



External Data Processors

Last updated: October 2021

CoGo uses third party service providers to provide services that involve data processing, for example web-hosting and analytics providers.

When we share your data with a third party, we have contracts in place with them which requires them to have in place the technical and organisational measures necessary to protect your personal data.

You can find the details of our policies and processes in our [Privacy Notice](#)

In the table below, you can find the current list of external data processors that CoGo works with. Please note that this list may be updated from time to time as we change, add or update our suppliers:

Name or class of processor	Data shared with processor	Purpose of processing	Location of data
Google Google.com	Email Name IP address, location, browser type, device used, operating system, pages accessed and date / time of access.	IT infrastructure Administration of emailing lists Track how users are using our website over time, as the website changes, in order to optimize the content we provide and marketing we do	US – we rely on the Privacy Shield framework
AWS Aws.com	Gender Name Age range Residence location (suburb) Email address Facebook ID Profile image Personal account number (PAN) of payment card Payment card transactions	IT infrastructure Application hosting	EU & Australia

Mailchimp Mailchimp.com	Name Email address Email opening tracking Email click tracking Areas of interest for job alert	Direct marketing and monitoring of the effectiveness of campaigns. Sending relevant new job emails.	US – we rely on the Privacy Shield framework
Typeform Typeform.com	Name Email address	Administering surveys and research	US – we rely on the Privacy Shield framework
Deloitte New Zealand <i>Accountants</i> <i>Deloitte.co.nz</i>	Name Email address Business information	Invoicing our business customers	NZ
Xero <i>Accounting software</i> Xero.com	Name Email address Business information	Invoicing our business customers	US – we rely on the Privacy Shield framework
Consents Online consents.online Account Score accountscore.com	Bank transactions	Matching your spending with your values and analysing potential “switches” Aggregated anonymously to communicate to businesses	EU
Red Bird Ventures Limited	Bank transactions	Matching your spending with your values and analysing potential “switches” Aggregated anonymously to communicate to businesses	NZ
Branch Branch.io	iOS Identifier for Advertising (IDFA) iOS Identifier for Vendors (IDFV)	Enabling users to deep link into the CoGo app, and providing CoGo with analytics that help us understand how users	US – we rely on the Privacy Shield framework

	<p>Android Advertising ID (GAAID)</p> <p>Android ID</p> <p>IP Address Developer ID</p> <p>Local IP address</p> <p>Phone number (only used with "Text Me the App" feature)</p>	engage with our product.	
<p>Amplitude</p> <p>Amplitude.com</p>	<p>Information about website and application browsing, activity, history, and device information (e.g., device identifiers (not Apple ID), operating system and IP addresses)</p>	<p>Understanding how people are using our product, in order to help us improve it.</p>	<p>US – we rely on the Privacy Shield framework</p>
<p>Facebook</p> <p>Facebook.com</p>	<p>Email</p>	<p>Matching users of our service to their Facebook accounts, so we can advertise to those users in Facebook.</p>	<p>US – we rely on the Privacy Shield framework</p>
<p>OneSignal</p> <p>onesignal.com</p>	<p>When permitted by the operating system, OneSignal may check to see if the device has specific applications installed, based on a limited list, for purposes that include attribution, relevancy of ads, and relevancy of notifications related to those applications.</p> <p>Purchases made within an app.</p> <p>Information about End User's transactions and interactions with apps and websites</p> <p>Mobile advertising identifiers, such as iOS IDFAs and Android Advertising</p>	<p>Provision of push notification services (emails or mobile notifications)</p>	<p>US – we rely on the Privacy Shield framework</p>

	<p>IDs (“Mobile IDs”). These Mobile IDs may be associated with other Information, including with Data Segments.</p> <p>Precise Location information, generally an End User’s lat/long data (i.e., GPS-level data) or WiFi information, which we may associate with Mobile IDs, and which may be collected whether or not an app is in use.</p> <p>Email address, which we may (in our discretion) hash or otherwise de-identify.</p> <p>IP address as well as system configuration information</p> <p>Information associated with or related to devices, such as device type (e.g., mobile, tablet); type and version of operating system (e.g., Android, iOS); network provider; mobile browser (e.g. Safari, Chrome, etc.); language setting; time zone; and network status type (such as WiFi).</p>		
<p>Stripe</p> <p>stripe.com</p>	<p>Name, credit card details for carbon offset payments</p>	<p>Stripe is a payment processing platform we use to collect payment for customer carbon offsetting</p>	<p>US – we rely on the Privacy Shield framework</p>
<p>Paypal</p> <p>paypal.com</p>	<p>Name, credit card details for carbon offset payments</p>	<p>Paypal is a payment processing platform we use to collect payment for customer carbon offsetting</p>	<p>US – we rely on the Privacy Shield framework</p>