Vygo Privacy Policy

1. Overview

Vygo Pty Ltd ACN 609 658 531 (collectively, Vygo, **we**, **us**, **our**) is committed to protecting your privacy. Vygo partners with educational institutions (**Institution Partners**) to deliver student support services including student experience, student wellbeing, student mentoring, peer community, career and alumni management services and access to digital wellbeing resources and learning materials, and related or additional services made available from time to time (**Services**). We have prepared this Privacy Policy to describe to you (whether you are an End User or Partner as defined under our Related Terms (defined below) our practices regarding personal information we collect from users of our Services, including the Vygo mobile app (**App**) and websites (collectively, **Platform**), and all other services provided by Vygo (**Services**).

Our processing of Personal Data is always carried out in line with the applicable law, which may include the Australian Privacy Principles contained in the *Privacy Act 1998* (Cth) (**Privacy Act**), the UK General Data Protection Regulation (**UK GDPR**), the General Data Protection Regulation (EU) 2016/679 (**EU GDPR**), the Data Protection Act 2018 (**DPA**) the California Consumer Privacy Act (**CCPA**), and the Family Educational Rights and Privacy Act (**FERPA**) or other geographically-specific data protection regulations applicable to Vygo.

This Privacy Policy also reflects to the applicable obligations of Vygo under the EU Data Act (Regulation (EU) 2023/2854), particularly Articles 3 to 6 on data access and portability, to enable secure access and sharing of user data, also known as access by design, while ensuring robust safeguards and interoperability.

We have implemented numerous technical and organisational measures to ensure the protection of Personal Data processed through the Services. However, no transmission or storage system can be guaranteed to be completely secure, and we do not guarantee that unauthorised access will never occur.

This Privacy Policy should be read in conjunction with our Terms of Service (viewable here), incorporating our Acceptable Usage Policy (viewable here) and any additional terms or policies for End Users; and for Institution Partners: our Platform Partner Terms (viewable here) and any additional ancillary agreements including Data Processing Addenda or Data Access and Sharing Addenda; that we may be party to, that support the provision of services through the Platform to both Institution Partners and the End Users (collectively, **Related Terms**).

2. Collection Statement

We may collect personal information about you in order to provide you with the Services through this Platform and for purposes otherwise set out in this Privacy Policy.

The information you provide will be collected by or on our behalf of us and may be disclosed to third parties that help us deliver our Services (including information technology suppliers, communication suppliers and our business partners), to Institution Partners, or as required by

law and as described in section 7 below. If you do not provide this information, we may not be able to provide all of the Services and functionality of the Platform to you. Please contact your educational institution to find out about alternatives to Vygo services available to you.

Our Privacy Policy explains:

(a) how we store and use, and how you may access and correct your personal information;

(b) how you can lodge a complaint regarding the handling of your personal information; and

(c) how we will handle any complaint.

If you would like any further information about our privacy policies or practices, please contact us.

By providing your personal information to us, you agree to the collection, processing, use, storage and disclosure of that information as described in the Privacy Policy and this collection notice.

We may disclose your personal information to recipients that are located outside of your region, including to third parties as outlined in this Privacy Policy.

3. Explicit warnings regarding privacy and confidentiality

We do not request, collect and store medical data or health records in any way. We strictly disclaim any liability for the unsolicited collection or storage of such information. PLEASE DO NOT USE PROFILE, CHAT, OR VIDEO FEATURES TO INPUT ANY MEDICAL OR HEALTH DATA INTO YOUR PROFILE.

Please be aware that any data or content you share with other users via the Platform is not confidential. Under our agreements with Institution Partners, your communications—including chat logs and video sessions—may be recorded and accessed by us or your educational institution.

We process this information to monitor for compliance with our Related Terms and your institution's policies or codes of conduct. This allows us to identify and address risky or harmful behaviour, and to enable us or your Institution Partner to intervene and provide assistance where necessary. As such, all content should remain professional, respectful, and appropriate for an educational environment, and you should have no expectation of privacy regarding your use of the Platform.

4. User Consent

Where we rely on your consent as the lawful basis to process your data under the GDPR or other applicable privacy law, we will always ask for you to positively affirm your acceptance. By clicking to accept this Privacy Policy you acknowledge and agree to be bound by this Privacy Policy.

We note that all contact or other data forms where consent is required to be given by you include no pre-checked checkboxes so that you are able to freely, affirmatively opt-in. We will also provide you with notice on the Services specifically detailing what it is that you are consenting to in clear and plain language as well ensuring that each matter which requires consent is clearly distinguishable.

For all areas of the Services where consent is given, it is just as easily able to be withdrawn from Vygo through the appropriate account settings on the Services. Vygo is not responsible for any information your Institution Partner has stored outside of Vygo, please contact your Institution Partner for removal of any such information.

If you believe that consent has not been given freely or in breach of the terms of this Privacy Policy, please contact us or your Institution Partner.

5. What personal data we collect

In this privacy policy "**Personal Information**" or "**Personal Data**" means any information that allows someone to identify you, including, for example, your name, address, telephone number, e-mail address, as well as any other non-public information about you that is associated with or linked to any of the foregoing data, and any online identifiers (such as IP address, device ID, or cookies) where these identify or could reasonably identify you, to the extent that this information may identify, relate to, describe, are capable of being associated with, or could be reasonably linked, directly or indirectly, with you or as otherwise defined under applicable law including the Privacy Act 1988 (Cth), the UK GDPR, the EU GDPR, the Data Protection Act 2018 (UK DPA), and the CCPA.

We may collect, use, store and transfer different kinds of Personal Information about you which we have grouped together as follows:

- ***'Identity Data'*** includes your name, username, profile photo, educational institution, student number, sex, race or ethnic origin, date of birth, pronouns, racial or ethnic origin, gender identity***,*** your username or similar identifier, password;
- ***'Contact Data'*** includes residential address, email address and telephone numbers;
- ***'Course Data'***, program and course details, student application records, student progress records, student enrolment status, student leave status, course instructor details; grade point average, study details, scholarship or fee paying status
- ***'Services Data'*** includes information and sensitive personal information about you, including invitations to use the Services; details about your use of the Services, your connections history and usage, your video or chat logs and other information you share

with other users, surveys that you have responded to; your interests, preferences and feedback;

- ***'Career Data'*** means career interests, previous employment information and academic performance information you submit to utilise career services;
- ***'Technical Data'*** includes internet protocol (IP) address, your login data for our Services, statistics on page views and sessions, acquisition sources, search queries and/or browsing behaviour, browser session data, webpage from which you came, webpage(s) or content you accessed, navigational and log data, information about your access and use of our Platform and services, including through the use of internet cookies, clickstream data, time zone settings and geolocation, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access the Platform, data contained with documents or files that you otherwise share with us, and other meta data. With your consent we may also collect information about your precise location using methods including GPS, wireless networks, cell towers, Wi-Fi access points and other sensors.;
- ***'Marketing Data'*** includes your preferences in receiving communications from us and our third parties and your Institution Partner, web analytics, marketing engagement data.

We will only collect personal information to provide and improve our Services, fulfil our contractual obligations, comply with legal requirements, and support our Institution Partners, or if it is reasonably necessary for one or more of our functions or activities and where we have a valid lawful basis under applicable data protection laws (for example, consent, performance of a contract, compliance with a legal obligation, or legitimate interests that are not overridden by your rights and freedoms).

Vygo recognises that certain categories of Personal Data (including data revealing racial or ethnic origin, gender identity, or data concerning minors) may constitute "**special category data**" or "**sensitive information**" under applicable laws, and applies heightened protection and consent requirements for such data. Vygo processes Personal Data both as a "data controller" (for account administration, platform operations and support) and as a "data processor" on behalf of our Institution Partners, who act as data controllers under applicable law and are solely responsible for determining the lawful basis and purpose for processing.

We do not collect, capture, or process biometric identifiers or biometric information (fingerprints, voiceprints, facial recognition data, retina/iris scans) as defined under US state biometric privacy laws. Profile photos are stored as standard image files and are not used for biometric identification.

When Institution Partners sign up for the Platform, they may send us certain personal data about their students so that Vygo may pre-populate accounts to provide the Services. Where the Family Educational Rights and Privacy Act (**FERPA**) applies to data shared by Institution Partners, it is processed in compliance with the statute

3 How we collect your Personal Data

We generally collect Personal Information:

- from you directly when you provide your details to us via our Platform;

- when you interact with us via our Platform; or
- from your Institution **Institution Partner**).

We generally collect sensitive information or special category data from you directly or otherwise with your consent, before or at the time of collection, unless an exception applies under applicable law — such as in an emergency, there is a serious threat to life. If we hold sensitive information about you, we will only disclose or use that information with your consent or if another exception applies under applicable laws.

6. How we use your Personal Data

6.1 Use of personal information

We collect, hold, use, and disclose Personal Information for purposes set out in the table below. The table also specifies the lawful basis we rely on when we process your Personal Information, which will be applicable only to UK and EEU Data Subjects:

Purpose for Collection	Type of Personal Information	Lawful Basis for Processing Under the GDPR
• To provide and deliver our Platform and Services, including facilitating real time communication between users to administer your Account and; to enhance our service offerings through usage and satisfaction surveys; and to verify the accuracy and completeness of information. • To enrich your User Content by appending metadata—such as hashtags for keyword association, geotags for location data, comments, or other identifiers—to optimize content discoverability and search functionality.	• Identity Data • Contact Data • Course Data • Services Data • Profile Data • Career Data • Marketing Data	• Performance of a contract with you: To deliver the Platform and Services, manage your Account, and facilitate user communications. • Your consent: Regarding your voluntary submission of User Content, Contact Data, and optional metadata (e.g., geotags) and to access your device's camera and microphone • Legitimate interests: To operate and improve our services, conduct surveys, and enhance content discoverability via metadata. • To comply with a legal obligation: To meet statutory duties, obligations to Institution Partners, and lawful disclosure requests.
• To enhance communication and user experience	• Identity Data • Contact Data	• Legitimate Interests: To improve the efficacy of

Purpose for Collection	Type of Personal Information	Lawful Basis for Processing Under the GDPR
through automated tools, including AI-driven sentiment analysis, automated message translation, and smart matching algorithms that connect Mentees with the most suitable Mentors.	• Course Data • Services Data • Profile Data • Career Data	matches and remove language barriers.
• To provide your Institution with detailed insights and reports regarding your engagement with the Services. This includes sharing data on session attendance, satisfaction feedback, and usage patterns to assist the Institution in monitoring student well-being, retention, and academic success.	• Identity Data • Contact Data • Course Data • Services Data • Profile Data • Career Data • Marketing Data	• Performance of a Contract: (If the contract is directly with the Institution Partner to provide these insights). • Legitimate Interests: To fulfill our value proposition to Institution Partners by demonstrating service impact. • Vital Interests: (Often relied upon by Universities when monitoring for "at-risk" students).
• To monitor User Content and communications for compliance with our Acceptable Use Policy; to detect bullying, harassment, or self-harm indicators; and to take appropriate action to protect the safety and well-being of our community.	•	• Legitimate Interests: To maintain a safe and respectful environment. • Vital Interests: To protect a user in the event of an emergency (e.g., self-harm risk detected).
• To comply with our legal and contractual obligations under applicable privacy, consumer protection, and education laws, including the GDPR; to enforce our	• Identity Data • Contact Data • Course Data • Services Data • Technical Data	• To comply with a legal obligation (including satisfying requirements under privacy, consumer protection, and education laws, and maintaining written records of

Purpose for Collection	Type of Personal Information	Lawful Basis for Processing Under the GDPR
Related Terms and policies; or where necessary for the establishment, exercise, or defence of legal claims. This includes processing personal data to detect, investigate, and prevent unlawful acts or policy breaches, and to safeguard the rights, property, and vital interests of data subjects or others.	• Marketing Data	disclosures to enforcement bodies) • Performance of a contract with you (to fulfill contractual commitments and enable the administration of our services) • Legitimate interests: to enforce our Related Terms and policies; to detect, investigate, and prevent potentially unlawful acts or policy breaches; and to protect the rights, property, and safety of our users and third parties • Vital interests: to protect the physical safety or life of an individual (where applicable)
• To administer your account and manage contractual relationships, including the negotiation, execution, and performance of agreements with you or your institution; to process payments and fulfill our obligations to Institution Partners; to facilitate internal record-keeping and administration; and to resolve disputes or identify, test, and rectify technical or service-related issues.	• Identity Data • Contact Data • Services Data • Technical Data • Marketing Data	• Performance of a contract with you: To negotiate, execute, and manage our agreement with you or your institution; to process payments; and to fulfill our contractual obligations to Institution Partners • To comply with a legal obligation - To satisfy statutory requirements regarding financial reporting, tax compliance, and consumer protection laws. • Legitimate interests: To facilitate effective internal administration and record-keeping; to recover outstanding debts; to resolve disputes; to manage and enforce our terms of business; and to identify, test, and

Purpose for Collection	Type of Personal Information	Lawful Basis for Processing Under the GDPR
		resolve technical or service-related problems.
• To contact and communicate with you (subject to applicable laws and your consent, where required), including providing technical support, responding to technical enquiries, recording your preferences, and keeping you informed about changes, updates, events, and other relevant matters	• Identity Data • Technical Data • Marketing Data	• Performance of a contract with you • Legitimate interests: to ensure we provide the best student experience (for example, to communicate transactional messages), maintain engagement and improve our services
• To customize and localize our Services based on your location, and to ensure that in-person meetings occur in locations that adhere to our safety requirements and policies.	• Identity Data • Technical Data	• Your consent: To access and collect precise location data via your device settings. • Legitimate interests: To ensure user safety by verifying that meetings occur in locations that comply with our policies, and to detect and prevent fraudulent location spoofing.
• To administer your account, subscription, and access rights; to facilitate login; and to personalize your experience on our Platform. This includes customizing the Services and retaining your information to streamline future interactions and eliminate the need for repeated data entry.	• Identity Data • Technical Data • Marketing Data	• Performance of a contract with you: To manage your subscription, facilitate authentication, and provide access to the Services. • Legitimate interests: To facilitate engagement with our business, customize the user experience, and ensure the efficient operation and convenience of the Platform.

Purpose for Collection	Type of Personal Information	Lawful Basis for Processing Under the GDPR
• To administer, secure, and maintain our business and Platform. This includes troubleshooting, data analysis, testing, system maintenance, fraud validation, and data hosting, as well as generating content and providing customer support.	• Identity Data • Contact Data • Technical Data • Marketing Data	• Legitimate interests: To operate our business efficiently; to provide administration and IT services; to ensure network and information security; and to detect and prevent fraud, and to ensure network and information security. • To comply with a legal obligation: To fulfill statutory requirements regarding data security, financial reporting, and fraud prevention. Necessary to comply with our legal obligations
• To utilize data analytics to enhance our App, Platform, and service offerings; to optimize marketing strategies; and to improve customer relationships and overall user experience.	• Technical Data • Usage Data • Marketing Data	• Legitimate interests: To maintain the relevance and functionality of our website; to develop and refine our products and services; to inform our marketing strategy; and to understand how users interact with our Platform.
• To process and evaluate your application for employment, including assessing your qualifications, skills, and suitability for the role.	Career Data	• Taking steps at your request prior to entering into a contract: To review your application and facilitate the recruitment process before potentially entering into an employment agreement. • Legitimate interests: To manage our recruitment and hiring activities and to select appropriate candidates for our organization.

Purpose for Collection	Type of Personal Information	Lawful Basis for Processing Under the GDPR
• To enable third-party service providers and contractors to perform functions on our behalf, including but not limited to IT service management, infrastructure support, and operational assistance.	• Identity Data • Contact Data • Course Data • Services Data • Technical Data • Marketing Data	• Legitimate interests: To ensure the efficient operation of our business by outsourcing specific technical and administrative tasks to qualified specialists. • Performance of a contract: To ensure our systems and services are maintained and delivered in accordance with our service agreements.

We agree not to use or disclose this personal information for a secondary purpose unless you consent to us doing so, or another exception applies under applicable laws, including Article 6(4) EU / UK GDPR (compatibility test for further processing) or APP 6 of the Australian Privacy Act 1988 (Cth).

In addition to the Lawful Bases set out in the table above, we may use your Personal Information (however collected) to fulfil a Legal Obligation if processing is necessary:

- to record your preferences (e.g. marketing) to ensure that we comply with applicable data protection laws;
- where we are required to assist government and law enforcement agencies or regulators;
- where we retain information to enable us to bring or defend legal claims; and/or
- where we are required to assist government and law enforcement agencies or regulators, including in relation to any eligible data breach declarations by any of them.

6.2 Creation of anonymous data

We also collect data in a form that does not, on its own, permit direct association with any specific individual. We may collect, use, transfer, and disclose non-personal information for any purpose where such information has been irreversibly anonymised or de-identified in accordance with Article 11 GDPR / UK GDPR and APP 11.2.

We may collect information regarding customer activities on our Services including the Platform. This information is aggregated and used to help us provide more useful information to our customers and to understand which parts of our Platform, products, and Services are of most interest. Aggregated data is considered non-personal information for the purposes of this Privacy Policy only where it can no longer reasonably be used to identify an individual.

7. Disclosure of your Personal Data

Vygo, as the platform provider, has access to data (including Personal Data) necessary to operate, maintain, and support the Services and Platform, subject to strict access controls and audit logging.

We may disclose your Personal Data to third parties for the purposes contained in this Privacy Policy, including without limitation to:

7.1 Universities and other institution partners

We may share some or all of your Personal Data with your Institution Partner subject to obligations consistent with this Privacy Policy, applicable law, and any other appropriate confidentiality and security measures we determine are necessary given the nature of the information being disclosed.

This includes Personal Information contained in chat or video logs. Such disclosure is likely to happen if the conversation is manually flagged by a participant in that chat or session and then if Vygo or your Institution Partner decides to review it. If the information is then reviewed, it will only be reviewed to determine if there is a breach of this Privacy Policy or our Related Terms, your Institution Partner's policies or to notify the relevant authorities if there is a risk of harm.

Where Vygo has a contractual relationship with your Institution Partner, it will also have access (as data controller) to such data in accordance with its internal privacy policies and institutional obligations.

Where your Institution Partner is based in the United States, such information may constitute "education records" under FERPA. Vygo processes this information as a "school official" with a legitimate educational interest, and only under the direction of your Institution Partner

If there is a situation where you have opted into a direct relationship with Vygo, to the extent otherwise permitted by law and this Policy, Vygo may contact you directly for marketing or any other purpose contemplated under this Privacy Policy.

7.2 IT Service Management

We use third-party analytics services to help understand your usage of our Services. In particular, we provide a limited amount of your information (such as sign-up date and some personal information like your email address) to an IT service management provider (**ITSM Provider**) and utilize the ITSM Provider to collect data for analytics purposes when you use the Platform.

As a data processor acting on our behalf, the ITSM Provider analyses your use of the Platform and tracks our relationship by way of cookies and similar technologies so that we can improve our service to you.

We may also use the ITSM Provider as a medium for communications, either through email, or through messages within the Platform. To enhance your user experience, the

ITSM Provider may also collect publicly available contact and social information related to you, such as your email address, gender, company, job title, photos, website URLs, social network handles and physical addresses.

You may request a copy of the ITSM Service Provider's privacy policy from us. If you would like to opt out of having this information collected by or submitted to the ITSM Provider, please contact us. Where required under UK/EU law, processing by ITSM Providers outside the EEA/UK will be governed by Standard Contractual Clauses (SCCs) or the UK IDTA to ensure equivalent protection.

7.3 Service Providers

We may share your Personal Data with service providers to:

(a) provide you with the Services that we offer you, including the Platform;

(b) conduct quality assurance testing;

(c) facilitate creation of accounts;

(d) provide technical support; and/or

(e) provide other services to Vygo.

The service providers (and if necessary, data processors) could include:

(a) information technology service providers such as web host providers and analytical providers;

(b) mailing houses;

(c) market research organisations to enable them to measure the effectiveness of our advertising and business impact; and

(d) specialist consultants.

These third party service providers are obligated not to use your Personal Data, other than to provide the services requested by Vygo and are bound by written data-processing or sub-processing agreements incorporating confidentiality, data-security, and international-transfer safeguards.

7.4 Affiliates and Acquisitions

We may share some or all of your Personal Data with our parent company, subsidiaries, joint ventures, or other companies under a common control (**Affiliates**), in which case we will require our Affiliates to honour this Privacy Policy and apply equivalent protection standards. If we are involved in a merger, acquisition or sale of assets we may disclose Personal Data collected by us to such entities that we propose to merge with or be acquired by and will assume the rights and obligations regarding your Personal Data as described in this Privacy Policy. This includes the disclosure of information to our

Institution Partners where we act as a data processor under a lawful and documented processing agreement.

7.5 Third parties including those you choose to share your data with

We may disclose your Personal Data to third parties to whom you expressly ask us to send your Personal Data or to third parties to whom you choose to send your Personal Data.

We may also, with your consent or at your direction, disclose your Personal Data to your authorised representatives. Such disclosures will be limited to the minimum information necessary for the relevant purpose and will be made in accordance with applicable data-protection laws and contractual safeguards.

7.6 Other disclosures

Regardless of any choices you make regarding your Personal Data (as described below), Vygo may disclose Personal Data if it believes in good faith that such disclosure is necessary:

(a) in connection with any legal investigation;

(b) to comply with relevant laws, regulations, enforceable governmental requests or to respond to subpoenas or warrants served on Vygo;

(c) to protect or defend the rights or property of Vygo or users of the Services;

(d) to investigate or assist in preventing any violation or potential violation of the law, this Privacy Policy, or our Related Terms;

(e) to protect the safety of any person or to protect the safety or integrity of our platform including for security reasons; and/or

(f) to detect, prevent or otherwise address fraud, security or technical issues.

We may share your Personal Data with such third parties subject to obligations consistent with this Privacy Policy and any other appropriate confidentiality and security measures, and on the condition that the third parties use your Personal Data only on our behalf and pursuant to our instructions (except where disclosure is made under a lawful requirement to a competent authority or regulator).

We will take reasonable steps to ensure that anyone to whom we disclose your personal information respects the confidentiality of the information and abides by the Privacy Act, the GDPR, the DPA and the CCPA (or equivalent privacy laws including the UK GDPR).

We will not share, sell, rent or disclose your Personal Data in ways different from what is disclosed in this Privacy Policy.

Where we act as a data processor our Partner may also provide us with instructions regarding disclosure. Vygo acts as a data processor on behalf of Institution Partners where applicable, including under FERPA. In these cases, Institution Partners are the

controllers and should be contacted directly for rights and requests relating to their processing.

8. If we can't collect your data

If you do not provide us with your Personal Data described above, some or all of the following may happen:

(a) we may not be able to provide the requested products or services to you, either to the same standard or at all;

(b) we may not be able to run competitions and promotions in a way that benefits you;

(c) we may not be able to provide you with information about products and services that you may want; or

(d) we may be unable to tailor the content of our Services to your preferences and your experience of our Services may not be as enjoyable or useful.

Where consent is required for processing under the UK/EU GDPR, the Australian Privacy Act, or other relevant applicant law, failure to provide, or the withdrawal of, such consent may limit certain features or prevent us from delivering parts of the Services, but will not otherwise affect your access to core functionality.

9. Cookies Policy

9.1 What are cookies?

A cookie is a small piece of text sent to your browser by a website that you visit. It helps the website to remember information about your visit, like your preferred language and other settings. That can make your next visit easier and the site more useful to you. Cookies play an important role. Without them, using the web would be a much more frustrating experience.

9.2 Use of cookies

Vygo’s Services including websites, online services, interactive applications, email messages, and advertisements may use cookies and other technologies such as pixel tags and web beacons. These technologies help us better understand user behaviour, tell us which parts of our applications people have visited, and facilitate and measure the effectiveness of advertisements and web searches.

We treat most information collected by cookies and other technologies as non-personal information. However, to the extent that Internet Protocol addresses or similar identifiers are considered personal information by local law, we also treat these identifiers as personal information. Similarly, to the extent that non-personal information is combined

with personal information, we treat the combined information as personal information for the purposes of this Privacy Policy.

Vygo and our partners also use cookies and other technologies to remember personal information when you use our Services. Our goal in these cases is to make your experience with Vygo more convenient and personal. For example, knowing your first name lets us welcome you the next time you visit the Platform. Knowing someone using your computer or device has accessed particular support sessions or viewed certain content, helps us make our advertising and email communications more relevant to your interests. Knowing your contact information, hardware identifiers, and information about your computer or device helps us personalize your experience and provide you with better customer service.

Pixel tags enable us to send email messages in a format customers can read, and they tell us whether mail has been opened. We may use this information to reduce or eliminate messages sent to customers.

Many of these cookies are removed or cleared when you log out but some may remain so that your preferences are remembered for future sessions.

Where required under the ePrivacy Directive or UK Privacy and Electronic Communications Regulations (PECR), Vygo will request your explicit consent before storing or accessing non-essential cookies (such as analytics or marketing cookies) through a cookie banner or preference centre.

9.3 Third Party Cookies

We do not sell Personal Information.

We do not sell your Personal Data, consistent with Section 1798.140 of the CCPA and the CPRA or applicable regional privacy legislation.

Where we disclose your Personal Data to third parties, including data processors, we will request that the third party handle your personal information in accordance with this Privacy Policy. The third party will only process your personal information in accordance with written instructions from us and we require that the third party implements appropriate safeguards, including Standard Contractual Clauses (SCCs), the UK International Data Transfer Addendum (IDTA), or other approved transfer mechanisms under applicable law for the transfer and processing of personal information.

When we refer to ‘processing’ in this clause and this Privacy Policy in general, we mean any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collecting, recording, organising, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available personal information.

Please note that we use the following third parties to process your Personal Data:

(a) Google Cloud Services;

(b) Algolia;

(c) Twilio; and

(d) Cronofy.

By providing us with your Personal Data, you consent to the disclosure of your Personal Data to third parties who reside outside your region and, if you are a United Kingdom (UK), European Union (**EU**) citizen, to third parties that reside outside the UK and EU.

Where the disclosure of your Personal Data is solely subject to Australian privacy laws (and not subject to the GDPR), you acknowledge that we are not required to ensure that those third parties comply with Australian privacy laws. However, we will take reasonable steps under APP 8 to ensure that overseas recipients do not breach the Australian Privacy Principles in relation to your Personal Data.

9.4 How to manage cookies

Some people prefer not to allow cookies, which is why most browsers give you the ability to manage cookies to suit you. If you want to disable cookies and you're using the Safari web browser, go to your browser preferences and then to the privacy pane to manage your preferences. For other browsers, check with your provider to find out how to disable cookies. Please note that certain features of the Services will not be available once cookies are disabled. You may also adjust your cookie preferences directly through our cookie banner or "Manage Cookies" link at the bottom of our website at any time.

9.5 Universal Opt-Out.

We honor Global Privacy Control (GPC) signals and similar browser-based opt-out preference signals as required by applicable state laws. Learn more at https://globalprivacycontrol.org/

10. Third party websites

When you click on a link to any other website or location, you will leave our website and go to another site and another entity may collect Personal Data or Anonymous Data from you. We have no control over, do not review, and cannot be responsible for, these outside websites or their content. Please be aware that the terms of this Privacy Policy do not apply to these outside websites or content, or to any collection of data after you click on links to such outside websites.

11. Managing your Personal Data

Subject to the applicable privacy regulations, you may request to access the Personal Data we hold about you by contacting us. All requests for access will be processed within a reasonable time.

11.1 Accessing or rectifying your Personal Data

We may, if required, provide you with tools and account settings to access, correct, delete, or modify the Personal Data you provided to us. You can find out more about how to do this, or if you are unable to access your Account to access or rectify your Personal Data, you may submit a request to us at privacy@vygoapp.com to correct, delete or modify your Personal Data and/or download the data for you.

In most cases, you may have access to Personal Data that we hold about you. We will handle requests for access to your Personal Data in accordance with applicable data protection laws. All requests for access to your Personal Data must be directed to the Privacy Officer as outlined further below.

We will deal with all requests for access to your Personal Data as quickly as possible. Requests for a large amount of information, or information that is not currently in use, may require further time before a response can be given.

On receiving an access request, we will provide the necessary Personal Data in a portable and easily accessible format, normally within 45 days of the request (or within 30 days where required under the UK/EU GDPR, subject to permitted extensions).

If you are a California resident, you may request that we:

Disclose to you the following information for the 12 months preceding your request:

(a) the categories of Personal Data we collected about you and the categories of sources from which we collected such Personal Data;

(b) the specific pieces of Personal Data we collected about you;

(c) the business or commercial purpose for collecting Personal Data about you;

(d) the categories of Personal Data about you that we otherwise shared or disclosed, and the categories of third parties with whom we shared or to whom we disclosed such Personal Data (if applicable).

11.2 Deletion

We keep Personal Data for as long as it is needed for our operations. If you deactivate and delete your Account, your data will no longer be visible on your Account. Vygo deletes user and customer data upon request or upon termination of our customer contract. Please keep in mind that third parties, including your institution, may still retain copies of information you have made public through our Services or which we have shared with them in accordance with this Privacy Policy.

If you wish to have us delete your Personal Data, please contact us. We will respond within the timeframes required by law and confirm deletion or anonymisation unless retention is required for compliance, recordkeeping, or dispute resolution purposes.

11.3 Object, restrict or withdraw consent

If you have an Account on the Services, including the Platform, you will be able to view and manage your privacy settings. Alternatively, if you do not have an Account, you may manually submit a request to us if you object to any Personal Data being stored, or if you wish to restrict or withdraw any consent given for the collection of your Personal Data.

You may withdraw your consent to the processing of all your Personal Data at any time. If you wish to exercise this right, you may do so by contacting us.

You may withdraw your consent or manage your opt-ins by either viewing your account on the Services or clicking the unsubscribe link at the bottom of any marketing materials we send you.

Please note that withdrawing consent will not affect the lawfulness of processing that was carried out before withdrawal or any processing performed on another lawful basis (such as contractual necessity or legitimate interests) under Article 6 GDPR / UK GDPR. Where Vygo acts as a data processor on behalf of an Institutional Partner, you should contact your Institution Partner (as the data controller) to exercise your rights in relation to the data that it controls, including access, correction, deletion, and portability requests. Vygo will assist the Institution Partner in responding to such requests in accordance with its contractual and legal obligations.

11.4 Portability

We may, if required and possible, provide you with the means to download the Personal Data you have shared through our Services in a structured, commonly used and machine-readable format, and to transmit that data to another controller if you request it, in accordance with Article 20 of the EU and UK GDPR. Please contact us for further information on how this can be arranged.

This right applies only to Personal Data that you have actively provided to us and that is processed by automated means, and only where the processing is based on your consent or a contract. Where Vygo acts as a data processor on behalf of an Institution Partner, you should contact your Institution to exercise this right, and Vygo will assist the Institution Partner in fulfilling such requests in accordance with its legal and contractual obligations.

11.5 Refusal to provide access to your information

In some cases, we may refuse to give you access to your Personal Data that we hold. This may include circumstances where giving you access would:

(a) be unlawful (e.g. where a record that contains Personal Data about you is subject to a claim for legal professional privilege by one of our contractual counterparties);

(b) have an unreasonable impact on another person's privacy; or

(c) prejudice an investigation of unlawful activity or the prevention, detection or prosecution of criminal offences.

Where we are unable or not required to provide access under applicable law, we will provide written reasons for our decision and information on how you may lodge a complaint with the relevant supervisory authority or the Office of the Australian Information Commissioner (OAIC).

11.6 Correcting your personal information

If you consider the Personal Data that we hold about you to be incorrect, incomplete, out of date or misleading, you can request that the Personal Data be amended.

We will amend any of your Personal Data that is held by us and that is inaccurate, incomplete or out of date if you request us to do so. If we disagree with your view about the accuracy or completeness of a record of your Personal Data that is held by us, and you ask us to associate with that record a statement that you have a contrary view, we will take reasonable steps to do so.

Where a record is found to be inaccurate, a correction will be made. Where a request is made for a record be amended because it is inaccurate, but the record is found to be accurate, the details of the request for amendment will be noted on the record.

In certain instances, we may not be required or able to provide you with access to your Personal Data. If this occurs, we will give you reasons for our decision not to provide you with such access to your Personal Data in accordance with the Privacy Act, the CCPA, the DPA and the GDPR (including Article 12(4) EU/UK GDPR).

There is no application fee for making a request to access your Personal Data. However, we may charge an administrative fee for the provision of information in certain circumstances such as if you make repeated requests for Personal Data or where the information is held by a third party provider.

Where we act as a data processor, we do so on behalf of our client and in accordance with their instructions. This means that should you wish to access, review, correct, transfer, modify or delete any Personal Data which we process on behalf of a client you should contact that client with your request. Vygo will assist the client (controller) in responding to such requests, as required under Article 28(3)(e) GDPR and equivalent provisions of the UK GDPR, the Australian Privacy Act and any other relevant applicable law.

11.7 Rights for EU and UK individuals

You may request details of the personal information that we hold about you and how we process it (commonly known as a "data subject request"). You may also have a right in accordance with

applicable data protection law to have your personal information rectified or deleted, to restrict our processing of that information, to object to decisions being made based on automated processing where the decision will produce a legal effect or a similarly significant effect on you, to stop unauthorised transfers of your personal information to a third party and, in some circumstances, to have personal information relating to you transferred to you or another organisation.

Where your request relates to processing carried out under legitimate interests (Article 6(1)(f) GDPR), you may object at any time on grounds relating to your particular situation, and we will cease such processing unless we demonstrate compelling legitimate grounds to continue.

If you are based in the UK, you may contact the Information Commissioner's Office (ICO) (www.ico.org.uk). If you are based in the EU, you may contact your local Data Protection Authority.

11.8 Rights for California and certain other US state individuals

If you reside in California or another state with similarly comprehensive privacy laws, you have the following rights:

(a) **Right to Know/Access**: Confirm whether we process your Personal Data and access such data, including categories and sources of information collected, purposes for collection and use, and categories of third parties with whom we share information.

(b) **Right to Correct**: Request correction of inaccurate Personal Information.

(c) **Right to Delete**: Request deletion of Personal Information we collected from you, subject to certain legal exceptions.

(d) **Right to Data Portability**: Obtain a copy of your Personal Data in a portable, readily usable format (where technically feasible).

(e) **Right to Opt-Out**: Opt out of:

- Sale of Personal Data (we do not sell)

- Sharing for cross-context behavioral advertising (we do not share for this purpose)

- Targeted advertising (we do not engage in targeted advertising)

- Profiling in furtherance of decisions that produce legal or similarly significant effects (we do not engage in such profiling)

(**f) Right to Limit Use of Sensitive Personal Information:** Request that we limit use of your Sensitive Personal Information to purposes permitted under applicable law. We only use Sensitive Personal Information (account credentials, precise geolocation, communication contents, protected characteristics, health data) for service delivery and other permitted purposes.

(g) **Right to Non-Discrimination:** We will not discriminate against you for exercising these rights.

(h) **Right to Appeal**: If we deny your request in whole or in part, you may appeal by contacting privacy@vygoapp.com within a reasonable time (California: 30 days; other states: as specified by state law). We will respond within 45-60 days depending on applicable state law. If we deny your appeal, you may contact your state attorney general to submit a complaint.

How to Exercise Your Rights:

Email: privacy@vygoapp.com

Phone: +1 (503) 828-3961

Online: https://vygoapp.com/au/contact

Office: 'Central Plaza One' Level 38, 345 Queen Street, Brisbane QLD, Australia, 4000

We will verify your identity before processing requests and respond within:

- California: 45 days (extendable by 45 days)

- Other states: as required by applicable state law

Authorized Agents: You may designate an authorized agent to submit requests on your behalf. We require written authorization or valid power of attorney and may still require direct identity verification.

12. Direct marketing materials

Where you opt into our direct marketing materials, or as otherwise permitted by law, we may send you direct marketing communications and information about our products and services that we consider may be of interest to you. These communications may be sent in various forms, including mail, SMS and email, in accordance with applicable marketing laws, such as Australia's Spam Act 2003 (*Cth*), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (UK) or the ePrivacy Directive (EU), and the United States CAN-SPAM Act of 2003. If you indicate a preference for a method of communication, we will endeavour to use that method whenever practical to do so. In addition, at any time you may opt-out of receiving marketing communications from us by contacting us (see the details below) or by using opt-out facilities provided in the marketing communications and we will then ensure that your name is removed from our mailing list.

We will not send unsolicited direct marketing to individuals under the age of 18 or to users located in jurisdictions that prohibit such communications. Where consent is required, we will seek clear, informed, and specific opt-in consent prior to sending marketing material, and will maintain records of consent for audit purposes.

13. Storage and Security of Your Personal Data

Vygo stores Personal Data in Google Cloud Services, which provides secure, ISO 27001-certified environments for data hosting. Further information about Google Cloud's

security controls can be found on their public trust and compliance pages. Vygo takes the security of your Personal Data very seriously. We will take all steps reasonable under the circumstances to protect your personal information from misuse, interference, loss; and unauthorised access, modification or disclosure. We will process Personal Data securely and apply and maintain appropriate technical and organisational measures to protect Personal Data in accordance with Article 32 EU and UK GDPR and APP 11.1 of the Australian Privacy Act.

In furtherance of this goal, Vygo is committed to high standards of privacy ensures our practices align with SOC 2 (Type II) controls and other industry frameworks such as ISO 27001 and NIST 800-53. We also maintain internal policies covering encryption, access control, password management, endpoint security, incident response, and data retention. You may request further details of our security and privacy policies by contacting us at privacy@vygoapp.com. The transmission and exchange of Personal Data is carried out at your own risk. We cannot guarantee the security of any Personal Data that you transmit to us or receive from us. Although we take measures to safeguard against unauthorised disclosures of Personal Data, we cannot assure you that Personal Data that we collect will not be disclosed in a manner that is inconsistent with this Privacy Policy. Where a transmission occurs over the internet or a public network, we use encryption (TLS 1.2 or higher) to mitigate risks, but users should exercise care when transmitting data online.

Our data retention policy sets forth details on how long we retain categories of personal information.

14. International Transfer and Disclosure of Personal Data

We ensure that all our suppliers are required to adhere to the Australian Privacy Principles in the Privacy Act and to implement comparable safeguards required by the EU and UK GDPR.

Where we transfer Personal Data from within or from the United Kingdom, European Union or EFTA States to a country outside those jurisdictions, we ensure an adequate level of protection for the rights of data subjects in accordance with Chapter V of the EU and UK GDPR. This may include:

a) transfers to countries that the European Commission or UK Government has determined provide an adequate level of protection; or
b) the use of Standard Contractual Clauses (SCCs) or the UK International Data Transfer Addendum (IDTA), together with additional technical and organisational measures to ensure equivalent protection.

We may disclose Personal Data to our related bodies corporate and third-party suppliers and service providers located overseas for some of the purposes listed above. We take reasonable steps to ensure that the overseas recipients of your Personal data do not breach the privacy obligations relating to your Personal Data and that all transfers are governed by written agreements consistent with Article 46 GDPR and APP 8.

We may disclose your Personal Information to entities located outside of your region, including the following:

(g) our related bodies corporate;

(h) our data hosting and other IT service providers, located in various countries; and

(i) other third parties located in various foreign countries.

We may disclose your Personal Data to entities within your region who may store or process your data overseas (for example, regional support teams or analytics providers). In all cases, we ensure that equivalent contractual safeguards and data-minimisation principles are applied.

15. Notifiable Data Breaches

We take data breaches very seriously. We use industry standard technical, administrative, physical, and organizational measures to protect the data we collect, including encrypting it at rest and as it is transferred from you to Vygo. While we take reasonable precautions against possible security breaches, no website or internet transmission is completely secure and we cannot guarantee that unauthorized access, hacking, data loss or other breach will never occur.

In the event of a breach, we will take reasonable steps to investigate the situation and, where appropriate, notify affected individuals in accordance with any applicable laws and regulations. We maintain a written Incident Response Plan and will document all breaches, remedial actions, and notifications for audit and compliance purposes.

15.1 If you reside in Australia

If there is a data breach and we are required to comply with the notification of eligible data breaches provisions in Part IIIC of the Privacy Act or any other subsequent sections or legislation which supersede this Part IIIC, we will take all reasonable steps to contain the suspected or known breach where possible and follow the following process set out in this clause.

We will take immediate steps to limit any further access or distribution where possible. If we have reasonable grounds to suspect that the data breach is likely to result in serious harm to any individuals involved, then we will take all reasonable steps to ensure an assessment is completed within 30 days of the breach or sooner if possible. We will follow the guide published by the Office of the Australian Information Commissioner (if any) in making this assessment.

If we reasonably determine that the data breach is not likely to result in serious harm to any individuals involved or that any remedial action we take is successful in making serious harm no longer likely, then no notification or statement will be made.

Where, following an assessment and undertaking remedial action (if any), we still have reasonable grounds to believe serious harm is likely, as soon as practicable, we will provide a statement to each of the individuals whose Personal Data was breached or who are at risk. The statement will contain details of the breach and recommendations of the steps each individual should take. We will also provide a copy of the statement to the Office of the Australian Information Commissioner.

15.2 If you reside in the United Kingdom, European Union or EFTA States:

We will endeavour to meet the 72-hour deadline required by the GDPR, to report any data breach to the supervisory authority where a data breach occurs that will likely be a risk to you.

Further, where there is likely to be a high risk to your rights, we will endeavour to contact you without undue delay.

We will review every incident and take action to prevent future breaches.

Notifications will comply with Articles 33 and 34 of the EU and UK GDPR, and we will maintain internal records of all breaches in accordance with Article 33(5).

15.2 If you reside in California and certain other US states:

For breaches affecting US residents, we comply with applicable state data breach notification laws:

- Notification: We will notify you without unreasonable delay (and in any case within the time required by applicable law) by email, Platform posting, or other appropriate means. Notice will describe the breach, affected information, our response, and steps you can take to protect yourself.
- Regulators: We will notify state attorneys general and consumer protection agencies to the extent required, typically when breaches exceed state-specific thresholds (typically 500-1,000 residents, or any residents in some states).
- Delays: We may delay notification where law enforcement determines it would impede criminal investigation.
- Your Rights: Where applicable and/or required, (a) you may receive free credit monitoring, identity theft resources, and additional breach information, and (b) you may file complaints with your state attorney general.

16. Automated individual decision-making, including profiling

If you reside in the United Kingdom, European Union or EFTA States, you have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you, or similarly significantly affects you, in accordance with Article 22 of the EU and UK GDPR. This right does not apply where the decision is necessary for entering into, or the performance of, a contract between us, is authorized by Union or Member State law to which we are subject and which also lays down suitable measures to safeguard your rights and freedoms and legitimate interests, or is not based on your explicit consent.

Vygo does not currently engage in automated decision-making or profiling that produces legal or similarly significant effects on individuals. Should this change, we will provide prior notice and implement appropriate safeguards, including human review, the opportunity to express your point of view, and the ability to contest any such decision, as required under Article 22(3) GDPR.

If you wish to exercise your rights, please contact us using the details in Section 20 below.

17. Integrity and Retention of Data

We take all reasonable steps to ensure that the Personal Data we collect about you is accurate, up to date and complete. Where we collect that information from you directly, we rely on you to supply accurate information.

Vygo ensures that any Personal Data we use or disclose is relevant and limited to what is necessary for the purposes for which it is processed, in accordance with the data-minimisation and accuracy principles under Article 5 EU/UK GDPR and APP 10.

We retain your Personal Data for the period necessary to fulfil the purposes outlined in this Privacy Policy unless a longer retention period is required or permitted by law. Once retention periods expire, we securely delete or anonymise Personal Data in accordance with our data retention policy].

When determining retention periods, we consider the nature and sensitivity of the data, the risk of harm from unauthorised use or disclosure, the purposes of processing, whether those purposes can be achieved by other means, and any applicable legal, regulatory, tax, or contractual requirements.

We may retain your information for fraud prevention or similar purposes (for example, to detect or prevent misuse of our platform or to comply with record-keeping obligations under contract or law).

18. Contact Information

Vygo welcomes your comments or questions regarding this Privacy Policy.

If you have a question regarding this Privacy Policy or you would like to make a complaint, please contact us by email by using our contact details on the Services or below.

18.2 If you reside in Australia

You can confidentially contact our Privacy Officer at:

Privacy Officer	Steven Hastie
Entity	Vygo Pty Ltd CAN 609 658 531
Telephone	+1 (503) 828-3961
Email	steven@vygoapp.com
Office Address	Central Plaza One' Level 38, 345 Queen Street, Brisbane QLD, Australia, 4000

Postal Address	Central Plaza One' Level 38, 345 Queen Street, Brisbane QLD, Australia, 4000
Website	vygoapp.com

If we do not resolve your enquiry, concern or complaint to your satisfaction or you require further information in relation to any privacy matters, please contact the Office of the Australian Information Commission at:

Telephone: 1300 363 992

Email: enquiries@oaic.gov.au

Office Address: Level 3, 175 Pitt Street, Sydney NSW 2000

Postal Address: GPO Box 5218, Sydney NSW 2001

website: www.oaic.gov.au

18.3 If you reside in the United Kingdom, European Union or EFTA States:

The data controller that is responsible for your Personal Data is:

Vygo Pty Ltd ACN 609 658 531

'Central Plaza One' Level 38 345 Queen Street Brisbane, QLD, Australia, 4000

Vygo has appointed Steven Hastie under Article 27 EU GDPR and Article 27 UK GDPR to act as its point of contact for data-protection matters within the EU and UK.

If you wish to raise a concern about our use of your Personal Data you have the right to do so with your local supervisory authority.

In the UK, this is the Information Commissioner's Office (ICO) (www.ico.org.uk). In the EU, you may contact your local Data Protection Authority.

19 Changes to this Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, legal requirements, or operational needs. Any updates will comply with applicable transparency obligations under the Australian Privacy Principles and, where relevant, the EU and UK GDPR (Articles 12 and 13) and applicable US state and federal law.

The date at the top of this Privacy Policy indicates when it was last revised. Material changes will be notified through the Platform (and by email where appropriate). Updates take effect from the date of publication and apply to information collected after that date.

Your continued use of the Platform or Services following such updates constitutes your acceptance of the revised Privacy Policy.

Last revised: May 2026