

Vigilance Privacy Policy

At Vigilance we take privacy very seriously and we comply with all applicable privacy and data protection laws when dealing with personal information.

We encourage you to read this **Policy** carefully. It will help you make informed decisions about sharing your personal information with us. The defined terms in this Policy have the same meaning as in our **Terms of Use**, which you should read together with this Policy. By accessing our Website and/or using our Web Services, you consent to the terms of this Policy and agree to be bound by it and our Terms of Use.

If you are based in the European Union (“**EU**”) or the United Kingdom (“**UK**”) and use our Website and/or Web Services, the additional terms in the addendum to this Policy (“**GDPR Addendum**”) apply to you.

This Policy does not limit or exclude any of your rights under applicable privacy and data protection laws.

1.0 Vigilance may collect your personal information

Vigilance is a provider of clever online business software that’s simple, smart, and secure and gives businesses real-time visibility of their data. The Web Services may involve the collection and storage of **personal information** which is information about an identifiable individual and includes personal data, personally identifiable information and equivalent information under applicable privacy and data protection laws, and may include information such as an individual’s name, email address and telephone number.

Vigilance collects and holds two categories of personal information:

Vigilance may collect personal information directly from you when you:

- register as a Customer to use the Web Services,
 - use the Web Services as a Customer,
 - contact the Vigilance support team,
 - visit our Website,
- together, “**Account and Marketing Data**”

The Account and Marketing Data we collect may include company/personal names, phone numbers, email addresses and any contact information you provide to us, location information, billing information, information about how you use our Website or the Web Services (for example, traffic volumes, time spent on pages), your IP address and/or other device identifying data, information contained in your correspondence with us or survey Responses and other information required to provide a service or information you have requested from us.

You can always choose not to provide your personal information to Vigilance, but it may mean that we are unable to provide you with the Web Services, our Website or our other services (together, **Services**).

Vigilance may also process personal information that forms part of the Customer Data (as defined in our Terms of Use). This may include personal information collected by our Customers, including our Customer's personnel or Invited Users' names, email addresses and telephone numbers, any personal information collected when our Customer's Invited Users (e.g. our Customer's suppliers) self on-board themselves on the Web Services and personal information collected when our Customers use the Web Services. This may include, where our Customers make payments to individuals, details of those payments, including amounts and bank account details.

We process Customer Data for the purposes of exercising our rights and performing our obligations under our Terms of Use and/or other agreements with our Customers that govern the processing of Customer Data ("**Customer Agreements**"). In doing so, we are acting as a data processor and/or agent and/or service provider (or the equivalent under applicable privacy and data protection laws) of the Customer for the purposes of applicable privacy and data protection laws. We will not collect or process Customer Data except as provided in our Customer Agreements and we require our Customers to comply with applicable privacy and data protection laws.

If you are an Invited User of one of our Customers, you should check the privacy policies of the Customer before providing personal information through the Web Services so that you can be informed of how the Customer will handle personal information.

The remainder of this privacy policy does not apply to Customer Data unless specifically stated otherwise.

1.5 Vigilance may also collect your personal information from other sources

In addition to information collected directly from you, Vigilance may collect Account and/or Marketing Data about you from other sources, including:

- Referral partners and other businesses, such as resellers, implementation partners, accountants, or other businesses who refer prospective customers to us. The information we receive from them typically includes your name, business name, email address, phone number, and information about the services you may be interested in.
- Publicly available sources, such as the Companies Office register, business websites, public professional directories, and public profiles on professional networking sites. We may use this information to verify business details, understand prospective customers'

needs, or maintain accurate records.

We use information collected from these sources for the same purposes set out in section 3.0, principally to provide and market the Web Services. We hold this information together with any information you give us directly, and your rights to access and correct it (set out in section 9.0) apply equally.

Where we collect your personal information indirectly and you have not already been told about the collection, we will take reasonable steps to let you know - typically in our first communication with you - unless an exception under the Privacy Act 2020 applies (for example, where notifying you would not be reasonably practical, where the information is publicly available, or where you have already been informed by the source).

2.0 Vigilance may receive personal information from you about others

Through your use of the Services, Vigilance may also collect information from you about someone else where you have authorised us to do so (for example, by choosing a feature of the Services that contemplates the interaction with a third party website or feature) or where the information is publicly available. If you provide Vigilance with personal information about someone else, you must ensure that you are authorised to disclose that information to Vigilance and that, without Vigilance taking any further steps required by applicable data protection or privacy laws, Vigilance may collect, use and disclose such information for the purposes described in this Policy. For information that Vigilance itself collects from publicly available sources or other third parties, see section 1.5 above.

This means that you must take reasonable steps to ensure the individual concerned is aware of and/or consents to the various matters detailed in this Policy, including the fact that their personal information is being collected, the purposes for which that information is being collected, the intended recipients of that information, the individual's right to obtain access to that information, Vigilance's identity, and how to contact Vigilance.

3.0 Vigilance collects, holds, and uses your personal information for limited purposes

Vigilance collects Account and Marketing Data so that we can provide you with the Web Services and any related services you may request. In doing so, Vigilance may use the personal information collected for purposes related to the Services including to:

- verify your identity and undertake credit checks of you (if necessary),
- provide the Web Services to you,
- notify you of new or changed services offered in relation to the Web Services,
- market our services and products (and those of our affiliates) relating to the Web Services to you, including contacting you via text, email or other electronic means for this purpose,
- carry out training of our personnel or affiliates in relation to the Web Services,

- assist with the resolution of technical support issues or other issues relating to the Web Services,
- comply with laws and regulations in applicable jurisdictions,
- communicate with you, including in response to a complaint,
- bill you and to collect money that you owe us, including authorising the processing of credit card transactions through our third party service provider,
- monitor your compliance with the Terms of Use, and
- use for any other purpose authorised by you or any applicable privacy laws.

We may transfer your information in the case of a sale, merger, consolidation, liquidation, reorganisation or acquisition.

By using the Services, you consent to your personal information being collected, held and used in this way and for any other use you authorise. Vigilance will only use your personal information for the purposes described in this Policy or with your express permission. It is your responsibility to keep your password to the Web Services safe. You should notify us as soon as possible if you become aware of any misuse of your password, and immediately change your password within the Web Services via the “Forgotten Password” process.

4.0 Vigilance can aggregate your non-personally identifiable data

By using the Services, you agree that Vigilance can access, aggregate and use non-personally identifiable data collected from you. This data will in no way identify you or any other individual.

Vigilance may use this aggregated non-personally identifiable data to:

- assist us to better understand how our customers are using the Web Services, for example, frequency of batches, busiest days of the month, quantity of payments made that bypass Vigilance,
- provide our customers with further information regarding the uses and benefits of the Web Services,
- enhance business productivity, including by creating useful business insights from that aggregated data and allowing you to benchmark your business’ performance against that aggregated data, and
- otherwise improve the Services.

5.0 Transfers and storage of personal information

Businesses that support the Services may be located outside New Zealand (the country where we are incorporated) and also outside of the country in which you are located. This means that the personal information we collect may be transferred to, and stored in, a country outside of New Zealand and the country where you are located.

As at the date of this Policy, our servers are located in Australia, hosted by Microsoft Azure Services, and your personal information will be routed through, and stored on, those servers. If

the location of our servers changes in the future, we will update this Policy. You should review our Policy regularly to keep informed of any updates.

Vigilance is incorporated and located in, and may access your personal information from, New Zealand. New Zealand is recognised by the European Commission and the UK government as a country that ensures an adequate level of data protection and we rely on this decision in transferring personal information to New Zealand.

By providing your personal information to Vigilance, you consent to Vigilance storing your personal information on servers hosted by Microsoft and accessing your personal information from New Zealand. While your personal information will be stored on servers located in Australia, it will remain within Vigilance's effective control at all times. The server host's role is limited to providing a hosting and storage service to Vigilance, and we've taken steps to ensure that our server hosts do not have access to, and use the necessary level of protection for, your personal information.

If you do not want your personal information to be transferred to a server located in the above named locations, you should not provide Vigilance with your personal information or use the Services.

6.0 Vigilance takes steps to protect your personal information

Vigilance is committed to protecting the security of your personal information and will at all times act carefully, to a high standard and in accordance with best industry practice we take all reasonable steps—to protect it from unauthorised access, modification or disclosure. Your personal information is stored on secure servers that have SSL Certificates issued by leading certificate authorities, and all data transferred between you and the Web Services is encrypted.

However, the Internet is not in itself a secure environment and we cannot give an absolute assurance that your information will be secure at all times. Transmission of personal information over the Internet is at your own risk and you should only enter, or instruct the entering of, personal information to the Web Services within a secure environment.

We will advise you at the first possible opportunity upon discovering or being advised of a security breach where your personal information is lost, stolen, accessed, used, disclosed, copied, modified, or disposed of by any unauthorised persons or in any unauthorised manner.

7.0 Vigilance only discloses your Personal Information in limited circumstances

Vigilance will only disclose the Account and Marketing Data provided to us by you to entities outside of Vigilance if it is necessary and appropriate to facilitate the purpose for which your personal information was collected pursuant to this Policy, including the provision of the Web Services.

Where we process personal information that forms part of the Customer Data, we will provide our Customers with access to this information in accordance with our Customer Agreements.

Other than in the case of a sale, merger, consolidation, liquidation, reorganisation or acquisition, Vigilance will not otherwise disclose your personal information to a third party unless you have provided your express consent. However, you should be aware that Vigilance may be required to disclose your personal information without your consent in order to comply with any court orders, subpoenas, or other legal process or investigation including by tax authorities, if such disclosure is required by law. Where possible and appropriate, we will notify you if we are required by law to disclose your personal information.

The third parties who host our servers do not control, and are not permitted to access or use your personal information except for the limited purpose of storing the information.

We share information about your use of the Website with our advertising and analytics partners through the use of cookies, web beacons and similar storage technologies. Please refer to the [Cookies section of this Policy for further information.](#)

8.0 Vigilance does not store your credit card details

If you choose to pay for the Web Services by credit card, your credit card details are not stored by the Web Services and cannot be accessed by Vigilance staff. Your credit card details are encrypted and securely stored by our chosen payment provider to enable Vigilance to automatically bill your credit card on a recurring basis.

9.0 You may request access to your personal information

It is your responsibility to ensure that the Account and Marketing Data you provide to us is accurate, complete and up-to-date. Subject to certain grounds for refusal set out at law, you may request access to the readily retrievable Account and Marketing Data we hold about you, or request that we update or correct any personal information we hold about you, by setting out your request in writing and sending it to us at support email address provided in the Site and Web Services.

Vigilance will process your request as soon as reasonably practicable, provided we are not otherwise prevented from doing so on legal grounds and provided that you first provide us with evidence to confirm that you are the individual to whom the personal information relates. If we are unable to meet your request, we will let you know why. For example, it may be necessary for us to deny your request if it would have an unreasonable impact on the privacy or affairs of other individuals, or if it is not reasonable and practicable for us to process your request in the manner you have requested. If you request a correction and we do not make that correction, we will take reasonable steps to note on the personal information that you requested the correction.

We may charge you our reasonable costs of providing to you copies of your personal information or correcting that information, to the extent permitted by law.

We'll only keep your personal information for as long as we require it for the purposes of fulfilling the purposes for which we have collected that information. However, we may also be required to keep some of your personal information for specified periods of time, for example under certain laws relating to corporations, money laundering, and financial reporting legislation.

We cannot provide you with access to, or update or correct any personal information we hold about you that is part of the Customer Data except on the Customer's written request or if required by applicable law. If you request access to, or an update or correction to, Customer Data, we will forward this request to the relevant Customer.

10.0 Vigilance uses cookies

In providing the Website, Vigilance utilises "cookies". A cookie is a small text file that is stored on your computer for record-keeping purposes. A cookie does not identify you personally or contain any other information about you but it does identify your computer.

Vigilance and some of our affiliates and third-party service providers may use a combination of "persistent cookies" (cookies that remain on your hard drive for an extended period of time) and "session ID cookies" (cookies that expire when you close your browser) on the Website and our Web Services, to for example, track overall website usage, and track and report on your use and interaction with ad impressions and ad services.

You can set your browser to notify you when you receive a cookie so that you will have an opportunity to either accept or reject it in each instance. However, you should note that refusing cookies may have a negative impact on the functionality and usability of the Website and Web Services. Note, Vigilance does not respond to or honour "Do Not Track" requests at this time.

When you visit the Website, Vigilance may use performance and targeting cookies.

Performance cookies collect information about how you use the Website e.g. which pages are the most visited and if you receive any error messages from any pages. These cookies do not gather information that identifies you. All information these cookies collect is anonymous and only used to improve how the Website works. Vigilance may receive reports from third party analytics partners as aggregate numbers and trends.

Targeting cookies are used to deliver advertisements that are relevant to you and your interests. They are also used to limit the number of times you have seen an advertisement as well as help measure the effectiveness of the advertising campaign. They remember that you have visited a website and this information may be shared with other organisations such as advertisers. This means that after you have been to the Website, you may see some advertisements about our services elsewhere on the Internet. Vigilance may use third party providers to present advertising relevant to your interests when you access the Website, generated from data relating to your access and use of the Website and your other browsing history. These third party providers place cookies on your browser to collect information about your past use of our

website and then places ads on sites across the Internet that are more likely to be of interest to you.

You may opt-out of targeted advertising at <http://www.youronlinechoices.eu/>. You can learn more about interest-based advertising and opt out of interest-based advertising from participating online advertising companies at the following links:

Network Advertising Initiative (NAI) – <http://optout.networkadvertising.org/>

Digital Advertising Alliance (DAA) – <http://optout.aboutads.info/>

Digital Advertising Alliance EU (EDAA) – <http://www.youronlinechoices.com/>

DAA AppChoices page – <http://www.aboutads.info/appchoices>

Please note that opting out of interest-based advertising does not mean you will no longer be served advertising. You will continue to receive generic ads.

You may also opt-out of targeted advertising at http://www.youronlinechoices.eu. Please note this does not opt you out of being served advertising. You will continue to receive generic ads.

Vigilance does not use performance or targeting cookies when you use our Web Services.

11.0 You can opt-out of any email communications

Vigilance sends billing information, product information, Vigilance company information, Web Services updates and Web Services notifications to you via email. Our emails will contain clear and obvious instructions describing how you can choose to be removed from any mailing list not essential to the Web Services. Vigilance will remove you from our mailing list at your request. Opting out of email communications will not remove you from receiving emails about breaches (where applicable) or changes to the Privacy or Terms of Use policies.

12.0 You are responsible for transfer of your data to third-party applications

The Services may allow you to follow a link to third-party applications or websites. Vigilance has no control over, and takes no responsibility for, the privacy practices or content of these applications and websites. You are responsible for checking the privacy policy of any such applications and websites so that you can be informed of how they will handle personal information.

13.0 Vigilance has a privacy complaints process

If you wish to complain about how we have handled your personal information, please provide our Privacy Officer with full details of your complaint and any supporting documentation:

- by e-mail at admin@vigl.biz, or
- by letter to The Privacy Officer, Vigilance Limited, PO Box 301130, Albany, Auckland, New Zealand

Our Privacy Officer will endeavour to:

SSLI-1721211487-69\5.3

- provide an initial response to your query or complaint within ten (10) business days, and
- investigate and attempt to resolve your query or complaint within the timeframes required under applicable privacy and data protection laws.

14.0 This policy may be updated from time to time

Vigilance reserves the right to change this Policy at any time, and any amended Policy is effective upon posting to this Website. Vigilance will communicate any significant changes to you by notification via the Web Services. Your continued access to or use of the Website or the Web Services will be deemed to be your acceptance of any amended Policy.

This Policy was last updated on 30 April 2026

GDPR addendum

If you are located in the EU or UK and use the Website and/or the Web Services, this GDPR Addendum forms part of the Vigilance Privacy Policy.

The GDPR and UK GDPR regulate the collection, processing and transfer of EU and UK individuals' personal data (as defined in the GDPR and UK GDPR). The personal information described in the Vigilance Privacy Policy is personal data under the GDPR and UK GDPR. We are committed to complying with the GDPR and UK GDPR when dealing with personal data of visitors to the Website and users of the Web Services based in the EU or the UK.

This GDPR Addendum was drafted with brevity and clarity in mind. It does not provide exhaustive detail of all aspects of our collection and use of personal data. However, we are happy to provide any additional information or explanation needed. Any requests for further information should be sent to admin@vigl.biz.

For the purposes of the GDPR and UK GDPR:

- Vigilance is the data controller (as defined in the GDPR and UK GDPR) when processing Account and Marketing Data; and
- Vigilance's customers are the data controller when processing Customer Data.

The remainder of this GDPR Addendum applies to Account and Marketing Data only, and does not apply to Customer Data.

1.0 Processing personal data

The personal data we may process consists of the Account and Marketing Data described in the Policy. We may process the Account and Marketing Data for the purposes outlined in the Policy.

The legal basis for our processing of Account and Marketing Data is your consent, or that processing is necessary for the performance of a contract to which you are a party, or that processing is necessary for compliance with a legal obligation to which we are subject under applicable laws.

Despite the above, we may process any of your personal data where such processing is necessary for compliance with applicable laws.

Where we process personal data based on your consent, you may withdraw your consent at any time.

You do not have to provide us with any data to access and use the website. However, you must provide us with your name and email address when using some of our services, such as signing up for our newsletter. The consequence of not providing your name and email address is that we will not be able to provide all of our services to you.

2.0 Your rights under the GDPR and UK GDPR

If you are located in the EU or the UK, your rights in relation to your personal data include:

- **right of access** - if you ask us, we will confirm whether we are processing your personal data and provide you with a copy of that personal data.
- **right to rectification** - if the personal data we hold about you is inaccurate or incomplete, you have the right to have it rectified or completed. We will take reasonable steps to ensure inaccurate personal data is rectified. If we have shared your personal data with any third parties, we will tell them about the rectification where possible.
- **right to erasure** - we delete your personal data when it is no longer needed for the purposes for which you provided it. You may request that we delete your personal data and we will do so if deletion does not contravene any applicable laws. If we have shared your personal data with any third parties, we will take reasonable steps to inform those third parties that they must delete such personal data.
- **right to withdraw consent** - if the basis of our processing of your personal data is consent, you can withdraw that consent at any time.
- **right to restrict processing** - you may request that we restrict or block the processing of your personal data in certain circumstances. If we have shared your personal data with third parties, we will tell them about this request where possible.
- **right to object to processing** - you may request that we stop processing your personal data at any time and we will do so to the extent required by the GDPR and/or UK GDPR (as applicable).
- **rights related to automated decision making, including profiling** – you have a right to not be subject to a decision based solely on automated processing including profiling, which produces legal effects concerning you or similarly significantly affects you, except where such automated decision making is necessary for entering into, or the performance of, a contract with you, is authorised by applicable laws or is based on your explicit consent. As at the date of this GDPR Addendum, Vigilance does not undertake any automated decision making or profiling using the Account and Marketing Data.
- **right to data portability** - you may obtain your personal data from us that you have consented to give us or that is necessary to perform a contract with you. We will provide this personal data in a commonly used, machine-readable and interoperable format to enable data portability to another data controller. Where technically feasible, and at your request, we will transmit your personal data directly to another data controller.
- **the right to complain to a supervisory authority** - you can report any concerns you have about our privacy practices to the relevant data protection supervisory authority.

Where personal data is processed for the purposes of direct marketing, you have the right to object to such processing, including profiling related to direct marketing.

If you would like to exercise any of your above rights, please contact us at admin@vigil.biz. If you are not satisfied by the way your query is dealt with by our data protection officer, you may refer your query to your local data protection supervisory authority.

3.0 Children

We do not intend to collect personal data from children aged under 16. If you have reason to believe that a child under the age of 16 has provided personal data to us through our website and/or by using our services, please contact our Privacy Officer.

4.0 International transfer of data

If you are located in the EU, the Account and Marketing Data we collect through the Website and/or the provision of the Web Services may be transferred to, and stored in, a country operating outside the European Economic Area (**EEA**). Under the GDPR, the transfer of personal data to a country outside the EEA may take place where the European Commission has decided that the country ensures an adequate level of protection. In the absence of an adequacy decision, we may transfer personal data provided appropriate safeguards are in place.

If you are located in the UK, the Account and Marketing Data we collect through the Website and/or the provision of the Web Services may be transferred outside of the UK. Under the UK GDPR, the transfer of personal information to a country outside the UK may take place where the European Commission (as at 31 December 2020) or the UK government has decided that the country ensures an adequate level of protection. In the absence of an adequacy decision, we may transfer personal information if other appropriate safeguards are in place.

Some of the Account and Marketing Data we collect is processed by third party data processors in other countries, including Australia. Where Account and Marketing Data is transferred outside the EEA or UK, it will only be transferred to countries or specified sectors within a country that have been identified as providing adequate protection for EU/UK data (e.g. to New Zealand), or to a third party where we have approved transfer mechanisms in place to protect your personal data (e.g. by entering into the European Commission's Standard Contractual Clauses or the UK's IDT Agreement or International Data Transfer Addendum to the European Commission's Standard Contractual Clauses). For further information, please contact us using the details set out above.

5.0 Data Retention policy

Account and Marketing Data that we collect and process will not be kept longer than necessary for the purposes for which it is collected, or for the duration required for compliance with applicable law, whichever is longer.