LSH Auto Australia
Internal Privacy Compliance Manual

INDEX

1 Introduction

LSH Auto (Sydney) Pty Ltd, LSH Auto (Melbourne) Pty Ltd and LSH Auto (Brisbane) Pty Ltd (collectively, **we, us**, **our** or **LSH Auto Australia**) recognise the importance of individuals' privacy.

This internal privacy compliance manual (**Manual**) is designed to complement our Privacy Policy, which is available to the public and is published on the Internet at https://www.lshauto.com.au/privacy-policy (**Privacy Policy**).

Unlike our Privacy Policy, this Manual is for the internal use of LSH Auto Australia only. You must not provide this Manual to any person outside of LSH Auto Australia or otherwise publish it or make it available to any third party.

We are required to comply with the *Privacy Act 1988* (Cth) (**Privacy Act**), including the Australian Privacy Principles (**APPs**) under the Privacy Act, in our handling of "personal information".

We have prepared this Manual to assist in our compliance with the Privacy Act, including the APPs, and to enable us to efficiently and appropriately deal with inquiries or complaints from individuals about our handling of personal information and compliance with the APPs.

This Manual provides a broad outline of the obligations set out in the Act and the APPs and is intended to provide high-level guidance to staff dealing with privacy-related requests and issues. It is not an exhaustive or authoritative statement of LSH Auto Australia's privacy obligations or the privacy laws in Australia. It is a guide only and should be consulted in conjunction with the Privacy Act and the APPs.

LSH Auto Australia intends to review this Manual periodically and may modify or remove portions at any time.

2 Privacy Officer

All employees need to have a general understanding of the privacy principles and should have completed all necessary privacy training. If you receive any complaints, enquiries or otherwise require any further information on LSH Auto Australia's privacy practices please contact our group Privacy Officer (details below).

Emilia Simone
Privacy Officer
LSH Auto Australia
43-47 O'Riordan Street
Alexandria, NSW, 2015
Telephone: 02 9697 7750
Email: Emilia.Simone@lshauto.com.au

3 Privacy complaints and non-compliance

3.1 Privacy complaints

The Privacy Officer is responsible for co-ordinating our response to any privacy complaints we may receive, and for handling enquiries relating to privacy (other than simple or routine enquiries).

Simple or routine enquiries (such as "where can I find your Privacy Policy" or "please update my phone number in your records") will often be managed by the team member in the dealership or in the Sales Department who is in contact with the customer. For this reason it is important that all team members have completed all necessary training and follow existing business processes.

Our Privacy Officer will be responsible to ensure that LSH Auto Australia handles any significant privacy complaints and queries in accordance with the Privacy Act and APPs.

If you receive or otherwise become aware of a privacy complaint about LSH Auto Australia or a possible or actual breach of the Privacy Act or APPs by LSH Auto Australia, please notify the Privacy Officer immediately.

3.2 Non-compliance and the role of the Privacy Commissioner

The Privacy Commissioner is the government regulator who has a range of investigative and enforcement powers to identify and deal with non-compliance with the Privacy Act or APPs.

These include the power to seek pecuniary penalties of up to $2.1 million for companies such as LSH Auto Australia and $420,000 for individuals, for serious or repeated interferences with privacy.

Breaches of the Privacy Act and APPs can be identified in a number of ways. These include for example, as a result of an assessment or investigation of an entity's practices undertaken by the Privacy Commissioner.

The Privacy Commissioner may undertake assessments of LSH Auto Australia's activities to determine compliance with the APPs (and any other applicable codes such as the Credit Reporting Code). These audits can be undertaken in the absence of any concern or complaint.

In addition, the Privacy Commissioner may undertake an investigation of an act or practice that may be an interference with privacy, either in response to a complaint, or at the Privacy Commissioner's own initiative (for example, in relation to an alleged breach that is reported in the media).

Generally however, a complaint by an individual must be made in the first instance to LSH Auto Australia, rather than to the Privacy Commissioner. The Privacy Commissioner may decline to take action where the individual has not first brought the complaint to LSH Auto Australia's attention. This underscores the importance of properly managing complaints from the outset, in order to minimise the likelihood that the complaint is escalated to the Privacy Commissioner.

At the conclusion of an investigation, the Privacy Commissioner may make a number of declarations, including that LSH Auto Australia redress any loss or damage to individuals whose privacy was breached. This can include a compensation order.

4 Coverage of the Privacy Act

4.1 Scope of the Privacy Act for LSH Auto Australia

The Privacy Act and the APPs regulate the way in with LSH Auto Australia handles "personal information".

The term "personal information" has a specific meaning under the Privacy Act, discussed further in Section 6 below.

4.2 Scope of the Privacy Act for third parties

The privacy regime in Australia includes various pieces of legislation, and includes separate Commonwealth and State/Territory regimes.

The Privacy Act applies to "APP Entities" which include organisations (such as individuals, companies, partnerships, trusts and unincorporated associations) and Commonwealth agencies (such as Commonwealth Government Departments, bodies established under Commonwealth legislation for public purposes, and the Australian Federal Police).

Some organisations can be exempt, however no general exemptions to the APPs apply to LSH Auto Australia. The most common exemption from the Privacy Act is for small business operators, which are individuals, companies, partnerships, unincorporated associations or trusts that have not (and where their related bodies corporate have not) had an annual turnover of more than $3m for any financial year since starting to carry on the business, provided that they do not provide a health service to an individual and hold health information, act as a credit reporting body, or act as a contracted service provider for a Commonwealth contract, or essentially trade (buy/sell) personal information. Another exemption applies to for registered political parties, and there is an exemption for individuals when not acting in a business capacity in connection with their personal, family or household affairs.

State and Territory authorities (such as State or Territory Departments, bodies established under State or Territory legislation for public purposes) are generally exempt from the Privacy Act, and are instead required to comply with the separate State privacy regimes.

Please contact the Privacy Officer if we will be collecting personal information from, or disclosing personal information to, State or Territory agencies, or businesses that may be exempt from the Privacy Act. In these situations, we many need to take different steps to ensure we comply with our privacy obligations.

4.3 Engaging sub-contractors and service providers

Generally LSH Auto Australia seeks to ensure that sub-contractors comply with the Privacy Act and the APPs. Sometimes LSH Auto Australia may have specific obligations under its own contracts to ensure that sub-contractors comply with privacy obligations.

5 The APPS

There are 13 APPs which prescribe minimum standards for the way in which LSH Auto Australia must handle Personal Information. The APPs cover the following categories:

- **Consideration of personal information privacy**
    - ☐ APP 1 - Open and transparent management of personal information
    - ☐ APP 2 - Anonymity and pseudonymity
- **Collection of personal information**
    - ☐ APP 3 - Collection of solicited personal information
    - ☐ APP 4 - Dealing with unsolicited personal information
    - ☐ APP 5 - Notification of the collection of Personal Information
- **Dealing with personal information**
    - ☐ APP 6 - Use or disclosure of Personal Information
    - ☐ APP 7 - Direct marketing

- ☐ APP 8 - Cross-border disclosure of personal information
- ☐ APP 9 - Adoption, use or disclosure of government-related identifiers

- **Integrity of personal information**
  - ☐ APP 10 - Quality of Personal Information
  - ☐ APP 11 - Security of Personal Information

- **Access to, and correction of, personal information**
  - ☐ APP 12 - Access to Personal Information
  - ☐ APP 13 - Correction of Personal Information

Sections 8 to 16 of this Manual are intended to provide an overview of the key aspects of these APPs and some tips and traps for compliance. If you have any specific areas of enquiry or concern please direct these to the Privacy Officer.

6 Personal information

6.1 What is personal information?

For the purposes of this Manual, "personal information" has the same meaning given under the Privacy Act. It means 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 (**Personal Information**). Personal Information can include details like an individual's name, signature, address, phone number, date of birth, driver's licence, location information (eg, from a vehicle GPS), employment information and online account information.

There are various sub-sets of Personal Information, such as “sensitive information” and “health information”, that attract different obligations under the Privacy Act and APPs. For example, there are more onerous obligations (higher standards) that apply to the handling of “sensitive information” and “health information”.

References to Personal Information in this Manual (and in our Privacy Policy and other privacy documentation) include these subsets of Personal Information, unless otherwise indicated.

Personal Information does not include information that has been de-identified so that the individual is no longer identifiable (whether from that information alone, or from that information in combination with other reasonably available information).

6.2 Sensitive information

Sensitive information is defined under the Privacy Act to include the following (**Sensitive Information**):

- personal information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership or a trade union, sexual orientation or practices or criminal record;
- health information about an individual;
- genetic information about an individual;

- biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- biometric templates.

Health information means any information or opinion about the health or disability of an individual, the individual's expressed wishes about the future provision of health services and a health service provided, currently or in the future, to an individual that is also personal information.

While LSH Auto Australia would not ordinarily collect Sensitive Information in the course of carrying on its business, it is possible that LSH Auto Australia may do so in certain circumstances (for example as part of its recruitment processes, or to meet the needs of customers who may have disabilities). Please be mindful of the additional requirements that apply to Sensitive Information (which are generally stated or summarised in this Manual). One example of such additional requirements is that LSH Auto Australia may only collect Sensitive Information if the relevant individual has consented.

6.3 Credit information

The Privacy Act includes specialised provisions regulating the handling of credit information (for example, credit reports about individuals obtained from credit reporting agencies). There is also a code of conduct, known as the CR Code (Credit Reporting Code) that applies under the Act and is legally binding.

Generally, LSH Auto Australia is not required to comply with the Privacy Act and APPs for the handling of credit information because LSH Auto Australia is not a credit provider – to the extent that credit is provided to individuals (eg, financing of vehicles), this is managed through third parties such as Mercedes-Benz Finance. If you receive any questions regarding credit management please refer at first instance to the Privacy Officer.

7 Acts or practices that are exempt

In limited circumstances some acts or practices may be exempt from compliance with the Privacy Act and APPs, for example certain acts and practices in relation to "employee records", or sharing Personal Information with related bodies corporate of LSH Auto Australia.

7.1 Sharing Personal Information with a related body corporate

Organisations are able to share Personal Information (other than Sensitive Information) with their related bodies corporate without breaching the APPs. This means that LSH Auto (Sydney), LSH Auto (Melbourne) and LSH Auto (Brisbane) can exchange personal information, such as customer details. However, particular customers may not be aware of this exception or the relationship between the LSH Auto Australia group companies, so care should be taken before Personal Information collected by one of these companies is used to contact customers of one of the other companies. You should generally not use Personal Information collected by one of the other group companies to conduct direct marketing.

This means that Personal Information (other than Sensitive Information) can be shared freely between such entities in corporate groups, but any subsequent handling of such information (for example, use or disclosure of that information by the receiving entity) must comply with the APPs.

7.2 Employee records

This Manual does not cover our processes and procedures for the handling of the LSH Auto Australia employee Personal Information. This is because we are not required to comply with the Act and the APPs in relation to acts or practices directly related to:

- a current or former employment relationship between us and an individual; and
- an "employee record" held by us and relating to the individual.

An employee record means a record of Personal Information relating to the employment of the employee (eg, the terms and conditions of an employee's employment and an employee's personal and emergency contact details, and information about the employee's performance and conduct).

It is important to note that the employee records exemption applies only to our current and former employees. It does not apply to Personal Information received about a prospective employee (eg, a resume or CV from a job applicant), independent contractors, consultants or volunteers, since such Personal Information does not relate to the employment of a current or former employee. LSH Auto Australia must comply with the APPs in handling Personal Information relating to such individuals.

Please contact Human Resources for further information about the proper handling of employee records.

8 Transparency about LSH Auto Australia privacy practices (APP 1)

8.1 Transparency and internal practices, procedures and systems

Under APP 1, LSH Auto Australia is required to manage Personal Information in an open and transparent way.

In doing so, LSH Auto Australia must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to LSH Auto Australia's functions or activities that:

- will ensure that LSH Auto Australia complies with the APPs; and
- will enable LSH Auto Australia to deal with enquiries or complaints from individuals about its compliance with the APPs.

This Manual and our other privacy-related documentation, policies and procedures are designed to promote compliance with this requirement.

This obligation requires us to keep privacy at the forefront of our consideration when planning new projects and systems that will involve Personal Information (for example, IT systems, conducting EDMs, and sharing of Personal Information with insurers or other clients). Please liaise with the Privacy Officer in connection with such projects and system development so we can ensure that our procedures are adhered to, and (if applicable) updated accordingly.

8.2 Privacy Policy

LSH Auto Australia is required to have a clearly expressed and up-to-date policy about the management of Personal Information by LSH Auto Australia that contains the information specified in APP 1.

Our Privacy Policy has been prepared for this purpose. It is available to the public on our website: https://www.lshauto.com.au/privacy-policy. Each dealer location also has its own privacy policy located on its website.

If a person external to LSH Auto Australia requests a copy of our Privacy Policy you should refer them to the website, and notify the Privacy Officer of the request. It is prudent to notify

the Privacy Officer since a request for a copy of our Privacy Policy might be a precursor to a complaint.

A person may request a copy of the Privacy Policy in a particular form (eg, hard copy), and LSH Auto Australia must take reasonable steps to provide a copy for free in the requested form. The Privacy Officer can help you deal with such routine requests.

8.3 Tips and traps

- **DO** familiarise yourself with our Privacy Policy and this Manual;
- **DO** notify the Privacy Officer of requests for our Privacy Policy;
- **DO** refer enquiries about LSH Auto Australia's privacy practices to the Privacy Officer;
- **DO** notify the Privacy Officer if you believe our privacy documents may need updating to reflect our practices, procedures and systems; and
- **DO NOT** provide this Manual to any member of the public or another organisation outside the LSH Auto Australia group.

9 Anonymity and pseudonymity (APP 2)

9.1 Background

APP 2 provides that individuals must have the option of dealing with us anonymously or by using a pseudonym.

If we receive a communication from an individual that is made anonymously or using a pseudonym, we must make an assessment as to whether we are able to appropriately deal with that communication without having that individual's Personal Information.

If we can deal with that individual anonymously (or through a pseudonym) we should not require the individual to provide his or her Personal Information (eg, his or her name, etc). Exceptions may include where LSH Auto Australia has legal obligations that require identification of the individual, or where is it is not practicable to deal with the person anonymously.

There are likely to be many situations where it is not practicable to deal with a person without obtaining their Personal Information. For example, we would generally not be able to sell a customer a vehicle or arrange a test drive without collecting the customer's Personal Information. However, an example of where it may be practicable to deal with a person anonymously is where a person makes a simple telephone enquiry (for example, about availability or price of a particular model vehicle).

If you are uncertain whether we can deal with an individual anonymously (or through a pseudonym) in a particular circumstance, please ask your Department Manager. If necessary, the Department Manager will refer the matter to the Privacy Officer.

9.2 Tips and traps

- **DO** give people the option of not identifying themselves if appropriate in the circumstances (for example, where the person is making a general enquiry over the phone); and

- **DO NOT** allow a person to be anonymous or use a pseudonym where it would be impractical or cause us to breach our legal requirements.

10 Collection of Personal Information (APPs 3, 4, 5)

The APPs differentiate between Personal Information that is solicited, and that which is unsolicited. Personal Information is solicited when we have asked an individual or a third party to provide it.

10.1 Solicited Personal Information

We must only collect solicited Personal Information (including Sensitive Information) if that information is reasonably necessary for one or more of our functions or activities.

If the Personal Information is Sensitive Information then additional criteria must be satisfied. Generally, this requires consent. With the exception of staff recruitment, it is LSH Auto Australia policy not to collect Sensitive Information, even if it is offered by the customer.

In the absence of consent, collection of Sensitive Information may be permissible if a situation in APP 3.4 applies (for example, the collection is required or authorised by Australian law or a court/tribunal order, or the collection is necessary for LSH Auto Australia to take action in relation to suspected unlawful activities or misconduct of a serious nature that relates to our functions or activities). You should consult with the Privacy Officer (who might seek specific legal advice) if seeking to rely on an APP 3.4 situation.

We must collect Personal Information directly from the individual to whom it relates (unless it is unreasonable or impracticable to do so).

10.2 Unsolicited Personal Information

Unsolicited Personal Information is received where Personal Information is volunteered or sent to us without our requesting. Examples might be a resume from someone seeking work, or additional details about someone's home or family situation that are not relevant to the services we are providing that are disclosed to us.

If we receive unsolicited Personal Information, we must make an assessment as to whether collection of that Personal Information is reasonably necessary for one or more of our functions and activities.

If so, then that information must be handled in accordance with this Manual and our Privacy Policy.

If not, we must, as soon as practicable after that assessment is made (but only if it is lawful and reasonable to do so), destroy the information or ensure that the information is effectively de-identified.

10.3 LSH Auto Australia notification requirements on collection

When we collect Personal Information, we must take reasonable steps to notify the relevant individual of the following matters:

- LSH Auto Australia's identity and contact details;
- if we collected the Personal Information from a third party, the fact and circumstances of the collection;
- whether the collection is required or authorised by law;

- the purposes of the collection;
- the main consequences if Personal Information is not collected;
- the identity of those entities we usually disclose Personal Information of that kind to;
- information about our Privacy Policy (eg, that an individual may request access to his or her Personal Information and information regarding our privacy complaints process); and
- whether we are likely to disclose Personal Information to overseas recipients, and if practicable, the countries where they are located.

The above notification must be provided before, or at the time LSH Auto Australia collects Personal Information. If this is not practicable, notification should be provided as soon as practicable after the collection. We have a standard form of this information that we use on our website contact pages and on various forms used in our dealerships.

10.4 Tips and traps

- **DO** only collect information that is reasonably necessary for our business;
- **DO NOT** collect Sensitive Information about a person unless they have consented to the collection and it is necessary for our activities; and
- **DO** act fairly and lawfully when collecting Personal Information (a good rule of thumb is to only collect information in a way that you would be comfortable with your information being collected);
- **DO** provide persons with an official LSH Auto Australia personal information collection statement when you collect their Personal Information (or as soon as possible afterwards);
- **DO** only collect information about an individual from a third party if it would not be reasonable or practical to collect it directly from the individual;
- **DO** promptly assess any unsolicited Personal Information to determine whether we could have collected it if it were solicited;
- **DO NOT** destroy any unsolicited Personal Information except in accordance with our policies and procedures, including this Manual.

11 Use and disclosure of Personal Information (APPs 6 and 10)

11.1 Background

We may use or disclose Personal Information for the specific purpose for which it was collected (known as the “primary purpose”).

Beyond that, we may use or disclose Personal Information for another purpose (the “secondary purpose”) if the individual from whom the information was collected:

- consents to that use and disclosure; or

- would reasonably expect that we would use or disclose the information for the secondary purpose, and that secondary purpose is related (or directly related in the case of Sensitive Information) to the primary purpose.

There are other exceptions (in addition to the ones in the dot points above), for example where the disclosure is required under an Australian law or by a court or tribunal, or because of court or dispute resolution proceedings. As these exceptions do not affect most LSH Auto Australia team members, you should seek guidance from the Privacy Officer and/or local Marketing Managers (who might seek specific legal advice) if a prospective use or disclosure is not covered by the two dot points above.

LSH Auto Australia generally requires our service providers/contractors to comply with the Privacy Act (please refer to section 4.3 above). This is generally achieved through contractual arrangements with the service provider/contractor. Please confirm with the Privacy Officer that appropriate privacy protections are in place if Personal Information will be given to a third party such as a service provider or contractor.

We must take reasonable steps to ensure that the Personal Information that we use and disclose is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

In the event that we do hold any Sensitive Information (bearing in mind the comments in sections 6.2 and 10.1 above), the Privacy Act imposes additional protections on the use and disclosure of that Sensitive Information. As noted above, we can only use Sensitive Information collected for a particular purpose for that specific purpose, unless the individual has consented to the secondary purpose or the secondary purpose would be within their reasonable expectations and is "directly" related to the primary purpose. You should not use Sensitive Information other than strictly for the purpose for which it was collected without the express approval of the group Privacy Officer.

Furthermore, Sensitive Information must only be used for the purpose of direct marketing where we have obtained (and have a clear record of) the express consent of the relevant individual. It is expected that in almost all cases we would not use Sensitive Information for marketing purposes.

11.2 Tips and traps

- **DO** use or disclose Personal Information only for the primary purpose for which it was collected, or a secondary purpose that has been approved by the Privacy Officer or Management for that Personal Information;
- **DO NOT** disclose, or agree to disclose, Personal Information to an overseas recipient unless you have followed written procedures for the disclosure or other approval from the Privacy Officer or Management; and
- **DO NOT** accept the terms and conditions of offshore service providers without prior approval from the Privacy Officer or Management, who will confirm if privacy related changes are required to those terms.

12 Overseas disclosure (APP 8)

12.1 Background

Before we disclose Personal Information to an overseas recipient (other than the individual themselves), we must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information. There are exceptions to this requirement.

LSH Auto Australia can be directly liable for the acts and practices of such overseas recipients in relation to the Personal Information that LSH Auto Australia discloses to them, where those acts and practices do not comply with the APPs.

It is important that LSH Auto Australia complies with the requirements under AAP 8 in disclosing Personal Information overseas, and that LSH Auto Australia puts in place measures to minimise its liability in connection with such disclosures.

As a first step when negotiating contracts with third parties (particularly third party service providers), it is necessary to establish whether or not LSH Auto Australia shares Personal Information with that party.

If we do share Personal Information, assurances in the contract with them should cover the type of information shared, their use of that information, security measures for the data and the possibilities for overseas disclosures, amongst other things. The Privacy Officer (who might seek specific legal advice) can assist with contract terms.

Before sending any Personal Information to a recipient located overseas, or agreeing to do so, contact the Privacy Officer to ensure that appropriate legal arrangements are in place.

12.2 Tips and traps

- **DO** follow all written procedures about overseas disclosures;
- **DO** refer any questions or concerns about an overseas disclosure to the Privacy Officer;
- **DO** confirm with all potential service providers where Personal Information will be stored, and whether there will be any offshore disclosures of such Personal Information;
- **DO NOT** disclose, or agree to disclose, Personal Information to an overseas recipient unless you have followed written procedures for the disclosure or other approval from the Privacy Officer or Management; and
- **DO NOT** accept the terms and conditions of offshore service providers without prior approval from the Privacy Officer or Management, who will confirm if privacy-related changes are required to those terms.

13 Government-related identifiers (APP 9)

13.1 Use and adoption

Government-related identifiers (such as Medicare numbers, passport numbers and driver's licence numbers) cannot be:

- adopted by LSH Auto Australia as its own identifiers to identify individuals (unless required or authorised by law); or
- used or disclosed by LSH Auto Australia unless an exception in APP 9.2 applies, such as (amongst others):
    - the use or disclosure of the identifier is required or authorised by Australian law;
    - the use or disclosure of the identifier is reasonably necessary for LSH Auto Australia to verify the identity of the individual for the purposes of LSH Auto Australia's functions or activities; or

- the use or disclosure of the government-related identifier is reasonably necessary for LSH Auto Australia to verify the identity of the individual or to fulfil its obligations to an agency or State or Territory government authority.

For example, LSH Auto Australia staff should not be able to enter a government-related identifier (eg, driver's licence number) into an LSH Auto Australia database (such as our DMS when a customer attends for vehicle servicing) to retrieve information about that individual.

13.2 Tips and traps

- **DO** notify the Privacy Officer if you notice a government-related identifier being used to identify individuals in our systems;
- **DO NOT** use or adopt a government-related identifier (such as a driver's licence number) as the way of identifying a person in our systems; and
- **DO NOT** seek to rely on an exception to APP 9 without obtaining express clearance from the Privacy Officer or Management to do so.

14 Security and quality of Personal Information (APPs 10 and 11)

14.1 Security and quality

We must take reasonable steps to ensure that the Personal Information we collect, use and disclose is accurate, up-to-date and complete. In addition, we must take reasonable steps having regard to the purpose we are using or disclosing Personal Information for to ensure that it is relevant.

We must take reasonable steps to ensure that the Personal Information we hold is protected from misuse, interference, loss and unauthorised access, modification and disclosure. For example, you should choose strong passwords and change them regularly in accordance with LSH Auto Australia policies. The security around our IT systems is protected and managed by the IT Department.

There are other areas such as non-electronic records where all LSH Auto Australia team members are responsible to maintain the security of Personal Information. For example, staff should not leave hard-copy documents on display in work areas accessible or visible to the public.

Subject to our record-keeping policies, when we no longer need Personal Information for any of our functions and activities and it is allowable by law, we must take reasonable steps to destroy the Personal Information or ensure that it is effectively de-identified. If you are unsure whether specific data should be kept or deleted, please check with the Privacy Officer.

For example, you should regularly delete emails from your account that contain the Personal Information of customers. If a customer sends you a scan of their driver's licence as proof of identity, then once that information has served its purpose, typically the email should be deleted. This is subject to any other specific LSH Auto Australia policies regarding retention of records (for example, we may be required to retain key documents relating to customer finance applications).

14.2 Links in emails

You should take care not to access links or otherwise engage with emails received from unknown sources, or which otherwise appear suspicious. You should not click any links or copy them into your web browser. Emails from hackers may be sent from an actual business

contact of yours (eg, where that person's email account has been compromised), or be designed to imitate legitimate correspondence.

If you suspect that an email you have received may not be legitimate, you should immediately contact the IT department for assistance. Depending on your relationship with the apparent sender of the email, you might also telephone them to confirm whether the email is legitimate – but avoid replying directly to the suspicious email. If you do access a link in an email, make sure to carefully check the URL of the website to confirm it is legitimate. If you are prompted to enter or re-enter login information for your email or other account (even if the webpage looks genuine), that may be an indication of suspicious activity.

Unfortunately, perpetrators of such scams are adept at deploying significant resources to compromise even the best security measures available, and LSH Auto Australia has been targeted by such scams in the past. We must therefore all be wary upon receiving unsolicited or suspicious emails, particularly those requesting personal information or containing links or attachments.

14.3 Tips and traps

- **DO** adhere to all LSH Auto Australia security policies in relation to electronic and hard-copy information;
- **DO**, where you think there may have been a breach of security, report the breach as soon as possible;
- **DO** exercise caution before accessing links in emails that you receive;
- **DO** consult with your Department Manager or the Privacy Officer prior to destroying or de-identifying Personal Information if you are uncertain about our retention requirements;
- **DO** consider whether information is likely to still be accurate, complete and up-to-date prior to using or disclosing it;
- **DO NOT** allow any unauthorised person to access your computer or any other device which may contain Personal Information collected by LSH Auto;
- **DO NOT** access Personal Information that you do not need to access in connection with your role; and
- **DO NOT** use or disclose information when you know that it is not (or might not be) correct.

15 Access to and correction of Personal Information (APP 12 and 13)

15.1 Access

If we hold Personal Information of an individual, we must give the individual access to that information on request, however some exceptions apply under APP 12.3.

Since Personal Information includes an opinion about a person, you should be mindful when recording any comments about a customer, for example in our DMS. There is the possibility that the customer could obtain access to the comments you write. This has the potential to lead to embarrassment and negative media attention for LSH Auto Australia.

We must not charge an individual for making a request to access their Personal Information, however we may charge the individual for giving access to their Personal Information. After we assess an application for access to Personal Information, we must notify the individual of any fee payable. Any such fee must not be excessive.

If we refuse a request for access to Personal Information, we must provide written reasons for the refusal and details of the mechanisms available to complain about the refusal (eg, the individual may make a complaint to the Privacy Commissioner).

Please forward all requests for access to Personal Information to our Privacy Officer and local Marketing Managers for assessment and actioning. Other LSH Auto Australia personnel should not deal with such requests given the potential risks involved (eg, wrongful disclosure or refusal to disclose) and the need to maintain careful records of compliance, applicable timeframes and disclosures made.

15.2 Correction

We are required to take reasonable steps to correct Personal Information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.

If we are satisfied that Personal Information we hold about an individual is not accurate, is not up-to-date, is incomplete, is irrelevant or is misleading, we must amend our records accordingly.

We must not charge the individual for requesting correction of their Personal Information.

If requested by the individual, we must take reasonable steps to notify third parties to whom we have previously disclosed Personal Information that it has been corrected. Please follow any operational procedures that apply in that case. If you are not sure or if there are no procedures, please refer to your Department Manager. If necessary, your Department Manager will consult the Privacy Officer.

If we refuse to correct Personal Information, we must provide written reasons for the refusal and notify the individual of the mechanisms available to complain about the refusal (eg, the individual may make a complaint to the Privacy Commissioner). Further, if we refuse to correct Personal Information, we must (on the request of the individual) add a statement to the relevant Personal Information which states that the Personal Information is inaccurate, out-of-date, incomplete, irrelevant or misleading. Any refusal to amend our records should follow any operational procedures that apply in that case. If you are not sure or if there are no procedures, please refer to your Department Manager. If necessary, your Department Manager will consult the Privacy Officer.

Please note:

- adequate identity verification will be necessary before dealing with such requests or disclosing Personal Information in response to them; and
- even where those procedures have been followed, if the enquiry is not straightforward or if you are unsure about the request, please refer to your Department Manager, and if necessary your Department Manager will consult the Privacy Officer.

15.3 Tips and traps

- **DO** always keep in mind that people can request access to their Personal Information;
- **DO NOT** record opinions about a person without considering the possibility that they will be able to obtain access to that information;

- **DO NOT** respond to a request for access or correction without following the appropriate procedures;
- **DO** promptly refer any non-straightforward access request to the Privacy Officer; and
- **DO** keep a record of disclosures of Personal Information made to other organisations.

16 Direct marketing (APP 7)

16.1 Use and disclosure for marketing

Direct marketing is essentially a direct communication by LSH Auto Australia to a person to promote the sale of goods or services to that person (for example, direct marketing to specific individuals, rather than a random letterbox drop around a neighbourhood). Direct marketing can be by mail, SMS, email or telephone.

The APPs apply to direct marketing using Personal Information, other than electronic marketing such as EDM emails or SMS messages. Electronic marketing is subject to different legislation and has slightly different requirements, as discussed further below.

Under the APPs, we must not use or disclose Personal Information for the purpose of direct marketing unless an exception applies. Generally, we are able to use Personal Information for direct marketing if:

- the individual has consented to use of their Personal Information for direct marketing; or
- the Personal Information was collected directly from the individual and they would have a reasonable expectation that we will use that Personal Information for direct marketing.

When disclosing Personal Information for the purpose of direct marketing, we must always allow an individual to request not to receive direct marketing communications.

In most cases the direct marketing must also include a prominent statement informing the individual that they may make an opt-out a request. If an individual opts out then we must make sure that request is promptly actioned.

In addition, if requested by the individual, we must notify them of the source from which we obtained the individual's Personal Information.

Rules can also apply under other legislation, for example under the *Do Not Call Register Act 2006* (Cth) and the *Spam Act 2003* (Cth) (**Spam Act**). The Spam Act will apply to commercial electronic messages. The key requirements under the Spam Act are that the individual has consented to receive the messages, that the sender of the messages is clearly identified, and that the message contains a functional unsubscribe facility.

Marketing issues and the laws surrounding marketing can affect all forms of marketing from simple flyers to more elaborate campaigns. All email and digital marketing campaigns will be overseen by the Marketing Team. Consult them or the Privacy Officer regarding any enquiries.

16.2 Tips and traps

- **DO** make sure any direct marketing activities are approved by the Privacy Officer or Management before you begin to use or disclose Personal Information in relation to such activities; and

- **DO** make sure that sender information, opt-out statement and opt-out method are included on all communications in the form approved by the Privacy Officer or the Marketing Team.

17 Data breach

The Privacy Act includes specific provisions regarding how an organisation must respond to certain data breaches. Our processes for responding to a data breach are set out in our Data Breach Response Manual. If you become aware of an actual or suspected data breach, you should refer to that document.