PUBLIC

Privacy Policy

Version 1.2 - December 2021

(Published on 3 December 2021)

Definitions:
- "we", "us" and "our" refer to "Data Zoo" [Data Zoo Pty Ltd (ACN 146 612 553); Data Zoo Limited (CN3287828); Data Zoo Pte Ltd (UEN201718678C); Data Zoo LLC (001051597); and IDUX Pty Ltd (ACN 650 643 824)].
- "you" or "user" means you and includes everyone who visits and interacts with Data Zoo including existing and prospective, customers, data subjects, employees, contractors, and interns etc.
- "Personal information" refers to information or data (linked or unlinked) that identifies an individual (directly or indirectly).

1 INTRODUCTION

1.1 Privacy at Data Zoo

We are a private sector identity verification service provider and a Gateway Service Provider (GSP) for the Australia Document Verification Service (DVS). We understand the universal importance of protecting your privacy, which we demonstrate through our commitment to compliance with privacy and data protection legislation and standards, wherever we operate. From our established APAC presence in Australia, New Zealand, and Singapore, and our US presence, we cross multiple jurisdictions around the globe, each with different protection measures that collectively aim to protect your privacy, whenever and wherever you or your personal information interacts with us.

At Data Zoo, we take a global approach to privacy, strongly emphasising compliance with global and regional data protection and privacy, standards, laws, and regulations. This includes compliance with the Australian Privacy Principles (*The Privacy Act 1988* and related legislation), the New Zealand Privacy Principles (*The Privacy Act 2020* and related legislation), the Singaporean *Personal Data Protection Act 2012,* The European Economic Area (EEA) *General Data Protection Regulation (GDPR)*; *Chinese Personal Information Protection Law 2021 (PIPL)*; and US data protection and privacy compliance against the Californian Consumer Protection Act (CCPA) and the Californian Privacy Rights Act of 2020 (CPRA).

This Privacy Policy sets out how we collect, use, share, store and safeguard your information when you interact with us by visiting our website or us in person, for marketing and sales purposes, or through our Verification. Our Policy extends to include your right to control your privacy, which includes having access, making corrections or deletions or objecting to the processing of your personal information. As an ethical and responsible Identity Verification Service provider, it is important for you to appreciate that once we receive your personal information, we apply the principle of data minimisation in our collection, storage, and use (see Retention, Disposal or Destruction of Personal Information) and maintain control and responsibility of what we hold for you. We do not sell your personal information to anyone. Where we share your personal information we will do so legitimately based on your consent or other lawful basis as outlined in this policy.

1.2 The Privacy and Data Protection Officer

If you have any queries regarding the content and subject matter of this policy; wish to request access, correction or deletion of your personal information; wish to withdraw your consent; wish to object to us processing your personal information, or require further assurance of how we securely use your personal information, please contact our Privacy and Data Protection Officer here, through our **Data Access Request webform** or by using the details below and we will do our best to deal with your complaint or query as soon as possible.

The Privacy and Data Protection Officer
Data Zoo Pty Ltd
Bay 8, 1-3 Middlemiss Street
North Sydney NSW 2060
AUSTRALIA
Telephone: +61 2 8014 4807
e-mail: privacy@datazoo.com

Verifiable Requests
When contacting us for access/disclosure, correction, or deletion requests to personal information you may need to first verify your identity. To do this, we may ask you for additional information, which may include asking you to confirm other Personal Information you have provided to us. We reserve the right to deny any requests for which identity cannot be reasonably verified. If you have authorised another person to make a request on your behalf, that person must also provide verification of their identity, in addition to your written authorisation accompanying a copy of your power of attorney allowing that person to make such a request on your behalf. We reserve the right to deny any request by an authorised agent if we are not reasonably able to confirm proper authorisation or verification of that agent.

Hyperlinks are provided to allow you to quickly move around this Privacy Policy and access external resources. You may also download a PDF copy of our Privacy Policy if you wish. If you require a printed copy of this Privacy Policy (at no charge) or require it to be available in another language or alternative format for accessibility (including users with disabilities), please contact our Privacy and Data Protection Officer.

2 VISITORS

You are a Visitor if you visit our websites or otherwise contact us.

2.1 Personal information we collect:

We collect personal information from Visitors:

(a) when you visit our website: through the use of Website analysis and Cookies; and when the visitor uses the "contact us", "book a demo", or online query form; or
(b) when you contact us through a marketing campaign, register and/or attend any of our events (e.g podcasts, and webinars), at conferences or marketing events, or connect/contact us via professional networking platforms such as LinkedIn; or
(c) when you email, telephone, or meet us in person.

We collect and securely store the **Visitor's Name**, the **Name of their Organisation**, **Email Address**, any **Email Correspondence**, **Telephone Number** and **IP Address**. We may also collect **Other Personal Information that the Visitor voluntarily submits** to us (see Unsolicited Personal Information).

Website Analysis and Cookies

Our web server collects information on the usage patterns of people visiting our website for the legitimate purpose to assess, develop and improve your usability of our services. The information is collected each time a user visits our website and consists of the date and time of visits; the number of users who visit the website; and the traffic patterns and pages viewed. We do not seek to identify your browsing activities. Our websites in the most part use only session-based cookies that collect and process the personal information of Customers and demonstration users for the functional purpose to keep them logged in during a session. We may also use cookies from third parties that include marketing companies we have engaged. Our Cookies (including preferences, and consents) are managed by a third-party provider. To find out what cookies we currently collect, how and why, see our Cookie Policy.

2.2 Why we collect personal information from Visitors

We will only ever use your personal information in accordance with the consent and purpose you have provided (Consent Management Policy available upon request) and in conformance with relevant and applicable Privacy Laws. We collect and process your information predominantly to respond to or facilitate your queries or requests. We may also collect your personal information and process it within our clients' specific legitimate interests[1], which may include the operation of our/their business, internal analytics, and to improve our website. Subject to your consent we may also provide you (via email or other medium) with updates on our services and marketing content. We do not share any Visitor personal information with third-party providers except where that Visitor is a Customer.

Right to Anonymity
Where possible, our systems will allow you to communicate with us on an anonymous basis or by using a pseudonym. We do not seek to identify you when you access our websites or otherwise contact us. The provision of personal information through the website or other means of communication is, therefore, entirely voluntary. Please note, however, that it may be difficult for us to fully respond to your query or enquiry without certain contact details. Communication with Customers requiring assistance in relation to specific accounts or the information which they have provided us for the purposes of establishing or using the account, may not be practically possible without further details being first provided by the Customer.

3 CUSTOMERS

Customers are organisations (through their authorised representatives) to who we provide identity verification services under contract (to enable Customers to verify individual Verification/Data Subjects) against a selection of data sources.

[1] Article 6(f), GDPR allows us to process people's personal data for the data controllers specific legitimate purpose unless their interests, rights and freedoms override that purpose

3.1 Why we collect personal information from Customers

We collect information about you, from the initial pre-contracting introduction of prospects to onboarding you as a Customer. This includes **Identifiers and Customer Record Information**,[2] your **Company Name; Company Registration Details**, the **Name of your Representative(s), Contact Telephone Number(s), Email Address(es) and Correspondence,** and **IP Addresses**. We may conduct additional enquiries and collect further information depending on the services which you request to acquire. This includes information obtained for due diligence purposes from publicly available sources such as, a Company Registry, Privacy Registry, Taxation Number Registry, your LinkedIn presence, and your website. **IP addresses** are collected as part of our security and authentication measures when providing you access to our services (see also Information Security Policy) .

3.2 The lawful basis for processing your personal information

With the exception of marketing purposes (for which we would seek consent), we collect and process your personal information on the lawful basis of 'legitimate interest', in that it is necessary in order to successfully enter into and perform a contract with you while complying with the relevant legal obligations. This legal basis for: communicating with you; conducting due diligence checks on you; securely providing identity verification services to you; providing information to specific organisations with whom you have authorised us to communicate; managing the Customer relationship and providing support to you.

3.3 Sharing or disclosing of your personal information

We do not share any of your personal information to any third-party service providers unless you are a Customer. We share Customer personal information with our third-party service providers, which includes the Customer Records Management Software, our External Accounts Management team, and Legal Counsel. All information shared is strictly limited to the legitimate purpose for which it is required (e.g. For the successful performance and management of the contract we have with you) and is subject to our information security controls (set out in our Information Security Policy), data processing agreements, and relevant privacy laws. A full list of the categories of our third-party service providers is available upon request.

We will otherwise only disclose your personal information in the following circumstances:

- where you have given your consent (within the scope of the specified purpose);
- where we are required to do so by law or enforceable request by a regulatory body;
- where it is necessary for the purpose of, or in connection with legal proceedings or in order to exercise or defend legal rights; and
- if we sell our company, merge with another company, or go into administration (we will treat all personal information in conformance with the relevant Privacy laws and obligations)

4 VERIFICATION SUBJECTS AND THEIR PRIVACY RIGHTS

4.1 Verification Subjects

A Verification or Data Subject is an individual who our Customers request to identify using our identity verification services.

We act as a Data Processer to process the personal information of Verification Subjects, on behalf of and according to the instructions provided by our Customers who act as Data Controllers. We have no interest in and exert no rights, over any personal information of any Verification Subjects that we process on behalf of our Customers. Upon completion of processing for a Customer we de-identify any personal information of a Verification subject immediately. Any personal information of a Verification Subject that is still to be fully processed or reprocessing is considered 'work-in-progress', we hold on behalf of the Customer. If you require further information on how your information is used, please contact the Customer organisation.

4.2 Verification Subject Personal Information Processing

Verification Subject personal information is processed against personal information either held and processed by Matching services provided by our suppliers, OR collected, compiled, maintained, and held by us in processes separate to those used by our Customers. The categories of personal information we handle in the course of verification process may include: **Identifiers** (**Name**, Address, Date of Birth, Government Identifiers); **Customer**

[2] As per CCPA 1798.140 (o)(1) within the definition and categories of personal information.

Records Information (Name, Address, Telephone Number, Passport Number, and State Identification Number); and **Biometric Information** (Face Matching and Voice Matching).[3]

4.2.1 Suppliers of Matching Services

Our suppliers of personal information matching services undergo a rigorous due diligence process to ensure that their information has been lawfully, collected, compiled, and made available for the purpose of identity verification. The actual data matching process is undertaken by the supplier using a secure Application Programming Interface (API) where we, on behalf of our Customer, will submit a Verification Subject's personal information to a supplier to receive a <Matched>, <Not Matched> or other response that we will return to the Customer. The Customer will interpret and incorporate responses according to their own matching rules and advise a result to the Verification Subject.

We do not extract, retain, make a record of, nor modify any personal information held by any supplier. Suppliers are subject to Privacy laws, regulations, and standards, in addition to their contractual obligations to us, which we regularly audit to ensure the integrity of our data sources.

4.2.2 Data Zoo Data (collected, compiled, maintained, and held by us)

We also collect, compile and hold personal information sourced from either, or a combination of: 1) the public domain such as published directories, lists and other publicly available sources, and/or 2) consented personal information sourced directly from individuals who have given their consent to their personal information being collected and compiled by us. In compliance with the *Privacy Act 1988 (Cth)* and/or *Privacy Act 2020 (NZ),* we regularly update and re-compile this data to maintain accuracy and reliability.

5 INTERNATIONAL DATA TRANSFERS

We are an Australian Company with a global presence. As such we have our servers securely and strategically located in Australia, New Zealand, Singapore, and Germany. We principally collect and store APAC personal information in Australia, New Zealand, or Singapore in compliance with the relevant privacy laws. EU personal data is treated in compliance with the GDPR, received and processed within the EU, and backed up /fail-safe to New Zealand (NZ is recognised by the EC as having adequate legislative protection of personal data). Where EU Personal Data is transferred from the EEA (or a country with EC recognised adequate legislative protection) to a non-EEA third-country that does not have adequate protection, we will ensure that adequate measures are in place to protect the personal data being transferred. Our Information Security Policy and standards together with the stringent level of due diligence conducted when contracting allows us to confidently satisfy the GDPR requirements to transfer personal data to third countries whose privacy laws may not have fully matured or have otherwise not considered to hold an EC adequacy protection decision. For further information on how we protect your personal information around the world please contact our Privacy and Data Protection Officer.

6 ACCESS TO PERSONAL INFORMATION

6.1 Process for accessing personal information

If you would like to request access to your personal information which we hold about you (or a person whom you are authorised to represent), to exercise your rights to access, correct/amend, delete, to object to the processing of, or to withdraw your consent to the use of or disclosure/sharing of your personal information outlined in this Privacy Policy, please submit a verifiable request to the Privacy and Data Protection Officer or complete our Data Access Request webform to initiate the request. We do not sell your personal information, nor provide any financial incentives tied to the collection or deletion of your personal information.

Your request should specify the format in which you wish to be provided the personal information (for example, in person, by email, or printed copy). This application is free of charge. However, we may make a reasonable charge for providing access to you. If we wish to charge you to access the personal information, we will notify you of this charge prior to giving you access to the personal information.

When a decision is made, access will be provided either free of charge or subject to a charge as follows:

a) No charge for access – we will notify you of the decision and (where you have requested that the information be provided to you by email or printed copy delivered or sent to you), we will also provide the personal information to you at the same time (except as set out below)

[3] CCPA 1798.140 (o)(1) defines personal information and outlines categories of personal information.

b) Access charge – we will notify you of its decision and the proposed charge for giving you access and the payment terms and method of payment. If you wish to discuss the proposed charge with us, you should contact our representative nominated in the notice. Once you have paid the access charge, we will provide the personal information to you (except as set out below).

Where the format of access is different from the format requested – If we conclude, acting reasonably, that it is not possible or practicable for us to provide your personal information in the format you have requested (for example because of the volume or nature of the personal information or your needs), we will contact you to agree a format in which we can give you access to the personal information. If you have requested access by in person or by telephone, we will contact you to arrange the time and place at which you may access the personal information.

6.2 Refusal of a request for access to personal information

In limited circumstances, access to your personal information may be refused in accordance with the Australian Privacy Principles. Where permitted we will promptly notify you of the reasons and consult with you to identify any alternative means of providing you access to your personal information (e.g. reducing the scope of request, or giving you access through an agreed intermediary). In those circumstances, you will not be charged for making a request to access your personal information, but you may be charged for the reasonable time and expense incurred in compiling information in response to your request.

6.3 Quality of personal information and right to correction or deletion of personal information

We make reasonable effort to ensure that the personal information that we collect is accurate, up-to-date, complete, and relevant, both at the time of initial collection, and throughout the period that we store it. If you consider that any personal information that we hold about you is inaccurate, out-of-date, incomplete, irrelevant, or misleading and you wish to have the information corrected or deleted, you should please submit a verifiable request to the Privacy and Data Protection Officer. This application is free of charge.

*If we **accept** your request:* we will take such steps as are reasonable in the circumstances to ensure that we correct or delete the information, having regard to the reasons for which the information is held.

*If we **decline** your request:* we will send you a written notice explaining the reasons for the refusal (except where it is unreasonable to provide an explanation), the complaint mechanism which you may follow, and other matters which we are required to include. Additionally, you may request that we add or associate a statement to the personal information stating that it is inaccurate, out-of-date, incomplete, irrelevant, or misleading. We will take reasonable steps (given the circumstances) to associate the statement in such a way to make it apparent to users of the information.

6.4 Timeframes and record keeping of your requests[4]

We acknowledge and confirm receipt of all requests by you to exercise your right to know/access, correct/rectify or erase/delete your personal information within ten (10) business days of receiving the request and will provide information as to how we will process the requests. We aim to then provide a full response to these requests within 45 calendar days of the date your request was received. If we cannot respond within this period, we will promptly notify you of the delay, the reasons for the delay, and the date by which we will provide a response (no later than 90 calendar days from the date your request was received). We will keep all records pertaining to the requests for a period of at least 24 months.

Retention of records exception

Within your rights, you may access all your personal information held by us to request correction/amendment or deletion except where we or an organisation to which we have provided your personal information as part of our verification services is required to retain that information as part of their legislative or compliance obligations. This includes for the legitimate purpose of records retention for compliance with Anti-Money Laundering, Anti-Corruption legislation or other laws or regulations.

[4] CCPA 999.317 timeframes and record keeping and CPRA 1798.130

7 SPECIFIC RIGHTS UNDER THE EEA/UK GDPR

Under the GDPR, you will have the following rights in relation to how we process the personal information we hold about you (your personal data):

(a) **Right to request access** – by contacting us via our **Data Access Request webform** or our Privacy and Data Protection Officer you may obtain confirmation from us as to whether or not your personal data is being processed by us, and where that is the case, request access to personal information we hold about you following our process for accessing personal information.

(b) **Right to rectification** – you have the right to obtain rectification of inaccurate personal data we hold concerning you.

(c) **Right to erasure** – you have the right to obtain the erasure of personal information we hold about you without undue delay in certain circumstances.

(d) **Right to restriction of processing or to object to processing** – you may require us to restrict the processing we carry out on personal information we hold about you in certain circumstances or to object to us processing your personal data.

(e) **Right to data portability** – you have the right to receive a copy of personal information we hold about you in a structured, commonly used, and machine-readable format.

(f) **Right to withdraw consent** – where you have provided your consent to us to process personal information we hold about you in a certain way, you have the right to withdraw your consent at any time. To learn more see our Consent Management Policy (available upon request) or contact our Privacy and Data Protection Officer.

(g) **Right to lodge a complaint** – you may lodge a complaint with the relevant data protection or supervisory authority in the EU. A list of the EU data protection authorities can be found at Data Protection Authorities - European Commission (europa.eu).

We will not charge you a fee if you wish to exercise any of your rights, except where we are permitted to do so by the EEA/UK GDPR. To exercise the above rights or to learn more about your rights under the EEA/UK GDPR, please complete our **Data Access Request webform** or contact our Privacy and Data Protection Officer

8 SPECIFIC RIGHTS UNDER THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018 (CCPA)

You may also have certain specific privacy rights against us afforded to you by Californian Privacy legislation, which includes:

a) **Right to know:** which entails your right to disclosure of what / how the business collects, uses, discloses, sells or shares your Personal Data (to the extent permitted by applicable law).

b) **Right to request deletion** of your personal information collected or maintained by the business.

c) **Right to Opt-out of the sale or sharing of your personal information to third parties**, where the business sells or shares personal data with contractors, service providers and other third-parties.

d) **Right to not receive discriminatory treatment** by the business for the exercise of your privacy rights conferred by the Californian Privacy legislation.

e) **Right to designate an authorised agent** to make a verifiable request under the CCPA on your behalf to us with a copy of your power-of-attorney document granting that right.

To exercise the above rights or to learn more about your rights under the CCPA, please complete our **Data Access Request webform** or contact our Privacy and Data Protection Officer

9 ADDITIONAL NOTES

9.1 Unsolicited Personal Information

We sometimes receive unsolicited personal information. This occurs where personal information is received by us where we have not taken any active steps to collect that information. In such cases, we will, review the unsolicited personal information within a reasonable amount of time to determine if it is reasonably necessary for our legitimate business purpose, including our contractual obligations with you and our obligations under law. If it is, we will handle the information in the same way as we handle the information we would actively collect from a person. If we do not need the information, we will destroy the information or de-identify it in line with our ongoing

application of the principle of data minimisation (see Retention, Disposal or Destruction of Personal Information for further detail).

9.2 Retention, Disposal or Destruction of Personal Information

We strongly adhere to the principle of data minimization in the collection, use, storage, and disposal/destruction of data. Personal data must be adequate, relevant, and limited to what is necessary to the purposes for which it is processed. We delete all personal information on conclusion of the Visitors or Customer's arrangements with us except where we are legally required to keep the personal information for a longer period. We then delete that information as soon as that period has expired/lapsed. Our Data Security and Storage arrangements and measures are addressed in our thorough Information Security Policy.

9.3 Disclosure of Personal information

We will not disclose information that identifies an individual, or enables an individual to be identified except as:

(a) specified in this Privacy Policy;
(b) authorised by the individual;
(c) as required under applicable laws; or
(d) as directed by courts, tribunals or other bodies having authority over us.

We will only disclose government issued document identifiers (such as National ID, Passport, or Driver Licence numbers) or identifiers issued by another entity or person, as part of an identification verification request on behalf of an individual who has provided their consent (Consent Management Policy available upon request).

9.4 Children

Our websites and activities are not directed at children. We do not knowingly collect, use, share or sell Personal Information from children under the age of 16 in the course of our business practices. As part our Digi-Tech Futures initiative at Woorabinda State School in Central Queensland, Australia, we will occasionally make or share (directly from the school) an awareness post on our LinkedIn business page and our website. These posts may include photographs of the children and the work the children have produced during the program in the classroom environment. All personal information and postings are received from the school with consent and approval of the school. All necessary consents and approvals are obtained from the parents of all the children photographed. Any consent change requests should be directed to the Privacy and Data Protection Officer.

10 Changes to this Privacy Policy

We reserve the right to change this Privacy Policy as required to maintain compliance with all applicable laws, to comply with changes in technology or to reflect changes in our business. If we consider it necessary, we will consult with the Office of the Australian Information Commissioner (OAIC), the New Zealand Privacy Commissioner, the Singaporean Personal Data Protection Commission, or other appropriate government representatives and other representative groups before implementing any change or review to this Privacy Policy.

When this Privacy Policy is updated, the updated policy will be published on our websites at: www.datazoo.com and www.idux.com.au. The most current version of our Privacy Policy will always be the version published on our website and any previously downloaded or printed versions should not be relied upon. We will identify each version, include a publication date, and ensure that superseded versions continue to be available upon request to our Privacy and Data Protection Officer.

11 Breach Of Policy

We will take all necessary measures to remedy any breach of this policy including the use of our disciplinary or contractual processes where appropriate.

12 Records

Records retained in support of this policy are listed in the **Document Control and Improvement Register**.

Change History

Version	Date	Record of Changes	Created By	Approved By
1.1	28.11.2021	Initial Issue of New comprehensive Privacy Policy (replaces and formalises all previous privacy policies). Updated for GDPR and CCPA	P-JL / FK	MA
1.2	03.12.2021	Updated Privacy Policy incorporating feedback from CCPA Audit	FK	MA