Tedoo
Behaviour Support & Therapeutic Services

Statement of Data Breach

Our identity and contact details

Tedoo Pty Ltd ABN 65 639 118 488
Email: enquiries@tedoo.com.au
Website: www.tedoo.com.au
Telephone: 0408 682 287

About the data breach

On 30 August 2024 between 2.37am and 2.54am we suffered a data breach incident. An unknown third party obtained access to an administration email account we maintain via Microsoft and, using the administrators email account (admin@tedoo.com.au) sent unauthorised emails to some individuals whose email addresses were stored in that account.

This incident was discovered at 7.15am on 30 August 2024 and immediate steps were taken to prevent any further access to the affected email account.

The kinds of information that may have been involved

Other than individuals' email addresses, the extent to which personal information held in the email account was accessed remains unknown to us, despite systems checking which has been undertaken. If personal information held in the email account was accessed, it will have been some of the following primarily via our Referral Form and Service Agreement documents:

- *NDIS participant*: name, disability type, date of birth, cultural background or ethnicity, address, telephone number, email address, NDIS number and NDIS funding information;
- *Primary contact person for dealings with us*: the name, address, email address and phone number of the primary contact for the NDIS participant who is noted in our records;
- *Service providers involved in their receipt of service (for example support coordinators, plan managers and support agencies)*: the name, email address and telephone number for those service providers.

In limited cases, emails in our email administration account (admin@tedoo.com.au) included other attached documents. The kinds of information which may have been in the attached documents were detailed information about NDIS participants' disability and/or diagnosis, the impacts of those disabilities/diagnosis, current and/or historical functioning/presentation and support needs. There may have also been recommendations for support for the NDIS participant.

What is being done

We sent an initial statement about the data breach to the Office of the Australian Information Commissioner on 2 September 2024.

We have taken the following measures to contain the breach:

- Fixed the vulnerability by disconnecting all unauthorised access to the administration email account;
- Conducted an internal investigation of the breach to endeavour to identify the cause and vulnerability;
- Changed passwords for all admin and other relevant user accounts;
- Sent initial emails to relevant primary contacts warning them of the phishing involved and not to click on any links;
- Notified the Australian Cyber Security Centre;
- Notified Microsoft;
- Sent further emails to primary contacts offering IDCARE's services (see further on this below);
- Limited physical access to communications devices issued by us to our contractors and staff;
- Decommissioned redundant email accounts and
- Put in place additional IT support for regular monitoring of our IT security.

Our recommended steps in response

It is possible that, as a result of the breach, you may receive unsolicited emails requesting you to provide account details or other confidential person information, to click on a link or to open an attachment. Please exercise extreme caution in how you handle such messages. You should not respond to them, not click any links provided and not open any attachments to them. Doing so may expose you to malware downloaded onto your communication devices.

Separately, we have engaged IDCARE's services. IDCARE's service are at no cost to you. If you wish to speak with one of IDCARE's expert Case Managers, please complete an online Get Help form at www.idcare.org or call 1800 595 160. Please note IDCARE specialist Case Managers are available from 9am – 5pm Monday to Friday, excluding Public Holidays. When engaging IDCARE, please use the referral code TEDOO24.