement.

3.2 Authority

The Privacy Officer is responsible for ensuring all suspected and actual data breaches are handled in accordance with this Plan, and for regularly reviewing this Plan for currency (which should occur no less frequently than annually on 1 April).

As at the date of this document, the Privacy Officer is **Emilia Simone**, who can be reached by email at **emilia.simone@lshauto.com.au** or telephone on +61 2 9697 7750.

4 Data Breach Response Plan

4.1 Background

This Plan provides the framework used by LSH Auto Australia to address a suspected or actual data breach.

In the event that LSH Auto Australia experiences a data breach, or suspects one has occurred, it is crucial that LSH Auto Australia identifies that actual or suspected data breach and then swiftly assesses and responds to it appropriately. A timely response can assist to minimise or potentially entirely avoid the impact on the business, and if a data breach involves personal information, the impact on the affected individuals.

4.2 What is a data breach?

A data breach is effectively an incident in which information held by LSH Auto Australia is compromised. This can include any unauthorised access, modification or disclosure of information, or any misuse, interference or loss of information, whether accidental or intentional, by any person, whether an LSH Auto Australia staff member or a third party.

4.3 What information can be subject to a data breach?

Any information held by LSH Auto Australia can be subject to a data breach irrespective of:

- the format or medium of that information (eg, electronic or in hard copy);
- whether the information is commercially sensitive;
- whether the information includes information about individuals; and/or
- whether the information is held by LSH Auto Australia or by a third party on LSH Auto Australia's behalf.

LSH Auto Australia's Data Breach Response Team (see section 7.1 below) (**Response Team**) would confirm the nature of the compromised information. This is necessary as different statutory requirements and contractual obligations apply to different types of information held by LSH Auto Australia, and this can alter the response required.

4.4 How do data breaches arise?

Data breaches can arise as a result of the actions of:

- LSH Auto Australia, including its Representatives; and/or
- third parties, such as a hacker gaining access to LSH Auto Australia's IT systems.

Data breaches are frequently understood as being breaches caused by third parties. However, data breaches are not limited to malicious actions, such as theft or hacking, and many data breaches occur as a result of the acts or omissions of an organisation's own personnel (including inadvertent ones).

LSH Auto Australia's response to a data breach will depend on the circumstances of the breach, including the nature of the breach, the information associated with it, whether any third parties are involved, the risks associated with it, and any relevant regulatory requirements.

4.5 Examples of data breaches

Set out below are some examples of data breaches that might affect LSH Auto Australia. This is not an exhaustive list, but is intended to give you a general understanding of what might constitute a data breach.

Data breaches that involve third parties outside of LSH Auto Australia may include:

- unauthorised remote access to LSH Auto Australia's IT systems due to a flaw or deficiency in LSH Auto Australia's information security systems, or a phishing scam that obtains access credentials;
- theft or loss of physical assets such as laptops, USB data or other storage devices, mobile phones or tablets;
- theft or loss of, or unauthorised access to, hard-copy documents; and/or
- unauthorised disclosure of personal information, such as by:
    - sending an email containing personal information to the wrong recipient;
    - attaching the wrong document to an email or uploading a document to the publicly accessible area of LSH Auto Australia's website rather than the intranet;
    - inadequate identity checking leading to disclosure of personal information to an unauthorised third party; and/or
    - sharing personal information with a third party that is not permitted to receive it.

As mentioned above, an incident does not need to involve a person outside of LSH Auto Australia in order to be a data breach. Data breaches can also occur exclusively within LSH Auto Australia. Examples of this could include:

- an employee accessing personal information that is not required for their work (eg, an employee notices that someone they know is applying for vehicle financing from LSH Auto Australia (via Mercedes-Benz Financial Services), and so they decide to accesses the person's information (including financial details) out of interest);
- an employee using another person's login credentials in order to access information beyond the legitimate requirements of the employee's own work; or
- a change to computer network access privileges or system configuration for an employee, that is exploited by that employee to gain unauthorised access to information (eg, salary information about other employees).

5 Internal notification of data breaches – all staff

5.1 Reporting data breaches

All LSH Auto Australia employees and contractors must immediately report a suspected or actual data breach to the Privacy Officer by email or by telephone, and take all reasonable steps permissible within their role to contain the breach.

The Privacy Officer will conduct an initial assessment of the suspected or actual data breach and initiate appropriate steps where required.

To assist their assessment, the Privacy Officer may request further details from you. The Privacy Officer may also discuss or liaise with other LSH Auto Australia personnel in conducting an initial assessment. It is important that you fully and promptly cooperate with the Privacy Officer in the assessment of a data breach.

The Privacy Officer will promptly refer the breach to the Response Team using the form set out in the Appendix, except for:

- minor breaches which can appropriately be handled by the Privacy Officer; or
- suspected data breaches that the Privacy Officer confirms definitively did not occur,

both of which must be reported (rather than referred) to the Response Team. Referral to the Response Team must occur immediately for data breaches that are not (or may not be) contained, irrespective of whether the initial assessment is complete.

The Response Team will be responsible to ensure that appropriate records are kept of the report and the incident. Your responsibility is to preserve all information you are able to that relates to the incident (for example, do not delete any emails pertaining to the event).

5.2 Confidentiality

Any suspected or known data breach is confidential information of LSH Auto Australia. No LSH Auto Australia personnel are permitted to discuss an incident:

- internally within LSH Auto Australia, except to report the incident to the Privacy Officer in accordance with this Plan or in the course of participating in the Response Team, or as otherwise directed by the Privacy Officer or Response Team; or
- externally, without prior written approval of the Privacy Officer.

All internal communications regarding a data breach incident must be restricted to those people that "need to know". The person who reported the breach may have very limited (or no) involvement once the Privacy Officer has been notified.

Other than reporting the incident to the Privacy Officer, personnel should not create any other documents or correspondence about the incident, unless directed by the Privacy Officer.

If you are aware of any documents or correspondence relating to the incident please immediately notify the Privacy Officer and provide copies as directed by the Privacy Officer.

If any internal personnel or external parties (eg, media) raise a suspected or known data breach incident involving LSH Auto Australia with you, you should immediately notify the Privacy Officer unless otherwise provided for in this Plan.

6 External notification of data breaches – Response Team

6.1 What is a notifiable data breach?

Under the Privacy Act, LSH Auto Australia must investigate certain data breaches involving personal information and may need to notify the Office of the Australian Information Commissioner (**OAIC**) and any individuals affected by the breach. Subject to some exceptions, a data breach will require notification to third parties such as the OAIC and/or affected individuals outside of LSH Auto Australia (being what is terms an "eligible data breach") if the following conditions are met:

- **A data breach occurs affecting personal information held by or on behalf of LSH Auto Australia**

  Generally, this occurs when there has been unauthorised access or unauthorised disclosure of personal information, or loss of personal information in circumstances where unauthorised access or disclosure is likely.

  "Personal information" is defined by the Privacy Act to mean any information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether that information or opinion is true or not, and whether it is recorded in a material form or not.

  For example, this could include contact details of past or prospective customers.

- **There is a likelihood of serious harm to affected individuals**

  This condition will be met where, from the perspective of a reasonable person in LSH Auto Australia's position, the data breach is likely to result in serious harm to one or more individuals whose personal information was affected by the data breach.

  "Serious harm" is not defined by the Privacy Act but the term is broad and can include financial, physical, psychological, emotional or reputational harm.

  Some examples of harm are fairly obvious, such as harm arising from identity theft or financial loss. Others may be less apparent, such as emotional harm, loss of employment opportunities, workplace or social bullying, or marginalisation.

  The Privacy Act sets out a non-exhaustive list of factors to be taken into account when making an assessment of the risk of serious harm. The requirement is that the risk of serious harm is more probable than not (rather than only a possible or theoretical risk).

- **Effective remedial action is not possible**

  LSH Auto Australia should take remedial steps to remove or reduce the risk of serious harm to affected individuals. If those remedial steps are successful in removing the risk of serious harm to affected individuals, the incident may no longer be classified as an eligible data breach.

  However, in some cases remedial action is not possible, or is not sufficient to prevent the likely risk of serious harm to all affected individuals.

The Response Team is responsible for determining whether a particular breach may be or is an eligible data breach.

If LSH Auto Australia suspects that an eligible data breach has occurred then LSH Auto Australia must investigate that suspicion by undertaking an assessment. For example, an assessment should be undertaken if LSH Auto Australia knows a data breach has occurred that involves personal information, or if it is not clear whether there is a likely risk of serious harm.

The assessment and notification processes for eligible data breaches must be completed within particular time frames under the Privacy Act. LSH Auto Australia may be subject to penalties, including financial penalties, if these requirements are not complied with.

Therefore, it is critical that all suspected and known data breaches are promptly notified to the Response Team in accordance with this Plan.

6.2 Other external breach notification obligations

In addition to LSH Auto Australia's obligations under the Privacy Act, it may also be necessary to notify third parties under other regimes or to satisfy LSH Auto Australia's contractual obligations.

For example, LSH Auto Australia may need to notify insurers and parent companies of the data breach. It may also be appropriate to notify law enforcement agencies in certain circumstances (eg, if hackers steal information from LSH Auto Australia's IT systems).

LSH Auto Australia may in particular have responsibilities to the OEM/franchisor under the dealer/franchise agreement. Failure to comply with any requirements under that contract may result in a breach of the dealer agreement.

The Response Team is responsible for identifying any such notification obligations.

7 Response team handling of data breaches

7.1 Response team

The Response Team will determine how to address any data breaches. This may include containment of the breach, assessment of the breach and consequent risks, remedial action and reporting of any such incidents, along with management of a subsequent business process improvement to minimise the likelihood of reoccurrence.

As at the date of this document, the Response Team consists of the employees listed below:

Name	**Position**	**Nominated substitute (if absent on leave)**
Emilia Simone	Privacy Officer	Head of Brand & Corporate Communications – Joanna Zhou
John Good	Managing Director	CFO
Aaron Cordy	CFO	Managing Director
Vaughan Blackman (Melbourne) / Susan Butler (Sydney) / Kenneth Got (Brisbane)	Dealer Principal of affected site(s)	Marketing Manager – Brenda Quach (Sydney) / Tania Kilpatrick (Melbourne) / Bianca Baron (Brisbane)
Alex Wong	Head of IT	IT Applications Manager – Yusuf Zarani

The roles and responsibilities of each member of the Response Team will depend on the circumstances of the data breach. For example, if a data breach involves an IT system compromise, then the IT team may have a greater responsibility in assessing the breach.

7.2 Response

Each data breach incident will likely have a unique set of circumstances, risks and contractual and regulatory requirements, and the response will need to have regard to these factors. The Response Team will deal with suspected and actual data breaches on a case-by-case basis.

Once a matter is escalated to the Response Team, the Response Team will plan and undertake a response tailored to the circumstances.

The response will vary depending on the nature of the breach, the information the subject of the breach, whether any third parties are involved in the breach, the risks associated with the breach, and any relevant regulatory requirements.

Generally, the response will involve reviewing all relevant materials and undertaking the steps set out below. There is a flow chart at the end of this section, outlining the steps that should generally be followed.

Step 1: Identify and report the breach

Responsibility: all Representatives

Report the actual or suspected data breach to the Privacy Officer as soon as possible by email, telephone or in person (whatever is most practical in the circumstances). The Privacy Officer will then engage with the Response Team to handle the data breach.

Step 2: Contain the breach to prevent any further compromise to personal information

Responsibility: Privacy Officer and Response Team

Immediately contain the data breach (eg, shut down the system that was breached, implement a forced change of passwords, recover or quarantine the affected records, or stop the unauthorised practice. If it is not practical to shut the system down, or if doing so would result in a loss of evidence, then revoke or change system access privileges or address weaknesses in physical or electronic security). This may assist the prevention of serious harm being suffered by any individuals.

Consider whether external advice or assistance from IT specialists or forensic experts is required.

Matters to consider:

- How did the breach occur?
- Has the breach been contained, or is action still required to contain the breach? If action is still required, what action is needed to secure the data?
- If the data breach involved unauthorised access to data, has the method of unauthorised access been shut down and were any copies made?
- Who has access to (or could access) the information?
- What remedial action is needed to reduce the risks to LSH Auto Australia and affected third parties?

Step 3: Conduct an assessment of the breach

Responsibility: Privacy Officer and Response Team

Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.

The following actions should be taken as part of this step:

- identify the nature of the compromised data. For example, whether the data includes commercially sensitive information, personal information or government related identifiers (eg, Tax File Numbers, driver's licence numbers, passport details, Medicare numbers), and if so, what types of information;

- consider engaging third party service providers to assist with the assessment and response to the breach. LSH Auto Australia has previously engaged:
    - Thomson Geer, to advise on the legal obligations and implications for LSH Auto Australia;
    - McGrath Nicol, to conduct a forensic analysis of a data breach;
    - IDCare, to assist in the management of the response to a data breach; and
    - RMK and Associates, to advise on the public relations implications of a data breach;
- identify any third party organisations that may also be involved in the data breach, such as a contractor to LSH Auto Australia;
- identify any contractual relationship between LSH Auto Australia and third parties (eg, insurers, service providers, customers) that may affect how the breach should be handled. For example, some contracts may include a clause requiring that the other party is notified of a breach. LSH Auto Australia may in particular have responsibilities to the OEM/franchisor under the dealer/franchise agreement. Failure to comply with any requirements under that contract may result in a breach of the dealer agreement;
- if the compromised data includes personal information, identify the number of affected individuals and the volume, type and sensitivity of personal information about those individuals affected, and evaluate the risk of serious harm for those individuals; and
- consider if any remedial steps are possible to reduce or alleviate the risks associated with the data breach (including the risks to affected individuals).

Matters to consider:

- remember that the kind of information involved in the breach is directly relevant to assessing whether an individual is likely to suffer serious harm. For example, a breach involving financially sensitive information (such as payslips or bank statements) may increase the risk that the affected individuals will suffer serious harm;
- the circumstances of the breach are also relevant. For example, lost hard-copy paperwork may have a similar level of risk as a breach of LSH Auto Australia's IT systems if the paperwork contains financially sensitive information; and
- the Privacy Act requires a reasonable and expeditious assessment of suspected eligible data breaches. What is expeditious in particular circumstances will depend on the facts at hand. The Privacy Act states that reasonable steps should be taken to ensure the assessment is completed as soon as practical (which should generally be within 30 days).

Step 4: Notify relevant parties

Responsibility: Privacy Officer

If the assessment under Step 3 has determined there has been a data breach, the Response Team must liaise with appropriate management personnel to:

- notify LSH Auto Australia's insurer(s) if required under the relevant insurance policy and ensure handling of the breach is consistent with the requirements of the insurance policy terms. This step requires prior approval by the CFO;

- liaise with external lawyers to determine if the breach is required to be notified to the OAIC or affected individuals by law. For example, assessing whether it is an eligible data breach under the Privacy Act; and

- consider whether it is appropriate to notify law enforcement, professional associations or any other third party due to the nature of the breach.

Depending on who the notification is being made to, there will be certain requirements that are required to be contained in each notification.

A notification to the OAIC must contain certain information, including:

- the identity and contact details of LSH Auto Australia (ie, the company or companies in the LSH Auto Australia group that were affected);

- a description of the eligible data breach that LSH Auto Australia has reasonable grounds to believe has happened;

- the kind or kinds of information concerned; and

- recommendations about the steps that affected individuals should take in response to the eligible data breach.

A notification to affected individuals must provide them with appropriate information to notify them of the personal information that has been comprised and the remedial steps that have been taken to lessen the adverse impact that might arise from the breach.

The Response Team should also consider publishing a notice regarding the data breach on the website of the relevant site(s). This may be required by the Privacy Act where it is not possible to identify and/or directly contact the affected individuals.

Matters to consider:

- remember that the various data breach notification regimes have certain timing requirements;

- carefully consider whether notification is required, as notifying individuals about a breach that poses little risk of serious harm can, by itself, cause undue anxiety or harm;

- consider how you will provide the notification to individuals (eg, email or post). This should generally be consistent with how LSH Auto Australia has communicated with an affected individual previously; and

- if a law enforcement agency is investigating, it may be appropriate to consult with them prior to making the breach public.

Step 5: Prevent future breaches

Responsibility: Privacy Officer and Response Team; all Representatives required to implement recommendations

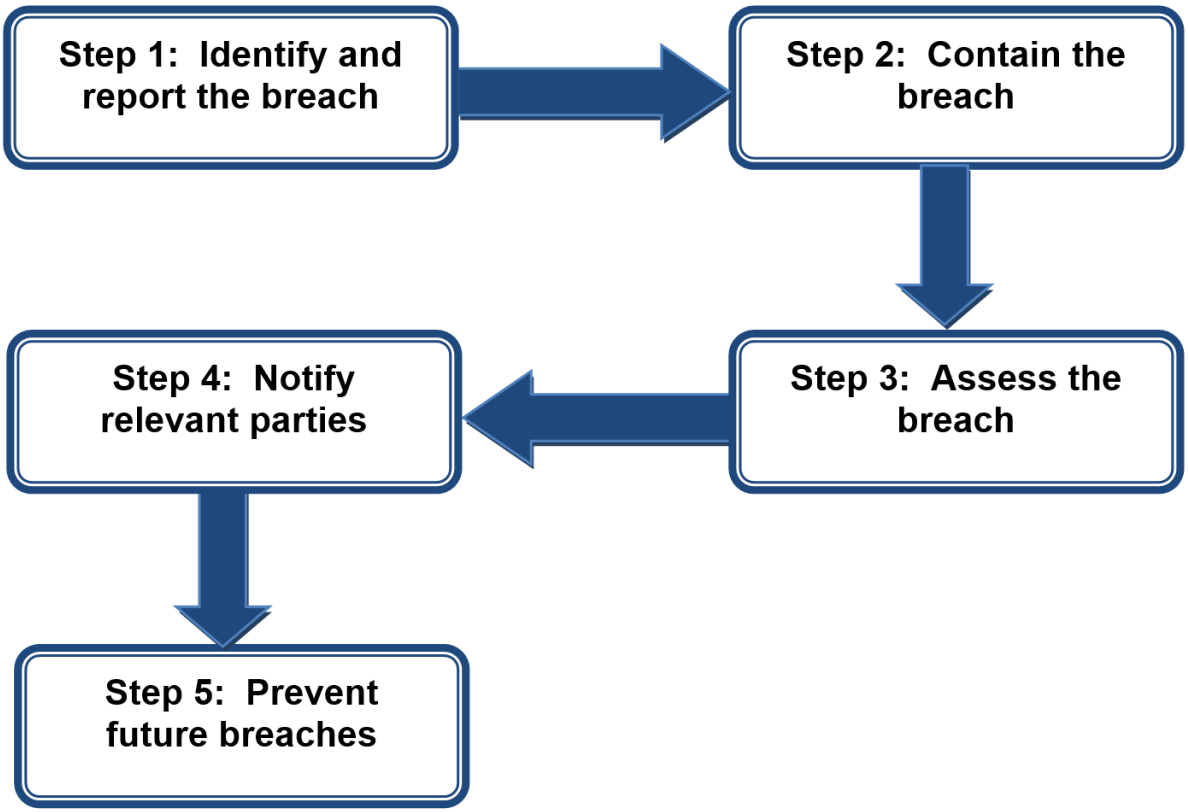
Irrespective of whether notification to any regulator or individual is required, a full investigation should be conducted. In doing so, LSH Auto Australia can address any weaknesses in data handling processes that may have contributed to the breach.

An important part of the response to any data breach is to take steps to prevent a similar breach from happening again and to ensure that, if a breach does occur, LSH Auto Australia is able to prevent whatever negative consequences may have otherwise occurred.

For this reason, following a data breach (whether or not it is an eligible data breach) the Response Team should prepare an incident report which may include:

- a review of the operation of this Plan, including any recommended amendments or updates to account for the investigation findings;
- any recommended amendments or updates to other policies and procedures to account for the investigation findings;
- the outcome of a security audit of physical and/or technical security, and other internal practices, relevant to the data breach;
- a review of the performance of any external service providers engaged to assist with the response to the data breach, and whether they should be engaged again in the event of a future similar incident;
- a review of and/or recommendations for employee training programs, including possible training programs for the Response Team; and/or
- a review of the suitability of LSH Auto Australia's service providers involved in or affected by the data breach, and the appropriateness of the contractual obligations imposed on those service providers.

The order of the steps above is indicative. Some actions may be undertaken in parallel or out of order. For example, it may be necessary to undertake an action in Step 3 to ensure that the breach is properly contained as required by Step 2. Depending on the nature of the data breach additional steps may also be necessary. For example, if a breach is suspected then an initial inquiry step may be required to ascertain whether such a breach is likely to have in fact occurred.



8 Incident without breach

In some cases, personnel may identify an improvement, shortcoming or gap in LSH Auto Australia's policies, procedures and systems for data protection and privacy (which may relate to the handling of suspected or actual data breaches). This might occur following a data breach, or might be identified without an actual data breach having occurred.

Representatives are required to promptly notify the Privacy Officer of any such suggested improvements or possible shortcomings or gaps.

Where the Privacy Officer is notified of such instances, they will assess the notification and review and may update policies, procedures and systems necessary to address the reported issues. They may also take such other steps as are reasonably necessary to assess the issue raised in the notification, and to take all necessary remedial steps to minimise the risk of a data breach or privacy breach arising as a result of that issue.

APPENDIX

Date: …./…../....

POTENTIAL DATA BREACH REPORTING FORM
CONFIDENTIAL

Date of incident: (or earliest known activity relating to the incident)	
Date that incident was reported to Privacy Officer:	
Who reported data breach to Privacy Officer:	
Description of data breach:	
How breach occurred: (If known)	
Dealership/s affected:	[Sydney / Melbourne / Brisbane]
How data breach was identified:	
Evidence retained:	[*eg, copies of scam emails, logs of system access*]
Steps taken to contain breach: (including status of those efforts)	[*eg, shut down of system that was breached, forced change of passwords, recovery of affected records, stop of unauthorised practice*]
Types of personal information affected:	
Estimated number of affected individuals:	
Other entities affected by the breach: (If any)	[*Eg, this may include LSH Auto's service providers*]
Any other comments or observations: (eg, any suggestions for next steps to be taken and the timing)	