Privacy Notice

About this Privacy Statement

This Privacy Notice applies to Navigate Global Payments Pty Limited (NGP, us, we, our) (ABN 75 615 699 888; AFSL 502711) and aims to explain in a simple and transparent way what personal data we gather about you and how we process it. It applies to the following NGP people:

- All past, present and prospective NGP customers. We are legally obliged to retain personal data about you, also for a certain period once the relationship has ended, in compliance with 'know your customer' regulations.
- Anyone involved in any transaction with our firm, whether it's in your personal capacity or as a representative of a legal entity (for example, a company manager, agent, legal representative, operational staff, etc.).
- Non-NGP customers such as payees or the contact persons of corporate clients.

Additionally, agencies and organisations regulated under the Australian ***Privacy Act 1988*** **('Privacy Act')** are required to notify affected individuals and the Office of the Australian Information Commissioner **(OAIC)** when a data breach is likely to result in serious harm to individuals whose personal information was breached.

The Notifiable Data Breaches **('NDB')** scheme applies to all agencies and organisations with existing personal information security obligations under the Privacy Act. It was established by the passage of the *Privacy Amendment (Notifiable Data Breaches) Act 2017.*

'Personal data' refers to any information that tells us something about you or that we can link to you. This includes your name, address, date of birth, account number, IP address or information about payments you've made from your account. By 'processing' we mean everything NGP can do with this data such as collecting, recording, storing, amending, organising, using, disclosing, transferring or deleting.

Examples of when you share personal data with us are when you become a customer, register with or use our online services, complete an online form, sign a contract, use our products and services or contact us through one of our channels.

We also use data that is legally available from public sources such as debtor registers, land registers, commercial registers, registers of association and the media, or is legitimately provided to NGP or third parties such as our customers, credit agencies or government departments.

Social Media

Our Social Media Terms of Use apply to your use of NGP's social media sites or facilities. If you engage with us on any of our social media channels, you agree to be bound by these terms.

The NGP Privacy Policy contains further information about how we manage your personal data (also called 'personal information') and your rights in relation to accessing, correcting your personal data or making a complaint in relation to how we manage your personal data. The Privacy Policy and our Social

Media Terms of Use can be found https://www.navigategp.com.au/

2. The types of data we collect about you

The personal data we may collect includes:

Identification data, such as your name, surname, date and place of birth, ID number and the IP address of your PC or mobile device.

Contact details, such as your mobile phone number, telephone number, email address and residential address.

Transaction data, such as your account number, and transactional information related to your account.

Financial data, such as invoices, credit notes, payslips, payment behaviour, the value of your property or other assets, your credit history, credit capacity, your previous or current insurance, financial products you have with NGP, whether you are registered with a credit register, payment arrears and information on your income.

Online behaviour and preferences data, such as the server or IP address of your mobile device or computer, the date and time of pages you visit on NGP websites and apps, documents downloaded, the site you visited prior to visiting our website, the browser you are using NGP to access our resources, if you have visited our website before and tracking NGP user preferences.

Data about your interests and needs that you share with us, for example when you contact NGP or fill in an online survey.

Audio-visual data, such as recordings of phone calls to NGP.

Sensitive data

We do not record sensitive data at NGP relating to your health, ethnicity, religious or political beliefs, or criminal record unless it is strictly necessary, or under the compulsion of law. When we do, it is limited to specific circumstances, for example, if you instruct us to pay a membership fee to a political party.

With your explicit consent or if required or allowed by law, we may collect your genetic or biometric data (your fingerprint, voice or facial features) which may be used to verify your identity or use it as an extra means of security in apps when you choose for such authentication to authorise transactions.

3. What we do with your personal data

We only use your personal data for legitimate business reasons, and to comply with our legal, as well as our regulatory obligations.

Administration. When you open an NGP account we are legally obliged to collect personal data that verifies your identity (such as a copy of your ID card or passport) and to assess whether we can accept you as a customer. We also need to know your address or phone number to contact you.

Product and service delivery. We use information about you to assess whether you are eligible for certain products and services and to meet our contractual obligations to you. If you provide information that is incomplete or inaccurate, we may not be able to provide the financial product or service or information to you.

Managing NGP customer relationships. We may ask you for feedback about our products and services

and share this with certain members of our staff to improve our service and customer experience. We might also use notes from conversations we have with you online, by telephone or in person to customise products and services for you.

Credit risk and behaviour analysis. To assess your ability to pay an amount, for example, a margin call, we may apply specific statistical risk models based on your personal data.

Cookies. We may use data collection devices such as 'cookies' in conjunction with our website. Cookies are commonly used on the internet. They are a small file placed onto a computer by a server. A cookie can later be identified by a server. We may use both 'persistent' and 'session cookies'. We may (or our marketing company may) evaluate the cookie information collected to measure the effectiveness of our advertising and how visitors use our site.

The information we collect through cookies may be combined with previous cookies collected information and other personal information you have provided us, allowing us to identify users at an individual level, their behaviours, activity and needs. Where our marketing company manages the information coming from our site on our behalf, we control how that data may and may not be used.

We may use cookies for various purposes such as:

- to provide you with better and more customised service and a more effective website
- collecting anonymous statistical information on things such as how many visitors our sites receive, how those visitors use the sites and where they came from.

Personalised marketing. We may send you letters, emails, or text messages offering you a product or service based on your personal circumstances or show you such an offer when you log in to our website or mobile apps. You may unsubscribe from such personalised offers. You have the right, not to consent or to object to personalised direct marketing NGP or commercial activities, including NGP profiling NGP related to these activities.

We may market our services to you through social media platforms using information you provide to us when you interact on our website or sign up for our services. Please contact us if you do not want to receive these sorts of adverts by email at marketing@navigategp.com.au

Providing you with the best-suited products and services. When you visit our website or call us, we **gather information** about you. We **analyse** this information to identify your **potential needs** and assess the suitability of products or services. For example, we may suggest, although do not provide financial advice on investment opportunities suited to your profile. We analyse your **payment behaviour**, such as large amounts entering NGP or leaving your NGP account. We assess your needs in relation to **key moments** when a specific financial product or service may be relevant for you based on previous interest. We assess your **interests** based on simulations you participate in on our website.

Improving NGP and developing NGP products and services. Analysing NGP how you use our products and services helps us understand more about you and shows us where we can improve.

For instance,

- When you open an account, we may measure the time it takes until your first transaction to understand how quickly you are able to use your account, and we can use this information to improve our customer on boarding, and overall customer experience.

- We analyse data on transactions between you and our corporate customers to offer information services to our corporate customers or provide them advice on how they can make better use of NGP's products and services. When NGP processes personal data for this purpose, aggregated data may be made available to the corporate customer. A corporate customer cannot identify you from these aggregated data.
- We analyse the results of our marketing NGP activities to measure their effectiveness and the relevance of our campaigns.
- We may use your data to send you personalised offers by post, email or on our website or mobile apps. You have the right to object at any time to personalised direct marketing NGP or commercial activities, including NGP profiling related to these activities.

Preventing NGP and detecting NGP fraud and data security. We have a duty to protect your personal data and to prevent, detect and contain data breaches. This includes information we are obliged to collect about you, for example to comply with regulations against money laundering, terrorism financing and tax fraud.

- We may process your personal data to **protect you and your assets** from fraudulent activities, for example if you are the victim of identity theft, if your personal data was disclosed or if you are hacked.
- We may use certain information about you for profiling (e.g. name, account number, age, nationality, IP address, etc.) to quickly and efficiently detect a particular crime and the person behind it.
- We use contact and security data (such as card readers or passwords) to secure transactions and communications made via remote channels. We could use this data to alert you.

Internal and external reporting. We process your data for our NGP operations and to help our management make better decisions about our operations and services. We also process your data to comply with a range of legal obligations and statutory requirements (anti-money laundering legislation and tax legislation, for example).

Data that we process for any other reason is anonymised or we remove as much of the personal information as possible.

4. Who we share your data with and why

To be able to offer you the best possible services and remain competitive in our business, we may share certain data internally and outside of NGP. This includes:

NGP

We transfer data across NGP for operational, regulatory or reporting purposes, for example to screen new customers, comply with certain laws, secure IT systems, analyse our portfolio or provide certain services (see section 'What we do with your personal data' for the full list). We may also transfer data to centralised storage systems or to process it for more efficiency. All internal data transfers are in line with our Data Protection Policy.

Independent agents

We may share information with independent agents who act on our behalf. These agents are registered in line with local legislation and operate with due permission of regulatory bodies in the relevant terms and conditions for your NGP product.

Government authorities

To comply with our regulatory obligations, we may disclose data to the relevant authorities, for example to counter terrorism and prevent money laundering. In some cases, we are **obliged by law** to share your data with external parties, including:

Public authorities, regulators and **supervisory bodies** such as the central banks of the countries where we operate.

Tax authorities may require us to report your assets (e.g. balances on deposit, payment or savings accounts or holdings in an investment account). We may process your social security number for this.

Judicial/investigative authorities such as the police, public prosecutors, courts and arbitration/mediation bodies on their express and legal request.

Lawyers, for example, in case of bankruptcy, **notaries,** for example, **trustees** who take care of other parties' interests, and **company auditors.**

Financial institutions

To process payments, we may have to share information about you with the other bank, such as your name and account number. We also share information with financial sector specialists who assist us with financial services like:

- exchange secure financial transaction messages
- payments and credit transactions worldwide
- processing electronic transactions worldwide
- settling domestic and cross-border security transactions and payment transactions.

Sometimes we share information with banks or financial institutions in other countries, for example when you make or receive a foreign payment.

Service providers

When we use other service providers, we only share personal data that is required for a particular assignment. Service providers support us with activities like:

- performing certain services and operations (including to conduct identification verification, name screening and other checks, which help us to comply with our regulatory obligations and manage our regulatory risks);
- designing and maintenance of internet-based tools and applications;
- marketing activities or events and managing customer communications;
- preparing reports and statistics, printing materials and designing products; and
- placing advertisements on apps, websites and social media.

5. Credit-related personal data

Where we collect your personal data and we disclose that personal data to a credit reporting body,

we're required by law to notify you of certain matters, which are set out below. If you want us to provide you with a hard copy of this information, then please contact us.

Which credit reporting bodies does NGP deal with?

We primarily deal with, and report certain credit-related personal data to, Creditor Watch which is major credit reporting bodies in Australia.

You can contact:

Creditor Watch by:

One of the methods specified at https://creditorwatch.com.au/contact/; or

Calling CreditorWatch on 1300 50 13 12.

Collection, use and disclosure of your credit-related personal data

Creditor Watch may include your credit-related personal data that we provide to it in credit reports to other credit providers to assist those credit providers to assess your credit worthiness.

If you fail to meet your payment obligations in relation to any margin you have with us or if we believe that you have committed a serious credit infringement, we may be entitled to disclose this to Creditor Watch.

You can find out further detail about how we manage your credit-related personal data in our Privacy Policy, including in relation to access and correcting your credit-related personal data and making complaints.

Creditor Watch policy on how it handles credit-related personal data can be found on its website at https://creditorwatch.com.au/features/enterprise/enhanced-credit-reporting/ and its privacy policy at https://creditorwatch.com.au/privacy/?customer=no.

Pre-screening Assessments

Under the Privacy Act, credit reporting bodies are prohibited from using or disclosing credit reporting information that they hold about you for the purposes of direct marketing. Subject to a number of restrictions, this general prohibition does not apply to the use of this information by the credit reporting body for the purpose of assessing whether you are eligible to direct marketing by credit providers.

This use of the information in this way is known as a "pre-screening assessment". The Privacy Act allows you to request a credit reporting body that holds credit information about you to not use that information for the purposes of a pre-screening assessment. The credit reporting body cannot charge you for making, or carrying out, the request.

Fraud - "ban period"

The Privacy Act gives you certain mechanisms to deal with fraud, including identity fraud.

If you believe on reasonable grounds that you have been, or are likely to be, the victim of fraud then you can ask Creditor Watch (or any other credit reporting body that holds information about you) not to use or disclose your credit reporting information during a "ban period".

The "ban period" is a period of 21 days starting on the day that you make the request, which can be

extended on your request if the credit reporting body believes on reasonable grounds that you have been, or are likely to be, the victim of fraud.

The credit reporting body cannot charge you for making, or carrying out, the request.

6. Your rights and how we respect them

We respect your rights as a customer to how your personal data is used. These rights include:

Right to access information

You have the right to ask us for an overview of your personal data that we process.

Right to rectification

If your personal data is incorrect, you have the right to ask us to rectify it. If we shared data about you with a third party that is later corrected, we will also notify that party.

Right to complain

Should you not be satisfied with the way we have responded to your concerns you have the right to submit a complaint to us.

We will attempt to resolve your complaint within 5 days or make a decision about your complaint and write to you to explain our decision within 45 days of receiving your complaint. If your complaint is not satisfactorily resolved by this time, you may access an external dispute resolution service or apply to the OAIC to have the complaint heard and determined. When we write to you about our decision, we will explain how you may access an external dispute resolution scheme or make a complaint to the OAIC.

The Privacy Commissioner can be contacted on the following details:

Visit www.oaic.gov.au

Email enquiries@oaic.gov.au

Call the Privacy Hotline: 1300 363 992

Write to: Office of the Australian Information Commissioner GPO Box 5218 Sydney NSW 2001

Right to anonymity or to use a pseudonym

You have the option of dealing with us anonymously or using a pseudonym in some cases (for example when you make inquiries about our products or services). However, we will need to know and verify who you are, under regulatory requirements, or as compelled by law before we can provide you with our financial products and services.

Exercising your rights

If you want to exercise your rights or submit a complaint, please contact us. There is a list of contact details for the NGP office is at the end of this Privacy Statement.

We aim to respond to your request as quickly as possible. Should we require more time to complete

your request, we will let you know how much longer we need and provide reasons for the delay.

In certain cases, we may deny your request. If it's legally permitted, we will let you know in writing why we denied it and we will let you know how you can make a complaint about the refusal. If relevant in the case of an access request, we will also attempt to find alternative means for you to access the information you are seeking.

7. Your Consent is Important

We may require your consent to use and/or disclose your information in particular ways. We may need to use your information for a purpose that is not related to the purpose for which we collected your information in the first place. Depending on the circumstances, this consent may be express (for example, you expressly agree to the specific use of your information by ticking a box) or implied by some action you take or do not take (for example, your agreement is implied by the fact that you have agreed to your product terms and conditions which contains information about the use or disclosure).

By providing us or your intermediary with your information, you consent to our use of this information and where relevant for the purposes, you consent to our disclosure of your Personal Information, including your Sensitive Information, to your intermediary, affiliates of NGP, our service providers, our business partners, medical and health practitioners, your employer, policy owners, government offices and agencies, regulators, law enforcement bodies, and as required by law within Australia or overseas. These laws generally include, but are not limited to, *the Anti-Money Laundering and Counter-Terrorism Financing Act 2006, Personal Property Securities Act 2009, Corporations Act 2001, Insurance Contracts Act 1984, Autonomous Sanctions Act 2011, Income Tax Assessment Act 1997, Income Tax Assessment Act 1936, Income Tax Regulations 1936, Tax Administration Act 1953, Tax Administration Regulations 1976, A new Tax System (Goods and Services Tax) Act 1999; FATCA and CRS Acts and the Australian Securities and Investments Commission Act 2001* as those laws are amended, and includes any associated regulations. From time to time other Acts may require, or authorise us to collect your personal information

8. Your duty to provide data

There is certain information that we must know about you so that we can commence execute and fulfil our associated contractual duties. There is also information that we are legally obliged to collect. Without this data, the regulatory authorities, for example, AUSTRAC, will prevent NGP from opening an account for you or perform certain activities.

If you do not provide us with the information requested, we will generally not be able to provide you with our products or services.

9. How we protect your personal data

We apply an internal framework of policies and standards across all our business to keep your data safe. These policies and standards are periodically updated to keep them in line with regulations and market developments. More specifically and in accordance with the law, we take appropriate technical and organisational measures (policies and procedures, IT security etc.) to ensure the confidentiality and integrity of your personal data and the way it's processed within Australia and equivalent jurisdictions. Navigate may also disclose your information to companies that are part of the Navigate Corporate Family which may be located overseas.

As transmission of data on the internet can never be ultimately secure, we do not and cannot guarantee security of information collected electronically or transmitted; however, we take all necessary steps to provide the best security available, and you acknowledge you are submitting information to us at your own risk.

In addition, NGP employees are subject to confidentiality and may not disclose your personal data unlawfully or unnecessarily.

10. What you can do to help us keep your data safe

We do our utmost to protect your data, but there are certain things you can do too:

Install anti-virus software, anti-spyware software and a firewall. Keep them updated.

Do not leave equipment and tokens (e.g. card) unattended.

Log off from your online account when you are not using it.

Keep your passwords strictly confidential and use strong passwords, i.e. avoid obvious combinations of letters and figures.

Be alert online and learn how to spot unusual activity, such as a new website address or phishing emails requesting personal information.

11. How long we keep your personal data

We are only allowed to keep your personal data for as long as it's still necessary for the purpose we initially required it. After this we look for feasible solutions, like archiving it.

Destroy or de-identify personal information

NGP takes reasonable steps to destroy or de-identify the personal information it holds once it is no longer needed for any purpose for which it may be used or disclosed under the APPs. **This requirement does not apply where the personal information is contained in a 'Commonwealth record' or where the entity is required by law or a court/tribunal order to retain the personal information.**

If we no longer require your personal information for a purpose, for example, to manage your financial product or provide you with a financial service, then we will take reasonable steps to securely destroy it or permanently remove all identifying features from that information. This obligation is subject to any legal requirements to keep personal information for a certain period of time – in most cases, personal information records are kept for a period of 7 years after their creation or 7 years after an account is closed.

Fostering a privacy and security aware culture

Our privacy and security governance arrangements include appropriate training, resourcing and management focus to foster a privacy and security aware culture among NGP staff. Personal information security is an integrated component of our entire business and not left to the compliance or ICT area alone. This has the active support of, and promotion by NGP's Board..

Appropriate training is provided in mitigating these issues and making staff aware of common personal information security threats (see 'Personnel security and training' section below).

12.Personnel security and training

At NGP, all our colleagues are aware of their privacy and security obligations (including senior management). Human error can be a contributing cause to data breaches and undermine otherwise robust security practices. Notwithstanding, NGP staff undergo training and are kept up to date on developments to Australia's privacy laws and regulations, to ensure your personal information is optimally protected.

13. Contact us

If you want to know more about NGP's data policies and how we use your personal data or if you have any questions about how we use your personal data, you can contact us by:

Emailing: compliance@navigategp.com.au

Writing to:

NGP Compliance Head

Suite 5.01, Level 5

140 Arthur Street

North Sydney; NSW 2060

14. Scope of this Privacy Statement

This is the Privacy Statement of NGP (Australia). We may amend this Privacy Statement to remain compliant with any changes in law and/or to reflect how our business processes personal data. This version was revised on 29th September 2020. The most recent version is available at www.navigategp.com.au. Our website has links to other websites, which are provided for your convenience. Please note that we are not responsible for the Privacy Policies of those websites.