AUSTRALIAN AUTOMOTIVE DEALER ASSOCIATION

DEALER BULLETIN

Notifiable Data Breaches Scheme

23 FEBRUARY 2018

To: ALL AADA MEMBERS

With increasingly complex on-board software and customer monitoring systems, motor vehicles and their associated servicing programs now gather significantly expanded personal information. At the same time, most OEMs and finance companies require dealers to participate in CRM and data-mining programs that leverage and share sensitive personal data. Dealers of course also run their own customer retention and marketing programs using the same information. Ultimately, dealers hold considerable amounts of personal data about customers, employees and other individuals with whom they deal.

As a result of the proliferation of end-users for customer data, dealers' businesses can be at risk of breaching the new privacy rules - in almost all cases, inadvertently so. We therefore provide below, a summary of new laws which have come in to effect requiring businesses to report instances of data breach, where that breach may result in individuals suffering serious harm. The NDB scheme requires a business who has experienced a data breach, to notify the Australian Information Commissioner and any individuals who may be subject to serious harm because of the breach.

This new scheme further highlights the importance of keeping data secure and ensuring that there are processes in the dealership that protect and control access to all personal data that a dealer may hold.

Businesses are only required to act if they think the breach may result in serious harm to the affected individuals. *Whether a data breach is likely to result in serious harm requires an objective assessment, determined from the viewpoint of a reasonable person in the entity's position.

*The notification to affected individuals and the Commissioner must include the following information:

- the identity and contact details of the organisation;
- a description of the data breach;
- the kinds of information concerned and;
- recommendations about the steps individuals should take in response to the data breach.

A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure.

*Examples of a data breach include when:

- a device containing customers' personal information is lost or stolen;
- a database containing personal information is hacked and;
- personal information is mistakenly provided to the wrong person.

More detailed information is available from the Office of the Australian Information Commissioner.

*Taken from the website of the Australian Information Commissioner

If you have questions, please a contact any of the team members listed below.

Brian Savage
Executive Director Operations
Australian Automotive Dealer Association Ltd
E: bsavage@aada.asn.au
M: +61 418 377 594