

Direction under s. 41(1) of the Privacy and Personal Information Protection Act 1998 in relation to Service NSW

As Privacy Commissioner appointed under Part 4, Division 1 of the *Privacy and Personal Information Protection Act 1998* (“the PPIP Act”), I, Samantha Gavel, hereby direct, pursuant to section 41(1) of the PPIP Act that:

1. Overview

This is a direction made under section 41(1) of the *PPIP Act*. It should be read in conjunction with the PPIP Act.

2. Interpretation

2.1 In this Direction, the following words have the respective meanings:

“**BDM**” means the business unit within the Department of Customer Service which is responsible for the registration of births, deaths and marriages, and includes the NSW Registrar of Births, Deaths and Marriages.

“**The customers**” means the individuals who have at any time been provided with a service by Service NSW.

“**DCS**” means the Department of Customer Service.

“**DRIVES**” means RMS’ DRiver and VEhicle System containing inter alia, the Driver Licence Register and Demerit Points Register, in accordance with Chapter 3 of the *Road Transport Act 2013*, the Vehicle Registration Register, in accordance with Chapter 4 of that Act, and the Photo Card Register in accordance with section 15 of the *Photo Card Act 2005*.

“**IPP**” means the Information Protection Principle set out in the section of the *PPIP Act* with the corresponding number;

“**Personal information**” has the same meaning as in s. 4 of the *PPIP Act*.

“**POI**” means proof of identity.

“**PPIP Act**” means the *Privacy and Personal Information Protection Act 1998*.

“**Service NSW**” means the Service NSW Division of the Government Service whose CEO has the functions conferred by the *Service NSW (One-stop Access to Government Services) Act 2013*.

‘TfNSW’ means Transport for New South Wales.

“Transport for New South Wales” means the corporation established under the *Transport Administration Act 1988* with the corporate name of Transport for NSW.

3. Background

- (a) Service NSW is a public sector executive agency. Service NSW is related to the Department of Customer Service, under Schedule 1 of the *Government Sector Employment Act 2013*.
- (b) BDM comprises employees of the Department of Customer Service.

4. Objectives of this Direction

- (a) Service NSW provides government services to the customers on behalf of, inter alia, Government agencies.
 - (b) Service NSW was recently the victim of a cyber attack that has potentially compromised the personal information of a large number of the customers.
- 4.1 Service NSW wants to contact impacted customers urgently for the purpose of notifying them of the potential compromise of their personal information and providing them with assistance to respond to the potential compromise of their personal information.
- 4.2 In order to contact the impacted customers as quickly as possible, so that their personal information is not further compromised, Service NSW wishes to rely on the most recent contact details available for the customers, some of whom may not have been provided with services by Service NSW for many years.
- 4.3 By virtue of requirements relating to the notification of changes to residential address under clause 122 of the Road Transport (Driver Licensing) Regulation 2017, clause 37 of the Road Transport (Vehicle Registration) Regulation 2017, and clause 9(1) of the Photo Card Regulation 2014 respectively, TfNSW holds the most reliable contact information for the majority of NSW citizens.
- 4.4 Accordingly, in order to obtain access to the most recent available contact information, Service NSW wishes to collect the most recent contact information held by TfNSW and BDM for the purposes of using that information to contact the customers as quickly as possible.
- 4.5 In order to avoid notifying the customers who are deceased, Service NSW also wishes to obtain access to the death status of the customers using information held by BDM.
- 4.6 BDM also wishes to take steps to safeguard its system from unlawful use by individuals who have obtained the personal information of customers.
- 4.7 IDCARE, a national identity and cyber support service, has been engaged to support customers whose data may have been compromised by the cyber-attack.

5. Process

- 5.1 Data will be securely provided by the forensic contractors engaged to analyse the mailboxes, to DCS. DCS will securely transfer data to TfNSW to enable the addition of mailing addresses, where possible. The data will then be securely transferred to BDM, to verify the customer is not deceased and to enable birth records to be flagged, where possible.
- 5.2 DCS will combine the data from TfNSW and BDM. The file containing this data will be securely transferred to Service NSW.
- 5.3 DCS will remove the records of deceased customers and customers where no mailing address has been located and securely transfer this file to a mailing house.
- 5.4 The mailing houses will securely arrange for letters to affected customers to be printed and enveloped and securely transferred to Australia Post. Letters to customers will be forwarded by person-to-person registered mail.
- 5.5 Service NSW will use the data to assist impacted customers when they contact Service NSW for further assistance.

6. Public Interest

- 6.1 This Direction has been made to permit the collection, use and disclosure of personal information by Service NSW, DCS, TfNSW and BDM for the purposes of Service NSW obtaining from the database administrators the most recent contact details, and death status for the customers, whose personal information was affected by the cyber-attack on Service NSW, and using those contact details to notify and provide assistance to the customers. This assistance will include the referral of customers to IDCARE for advice on steps to take to minimise the risk of identity theft and/or financial fraud. Service NSW may also coordinate reissuing of NSW Driver Licence and Photo ID Cards subject to TfNSW approval for particular customers.
- 6.2 The public interest in permitting the collection, use and disclosure of personal information, in circumstances that might not otherwise be authorised by the *PIIP Act*, is the protection of the personal information of the customers, the integrity of which may have been compromised by the cyber-attack.
- 6.3 That public interest is served by enabling the exchange of the latest information about the contact details and death status of the customers between Service NSW, DCS, TfNSW and BDM to enable the most privacy-secure means of contacting the customers as quickly as possible.
- 6.4 The public interest in Service NSW, DCS, TfNSW and BDM complying with the relevant IPPs is outweighed by the public interest in permitting them to exchange information to enable Service NSW to urgently contact the customers to endeavour to protect their personal information from being compromised or further compromised.

7. Information exchange agreements

- 7.1 Service NSW will enter into information exchange agreements with DCS, TfNSW and BDM documenting the roles and responsibilities of each party, including information governance arrangements, data security arrangements, data retention, access protocols, reporting requirements (including the reporting of breaches), and audit requirements.

8. Breach

- 8.1 If Service NSW, DCS, TfNSW or BDM collect, use or disclose personal information other than in accordance with this Direction, Service NSW must notify the NSW Privacy Commissioner within 48 hours of confirmation that such a contravention has occurred.

9. Reporting and Auditing

- 9.1 Service NSW will report to the NSW Privacy Commissioner on compliance with this Direction, including the following matters:

9.1.1 confirmation by Service NSW regarding the correctness of all disclosures in connection with this Direction;

9.1.2 detail of any complaints received from the public regarding the collection, use and disclosure of personal information under this Direction;

9.1.3 subject to clause 8.1, any data breaches arising from this Direction involving personal information, or where breaches could have arisen;

9.1.4 the results of all audits conducted in accordance with paragraph 9.2.

- 9.2 Service NSW will appoint an auditor, independent of the agencies concerned, within 6 months of the conclusion of this Direction to assess compliance with this Direction. This compliance audit will assess the security of systems and processes protecting the collection, use and disclosure of personal information regarding this Direction. This compliance audit may include information provided by other parties, so long as these other parties are confirmed by the auditor to be independent of the agencies concerned.

10. Duration

- 10.1 This Direction has effect from the date of this direction until **31 January 2021**.

11. Modification of Information Protection Principles

- 11.1 The application of the information protection principles under Division 1, Part 2 of the *PPIP Act* to Service NSW, DCS, TfNSW and BDM is modified to the extent described below.

- 11.2 **IPP 1:** For the purposes of s. 8(1) of the *PPIP Act*, the collection by Service NSW, DCS, TfNSW and BDM of personal information is taken to be for a lawful purpose that is related to a function or activity of those agencies if the collection is for the purposes of this Direction and the collection is reasonably necessary for those purposes.

- 11.3 **IPP 2:** Notwithstanding s. 9 of the *PPIP Act*, Service NSW, DCS, TfNSW and BDM may collect personal information about the customers for the purposes of this Direction, but s. 9 otherwise applies to them.
- 11.4 **IPP 9:** Notwithstanding s. 16 of the *PPIP Act*, the personal information used by Service NSW, DCS, TfNSW and BDM in relation to the customers is taken to be relevant, accurate, up to date, complete and not misleading having regard to the purposes of this Direction, but s. 16 otherwise applies to them.
- 11.5 **IPP 10:** For the purposes of s. 17 of the *PPIP Act*, use of personal information about the customers by Service NSW, DCS, TfNSW and BDM for the purposes of this Direction is taken to be use for the purpose for which it was collected, but s. 17 otherwise applies to them.
- 11.6 **IPP 11:** For the purposes of s. 18 of the *PPIP Act*, disclosure of personal information about the customers by Service NSW, DCS, TfNSW or BDM for the purposes of this Direction is taken to be a disclosure that is directly related to the purpose for which the information was collected and is taken to have been made in circumstances where the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure, but s. 18 otherwise applies to them.
- 11.7 **IPP 12:** Service NSW, DCS, TfNSW or BDM need not comply with s. 19(1) of the *PPIP Act* where the database administrator or Service NSW is satisfied that it is necessary, for the purposes of this Direction, to disclose a third person's personal information, but s. 19 otherwise applies to them.

Signed by me on 5 August 2020



Samantha Gavel
Privacy Commissioner