IDCARE Privacy Policy

Statement of Affirmation

Identity Care Australia & New Zealand Ltd. (ABN 84 164038 966) and IDCARE Limited (4918799), referred to herein as IDCARE, affirm our commitment to the privacy laws, regulations and principles of Australia and New Zealand.

Date of Endorsement: 12 January 2022
Version Number: 4.0
Policy Number 4/2022

About this Privacy Policy

This Policy is about you, your information and what IDCARE requires about you to perform our services. We have tried to write it in a way that uses plain language. In this Policy we inform you about the personal information we collect, retain, use and share with others. It's important to us that you understand this, and that if you object, the ways you can tell us not to do this.

Business Purpose

Privacy laws mention terms like "business purpose" when it comes to collecting personal information. IDCARE's primary business purpose is providing benevolent services to community members impacted by identity theft, cybercrimes and scams. We do this in a few ways, including case management (working with individuals to respond to risks), response and protection services (how we can proactively engage others on your behalf to reduce risks relating to the misuse of your identity), and by informing organisations on how they can improve their response efforts to lessen harm to people in the future. We also do a bunch of things for the community, including presentations and other engagement activities. That's why a big part of what we do is educational – informing people and organisations about what's occurring, how to prevent, and how to respond.

What We Collect, Why and How

To perform our business purpose, IDCARE collects personally identifiable information in the following ways:

Website Usage

IDCARE's websites (**www.idcare.org** and **www.idcare.org.nz**) stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customise your browsing experience and for analytics and metrics about our visitors to our websites and social media platforms. Users may disable cookies when on these sites.

General Enquiry, Subscriber Enquiry and Get Help Web Forms

When you complete our online website forms or engage via the phone, IDCARE collects the following information:

- Your first name;
- Contact information, such as phone number and email address;
- Digital device and online attributes, such as IP address, device identifier, browser, geo-location approximation, site usage statistics, and online site pathways to IDCARE's Get Help Form;
- Other information attributes relating to the crime experienced or organisation that requires IDCARE information and assistance.

We collect this information because we need to know who to contact that needs our help, and if the line drops out, how we can reach people. We collect digital device and online attributes because it helps us understand whether the crimes people confront are targeting specific devices, applications and locations.

Marketing, email & newsletters

We use Mailchimp as our marketing platform. By subscribing to our online newsletter, Cyber Sushi, you acknowledge that your information will be transferred to Mailchimp for processing. This information consists of:

- Your first name;
- Your email address;
- Your interests.

Learn more about Mailchimp's privacy practices here.

Case Management

When calls are made using some of our calling systems, they may be recorded. We tell people when this happens and give them the opportunity to not have the call recorded. If call recording is turned off, clients will in no way be disadvantaged in using IDCARE's community services. We prefer to record calls so that we can help our Case Managers learn and develop. Senior staff and mentors review the content of case management calls, evaluate the planning advice shared, the client reactions and impacts to advice provided, and the adequacy and accuracy of the content. Case management also results in the collection of an individual's first name, email address and phone number.

Identity Verification (including the App)

Where clients seek IDCARE's assistance to respond on their behalf in the protection of their personal, account and/or credential information, clients will be required to complete a formal identity verification process ('Verification'). This process requires IDCARE to verify an individual's identity, document or related data. Verification data can include the capture of some or all of the following:

- Facial image;
- Full name;
- Date and place of birth;
- Residential address;
- Telephone number (Mobile and a Landline);
- Email address;
- Employer's name;
- Passport number and expiry date (if no Australian or New Zealand Driver Licence);
- Driver licence number, card number, and expiry date;
- Proof of Age Card (if no Australian or New Zealand Passport or Driver Licence);
- ImmiCard (if no Australian or New Zealand driver licence);
- New Zealand Certificate of Identity (if no New Zealand driver licence);
- Medicare number and Expiry Date.

We request this information so that we can verify the identity of our clients in order to act on their behalf with external responding organisations when an identity is at risk of misuse. Verification processes also rely on searching personally identifiable information, including sensitive biometric information, provided to IDCARE by individuals against third party information sources, including identity validation and verification services.

MyData.Care Client Portal

Additional protection and response services may be offered and accessible to individuals via the Client Portal (MyData.Care). These services, if requiring additional action by users, such as the completion of online forms and the application of response measures by third parties on behalf of clients, are subject to separate IDCARE or third party (if delivered by third parties) Terms & Conditions. Where such services rely on responses by third parties, such as Credit Reporting Agencies, law enforcement, financial institutions, and identity credential issuers, individual users will be subject to the third-party Terms & Conditions and Privacy Policy provisions. This will be made clear in the relevant IDCARE Terms & Conditions.

IDCARE may push alerts to changes detected in relation to an individual's personal information or account usage detected by IDCARE monitoring, profiling and protection services to individual users. The Alerting function requires users to permit IDCARE to push change notifications to a confirmed mobile phone number and/or email account. The Alerting function within the Client Portal is subject to its own Terms & Conditions, but is also consistent with the provisions of this Policy where privacy matters are concerned.

Technical Network and Device Remediation Services and "eDiscovery"

Some of the services we provide individuals and organisations involve technical network and device remediation support. In other words, if a computer or business computer network has been impacted by a cybercrime, we can help and deliver services to fix this (this is called network and device remediation). These Services are subject to separate Terms & Conditions, which are also consistent where privacy is concerned with the provisions of this Policy. Such services may collect the following attributes:

- Device security settings;
- Application security settings (such as email and social media);
- Device identification / serial numbers;
- Browser security settings and usage;
- Anti-virus and anti-malware.

We also provide a unique service identifier and may provide a Certificate of Completion. These, along with the attributes collected, may be shared with third-parties, such as an individual's financial institution, application provider, or law enforcement agency, where consent from the individual has been provided, and where:

1. IDCARE has been requested to perform these services for the individual or organisation on their behalf; and/or
2. would benefit from being informed about new malware, application or related service delivery vulnerabilities.

Sharing of this information is contingent on the individual providing consent and agreeing to the third-party's own Privacy Policy and/or relevant Terms & Conditions.

Identity Protection and Alerting Services

Third-parties may search against IDCARE's verification holdings where agreements are in place between IDCARE and the third party and such searching is conducted in a manner consistent with this Privacy Policy and the Terms & Conditions of any relevant IDCARE service the individual has provided consent to use. Specifically searching by third-parties occurs where the information retained by IDCARE may assist with the investigation by third-parties of alleged indicatable offences (Cwth,States and Territory) or in the case of New Zealand, a Category 3 offence as defined by the Criminal Procedure Act 2011 (NZ). Access is provided on the basis that the subscribing organisation is seeking to detect and/or confirm that an indictable offence may have occurred, including fraud, identity crime and cybercrime related offences.

Collection and Usage of Facial Imagery

Where IDCARE receives permission to act on behalf of an individual these processes may require IDCARE verify an individual's identity. This can include the capturing of facial imagery as part of the verification process because the very nature of most identity theft reported by clients to IDCARE involves the compromise of common identity credential information (such as driver licences and passports). Therefore, the collection of facial imagery is an important addition to the verification process and is matched against third-party templates in a manner that does not involve the retention by that third-party of the templated biometric (ie. the measure of an individual's face). We do this level of verification to reduce risks relating to criminals impersonating identity theft victims in order to access further information about their victim via IDCARE services. This information is collected only where individuals provide consent for IDCARE to act on their behalf to protect and respond to the theft of their identity information.

Verification involves requesting of third parties whether the biometric template IDCARE has collected about a person is consistent with the biometric template and the related personally identifiable information that is held by the third-party (such as name, date of birth, driver licence or passport number and address). Third parties that may receive such requests from IDCARE include Government identity credential issuers, financial institutions, telecommunications providers, and digital identity issuers and verifiers. IDCARE may deny access to specific services or request an individual to provide alternative information to assist the verification assessment if inconsistencies are found and cannot be resolved.

IDCARE monitors the online environment for evidence of identity compromise and misuse in order to place protective and responsive measures that advance the integrity of our identity system and reduce harm to impacted persons. Some information detected may include government-issued photo identification. Where such information is detected IDCARE will make an effort to notify the impacted person, response system stakeholders (such as the document issuing agency), and the organisation that may have been the source of the breached data. Notifying impacted persons may include working with relevant law enforcement agencies or relying upon the breached organisation to determine the need for notification in accordance with privacy laws. If a responsible organisation does not appear to have responded to this discovery consistent with these laws, IDCARE reserves the right to notify the relevant privacy regulator of the detection. IDCARE collects such information only for the purposes of notifying impacted individuals, document issuing organisations, and responsible entities (those who collected the information from individuals in the first instance). Should impacted persons require assistance from IDCARE to implement relevant protection and response measures, the individual may provide consent for IDCARE to share their information as needed to initiate actions as captured in this Policy under the "Identity Verification (including the App)" provisions.

Sharing of Personally Identifiable Information with Third Parties ("Sharing Provision")

IDCARE may share personally identifiable information with third parties, such as law enforcement, financial institutions, Government agencies (including identity document issuing agencies) and other identity repair response organisations in the following circumstances:

- Where the individual has consented for IDCARE to share such information; and/or
- Where it is assessed by IDCARE to be a situation where an individual has an immediate threat to their life (for example, a client is assessed to be at imminent risk of self-harm and IDCARE reports this instance to local law enforcement or another service provider to conduct a physical welfare check); and/or·
- Where IDCARE has been issued with a subpoena, warrant or related legal request from a Court or relevant law enforcement body; and/or·

- Where IDCARE believes such information may be necessary for the enforcement of the laws of any Australian State or Territory, the Commonwealth or New Zealand in relation to an alleged serious crime or offence (where the alleged offence is punishable by imprisonment for a period exceeding 12 months or in the case of New Zealand an alleged Category 3 offence as per the Ministry of Justice Guidelines).

IDCARE will take all reasonable attempts to protect personally identifiable information collected by clients. At least annually IDCARE undertakes risk assessments in relation to our collection, storage, sharing, and destruction of personal information (guided by the ISO 31000 standard on risk management).

IDCARE operates a "defence in depth" approach to the information it collects, stores and communicates, including, but not limited to:·

- All data transmitted over the internet is done over HTTPS;
- Cloudflare is used extensively to block potentially malicious requests. Rate limits on APIs are implemented at both the code level and via Cloudflare;
- Regular security scans are performed to identify code or configuration vulnerabilities;
- Firewalls are employed to limit access to services running on Microsoft Azure;
- All handling of personal information by staff is subject to specific policies and guidelines which are reviewed regularly for compliance;
- Data at rest is encrypted;
- Staff are regularly assessed and educated about cyber security threats and threat response;
- Any and all investigations performed of malicious code, sites and dark net actions are performed using external networks, interfaces and unattributable settings;

Dealing with Unsolicited Personal Information

During Case Management or at times when assisting with the remediation of a suspected data breach, IDCARE may be provided personal information it has not requested. Only if the information is determined to be relevant to the services provided by IDCARE shall such information be retained.If the information is not deemed to be relevant to the Services and business purpose of IDCARE, such information shall be permanently removed (destroyed).

Direct Marketing

Unless otherwise stated in the Terms & Conditions of a specific service, IDCARE shall not use the personal information acquired for the purposes of direct marketing. Should an individual client or organisation request of IDCARE to perform protection and response services involving a third party or if IDCARE recommends actions that involve a individual client or organisation engaging another party, then IDCARE is not responsible for any subsequent direct marketing that party may perform or have performed by others. These conditions will be subject to the third party's Terms & Conditions and any related Privacy Policy they have.

Overseas Collection & Sharing of Personally Identifiable Information

IDCARE as a trans-Tasman organisation shall at times require information be stored or backed-up on either side of the Tasman (Australia and New Zealand). This means that personally identifiable information collected from or on Australians and New Zealanders in the course of delivering our business purpose may be stored in Australia or New Zealand. IDCARE individual client and organisational subscriber services may also require that such information, as per this privacy policy, be shared with third parties that operate on either side of the Tasman (Australia and New Zealand) in order to achieve our business purpose.

Retention of Personally Identifiable Information

IDCARE only retains personal information for as long as is it is required for the purposes protecting and responding to risks relating to such information. Individuals may request at any time that information IDCARE has collected about them is corrected or permanently deleted (see next section). Case information is anonymised (de-identified) and retained for statistical analysis, such as time series analysis. This information is backed-up periodically and stored in a non-networked or Internet-enabled environment.

Access, Deletion, Correction, Feedback and Complaints

If you wish to access information collected by IDCARE relating to your circumstances, seek correction of information held about these circumstances, have your personally identifiable information deleted, or make a complaint about how we have dealt with your matter, please send a written request, including your case number, to:

- Privacy Officer IDCARE PO Box 412 Caloundra QLD Australia 4551.

Requests may also be emailed using our feedback form, with the words "Attn: Privacy Officer" in the subject line accessed at www.idcare.org or by emailing direct **feedback@idcare.org**.

To assist IDCARE in responding to your request we would be grateful if you could provide your IDCARE Case Number (if relevant) and the estimated date of your engagement with IDCARE.

IDCARE will inform you via your preferred contact channel of the result of your request within 30 days.

If we have not resolved your issue to your satisfaction and within our responsibilities, complaints about IDCARE and the handling of your personal information may be made to the relevant Privacy Commissioners in Australia and New Zealand: (**www.oaic.gov.au** ph: 1300 363 992 and **www.privacy.org.nz** ph: 0800 803 909). These organisations have extensive materials about your privacy rights and response considerations.