Rabobank Privacy **Policy**

Rabobank

At Rabobank, we have a deep understanding of farming life and are passionate about supporting our farming clients to grow. For our online clients, making their savings grow also means helping our farmers to grow the food we all put on our plates. That's something that they can feel good about!

We believe in 'old fashioned' personal service and, as part of that service, you share and trust us with, all kinds of Personal data. We are committed to honouring your trust in us because we take your privacy seriously.

The purpose of this Privacy Policy is to assist your understanding of our privacy practices and for you to make informed decisions about your Personal data. To achieve this, we have included examples of the types of processing activities we generally carry out.

Key concepts to assist your reading of this document:

When we use the terms RAG entity, we, our, us; it means each member of the Rabobank Group based in Australia, being:

- Coöperatieve Rabobank U.A. (Australia Branch) (ABN 70 003 917 655)
- Rabobank Australia Limited (ABN 50 001 621 129)
- Rabo Australia Limited (ABN 39 060 452 217)
- Rabo Equipment Finance Limited (ABN 37 072 771 147)
- Soft Commodity Trading Pty Limited (ABN 45 085 595 562)
- GrainCorp Pools Pty Limited (ABN 45 095 759 890)

Each member within the Rabobank Australia Group (RAG) that collects and processes your Personal data, does so in accordance with its legal obligations under the Privacy Act 1988.

Personal data

Personal data means any data that relates to an identified person or an individual who can be reasonably identified. Personal data can also include an opinion, whether the data or opinion is true or not; or recorded in a material form or not. Common examples include your name and address, email, date of birth and also data such as your income.

Additionally, data relating to individuals operating as a sole trader, a commercial partnership or professional partnership is also considered Personal data. Data relating to a legal entity (e.g. a company) is not Personal data, but data relating to a legal entity's directors, contact person or representative does count as Personal data.

Processing of Personal data

Processing of Personal data means any operation that is performed on Personal data. This includes the collection, recording, storage, organisation, alteration, use, transfer, disclosure (including the granting of remote access), transmission or deleting of Personal data.

Do we process your Personal data?

We process Personal data if we have or have had a business relationship with you. We also process Personal data if we have had contact with you and/or your representatives or you wish to have a business relationship with us.

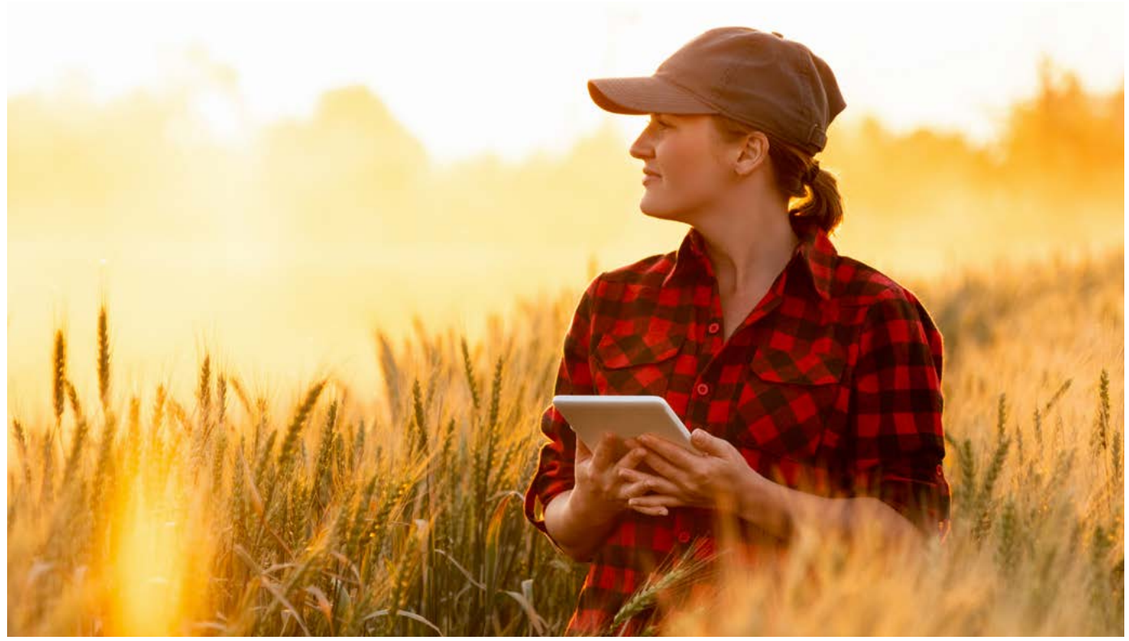
We process Personal data of:

- Clients and their authorised representatives (including legal advisers, financial advisers, executors, administrators, trustees and attorneys acting under a power of attorney);
- People in their capacity as security providers, (ultimate) beneficial owners and guarantors;
- People who show an interest in us or our products and services and have left their Personal data with us (e.g. if you have visited our website or walked into a local branch); and
- People who are connected in another way with a business or organisation with which we have, or have had a business relationship (e.g. employees, executive directors or, contacts of service providers).

What kinds of Personal data do we process?

Types of data	What kinds of data might be involved?	Examples of how we use the data
Data that allows an individual to be identified directly or indirectly	Name, address, telephone number, email address, data provided in your identity document such as driver's license number or passport number.	• For identification purposes in compliance with laws; • To draw up an agreement; or • To contact you
Location data	Data that shows where you are.	To find out where and when you used your debit card. We do this to combat fraud. For example, the data provided by the ATM using your debit card.
Data relating to or used for agreements	Data about your financial situation, the products you have, your investment profile and data used for obtaining finance, such as payslips and the value of your property.	To assess your application for a product or service. For example, if you have, or apply for, a loan with us, we want to assess your application for the loan.
Payment and transaction data	When a payment is made, data about the person you paid or who paid you, when the payment took place and what the balance in your account is.	• To execute a payment for you; • To be able to check whether the bank account number entered matches the name that is specified in a payment instruction; • To pass your data on to the other bank (if you make use of the Open Banking platform); • For your security and ours. For example, if a payment is made in Australia and in another country at the same time, we may be able to take measures; or • To identify financial difficulty early.
Sensitive Personal data and Tax File Numbers (TFNs)	Sensitive Personal data concerning your health, biometric data, data related to criminal convictions and offences, data which reveal your racial or ethnic origin or political opinions.	If you give your consent for this, we record information concerning your health for purposes such as: • Providing extra care and helping you to access your banking services when you are experiencing a vulnerability; • Reasons relating to financial hardship; or • If you want to use a modified security token to assist with a visual impairment In the context of combating terrorism, we are required to record information about your country of birth. We are also required to do this in connection with tax obligations. In addition, we record Sensitive Personal data in the context of payments, for example if you make a payment at a pharmacy or transfer money to a political party. TFNs will only be used as authorised by taxation, personal assistance or superannuation laws such as applying a TFN to your deposit account for withholding tax purposes.
Recorded calls, conversations with our employees, recordings of video chat, video surveillance, record of emails and social media	• Conversations we have with you by telephone and video sessions • Conversations we have with you in person that we record • Email and hard copy correspondence • Camera images and attendance records that we take in banking premises such as local branches • Comments, video, photographs, likes, public posts that you post on our social media pages	• We may use the recorded calls, emails and video conversations to combat fraud, fulfil legal obligations, monitor and improve the quality of our products and services, and train, coach and assess our employees; • Camera surveillance is used to combat and investigate fraud, to safeguard you and our employees and to monitor quality of the surveillance footage itself; or • We collect comments, videos, photographs, likes, public posts that you post on our social media pages in order to answer questions, share information that you may have requested and improve the quality of our products and services

Types of data	What kinds of data might be involved?	Examples of how we use the data
Data that tells us about the use of our website and the app	• Cookies • IP address • Data relating to the device on which you use our online services or our website • Data about browsing behaviour, browsing capabilities and preferences pages viewed, and browser type such as chrome or safari	• To understand your behaviour (e.g. webpages you have visited) and track your preferences on our website. For more information refer to our *Cookies page*. • To combat fraud; • To improve the functionality of our website; • For displaying targeted advertisements or banners; or • We use web analytics packages and our content management system to enable us to analyse data, learn about our visitors and measure the performance of our website and web content
Data we receive from other parties	• Data obtained from public registers (e.g. ASIC companies' register) or an individual's credit history or verification of identity from a Credit Reporting Body (e.g. Equifax) • Data obtained from other businesses to which you have given consent to share your data (e.g. other banks under Open Banking)	• We use this data to check whether you can be granted credit, or to check the value of a property; or • We may receive the Personal data of multiple directors or ultimate beneficial owners of a company from one representative within that company such as the CFO for the purposes of on boarding that company as a client
Data we share with other parties	• Financial data • Loan data • Data we provide to other parties that we engage to help us provide services • Data you have asked us to share with another party • Data we have to share with our regulators or enforcement agencies (e.g. Police)	• Common regulators include the Australian Prudential Regulation Authority (APRA), the Australian Securities and Investments Commission (ASIC), Australian Transaction Reports and Analysis Centre (AUSTRAC); • Other parties (such as marketing agencies) that process data on our behalf because they are involved in the provision of our services; • You may also ask us to share specific data with a third party, for example under the Open Banking regime; or • We many need to use or disclose your data in order to detect, prevent or investigate any suspected or actual fraud, crime, misconduct or unlawful activities. An example would include third parties that assist us with electronic verification of ID.
Data we require to combat fraud, to protect your security and ours, and to prevent money laundering and the financing of terrorism	• The data we keep in our internal and external registers, fraud detection systems, sanction lists, location data, transaction data, identity information, camera images, cookies, IP addresses • Data relating to the device on which you use our online services	• In order to comply with legal obligations and prevent you, the financial sector, RAG or our employees, we check whether you appear in our internal or external registers and whether your name appears in sanction lists; • We use location and transaction data in order to monitor payments to prevent fraud, money laundering and terrorist financing; or • We may use your IP addresses and device details to combat online fraud and scams



How do we collect your Personal data?

The collection of most Personal data will be directly from you and with your consent, which will usually be obtained at or around the time you contact us or take out a product or service with us. Examples include data when you enter into an agreement with us, data you enter on our website so we can contact you, and data arising from the services we provide in areas such as payments.

We may also receive your data from:

- Other financial institutions and enforcement agencies in the context of combating fraud, money laundering or terrorism financing;
- Suppliers or other parties we work with. For example, your credit history from a credit reporting body;
- Public sources like newspapers, public registers (e.g. ASIC companies' register), websites and open sources of social media; and
- Another party who, with your consent, can share data with us.

At or before the time or, if that is not practicable, as soon as practicable after, we collect Personal data about an individual, we will take reasonable steps in the circumstances to let that individual know we have their Personal data.

If you, your business or organisation transfers any Personal data concerning other people, employees, executive directors or ultimate beneficial owners to us, we expect you, your business or organisation to inform them about this. You can give this Privacy Policy to them so that they can learn how we deal with their Personal data.

What are Rabobank's legal bases and purposes for processing your Personal data?

To provide you with the best possible service, we need to know you well and develop our client insights about you. In order to do that, we collect and process your Personal data only where we have lawful grounds to do so and when we deem it reasonably necessary for one or more of our functions or activities. To assist your understanding, below are the common lawful grounds and purposes for which we may collect and process your Personal data.

In all cases, we will notify you of the lawful ground and the purpose for processing your Personal data.

Lawful grounds for processing your Personal data

We may process your Personal data on the following lawful grounds:

- Legal obligation: where we process your Personal data to comply with our legal obligations.
- Perform an agreement: where we process your Personal data to enter into an agreement or perform our obligation under our agreement with you.
- Consent: where you have provided your consent to us to process your Personal data.

In addition to the above common lawful grounds, we may also process your Personal data if we have a legitimate interest in doing so, and as long as the legitimate interest does not prejudice your right to privacy. We will only process your Personal data on the ground of legitimate interest if the other lawful grounds do not apply. Our legitimate interests include:

- Protecting our own financial position.
- Combatting fraud to prevent damage to us, but also the financial sector, and to protect yours and our security.
- Improving our business processes, taking measures in the context of company management and performing audits on our internal processes.
- Transferring loans, merging or taking over companies to remain a financially sound bank.
- Ensuring that our clients are financially healthy. For example, identifying at an early stage that you may have payment problems.
- We have an interest in direct marketing and we want to keep you informed of new or existing products that we believe fit you.

Purposes for processing your Personal data

To enter into a business relationship and agreement with you

We need to have your Personal data if you want to become a client, or if you want to use a new product or service or contact us.

- When you become a client, we establish your identity for all our products to comply with our legal obligations. As part of this, we may store copies of your identity documents.
- If you wish to become a client, or are already a client of ours, we will consult registers and warning systems of RAG (internal registers) and the financial sector (external registers). We also check that you are not on any national or international sanction lists.
- We assess whether the requested product or service is suitable for you. For example, we assess whether we can provide you with credit. When making this assessment, we also use data that we obtain from other parties, such as credit reporting bodies like Equifax.
- We use your financial information to assess whether we should provide you with a certain amount of credit. In some cases, we do this because we are required to do so under, for example, our responsible lending obligations under the National Consumer Credit Protection Act.
- If necessary, we will use a credit rating based in part from Personal data. For this we may use for example, your balance data or the number of times a debit is reversed. We can also see if you use your credit and how much you use. We may use a credit rating as part of our assessment when deciding whether or not to grant you credit, to calculate the price you have to pay in the case of business financing and to identify payment arrears early. The decision whether or not to grant you credit and to determine pricing is not fully automated. Also when identifying early payment arrears, automatic decision-making does not take place.

To perform agreements and carry out instructions

When you are a client of ours, we want to continue to provide personal service. We execute the instructions we receive from you and perform the agreements we have entered into with you. We process Personal data to achieve this purpose.

- If you make a payment through us, we transfer your data to another bank. The payee can also see and record your payment data. Both the person who issues the payment instruction and the beneficiary (payee) may enquire about specific data relating to the other party's account.
- We make recordings of telephone conversations, email messages, camera images and video chat sessions. The purposes for which this is done include proving that you issued a particular instruction. We may also do this to combat fraud, fulfil legal obligations, monitor and improve the quality of our products and services, and train, coach and assess our employees.
- If, for example, you are applying for a loan or you want to invest, then when assessing the application we can also include information about other products that you have with us e.g. a savings account. We can also take this information into account during the term of the provided service.
- We also provide you with information about the transactions in your bank account, or credit or financing, or, if you are at risk of falling behind on your payments, we will contact you to look for a solution.
- You may also ask us to disclose your personal data to a third party, in which case we will transfer your Personal data to that party.
- When a client passes away, we may need to obtain Personal data of an executor, administrator or next-of-kin in order to accept instructions in relation to the deceased estate.

To protect your security and integrity as well as the security and integrity of the bank and the financial sector

We collect and use your Personal data to protect you, the Bank and the security of the financial sector. We also do this for the purpose of preventing fraud, money laundering and the financing of terrorism.

i. Client Due Diligence

We check whether we can accept you as a client when we enter into a business relationship with you and during that business relationship. For example, your transaction data may cause the Bank to conduct an enhanced due diligence on your account(s) and relationship with the Bank.

If you do not provide the Bank with all of the required information, we may not be able to continue our Banking relationship with you.

ii. Internal and external registers and warning systems

If you seek to become a client, or are already a client of ours, we will consult our internal registers and warning systems and, additionally, external registers available within the financial sector.

In addition, public authorities send us lists of individuals, which we have to enter in our internal registers and warning systems. These are individuals with whom financial institutions must not do business, or to whom the financial sector must pay extra attention.

iii. Publicly accessible sources

We consult publicly accessible sources, such as public registers, newspapers, the internet and public profiles of your social media, in an effort to combat fraud, money laundering and terrorism financing and protect the bank.

iv. Fraud, Money Laundering and Terrorism Financing

We may perform analysis aimed at preventing fraud, money laundering and terrorism financing to assist in protecting you and the bank. For example, we may collect data in respect to your usual transaction behaviour in order to detect and reduce money laundering and terrorism financing. If the observed behaviour differs from your usual transactional behaviour or there are other

indicators, this may form grounds for suspending or blocking payments as well as restricting access to accounts. This may be done by fully automated means in given circumstances.

We make recordings of telephone and video conversations, email messages and camera images (at our branches), for example, and may document these recordings. We do this in the context of investigating fraud. We may also do this to fulfil legal obligations, monitor and improve the quality of our products and services, improve our assessment processes and train, coach and assess our employees.

To help develop and improve products and services

In order to provide you with the best possible service and to continue to innovate and develop as a bank, we are constantly improving our products and services. We do this for our clients, ourselves and other parties.

- We sometimes combine data sources, such as data on the products you receive from us and the balance in your account. We conduct benchmarking for our corporate clients, which provides these clients with additional information on how they perform in comparison to other businesses. The results of these studies relate to groups of clients, and never an individual client (this is known as aggregate data).
- We also process data when analysing your visit to our website. We do this with the aim of improving our website and the experience you have. We use cookies for this. For more information refer to our *Cookies page*.
- Analysing Personal data allows us to see how you use our products and services. We also use the results of this analysis to categorise clients into groups, for example based on age. With this we create client and interest profiles. In making this analysis we sometimes also use information that we have received from other parties, for example if we have received data from public sources such as the newspaper or the internet. You always have the right to object to this data processing.
- For this we might use models in which we can compare your situation with other clients on the basis of their characteristics. We may also make use of your transaction data, reversals or other data that can help prevent financial difficulty. If we foresee that you might get into financial difficulty then we are happy to help you. We can do this ourselves or by pointing out possible organisations that can help you organise your financial administration.
- We also carry out research in order to improve our products and services. For example, we may ask you to give your feedback to a product or to review a product. You are not required to cooperate in such surveys.
- We sometimes use other parties to process your Personal data for this purpose, for example in order to measure or ask you how we can improve our services. In that case, these other parties act on our instructions and in line to a contract with confidentiality obligations.

For account management, promotional and marketing purposes

We process your Personal data for account management, promotional and marketing purposes. In doing so, we use data we have directly obtained from you, such as payment data or information we have indirectly obtained via cookies, for example your activity on our website, as well information not obtained directly from you, including public registers and publicly available sources (such as the internet and social media).

- We may use your data to inform you about our product or service that might be of interest to you. We will not share your information with a third party in this context, unless you ask us and you give us permission.
- We also use the services of advertisers in order to display advertisements to a specific target group. We indicate which target group or type of profile our advertisement is intended for. The advertiser then displays the advertisement to the people who are in the target group or fulfil the profile. We never share Personal data relating to individual clients with such advertisers. We may collect your data together with providers of social network services if, for example, you post comments, videos, photos, likes and public messages on our social media company pages or post comments about us on a website or social network that we do not manage.
- We may also use this analysis to provide our clients with information for benchmarking purposes. If we use your data for this analysis or produce profiles, we will make sure that your data is de-identified to the greatest possible extent and that they are made only available to a few employees at the bank.

If you do not want your data to be used by us for the purpose of direct marketing or by post, email or telephone, you can let us know, refer to section 'What rights do you have to your Personal data?' of this policy for details or alternatively visit our *Individual Rights portal*.

Please note that from time to time, we may be legally obligated to contact you even if you have opted-out of direct marketing messages. These are known as service messages, for which you may be entitled to depending on your relationship with us.

To enter into and perform agreements with suppliers and other parties we work with

If you have contact with us in the context of a supplier arrangement or business partnership, we may process your Personal data, for example so that we can establish whether you are permitted to represent your business or whether we can give you access to our locations. Where necessary, we may consult internal and external registers and warning systems before we enter into our agreement and also while the agreement is in effect in the context of screening.

To comply with legal obligations

i. Legislation

We have to collect and analyse a large amount of data relating to you and sometimes transfer such information to government authorities under various national and international legislation and regulations that apply to us and other members of the Rabobank Group.

For example, we must comply with legislation designed to combat fraud, crime and terrorism, such as Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) and Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1), in order to be able to offer you financial products and services.

We are required to perform client due diligence and to conduct further inquiries if you hold specific assets or if an unusual transaction takes place in your account. If we spot an unusual transaction, we must notify the relevant law enforcement agency. Under this law, we have to establish who the ultimate beneficial owner is of a business or organisation with which we have a business relationship.

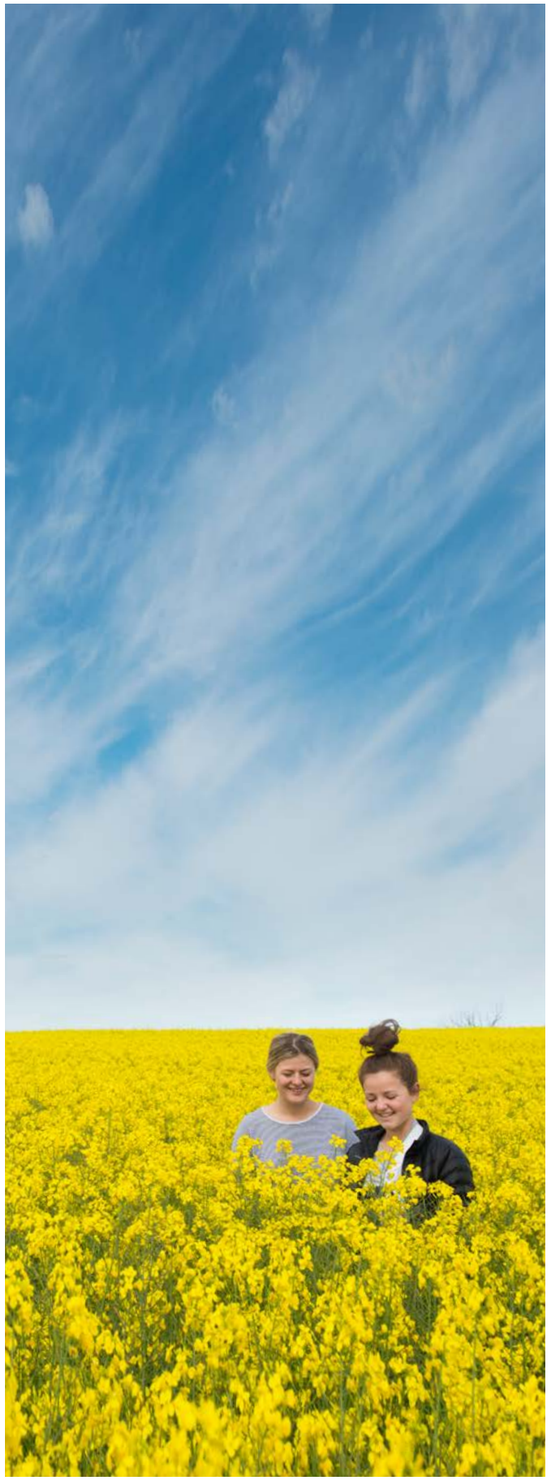
We may receive requests for data from regulators and authorities as well as organisations such as the intelligence services. If they do this, we are required by law to cooperate with the investigation and transfer data relating to you. We can also enter into partnerships with, for example, the police and the public prosecutor to combat (large-scale) fraud, money laundering and terrorist financing.

ii. Risk models

Australian regulations allow for us to produce risk models if you apply for a loan or credit or if you have received a loan or credit from us. This is so that we are able to determine which risks we are exposed to and the size of the buffer we need to maintain. We process your Personal data as part of this purpose.

We can also use these risk models before we offer you a credit. We may also use these models when determining the price for business financing, to prevent situations in which you are unable to repay your financing, or are unable to repay it on time. We may also use profiling and techniques for making decisions in partially automated manner.

These risk models may also predict how likely it is that you will fall behind on your payments. We can use the information they provide to prevent or deal more quickly with any payment



problems, for example in consultation with you. We will then process your Personal data for this purpose. We will do this for various reasons. These include performing our agreement with you and because we are required to do this by law.

iii. Providing data to the government

Legislation and regulations may require that we transfer data (analysed or otherwise) relating to you to a government institution, a tax authority or a regulator within or outside Australia.

iv. Making and documenting recordings

We make recordings of telephone conversations, email messages and video chat sessions to comply with legal obligations, for example in the context of investment services. We may also do this to fulfil legal obligations linked with record keeping, to monitor and improve the quality of our products and services, to combat and investigate fraud and to train, coach and assess employees.

To carry out business processes and for the purpose of management reports and internal management

i. Determining credit risk associated with loans and credit facilities

Lending involves credit risk. We have to determine what that risk is, so that we can calculate the security we need to maintain. In connection with this, we process Personal data relating to your loans and credit facilities.

ii. Audits and investigations

We also use your Personal data to perform our internal and external audits and investigations required of us as a bank. We also may engage with a third party to assist us in this process, however, a contractual arrangement will be in place to protect any Personal data shared.

iii. Improving our own business processes

We also use data to analyse and improve our business processes so that we can help you more effectively or make our processes more efficient, and to build management reports. We also have to validate the models we use. Where possible, we will de-identify or aggregate your data first.

How long do we keep your Personal data?

We do not keep your Personal data for longer than is necessary to fulfil the purposes for which we collected the data or the purposes for which data is reused. We have adopted a Record Keeping standard which specifies how long we keep data. We are required to keep some of your data for certain periods of time under law, such as the Corporations Act, the Anti-Money Laundering & Counter-Terrorism Financing Act, and the Financial Transaction Reports Act. When we no longer have a legal basis for using your data, we will delete, destroy or de-identify your Personal data.

In specific situations, we may keep the data for longer than we specify in our Record Keeping standard. We will do this if, for example, we are requested by authorities for data to assist in an investigation, or if you have submitted a complaint, or there are ongoing legal proceedings.

Do we also process Sensitive Personal data?

Sensitive Personal data includes data concerning health and genetic information, criminal record, biometric data and data which reveals racial or ethnic origin information. Our collection of Sensitive Personal data is restricted to circumstances where we have obtained your express consent and to certain other permitted situations. We will also make sure that the data is relevant to one or more of our business purposes prior to collection. For example, if you ask us to record that you are unable to make your regular payment due to recent medical expenses, we will ask for your consent to record this information, so that we may assist you with keeping up to date with your payments going forward.

We may use biometric data, such as your fingerprint or a face scan, for authentication purposes such as access to our mobile banking application.

We access internal and external registers and warning systems for the financial sector and may process data about criminal convictions in this context. The purpose of these registers and warning systems is to protect our interests and that of financial institutions and their clients, for example by detecting and recording cases of fraud.

We may also, indirectly process Sensitive Personal data when processing payments, for example if you make a payment at a pharmacy or transfer money to a political party. Such data may be used to gather information about your health or your political inclinations.

We will only process the information if this is necessary so that we can provide our services. If you have given us consent to record Sensitive Personal data, you may withdraw that consent at any time. Please visit our *Individual Rights Portal* for more information on the rights available to you.

Do we use automated decision-making including profiling?

Automated decisions are decisions that are made about you solely by computers without any human intervention. If these decisions have legal consequences for you, then we are not allowed to use automated-decision making. If automated-decision making is necessary to enter into or perform a contract, is authorised by law, or if you give us your explicit consent, then you have the right to consult someone at the bank and to express your point of view and contest the decision.

In the following situations we might use automated decision making that might affect you:

- When you apply for credit from us, we may use a credit rating for you. This rating is used by authorised staff to determine whether or not you might receive credit. The decision to provide you credit is not fully automated.
- When a payment is not in line with your usual pattern of spending, we might use automated decision making and stop the payment (temporarily). We do this to avoid fraud on your account. If we stop the payment, we will inform you as quickly as possible.

Who has access to your Personal data?

Within RAG, your Personal data can be accessed only by individuals who need to have access, owing to their position. All of these people are bound by a duty of confidentiality. We have practices and policies in place to provide a high level of security to protect Personal data.

We take all reasonable precautions to protect your Personal data by:

- Regularly assessing the risk of misuse, interference, loss and unauthorised access to Personal data we hold from both internal and external threats;
- Taking action to address any identified risks such as the use of dedicated secure networks or encryption when we send Personal data electronically or the implementation of physical security measures to our locations;
- Conducting regular reviews and audits to assess the quality of the actions we have implemented.

Do we use Personal data for any other purposes?

If we want to use Personal data for any purpose other than the purpose for which it was obtained, we may do this as long as the two purposes are closely related and you would reasonably expect us to use the Personal data for this purpose. We may also be required to do so in compliance with laws.

If there is not a sufficiently strong connection between the purpose for which we obtained the data and the new purpose, we will ask you to give your consent if we still want to use this data. You can always withdraw your consent. Please visit our *Individual Rights Portal* or section 'What rights do you have to your Personal data?' of this Policy for more information on the rights available to you.

Do we disclose your Personal data to other parties and to overseas countries?

Other parties

Depending on the product or service we provide to you, we may disclose your Personal data to:

- Brokers, agents and intermediaries who refer your business to us;

- Valuers and insurers if property is being provided as security for a loan from us;
- Other product and service providers for whom we act, so that they can provide you with the product or service you seek or have expressed interest in;
- A person acting on your behalf, including your financial adviser, solicitor, settlement agent, accountant, executor, trustee, guardian or attorney;
- Other financial institutions and organisation at their request if you seek credit from them;
- Agents and other persons who assist us to dispose of property or equipment given as security for a loan;
- Other owners, borrowers and guarantors and their respective directors, trustees and beneficiaries (if any) related to any account you have with us, including an application for an account;
- Any party pursuant to any domestic or international law or regulatory requirement, including a court or tribunal or an overseas government instrumentality or regulatory body which has jurisdiction over any member of the Rabobank Group (including those outside Australia);
- Members of the Rabobank Group (including those outside Australia) and their associated entities. An example of an associated entity is Achmea Schadeverzekeringen N.V;
- To a law enforcement body if reasonably necessary to assist with the enforcement of any law; and
- If you have been referred to us, the person who made the referral.

Personal data will only be disclosed to third parties not identified in this document if you have consented or if you would reasonably expect us to disclose data of that kind to those third parties and the purpose of that disclosure is related to the primary purpose for which the data was collected.

Outsourcing

We may disclose your Personal data to third party service providers when we outsource certain tasks and operations, including mailing, printing, direct marketing and data technology services.

Where we disclose Personal data to an external outsource provider, we enter into contracts with confidentiality arrangements in place, so that these providers meet our privacy standards in protecting your Personal data, comply with the Australian Privacy Act and use or disclose Personal data only for the specific service we ask them to perform or the product/service we ask them to provide.

Securitisation

Securitisation involves the pooling and selling of assets such as loans to a special purpose vehicle. To undertake this process, we may disclose Personal data to any person to whom our rights in pooled assets are to pass or proposed to pass and to any ratings agencies, trustees, investors and advisers involved in the transaction.

Exchanging data with credit reporting bodies

We need to be in a good position to decide whether or not you are likely to repay your loan when you apply to us for credit. To do this we may consider your current financial position and on your credit history. This means that we will consider the data you give us in your application and may make enquiries with and obtain further data from a credit reporting body and other credit providers you have borrowed from previously.

We may collect, hold and disclose your credit-related data as reasonably necessary for our business purposes and as permitted by law such as to make decisions as to whether to provide you with credit, evaluate your credit worthiness, manage credit provided to you and participate in the credit reporting system and providing data to credit reporting bodies as permitted by Part IIIA of the Privacy Act. Where the Privacy Act applies, we can only give your credit-related data to a credit reporting body if we have told you first that we will do so and we can only obtain data about you from a credit reporting body if we have your consent.

For further information relating to how we deal with credit-related data obtained from a credit reporting body, you can refer to our *Credit Reporting Policy*.

Disclosure of Personal data to overseas recipients

We may disclose Personal data to overseas recipients, including to:

- Other members of the Rabobank Group for consolidated reporting and compliance purposes (including regulatory and legislative requirements of any member of the group), the effective administration and management of facilities, storage of data and for marketing;
- Entities which provide services required to supply you with your products and services; and
- Government or regulatory bodies (including in The Netherlands and the European Union) which have authority over any members of the Rabobank Group.

We also disclose Personal data to entities located overseas which provide us with services required for storage and hosting purposes and also to supply products and services to our clients. Countries to which your Personal data may be disclosed are The Netherlands, the United Kingdom, Belgium, Luxembourg, Singapore, Hong Kong, the United States, New Zealand, India and Canada.

Where we disclose Personal data overseas we take reasonable steps to certify the recipient meets our privacy standards in protecting your Personal data and complies with the Australian Privacy Act. We do so by entering into contracts with confidentiality arrangements in place and to confirm that they use or disclose Personal data only for the specific service we ask them to perform or the product/service we ask them to provide.

What rights do you have to your Personal data?

Right of access to and correction of Personal data

You may ask us whether we process Personal data relating to you, and if we do, which data this concerns. In that case, we can provide you with access to the Personal data processed by us that relates to you. If you believe your Personal data has been processed incorrectly or incompletely, you may request that we change or supplement the data (correction).

Right to deletion of Personal data

You may request that we delete Personal data concerning yourself that we have recorded, for example if you object to the processing of your Personal data. We don't always have to do that; and sometimes we are not allowed to do this either. For example, if we still have to store your data due to legal obligations relating to record keeping. We will inform you if this is the case.

Right to restriction of processing

You may request that we temporarily restrict the Personal data relating to you that we process. This means that we will temporarily process less Personal data relating to you.

Right to object to processing

If we process your data because we have a legitimate interest in doing so, for example if we make recordings of telephone calls but this is not required by law, you may object to this. In that case, we will reassess whether it is indeed the case that your data can no longer be used for that purpose. We will inform you of our decision, stating the reason. The operation of this right may impact the way we continue to provide you with products and services, we will inform you if this is the case so you may make an informed decision.

Right to object to direct marketing

You have the right to request that we stop using your data for direct marketing purposes. It may be the case that your objection only relates to being approached through a specific channel, for example if you no longer wish to be contacted by telephone but still want to receive our offerings per email. We will then take steps to make sure you are no longer contacted

through the relevant channel. As mentioned earlier in this Policy, we may be legally obligated to contact you even if you have opted-out of direct marketing messages. These are known as service messages, for which you may be entitled to depending on your relationship with us.

- For Rabobank Australia clients: If you wish to stop or change the channel in which we contact you, email us on *fm.au.maps@rabobank.com*
- For Rabobank Online Savings Australia clients: If you wish to stop receiving marketing emails from us, let us know at *www.rabobank.com.au/unsubscribe/* or contact our Client Services Unit on 1800 445 445.

How do you make a rights request?

To make a rights request to your Personal data please visit our *Individual Rights Portal*. You may also contact us through the channels described in the section below.

If you make an Individual Rights request, we will answer this within one month after we have received the request.

Do you have a complaint concerning the processing of your Personal data?

If you have a general concern or complaint about the processing of your personal data, we want to hear from you. In the first instance, please contact us by using the details below:

Farm Business (Rural Banking) clients

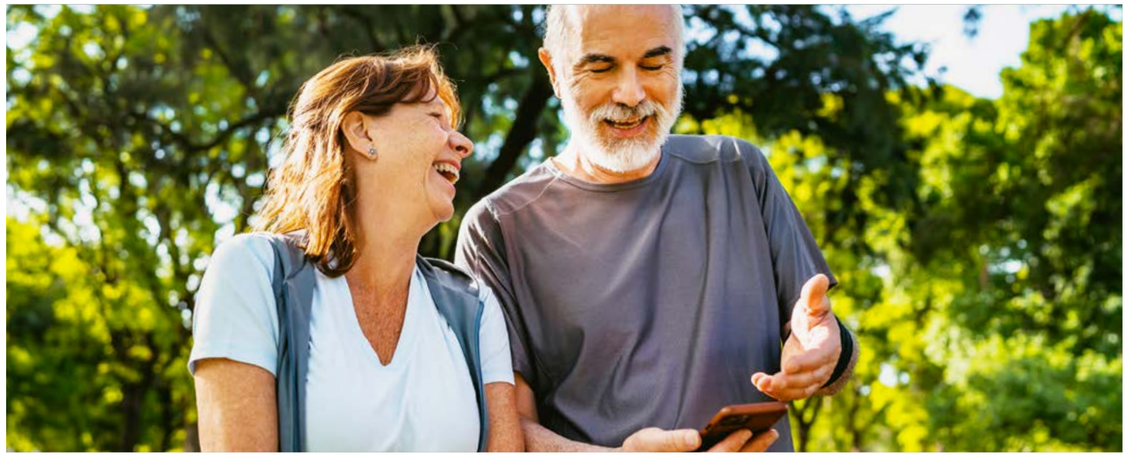
- Visit our website and complete our online form: *www.rabobank.com.au/compliments-and-complaints*
- Phone: 1800 025 484 (free call), Mon-Fri 6am - 8pm (Sydney time) or call your local area manager.
  If you're overseas call: +61 2 8115 2240
- Email: *Sydney.client.services@rabobank.com*
- Mail: Client Services Manager, Rabobank, GPO Box 4577, Sydney, NSW 2001
- Call or visit your local branch and speak directly to your Rural Manager or contact your local Rabobank branch. Often a discussion with a staff member who is familiar with your business can provide a quick resolution. If you are not satisfied or uncomfortable addressing your complaint with your local team, you can ask to speak to a Branch Manager or Regional Manager by contacting your local Rabobank branch on 1300 30 30 33
- Contact the Office of the Australian Information Commissioner (OAIC) by visiting their website on *www.oaic.gov.au*, sending an email to *enquiries@oaic.gov.au* or phoning 1300 363 992

Rabobank Online Savings clients

- Visit our website and complete our online form: *www.rabobank.com.au/compliments-and-complaints*
- Phone: 1800 445 445 (free call), Mon-Fri 6am - 8pm (Sydney time). If you're overseas call: +61 2 8115 2558
- Email: *clientservicesAU@rabobank.com*
- Mail: Client Services Manager, Rabobank, GPO Box 4577, Sydney, NSW 2001
- Contact the Office of the Australian Information Commissioner (OAIC) by visiting their website on *www.oaic.gov.au*, sending an email to *enquiries@oaic.gov.au* or phoning 1300 363 992

When sending your message to us, please include your name, address and contact details, as well as your complaint and what action(s) you have taken (e.g. requested your card to be stopped with the Merchant). Also let us know what you would like to see as an outcome.

For security reasons, please DO NOT provide any confidential or account specific information via email or post.



Our Client Services specialists will aim to promptly resolve your complaint and/or any issues identified. If more action is needed, they will escalate the matter to the appropriate person.

Will Rabobank provide additional assistance to make a complaint?

Should you require additional assistance to make your compliant, Rabobank has the following services available to you:

National Relay Service (NRS)

A Government initiative that offers phone service for people who have speech and hearing impairments. It is available free of charge through the following channels by:

Phone

Voice Relay number: 1300 555 727
SMS Relay number: 0423 677 767
Talk to Text number: 133 677

Internet

National Relay Chat Call services:
https://nrschat.nrscall.gov.au/nrs/internetrelay
National Relay service: *https://www.communications.gov.au/what-we-do/phone/services-people-disability/accesshub/national-relay-service*

Free translation services are available to you, if you have limited English, where you can get the help of a translator or interpreter (telephonically or face to face) to help you lodge your complaint. Please contact us and we will make the necessary arrangements for a translator or interpreter through National Accreditation Authority for Translators and Interpreters (NAATI).

What is the Rabobank complaint management process and how long it will take to respond to my complaint?

We will give you written acknowledgement of your complaint within 24 hours (one business day), of receipt of your complaint.

We will investigate and respond to your complaint within 30 calendar days.

If we are unable to resolve your complaint within 30 calendar days, we will tell you:

- The reasons for the delay;
- Your right to complain to Australian Financial Complaints Authority (AFCA) and/or the Office of the Australian Information Commissioner (OAIC); and
- Contact details of AFCA and OAIC.

In limited circumstances, we may need more time to resolve your complaint. If that's the case, we will inform you of the reasons for the delay, provide you with monthly updates and specify a date by which we will provide you with a resolution.

What if I am not happy with the resolution of my complaint?

If you are not satisfied with the resolution offered or if your complaint is not resolved within 30 calendar days, you have the following options:

Access our external dispute resolution service, the Australian Financial Complaints Authority (AFCA).

Website: *www.afca.org.au*
Phone: 1800 931 678

Access the Office of the Australian Information Commissioner (OAIC).

Email: *enquiries@oaic.gov.au*
Phone: 1300 363 992
If you're overseas call: +61 2 9284 9749
Mail: GPO Box 5218, Sydney NSW 2001

AFCA provides a free and independent service to resolve complaints by consumers and small businesses about financial services firms where that complaint falls within AFCA's terms of reference. Decisions made by AFCA are binding on us. However, time limits may apply to complaints to AFCA so you should act promptly or consult the AFCA website to find out if or when the time limit relevant to your circumstances expires. For more information, please refer to AFCA's brochure *'How to Resolve your Dispute'* from AFCA website or request a copy of this brochure from one of our staff members.

Can we change this Privacy Policy?

Yes, we review our Privacy Policy on a regular basis and that means that it may change from time to time. This is possible if there are new data processes and these changes are important to you. We will of course keep you informed of material changes to this Policy. You can always find the most current version of our Privacy Policy at *www.rabobank.com.au*.

Latest version: February 2023

How to contact the Privacy Officer?

If you have any general feedback or queries regarding the way Rabobank handles your Personal data, you may also contact the Privacy Officer:

Email: *sydney.privacy@rabobank.com*
Mail: The Privacy Officer, Rabobank Group,
GPO Box 4577, Sydney NSW 2001

14386 / FEB 2023

We value your privacy.

Rabobank Australia Limited
ABN 50 001 621 129
AFSL 234 700
Australian Credit Licence: 234 700

To contact our Privacy Officer
Email sydney.privacy@rabobank.com
Mail Privacy Officer, Rabobank Group
GPO Box 4577, Sydney NSW 2001

Rabobank