

Memorandum of Understanding for Access to Withheld Data

Between

Domain Name Commission Limited, 89 The Terrace, Wellington

And

The Ministry of Business, Innovation and Employment acting by and through the Computer Emergency Response Team ("**CERT NZ**")

1. Introduction

1.1 Background

- a. This Memorandum of Understanding (**MOU**) sets out an agreement between Domain Name Commission Limited (**DNCL**) and CERT NZ regarding access to the Withheld Data (as defined below) from a .nz domain registration data query (the .nz Query).
- b. This MOU does not replace the existing Mutual Non-Disclosure Agreement dated 20 February 2017 between DNCL and CERT NZ ("**Existing Agreement**").
- c. .nz is the country code top level domain (**ccTLD**) for New Zealand. Internet New Zealand Incorporated (**InternetNZ**) holds the delegation for .nz. DNCL is a fully owned subsidiary of InternetNZ and has been established to manage the day to day functions and oversight of the .nz domain name space on their behalf under the terms of an Operating Agreement.
- d. Like all other top level domains, .nz operates a .nz domain name registration data query (**Query**). A Query of a .nz domain name returns information about that domain name including its status and details of the person or entity who registered that domain (**Registrant**) if it is registered.
- e. Following a recent review, changes have been made to the .nz policies around the .nz Query. These changes mean that individual Registrants that are not using the domain name to any significant extent in Trade are able to withhold the information displayed about them on any relevant domain registration records by withholding their telephone number and contact address information (**Withheld Data**). All other information regarding the domain name's Registrant is returned as a result of a Query, including the Registrant's name, email and country.
- f. The .nz policy around Withheld Data includes procedures around when the Withheld Data can be released to third parties. The policy also allows for MOUs to be entered into with appropriate entities who may require regular and ongoing access to the Withheld Data.
- g. DNCL operates in an open and transparent manner consistent with the InternetNZ principles. One of DNCL's key responsibilities under the Operating Agreement is to ensure compliance with the .nz policy framework, which includes reporting on activities relating to Withheld Data.
- h. CERT NZ supports businesses, organisations, and individuals in New Zealand who are or may be affected by cyber security incidents or potential threats. It provides trusted and

authoritative information and advice, and reports generally on the cyber security threat landscape in New Zealand.

- i. Five key foundation services and functions of CERT NZ are threat identification, vulnerability identification, incident reporting, response coordination and readiness support.
- j. As part of CERT NZ's operations, information relating to domain name registrants is or may be required for a variety of reasons.

1.1 Purpose

The purpose of this MOU is to outline the circumstances when CERT NZ may access the Withheld Data, the restrictions on such access and to support DNCL's public reporting relating to access to Withheld Data.

2. Principles and Policies

2.1 This MOU represents commitments by each party in respect to accessing Withheld Data and reporting on such access and the relationship arising between the parties as a result. This MOU, and the commitments and relationship recorded by it, are founded on the following principles:

- a. That all activities under this MOU align with the .nz policies to the extent such alignment is reasonably possible.
- b. Balancing the rights of Registrants against the benefits of Registrant accountability, including consideration of:
 - i. Registrants' expectation that Withheld Data will be closely protected and will not be disclosed unless the requester gives a Permitted Reason; and
 - ii. Registrants' rights to be notified of requests for Withheld Data.
- c. Timely access to Withheld Data.
- d. Supporting public transparency of requests for Withheld Data.

3. Acknowledgements

3.1 DNCL acknowledges that CERT NZ has and will have legitimate reasons to require access to Withheld Data.

3.2 CERT NZ acknowledges that:

- a. a Query may provide it with sufficient information in most cases, and access to Withheld Data will be restricted to circumstances satisfying one or more Permitted Reasons (as set out in clause 4.3); and
- b. DNCL will report publicly at a high level only on requests for access to Withheld Data.

3.3 Both parties acknowledge that there will be occasions when access to the Withheld Data is needed in a timely manner to prevent possible security issues and harm and this requirement is reflected in the nature of this MOU. The parties will work together as much as possible to resolve any such security issues.

4. Access to Withheld Data

4.1 Access: DNCL will:

- a. subject to clause 4.2, provide CERT NZ with access to Withheld Data where CERT NZ provides the following information:
 - i. the name and position of the requestor from CERT NZ;
 - ii. the reason or reasons the Withheld Data is required by CERTNZ, at least one of which is a Permitted Reason under the Privacy Act 1993; and
- b. ensure that all access pursuant to clause 4.1a is as easy as practicable for CERT NZ.

4.2 No Access: DNCL may:

- a. suspend CERT NZ's access to Withheld Data if DNCL reasonably believes that the security and stability of the .nz ccTLD is affected [by CERT NZ's access].

4.3 Permitted Reason: Each of the following is a permitted reason for which CERT NZ may access the Withheld Data of a Registrant:

- a. investigation and remediation of incidents including phone or email contact with the registrant
- b. identification of parties subject to a vulnerability report or disclosure
- c. any other reason reached in agreement with DNCL

5. Use of information

5.1 Use of information about CERT NZ's access: DNCL is permitted to:

- a. publish this MOU on the DNCL website;
- b. use information obtained from monitoring the activities of CERT NZ under this MOU (with prior notification to CERT) in transparency reports published on the DNCL website.
- c. on a monthly basis, where applicable, notify Registrants whose Withheld Data has been accessed by CERT NZ, unless CERT NZ provides DNCL with grounds as to why notification should not be reasonable in the circumstances

5.2 Consent to use of information: CERT NZ hereby consents to the use of information by DNCL to the extent that such use is in accordance with clause 5.1 provided it protects the privacy of CERT NZ staff.

5.3 Use of Withheld Data by CERTNZ: CERTNZ agrees to:

- a. use any Withheld Data accessed in accordance with this MOU.
- b. keep the Withheld Data confidential, other than where the Withheld Data is required to be disclosed in accordance with a Permitted Reason.

6. Relationship management

6.1 Communication: Each party commits to ensuring that communication between the parties In respect of this MOU is:

- a. open;
- b. regular

6.2 Clarifications: DNCL may at any time contact CERT NZ to seek clarification or explanation relating to CERT NZ's access to Withheld Data, to which CERT NZ must provide a reasonable clarification or explanation within 7 working days.

6.3 Dispute resolution:

- a. Relationship Managers must attempt to resolve any dispute or other issue between the Parties in relation to the interpretation or performance of this MOU (the **Dispute**) at the earliest opportunity.
- b. The Parties and their representatives must act in good faith and make every effort to resolve any differences or dispute through open communication and consensus within ten working days of being informed of the Dispute from the other agency.
- c. If the Dispute remains unresolved at the end of ten working days, the Dispute must be referred in writing to the Director of the relevant operating unit of each Party for final resolution.

7. Term

- 7.1 **Commencement Date:** This MOU takes effect on the date that it is signed by all parties or, if signed by them on different days, the date the last party signs it (**Commencement Date**).
- 7.2 **Duration:** This MOU continues from the Commencement Date until terminated in accordance with clause 8.

8. Termination

- 8.1 **Termination:** This MOU may be terminated:
 - a. at any time by the mutual agreement of the parties, provided such mutual agreement is recorded in writing;
 - b. on the expiry of 30 calendar days after either party gives written notice to the other to terminate the MOU; or
 - c. immediately if either party can demonstrate that the other party has materially breached the terms of this MOU and compromised its security and/or integrity.

9. Review of MOU

- 9.1 **First review:** A review of the terms of this MOU in accordance with the requirements in clause 10.3 will be undertaken two years after the Commencement Date ("First review").
- 9.2 **Subsequent review:** After the first review, each subsequent review will occur at a time agreed by the parties, subject to a minimum of one review every three years.
- 9.3 **Review requirements:** Every review conducted under this clause 9 will:
 - a. assess how this MOU is functioning; and
 - b. determine whether there are any issues or difficulties that need to be addressed. Any amendments to this MOU will be agreed between the parties in writing.

10. General

11.1 The Parties agree that they will comply with all relevant laws, and in particularly privacy laws, in New Zealand at all times. This MOU is subject to the laws of New Zealand and the exclusive jurisdiction of the New Zealand Courts.

**Signed for and on behalf
of Domain Name
Commission Limited:**



Name:

BREAT CAREY

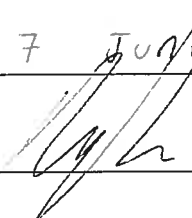
Title:

DOMAIN NAME COMMISSIONER

Date:

7 JUNE 2018

Witness:



Name:

DYLAN CONNOLLY

Title:

COMPLAINTS AND COMPLIANCE MANAGER

**Signed for and on behalf
of Ministry of Business,
Innovation &
Employment:**



Name:

ROB POPE

Title:

DIRECTOR, CERT NZ

Date:

8 JUNE 2018

Witness:

Janison Johnson

Name:



Title:

Principal Advisor, CERT NZ