Rabobank Group

Privacy Code

Introduction

Rabobank Group has committed itself to the protection of personal data it processes of its employees, customers and other individuals in its Code of Conduct.[1]

This Rabobank Group Privacy Code indicates how this principle will be implemented in respect of personal data of customers and other individuals that are processed by a Rabobank Entity in the context of its business activities as a financial services company.

The Rabobank Entities worldwide provide financial services, including factoring, vendor financing and leasing. These services are to a large extent regulated by financial services regulations and supervised by financial authorities. Under applicable financial services regulation strict confidentiality and security requirements apply to the processing of data of customers and other individuals. This Rabobank Group Privacy Code applies to the extent it provides supplemental protection to the personal data of customers and other individuals processed by Rabobank Entity in the context of its business activities.

For the rules applicable to employee data refer to the *Rabobank Group Privacy Code for Employee Data*.

Article 1 – Scope, Applicability and Implementation

Scope	1.1	This Code addresses the Processing of Personal Data of Customers, Suppliers, Business Partners and other Individuals by a Rabobank Entity or a Third Party Processor on behalf of a Rabobank Entity. This Code does not address the Processing of Personal Data of Employees in the context of their employment relationship with a Rabobank Entity.
Electronic and paper-based Processing	1.2	This Code applies to the Processing of Personal Data by electronic means and in systematically accessible paper-based filing systems.

[1] Code of Conduct Rabobank Group, readopted by the Managing Board on 23 August November 2018.

Applicability of local law and Code	1.3	Individuals will keep any rights and remedies they may have under applicable local law. For the avoidance of doubt: (i) where applicable local law provides more protection than this Code, local law will apply in addition to this Code and (ii) where this Code provides more protection than applicable local law or provides additional safeguards, rights or remedies for Individuals, this Code will apply in addition to applicable law. In the event that the General Data Protection Regulation provides for less protection than this Code, a Rabobank Entity may choose to apply this Code or the General Data Protection Regulation.
Sub-policies and notices	1.4	A Rabobank Entity may supplement this Code through sub-policies or notices that are consistent with this Code.
Accountability for compliance with this Code	1.5	The Privacy Executives will be accountable for compliance with this Code.
Effective Date	1.6	This Code has been adopted by the Managing Board. It has entered into force as of 1 April 2014 (**Effective Date**). An update to this Code has been adopted by the Managing Board on 12 November 2018. It will be published on the **Rabobank website**. It will be made available to Individuals upon request.
Code supersedes prior policies	1.7	This Code will supersede all Rabobank Group privacy policies and notices that exist on the Effective Date to the extent they are in contradiction with this Code.
Implementation	1.8	This Code will be implemented in the Rabobank Group based on the timeframes specified in Article 22.

Article 2 – Purposes for Processing Personal Data

Lawful Processing	2.1	Personal Data will be Processed lawfully. Lawful Processing of Personal Data means that a Rabobank Entity shall not Process Personal Data, unless one of the following conditions applies: (i) a Rabobank Entity needs to Process the data to: a) perform, or take steps with a view to enter into, a contract with the relevant Individual; b) comply with a legal obligation to which a Rabobank Entity is subject; or c) protect the vital interests of the Individual concerned; (ii) a Rabobank Entity needs to carry out such Processing to pursue

Rabobank Entity's legitimate interests, and these interests do not prejudice the interests or fundamental rights and freedoms of the Individual concerned;

(iii) the Individual concerned has consented to the Processing, by providing a freely given, specific, informed and unambiguous indication of the Individual's wishes by a clear affirmative action; or

(iv) in circumstances permitted by applicable data protection laws.

A Rabobank Entity shall not use Personal Data for new purposes without following its internal procedures to verify that such processing can take place lawfully as referred to in Article 3.

Legitimate Business Purpose

2.2 A Rabobank Entity shall Process Personal Data in the context of the provision of financial services, including factoring, vendor financing and leasing, for one (or more) of the following purposes (**Business Purposes**):

(i) **Assessment and acceptance of a Customer, conclusion and execution of agreements with a Customer and the settlement of payment transactions.** This purpose includes Processing of Personal Data that is necessary in connection with the assessment and acceptance of Customers including confirming and verifying a Customer's identity (this may involve the use of a credit reference agency or other Third Parties) and conducting due diligence, screening against publicly available government and/or law enforcement agency sanctions lists and the use of and participation in Rabobank's incident registers and financial sector warning systems. This activity also includes the Processing of Personal Data in connection with the execution of agreements, including the delivery of Customer Services, and the settlement of payment transactions in the context of which a Rabobank Entity may provide Personal Data to the counterparty or other parties as necessary e.g. for verification or reconstruction purposes.

(ii) **Development and improvement of products and services.** This purpose includes Processing of Personal Data necessary for the development and improvement of a Rabobank Entity's products and/or services, research and development.

(iii) **Conclusion and execution of agreements with Suppliers and Business Partners.** This purpose addresses the Processing of Personal Data necessary to conclude and execute agreements with Suppliers and Business Partners, including required screening activities (e.g. for access to a Rabobank Entity's

premises or systems), and to record and financially settle delivered services, products and materials to and from a Rabobank Entity.

(iv) **Relationship management and marketing**. This purpose includes maintaining and promoting contact with Customers, Suppliers and Business Partners, account management, customer service and the development, execution and analysis of market surveys and marketing strategies.

(v) **Business process execution, internal management and management reporting.** This purpose includes the management of company assets, credit assessment (including setting credit limits) and risk management, conducting internal audits and investigations, finance and accounting, implementing business controls, provision of central processing facilities for efficiency purposes, managing mergers, acquisitions and divestitures, Processing Personal Data for management reporting and analysis, Archive and insurance purposes, legal or business consulting, and preparing for or engaging in dispute resolution.

(vi) **Safety, security and integrity, including the safeguarding of the security and integrity of the financial sector**. This purpose includes the protection of the interests of one or more Rabobank Entities and their Employees and Customers, including the safeguarding of the security and integrity of the financial sector, in particular the detecting, preventing, investigating and combating (attempted) criminal or objectionable conduct directed against one or more Rabobank Entities or their Employees and Customers, including the use of and participation in a Rabobank Entity's incident registers and financial sector warning systems. This activity also includes the authentication of Customer, Supplier and Business Partner status and access rights.

(vii) **Compliance with law.** This purpose addresses the Processing of Personal Data necessary for the performance of a task carried out to comply with a legal obligation or sectorial recommendation to which one or more Rabobank Entities are subject, including in relation to the prevention of money laundering, financing of terrorism and other crimes, customer due diligence and the duty of care towards Customers (e.g. credit monitoring) and the disclosure of Personal Data to government institutions and supervisory authorities, including tax authorities, in relation thereto; or

(viii) **Protection of the vital interests of Individuals.** This is where Processing is necessary to protect the vital interests of an

Individual.

Where there is a question whether a Processing of Personal Data can be based on a Business Purpose listed above, the appropriate Privacy Coordinator will be consulted before the Processing takes place.

Consent 2.3 If a Business Purpose does not exist or if applicable local law so requires a Rabobank Entity shall (also) seek consent from the Individual for the Processing.

Where Processing is undertaken at the request of an Individual (e.g. he subscribes to a service or seeks a benefit), he will be deemed to have provided consent to the Processing which is necessary for the performance requested by the Individual.

When seeking consent, a Rabobank Entity shall inform the Individual:

(i) of the purposes of the Processing for which consent is required and
(ii) other relevant information (e.g., the nature and categories of the Processed Data, the categories of Third Parties to which the Personal Data are disclosed (if any) and how Individuals can exercise their rights).

Denial or withdrawal of consent 2.4 The Individual may both deny consent and withdraw consent at any time. A Rabobank Entity shall inform the Individual of this right prior to obtaining his consent. The withdrawal of consent will not affect the lawfulness of the Processing based on such consent before its withdrawal.

Consent under GDPR 2.5 A Rabobank Entity shall ensure that any consent for Personal Data collected under the GDPR and this Code will meet the criteria of article 7 of the GDPR.

Article 3 – Use for Other Purposes

Use of Data for Secondary Purposes 3.1 Generally, Personal Data will be used only for the Business Purposes for which they were originally collected (**Original Purpose**). Personal Data may be Processed for a legitimate Business Purpose of a Rabobank Entity different from the Original Purpose (**Secondary Purpose**) only if the Original Purpose and Secondary Purpose are closely related. When assessing if a Processing of Personal Data can be based on a Secondary Purpose, the appropriate Privacy Coordinator will be consulted.

Depending on the sensitivity of the relevant Personal Data and whether use of the Data for the Secondary Purpose has potential negative consequences

for the Individual, the secondary use may require additional measures such as:

(i) limiting access to the Data
(ii) imposing additional confidentiality requirements
(iii) taking additional security measures
(iv) informing the Individual about the Secondary Purpose
(v) providing an opt-out opportunity or
(vi) obtaining an Individual's consent in accordance with Article 2.3 or Article 4.4 (if applicable).

Article 4 – Purposes for Processing Sensitive Data

Lawful Processing of Sensitive Data

4.1 Sensitive Data willbe Processed lawfully. Lawful Processing of Sensitive Data means that a Rabobank Entity shall not Process Sensitive Data unless:

(i) this is necessary for the performance of a task carried out to comply with or allowed by law;
(ii) this is necessary for the establishment, exercise or defense of a legal claim;
(iii) this is necessary to protect a vital interest of an Individual, but only where it is impossible to obtain the Individual's consent first;
(iv) if the Sensitive Data have manifestly been made public by the Individual;
(v) this is necessary for archiving for the purposes of public interest, scientific or historical research purposes or statistical purposes;
(vi) this is necessary for carrying out a Rabobank Entity's obligations or exercising specific rights of a Rabobank Entity or the relevant Employee(s) in the field of employment, social security and social protection law, authorized by law; (see under (i) above);
(vii) the Individual concerned has given his explicit consent, based on a full understanding of why the Sensitive Data is being collected; or
(viii) the Processing is authorized by a Data Protection Authority.

Please see below the more specific legitimate purposes to Process Sensitive Data of Individuals. A Rabobank Entity shall only Process Sensitive Data for the purposes below if one of the criteria above is also fulfilled.

Specific purposes for Processing Sensitive Data

4.2 This Article sets forth specific rules for Processing Sensitive Data. A Rabobank Entity shall Process Sensitive Data only to the extent necessary to serve the applicable Business Purpose.

The following categories of Sensitive Data may be collected, used or otherwise Processed only for one (or more) of the purposes specified below:

(i) **Racial or ethnic data**: in some countries photos and video images of Individuals qualify as racial or ethnic data. A Rabobank Entity may process photos (e.g. a copy of a passport containing a photo) and video images for the protection of one or more Rabobank Entities and their Employees, site access and security reasons, the identification and authentication of Customer, Supplier or Business Partner status for compliance with financial regulatory laws, anti-money laundering and financing of terrorism laws and access rights for demographic reporting under applicable anti-discrimination laws, to record decisions made in the course of business for future reference and for verifying and confirming advice provided by a Rabobank Entity to Individuals (e.g. when Individuals participate in video conferencing which is recorded).

(ii) **Criminal data**: (including data relating to criminal behavior, criminal records or proceedings regarding criminal or unlawful behavior) for protecting the interests of one or more Rabobank Entities, their Employees and Customers, including the safeguarding of the security and integrity of the financial sector with respect to criminal offences that have been or, given the relevant circumstances, are suspected to be or have been, committed against a Rabobank Entity or its Employees and Customers, and further for the use of and the participation in Rabobank Entity's incident registers and financial sector warning systems. This also includes mandatory checks against sanction lists pursuant to applicable sanctions legislation.

(iii) **Physical or mental health data:** insofar as necessary for the assessment and acceptance of a Customer, the execution of an agreement with a Customer, and compliance with a Rabobank Entity’s duty of care towards Customers.

(iv) **Religion or beliefs:** insofar as necessary for accommodating specific products or services for a Customer, dietary requirements or religious holidays.

(v) **Biometric data:** insofar as necessary for authentication and security purposes.

General Purposes for Processing of Sensitive Data	4.3	In addition to the specific purposes listed in Article 4.2 above, all categories of Sensitive Data may be Processed under (one or more of) the following circumstances: (i) as required for the performance of a task carried out to comply with a legal obligation or sectorial recommendation to which one or more Rabobank Entities are subject; (ii) for the establishment, exercise or defense of a legal claim; (iii) to protect a vital interest of an Individual, but only where it is impossible to obtain the Individual's consent first; (iv) to the extent necessary for reasons of substantial public interest; (v) if the Sensitive Data have manifestly been made public by the Individual; or (vi) archiving for the purposes of public interest, scientific or historical research purposes or statistical purposes.
Consent, denial or withdrawal of consent	4.4	In addition to the specific purposes listed in Article 4.2 and the general purposes listed in Article 4.3, all categories of Sensitive Data may be Processed if the Individual has given his explicit consent to the Processing thereof. If one of the purposes listed in Articles 4.2 and 4.3 apply, a Rabobank Entity shall in addition seek consent if applicable local law so requires. The information requirements set out in Article 2.3 and Article 2.4 will apply to the granting, denial or withdrawal of consent.
Prior Authorization of Privacy Coordinator	4.5	Where Sensitive Data are Processed based on a requirement of law other than the local law applicable to the Processing, the Processing will require the prior authorization of the appropriate Privacy Coordinator.
Use of Sensitive Data for Secondary Purposes	4.6	Sensitive Data of Individuals may be Processed for Secondary Purposes in accordance with Article 3.

Article 5 – Quantity and Quality of Data

No Excessive Data	5.1	A Rabobank Entity shall restrict the Processing of Personal Data to Data that are reasonably adequate for and relevant to the applicable Business Purpose. A Rabobank Entity shall take reasonable steps to delete Personal Data that are not required for the applicable Business Purpose.
Storage period	5.2	A Rabobank Entity shall specify – e.g. in a policy, statement, records retention schedule or in new systems via 'privacy by design'- a storage

period for which certain categories of Personal Data may be kept, which means not for longer than necessary and/or required by applicable laws and regulations.

Promptly after the applicable storage period has ended, the Record Keeping Coordinator shall direct that the Data will be:

(i) securely deleted or destroyed
(ii) anonymized or
(iii) transferred to an Archive (unless this is prohibited by law or an applicable records retention schedule).

Quality of Data 5.3 Personal Data will be accurate, complete and kept up-to-date to the extent reasonably necessary for the applicable Business Purpose.

Accurate, complete and up-to-date Data 5.4 It will be the responsibility of the Individuals to inform a Rabobank Entity regarding any changes in his Personal Data in order to keep his Personal Data accurate, complete and up-to-date. Individuals should inform a Rabobank Entity regarding any changes in accordance with Article 7.2.

Article 6 – Individual Information Requirements

Information requirements 6.1 Where and insofar as the Individual does not already have this information a Rabobank Entity shall provide Individuals with the following privacy information:

(i) which Rabobank Entity or Rabobank Entities are solely or jointly responsible for the Processing;
(ii) the contact details of the relevant Global/Local Data Protection Officer or designated central point of contact;
(iii) the Business Purposes for which their Personal Data are Processed;
(iv) to the extent the GDPR applies to the Processing, the legal basis for the Processing of their Personal Data and, if the processing is based on the legitimate interests of a Rabobank Entity, of the legitimate interests pursued by a Rabobank Entity;
(v) the categories of Third Parties to which the Personal Data are disclosed (if any);
(vi) if applicable, the fact that Personal Data will be transferred to a Third Party located in a Non-Adequate Country, including the safeguards in place to protect the Personal Data; and
(vii) to the extent applicable, any other relevant information, such as:
(a) the retention period of the Personal Data or the criteria to

determine the retention period;

(b) the Individual's rights and how these rights may be exercised;
(c) the right to withdraw consent;
(d) the right to lodge a complaint to a Data Protection Authority;
(e) whether an Individual is required to provide Personal Data or if this is optional;
(f) about the existence of automated decision making, including profiling, and, where required by applicable law, about the logic behind and envisaged consequences of this automated decision making; and
(g) if the Personal Data were not obtained from the Individual, the source from which the Personal Data originate.

Personal Data not obtained from the Individual

6.2 If applicable local law so requires, where Personal Data have not been obtained directly from the Individual, a Rabobank Entity shall provide the Individual with the information as set out in Article 6.1:

(i) within one month after the Personal Data are recorded in a Rabobank Entity's database;
(ii) at the time that the Personal Data are used for a mailing, provided that this mailing is done within six months after the Personal Data are recorded in a Rabobank Entity's database; or
(iii) at the time that the Personal Data are first disclosed to a Third Party, provided that this disclosure is done within six months after the Personal Data are recorded in a Rabobank Entity's database.

Exceptions

6.3 The requirements of Article 6.2 may be set aside if:

(i) it is impossible or would involve a disproportionate effort to provide the information to Individuals;
(ii) it results in disproportionate costs;
(iii) the Individual already has this information; or
(iv) disclosure is expressly required by applicable law.

These exceptions will qualify as Overriding Interests.

Article 7 – Individual Rights

Rights of Individuals

7.1 Every Individual may request an overview of his Personal Data Processed by or on behalf of a Rabobank Entity. Where reasonably possible, the overview will contain information regarding the source, type, purpose categories of recipients and envisaged retention period or criteria to determine such retention period of the relevant Personal Data.

If the Personal Data are incorrect, incomplete or not Processed in compliance with applicable law or this Code, the Individual may have his Data rectified, deleted, blocked or their Processing restricted (as relevant).

In addition, the Individual may :

a) object to the Processing on the basis of compelling grounds related to his particular situation;
b) object to receiving marketing communications on the basis of Article 9.5;
c) be informed of the safeguards implemented by a Rabobank Entity to provide an adequate level of protection of Personal Data transferred to a Third Party located in a Non-Adequate Country;
d) restrict the Processing if he contests the accuracy of his Personal Data, or if the Individual objects to the Processing or does not agree to deletion of his Personal Data;
e) restrict the Processing if the Processing is unlawful and the Individual objects to the deletion of his Personal Data; and
f) receive a machine-readable copy of his Personal Data and, where technically possible, to have a Rabobank Entity transmit his Personal Data to a Third Party directly. This right will only apply where the GDPR applies and the Processing is carried out by automated means and is based on consent as set forth in Articles 2.3 or 4.3, or based on a contract.

Where the Individual objects to the Processing following this article and this objection is justified, and a Rabobank Entity has no compelling legitimate grounds for the Processing that override the Individual's interests, the objected Processing will be ceased.

Procedure

7.2 The Individual shall send his request to the contact person or contact point indicated in the relevant privacy statement or notice. If no contact person or contact point is indicated, the Individual may send his request through the general contact section of a Rabobank Entity's website.

Prior to fulfilling the request of the Individual, an Individual may be asked to provide proof of his identity to a Rabobank Entity.

If a Rabobank Entity Processes a large quantity of Personal Data relating to an Individual, a Rabobank Entity may require the Individual to:

(i) specify the categories of Personal Data to which he is seeking access
(ii) specify, to the extent reasonably possible, the data system in which the Personal Data are likely to be stored
(iii) specify, to the extent reasonably possible, the circumstances in which a Rabobank Entity obtained the Personal Data
(iv) pay a fee to compensate a Rabobank Entity for the reasonable costs relating to fulfilling the request of the Individual; and
(v) in case of a request for rectification, deletion, or blockage, specify the reasons why the Personal Data are incorrect, incomplete or not Processed in accordance with applicable law or tise Code.

Response period

7.3 Within one month of a Rabobank Entity receiving the request, the contact person, contact point, or Privacy Coordinator shall inform the Individual in writing either (i) of a Rabobank Entity's position with regard to the request and any action a Rabobank Entity has taken or will take in response or (ii) of the ultimate date on which he will be informed of a Rabobank Entity's position. This date will be no later than two months thereafter. A Rabobank Entity shall explain the reasons of this delay.

Complaint

7.4 An Individual may file a complaint in accordance with Article 17.3 if:

(i) the response to the request is unsatisfactory to the Individual (e.g. the request is denied);
(ii) the Individual has not received a response as required by Article 7.3; or
(iii) the time period provided to the Individual in accordance with Article 7.3 is, in light of the relevant circumstances, unreasonably long and the Individual has objected but has not been provided with a shorter, more reasonable time period in which he will receive a response.

An Individual can file a complaint with a relevant Data Protection Authority or

seek judicial remedy in addition to the internal complaint process if a Rabobank Entity does not take action on the request of the Individual.

Denial of requests	7.5	A Rabobank Entity may deny an Individual request if: (i) the request does not meet the requirements of Articles 7.1 and 7.2; (ii) the request is manifestly unfounded or not sufficiently specific (and the Individual was given the opportunity to specify his request); (iii) the identity of the relevant Individual cannot be established by reasonable means; (iv) the request is made within an unreasonable time interval of a prior request or otherwise constitutes an abuse of rights. A time interval between requests of 6 months or less will generally be deemed to be an unreasonable time interval; or (v) an Overriding Interest exists as set forth in Article 12.
Notification of correction or deletion	7.6	If a Rabobank Entity grants the Individual's request for rectification or erasure of his Personal Data or restriction of the Processing thereof, it shall ensure rectification or erasure of the Personal Data and notify recipients of these Personal Data where reasonably possible and proportional.

Article 8 – Security and Confidentiality Requirements

Data security	8.1	A Rabobank Entity shall take appropriate commercially reasonable technical, physical and organizational measures to protect Personal Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access. To achieve this, Rabobank Group has developed and implemented the Rabobank Group Information Security Policy and other sub-policies.
Employee access	8.2	Employees will be authorized to access Personal Data as necessary to serve the applicable Business Purpose and to perform their job as instructed by a Rabobank Entity.
Confidentiality obligations	8.3	Employees who access Personal Data are subject to their confidentiality obligations.
Data Security	8.4	In accordance with applicable law, a Rabobank Entity shall notify the

Breach notification requirement		Individual of a Data Security Breach if the breach is likely to result in a high risk to the rights and freedoms of natural persons. A Rabobank Entity shall notify the Individual without undue delay following discovery of such breach. This obligation will not apply if a law enforcement or financial supervisory authority determines that notification would impede a criminal investigation or cause damage to national security or the notification might endanger trust in financial market stability. In this case, notification will be delayed or omitted. A Rabobank Entity shall respond promptly to inquiries of Individuals relating to such Data Security Breach. A Rabobank Entity shall also notify the relevant Data Protection Authorities of Data Security Breaches in accordance with applicable law.

Article 9 – Direct Marketing

Direct marketing	9.1	This Article sets forth requirements concerning the Processing of Personal Data for direct marketing purposes (e.g. contacting the Individual by email, fax, phone, SMS or otherwise, with a view of solicitation for commercial or charitable purposes).
Consent for direct marketing (opt-in)	9.2	If applicable law so requires, a Rabobank Entity shall only send to Individuals unsolicited commercial communication by fax, email, sms and mms with the prior consent of the Individual ("opt-in"). If applicable law does not require prior consent of the Individual, a Rabobank Entity shall in any event offer the Individual the opportunity to opt-out of such unsolicited commercial communication.
Exception (opt-out)	9.3	Prior consent of the Individual for sending unsolicited commercial communication will not be required if: (i) an Individual has provided his electronic contact details to a Rabobank Entity in the context of a sale of a product or service of such Rabobank Entity; (ii) such contact details are used for direct marketing of such Rabobank Entity's own similar products or services; and (iii) provided that an Individual clearly and distinctly has been given the opportunity to object free of charge, and in an easy manner, to such use of his electronic contact details when they are collected by the Rabobank Entity.
Information to be provided in each communication	9.4	In every direct marketing communication that is made to the Individual, the Individual will be offered the opportunity to opt-out of further direct marketing communications, including profiling related to this direct marketing.

Objection to direct marketing	9.5	If an Individual objects to receiving marketing communications from a Rabobank Entity, or withdraws his consent to receive such materials, a Rabobank Entity will take steps to refrain from sending further marketing materials and from Processing that Individual's Personal Data for direct marketing purposes, including profiling related to this direct marketing.
Third Parties and Direct marketing	9.6	No Personal Data will be provided to Third Party Controllers for purposes of direct marketing without the prior consent of the Individual.
Personal Data of Children	9.7	A Rabobank Entity shall not use any Personal Data of Children for Direct Marketing, without the prior consent of their parent or custodian.
Direct Marketing records	9.8	A Rabobank Entity shall keep a record of Individuals that used their "opt-in" or "opt-out" right and shall regularly check the public opt-out registers.

Article 10 – Automated Decision Making and Profiling

Automated decisions	10.1	Automated tools may be used to make decisions about Individuals but decisions with a negative outcome for the Individual will not be based solely on the results provided by the automated tool. This restriction will not apply if: (i) use of automated tools is necessary for the performance of a task carried out to comply with a legal obligation or sectorial recommendation to which a Rabobank Entity is subject, including the prevention of money laundering, financing of terrorism and other crimes, customer due diligence and the duty of care towards Customers (e.g. credit monitoring); (ii) the decision is made by a Rabobank Entity for purposes of (a) entering into or performing a contract or (b) managing the contract, with the Individual; or (iii) the Individual has given his explicit consent.
Sensitive Data	10.2	When Processing Sensitive Data, the exceptions of Article 10.1 will not apply, unless the conditions of Article 4 and Article 10.3 are met.
Suitable measures	10.3	In the cases referred to in Article 10.1(i) and (ii), a Rabobank Entity shall take suitable measures to safeguard the legitimate interests of the Individual, e.g. by providing the Individual with an opportunity to express his point of view

Article 11 – Transfer of Personal Data to Third Parties

Transfer to Third Parties 11.1 This Article sets forth requirements concerning the transfer of Personal Data from a Rabobank Entity to a Third Party. Note that a transfer of Personal Data will include situations in which a Rabobank Entity discloses Personal Data to Third Parties or where a Rabobank Entity provides remote access to Personal Data to a Third Party.

Third Party Controllers and Third Party Processors 11.2 There will be two categories of Third Parties:

(i) **Third Party Processors:** these are Third Parties that Process Personal Data solely on behalf of a Rabobank Entity and at its direction; and

(ii) **Third Party Controllers:** these are Third Parties that Process Personal Data and determine the purposes and means of the Processing.

Transfer for applicable Business Purpose only 11.3 A Rabobank Entity may transfer Personal Data to a Third Party to the extent necessary to serve the applicable Business Purpose This will include Secondary Purposes as per Article 3 or purposes for which the Individual has provided consent in accordance with Article 2.3.

Third Party Controller safeguards 11.4 A Rabobank Entity shall seek to safeguard the data protection interests of Individuals when Personal Data are transferred to Third Party Controllers. Business Contact Data may be transferred to a Third Party Controller without safeguards if it is reasonably expected that such Business Contact Data will be used by the Third Party Controller to contact the Individual for legitimate business purposes related to Individual's job responsibilities.

Third Party Processor contracts 11.5 Third Party Processors may Process Personal Data only if they have a written contract with a Rabobank Entity. The contract with a Third Party Processor will include the following provisions:

(i) the Third Party Processor shall Process Personal Data only in accordance with a Rabobank Entity's documented instructions and for the purposes authorized by a Rabobank Entity;

(ii) the Processor shall and have persons it authorizes to Process Personal Data, keep the Personal Data confidential;

(iii) the Processor shall take appropriate technical, physical and organizational security measures to protect the Personal Data

(iv) the Third Party Processor shall not permit subcontractors and affiliates to Process Personal Data in connection with its obligations to a Rabobank Entity without the prior written consent of a Rabobank Entity;

(v) the Third Party Processor shall ensure that its subcontractors and

affiliates abide by a level of data protection no less protective than the obligations as set out in the contract between the Third Party Processor and a Rabobank Entity;

(vi) a Rabobank Entity may review the security measures taken by the Third Party Processor and the Third Party Processor shall subject its relevant data processing facilities to audits and inspections by a Rabobank Entity, a Third Party on behalf of a Rabobank Entity or any relevant government authority

(vii) the Third Party Processor shall promptly inform Rabobank Entity of any actual or suspected security breach involving Personal Data;

(viii) the Third Party Processor shall take adequate remedial measures as soon as possible and shall promptly provide a Rabobank Entity with all relevant information and assistance as requested by a Rabobank Entity regarding the security breach; and

(ix) at the choice of a Rabobank Entity, the Third Party Processor shall delete or return all Personal Data to a Rabobank Entity at the end of the provision of services relating to the Processing of Personal Data and shall delete all copies of the Personal Data, unless storing the Personal Data is required by applicable law.

Transfer of Data to a Non-Adequate Country

11.6 This Article sets forth additional rules for the transfer of Personal Data from the EEA to a Third Party located in a country that is not considered to provide an "adequate" level of protection for Personal Data (**Non-Adequate Country**).

Personal Data may be transferred to a Third Party located in a Non-Adequate Country only if:

(i) the transfer is necessary for the performance of a contract with the Individual, for managing a contract with the Individual or to take necessary steps at the request of the Individual prior to entering into a contract, e.g., for processing orders;

(ii) a contract has been concluded between a Rabobank Entity and the relevant Third Party that provides for safeguards at a similar level of protection as that provided by this Code; the contract shall conform to any model contract requirement under applicable local law (if any);

(iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Individual between a Rabobank Entity and a Third Party;

(iv) the Third Party has been certified under a code of conduct or certification program any other similar program that is recognized under applicable local law as providing an "adequate" level of data protection;
(v) the Third Party has implemented Binding Corporate Rules or a similar transfer control mechanisms which provide adequate safeguards under applicable law;
(vi) the transfer is necessary to protect a vital interest of the Individual;
(vii) the transfer is necessary for the establishment, exercise or defense of a legal claim;
(viii) the transfer is necessary to satisfy an important reason of public interests; or
(ix) the transfer is necessary for the performance of a task carried out to comply with a legal obligation or sectorial recommendation to which the relevant Rabobank Entity is subject.

Items (viii) and (ix) above require the prior approval of the Global/Local Data Protection Officer.

Consent for transfer

11.7 If none of the grounds listed in Article 11.6 exist or if applicable local law so requires a Rabobank Entity shall (also) seek consent from the Individual for the transfer to a Third Party located in a Non-Adequate Country.
Prior to requesting consent, the Individual will be provided with the following information:

(i) the purpose of the transfer
(ii) the identity of the transferring Rabobank Entity
(iii) the identity or categories of Third Parties to which the Personal Data will be transferred
(iv) the categories of Personal Data that will be transferred
(v) the country to which the Personal Data will be transferred; and
(vi) the fact that the Personal Data will be transferred to a Non-Adequate Country and the possible risks related to such a transfer.

Article 2.4 will apply to denial or withdrawal of consent.

Transfers between Non-Adequate Countries

11.8 This Article sets forth additional rules for transfers of Personal Data that were collected in connection with the activities of a Rabobank Entity located in a Non-Adequate Country to a Third Party also located in a Non-Adequate Country. In addition to the grounds listed in Article 11.6, these transfers will be permitted if they are necessary:

(i) for compliance with a legal obligation to which the relevant Rabobank Entity is subject;
(ii) to serve the public interest; or
(iii) to satisfy a Business Purpose of a Rabobank Entity.

Non- repetitive transfers

11.9 Where Articles 11.6 (i) through (ix), 11.7 and 11.8 do not apply, the transfer may take place when:

(i) the transfer is not repetitive;
(ii) the transfer concerns a limited number of Individuals;
(iii) the transfer is necessary for a compelling legitimate interest of a Rabobank Entity which is not overridden by the rights and freedoms of the Individual; and
(iv) a Rabobank Entity has implemented suitable safeguards to protect the Personal Data.

A Rabobank Entity shall, to the extent necessary under applicable law, inform the relevant Data Protection Authority of the transfer and the Individual about the transfer and the compelling legitimate interest pursued by the transfer.

GDPO/LDPO approval

11.10 A transfer based on Article 11.6(viii), 11.6(ix) or 11.9 will require the prior approval of the Global Data Protection Offier or Local Data Protection Officer.

Article 12 – Overriding Interests

Overriding Interests

12.1 Some of the obligations of a Rabobank Entity or rights of Individuals under this Code may be overridden if, under the specific circumstances at issue, a pressing need exists that outweighs the interest of the Individual (**Overriding Interest**). This rule will be subject to the rights of Individuals under applicable law and only apply if there are no other legal grounds for data transfers available under applicable law. An Overriding Interest will exist if there is a need to:

(i) protect the legitimate business interests of a Rabobank Entity including
  (a) the health, security or safety of Individuals or other individuals
  (b) a Rabobank Entity's intellectual property rights, trade secrets or reputation
  (c) the continuity of one or more Rabobank Entiies' business operations
  (d) the preservation of confidentiality in a proposed sale, merger or acquisition of a business or
  (e) the involvement of trusted advisors or consultants for business, legal, tax, or insurance purposes

(ii) prevent or investigate (including cooperating with law enforcement) suspected or actual violations of law or

(iii) defend or otherwise protect the rights or freedoms of one or more Rabobank Entities, their Employees or other persons.

Exceptions in the event of Overriding Interests

12.2 If an Overriding Interest exists, one or more of the following obligations of a Rabobank Entity or rights of the Individual may be set aside:

(i) Article 3.1 (the requirement to Process Personal Data for closely related purposes)

(ii) Article 6.1 and 6.2 (information provided to Individuals, Personal Data not obtained from the Individuals)

(iii) Article 7 (rights of Individuals)

(iv) Articles 8.2 and 8.3 (Employee access limitations and confidentiality requirements) and

(v) Articles 11.4, 11.5 and 11.6 (ii) (contracts with Third Parties).

Sensitive Data

12.3 The requirements of Articles 4.2 and 4.3 (Sensitive Data) may be set aside only for the Overriding Interests listed in Article 12.1 (i) (a), (b), (c) and (e), (ii) and (iii).

Consultation with Global

12.4 Setting aside obligations of a Rabobank Entity or rights of Individuals based on an Overriding Interest will require prior consultation of the Global/Local

Data Protection Officer Data Protection Officer.

Information to Individual 12.5 Upon request of the Individual, a Rabobank Entity shall inform the Individual of the Overriding Interest for which obligations of Rabobank Entity or rights of the Individual have been set aside. This rule will not apply if the particular Overriding Interest sets aside the requirements of Articles 6.1 or 7.1, in which case the request will be denied.

Article 13 – Supervision and Compliance

Global Data Protection Officer 13.1 Rabobank shall appoint a Global Data Protection Officer who is responsible for:

(i) supervising compliance with this Code;
(ii) coordinating, communicating and consulting with the Local Data Protection Officers/Privacy Coordinators network on central data protection issues;
(iii) providing annual data protection compliance reports, as appropriate, to the Head of Compliance on data protection risks and compliance issues as described in article 16.2;
(iv) coordinating, in conjunction with the Local Data Protection Officers/Privacy Coordinators network and the relevant compliance officers, official investigations or inquiries into the Processing of Personal Data by a government authority;
(v) dealing with conflicts between this Code and applicable law as described in article 20.2 (to the extent that this is not the responsibility of the Local Data Protection Officer);
(vi) approving transfers as described in articles 20.1 and 11.6 (to the extent that this is not the responsibility of the Local Data Protection Officer);
(vii) in consultation with the relevant Local Data Protection Officer/Privacy Coordinator, advising on the execution and periodic review of a Privacy Impact Assessment before a new system or a business process involving Processing of Personal Data is implemented;
(viii) monitoring the process of dealing with Data Security Breaches and managing Data Security Breaches with a global scope;
(ix) deciding on complaints as described in article 17; and
(x) devising the data management processes, systems and tools to implement the framework for data protection management as established by the Privacy Committee, including:
    (a) to maintain, update and publish this Code and

related sub-policies;

(b) tools to collect, maintain and update information regarding the structure and functioning of all systems that process personal data;

(c) data privacy training and awareness for employees to comply with their responsibilities under this Code;

(d) appropriate internal control systems to monitor, audit and report compliance with this Code and ensure that Rabobank Group's internal audit department can verify and certify such compliance in line with the Rabobank Group periodic assurance process ("In Control");

(e) procedures regarding data protection inquiries, concerns and complaints; and

(f) determine and update appropriate sanctions for violations of this Code (e.g. disciplinary standards).

Privacy Committee

13.2 The Head of Compliance will establish a Privacy Committee. The Privacy Committee shall create and maintain a framework for:

(i) the development, implementation and updating of local Individual data protection statements, policies and procedures;

(ii) the maintaining, updating and publishing of this Code and related sub-policies;

(iii) the creating, maintaining and updating of information regarding the structure and functioning of all systems that Process Personal Data (as required by Article 14);

(iv) the development, implementation and updating of the relevant data protection training and awareness programs;

(v) the collecting, investigating and resolving privacy inquiries, concerns and complaints; and

(vi) determining and updating appropriate sanctions for violations of this Code (e.g., disciplinary standards).

Local Data Protection Officers / Privacy Coordinators

13.3 The Global Data Protection Officer will act as the Local Data Protection Officer for Rabobank in the Netherlands. The Global Data Protection Officer shall establish a network of Privacy Coordinators and Local Data Protection Officers sufficient to direct compliance with this Code within Rabobank Group. Privacy Coordinators support their Organisational Unit with tasks related to privacy compliance in general. Local Data Protection

Officers will be appointed where required due to the location or organisational nature of an Organisational Unit.

The Local Data Protection Officers/Privacy Coordinators will perform the following tasks:

(i) implement the data protection management processes, systems and tools, devised by the Global Data Protection Officer to implement the framework for data protection management established by the Privacy Committee in their respective Organisational Unit;
(ii) support and assess overall data protection management compliance within their Organisational Unit;
(iii) regularly advise their Privacy Executive and the Global Data Protection Officer on privacy risks and compliance issues;
(iv) maintain (or ensure access to) an inventory of the system information about the structure and functioning of all systems that process personal data (as required by Article 14.2);
(v) be available for requests for privacy approvals or advice as described in article 7;
(vi) provide information relevant to the annual data protection compliance report of the Global Data Protection Officer (as required in Article 16);
(vii) assist the Global Data Protection Officer in the event of official investigations or inquiries by government authorities;
(viii) own and authorize all appropriate privacy sub-policies within their Organisational Unit;
(ix) direct that stored data be deleted or destroyed, anonymized or transferred as required by article 5.2;
(x) in consultation with the Global Data Protection Officer, if necessary, advise on the execution and periodic review of a Privacy Impact Assessment before a new system or a business process involving Processing of Personal Data is implemented;
(xi) monitoring the process of dealing with Data Security Breaches and managing Data Security Breaches with a local scope, including escalation to the Global Data Protection Officer if necessary;
(xii) decide on and notify the Global Data Protection Officer of complaints as described in article 17; and
(xiii) cooperate with the Global Data Protection Officer, other Privacy Coordinators and Local Data Protection Officers, and, where applicable, the designated compliance officers to:
(xiv) ensure that the instructions, tools and training are in place to

enable the Organisational Unit, to comply with this Code;

(xv) share and provide guidance on best practices for data protection management within their Organisational Unit;

(xvi) ensure that data protection requirements are taken into account whenever new technology is implemented in their Organisational Unit;

(xvii) notify the Privacy Executive of the involvement of external service providers with data processing tasks for their Organisational Unit.

Privacy Executive

13.4 The Privacy Executive will be accountable for the implementation of effective data protection management in his Organisational Unit, the integration of effective data protection into business practices, and that adequate resources and budget are available.

Privacy Executives will be accountable for:

(i) ensuring overall data protection management compliance within their Organisational Unit, also during and following organisational restructuring, outsourcing, mergers and acquisitions and divestures;

(ii) implementing the data management processes, systems and tools, devised by the Global Data Protection Officer to implement the framework for data protection management established by the Privacy Committee in their respective Organisational Unit;

(iii) ensuring that the data protection management processes and systems are maintained up to date against changing circumstances and legal and regulatory requirements;

(iv) ensuring and monitoring ongoing compliance of third parties with the requirements of this Code in case Personal Data are transferred by a Rabobank Entity to a Third Party (including, where required, entering into a written contract with such Third Parties and obtaining a sign off of such contract from the legal department);

(v) ensuring that relevant individuals in their Organisational Unit follow the prescribed data protection training courses; and

(vi) directing that stored Personal Data be deleted or destroyed, anonymized or transferred as required by article 5.2.

(vii) carrying out a Privacy Impact Assessment (PIA) before a new system or a business process involving Processing of Personal Data is implemented.

(viii) informing the Global Data Protection Officer of any new legal requirement that may interfere with a Rabobank Entity's's ability to

comply with this Code as required by Article 20.3.

Privacy Executives will be responsible for:

(ix) consulting with the Global Data Protection Officer in all cases where there is a conflict between applicable local law and this Code as described in Article 20.

Default Local Data Protection Officer or Privacy Coordinator

13.5 If at any moment in time there is no Local Data Protection Officer or Privacy Coordinator designated for a function, business or Organisational Unit, the designated compliance officer for the relevant function,business or Organisational Unit is responsible for supervising compliance with this Code.

GDPO or LDPO with a statutory position

13.6 Where the Global Data Protection Officer or a Local Data Protection Officer holds his position pursuant to law, he shall carry out his job responsibilities to the extent they do not conflict with his statutory position.

Article 14 – Policies and Procedures

Policies and procedures

14.1 A Rabobank Entity shall develop and implement sub-policies and procedures to comply with this Code.

Processing information

14.2 A Rabobank Entity shall maintain readily available information regarding the structure and functioning of all systems and processes that Process Personal Data (e.g. inventory of systems and processes, Privacy Impact Assessments).

Privacy Impact Assessment

14.3 A Rabobank Entity shall conduct a Privacy Impact Assessment prior to the Processing if it is likely to result in a high risk to the rights and freedoms of Individuals, especially in case of use of new technologies. The PIA will be performed prior to implementation of the envisaged IT system or Processing.

The outcome of a PIA is to identify the necessary measures to minimize risk and comply with applicable data protection law (including the GDPR). The Global Data Protection Officer will consult with the lead Data Protection Authority prior to Processing taking place, when required to do so.

Article 15 – Training

Employee

15.1 A Rabobank Entity shall provide training on this Code and related

training		confidentiality obligations to Employees who have permanent or regular access to Personal Data.

Article 16 – Monitoring and Auditing Compliance

Audits	16.1	Rabobank Group internal audit shall audit internal control, risk management and governance systems and processes that involve the Processing of Personal Data for compliance with this Code. The audits may be carried out in the course of the regular activities of Rabobank Group internal audit or at the request of the Global Data Protection Officer. The Global Data Protection Officer may request to have an audit as specified in this Article 16.1 conducted by an external auditor. Applicable professional standards of independence, integrity and confidentiality may be observed when conducting an audit. The Global Data Protection Officer and the appropriate Privacy Coordinators will be informed of the results of the audits. Reported violations of this Code will be reported back to the relevant Privacy Executive. The Global Data Protection Officer shall provide a copy of the audit results to the Dutch Data Protection Authority or relevant Data Protection Authority upon request.
Annual data protection report	16.2	The Global Data Protection Officer shall produce an annual data protection compliance report for the Head of Compliance on compliance with this Code, data protection risks and other relevant issues. Each Privacy Coordinator shall provide information relevant to the report to the Global Data Protection Officer.
Mitigation	16.3	A Rabobank Entity shall, if so indicated, ensure that adequate steps are taken to address breaches of this Code identified during the monitoring or auditing of compliance pursuant to this Article 16.
Audit by Data Protection Authority	16.4	When a Data Protection Authority evaluates data transfers by a Rabobank Entity established in its country, the Rabobank Entity shall comply with binding (i) decisions or orders, (ii) requests for an audit and (iii) requests for information including providing a copy of the internal audit results as set forth in Article 15.1 to said Data Protection Authority. This obligation will be without prejudice to any rights or obligations the Rabobank Entity has under applicable law.

Article 17 – Complaints Procedure

Complaint 17.1 Individuals may file a complaint regarding compliance with this Code or violations of their rights under applicable local law in accordance with the complaints procedure set forth in the relevant privacy policy or contract. The complaint will be forwarded to the appropriate Privacy Coordinator.

The appropriate Privacy Coordinator shall:

(a) notify the Global Data Protection Officer and if applicable the Local Data Protection Officer;
(b) initiate an investigation and
(c) when necessary, advise the business on the appropriate measures for compliance and monitor, through to completion, the steps designed to achieve compliance.

The Global Data Protection Officer or appropriate Local Data Protection Officer may consult with any government authority having jurisdiction over a particular matter about the measures to be taken.

Reply to Individual 17.2 Without prejudice to article 7 of this Code, the Individual shall be informed without undue delay and in any event within a month of a Rabobank Entity receiving a complaint in writing or electronically either (i) of Rabobank Entity's position with regard to the complaint and any action Rabobank Entity has taken or will take in response or (ii) when he will be informed of Rabobank Entity's position, which date will be no later than eight weeks thereafter. The appropriate Privacy Coordinator shall send a copy of the complaint and his written reply to the Global Data Protection Officer and, if applicable, the Local Data Protection Officer.

Complaint to Global Data Protection Officer 17.3 An Individual may file a complaint with the Global Data Protection Officer and, if applicable, the Local Data Protection Officer if:

(i) the resolution of the complaint by a Rabobank Entity is unsatisfactory to the Individual (e.g., the complaint is rejected)
(ii) the Individual has not received a response as required by Article 17.2
(iii) the time period provided to the Individual pursuant to Article 17.2 is, in light of the relevant circumstances, unreasonably long and the Individual has objected but has not been provided with a shorter, more reasonable time period in which he will receive a response or
(iv) in one of the events listed in Article 7.4.

The procedure described in Articles 17.1 through 17.2 will apply to

complaints filed with the Global Data Protection Officer and if applicable the Local Data Protection Officer.

Complaint to Data Protection Authorities	17.4	If an Individual is not satisfied with the replies to his complaint, the Individual has the right to lodge a complaint with the relevant Data Protection Authorities or competent courts in accordance with Article 18.4.

Article 18 – Legal Issues

Local law and jurisdiction	18.1	Any Processing by a Rabobank Entity of Personal Data will be governed by applicable local law. Individuals will keep their own rights and remedies as available in their local jurisdictions. Local government authorities having jurisdiction over the relevant matters will maintain their authority.
Law applicable to Code; Code has supplemental character	18.2	This Code will be governed by and interpreted in accordance with Dutch law. This Code will apply only where it provides supplemental protection for Personal Data. Where applicable local law provides more protection than this Code, local law will apply. In the event that the General Data Protection Regulation provides for less protection than this Code, A Rabobank Entity may choose to apply this Code or the General Data Protection Regulation.
Co-operation between Data Protection Authorities	18.3	Data Protection Authorities will coordinate their evaluations of data transfers under the Code. When a Data Protection Authority evaluates data transfers by a Rabobank Entity established in its country against this Code, the Dutch Data Protection Authority will provide cooperation and assistance where required. This will include providing audit reports available with the Dutch Data Protection Authority insofar as relevant to evaluate the aforementioned data transfers against this Code.
Code enforceable against Rabobank only	18.4	Any additional safeguards, rights or remedies granted to Individuals under this Code will be granted by and will be enforceable against Rabobank only. The courts in the Netherlands, and – to the extent applicable – the courts in the jurisdiction of the data controller or data processor located in the European Union, and the courts in the member state of the European Union where the individual has his habitual residence will have jurisdiction over any supplemental rights provided by the Code
Out of court settlement option	18.5	Without prejudice to any rights Individuals have under applicable law, Individuals are encouraged by Rabobank Group to first direct their complaints or claims concerning any supplemental right the Individual may have under this Code to Rabobank before filing a complaint or claim to a

competent government authority or court.

Code enforceable against Rabobank only

18.6 Any additional safeguards, rights or remedies granted to Individuals under this Code will be granted by and will be enforceable in the Netherlands against Rabobank only.

Available remedies and limitation of damages

18.7 Individuals will only be entitled to remedies available to data subjects under the Dutch data protection laws, the Dutch Civil Code and the Dutch Code on Civil Procedure. However, Rabobank will be liable only for direct damages suffered by an Individual resulting from a violation of this Code. Where an Individual can demonstrate that it has suffered damage and establish facts which show it is plausible that the damage has occurred because of a violation of the Code, it will be for Rabobank to prove that the damages suffered by the Individual due to a violation of the Code are not attributable to the relevant Rabobank Entity. Damages claimed in cases where the GDPR does not apply to the relevant Processing are limited to direct damages only. Damages claimed in cases where the GDPR does apply to the relevant Processing may constitute both direct and indirect damages.

Mutual assistance and redress

18.8 All Rabobank Entities shall co-operate and assist each other to the extent reasonably possible to handle:

(i) a request, complaint or claim made by an Individual or
(ii) a lawful investigation or inquiry by a competent government authority.

The Rabobank Entity who receives a request, complaint or claim from an Individual shall be responsible for handling any communication with the Individual regarding his request, complaint or claim except where circumstances dictate otherwise.

The Rabobank Entity that is responsible for the Processing to which the request, complaint or claim relates, will bear all costs involved and reimburse Rabobank.

Article 19 – Sanctions for Non-compliance

Non-compliance

19.1 Any act by an Employee that goes against this Code will be considered a significant violation of the Code of Conduct Rabobank Group and/or the Employee's labour agreement and could lead to sanctions.

Article 20 – Conflicts Between the Code and Applicable Local Law

Conflict of law when transferring Data	20.1	Where a legal requirement to transfer Personal Data conflicts with the laws of the Member States of the EEA or the law of Switzerland, the transfer will require the prior approval of the Global Data Protection Officer or, if applicable, the Local Data Protection Officer. The Global Data Protection Officer or, if applicable, the Local Data Protection Officer shall seek the advice of the Head of Legal.
Conflict between Code and law	20.2	In all other cases, where there is a conflict between applicable local law and the Code, the relevant Privacy Executive will consult with the Global Data Protection Officer to determine how to comply with this Code and resolve the conflict to the extent reasonably practicable given the legal requirements applicable to the relevant Rabobank Entity.
New conflicting legal requirements	20.3	The relevant Privacy Executive shall promptly inform the Global Data Protection Officer of any new legal requirement that may interfere with a Rabobank Entity's ability to comply with this Code.
Reporting to competent authority	20.4	In the event of a conflict as set forth in this Article 20, the Global Data Protection Officer may seek the advice of the Dutch Data Protection Authority or another competent government authority.

Article 21 – Changes to this Code

21.1 Any changes to this Code will require the prior approval of the Head of Compliance. The Global Data Protection Officer shall keep a record of any changes
made to this Code. Rabobank shall notify the Dutch Data Protection Authority and the Rabobank Entities of any modification to this Code without undue delay.

21.2 This Code may be changed by Rabobank without Individual's consent even though an amendment may relate to a benefit conferred on Individuals.

21.3 Any material change will enter into force with immediate effect after it has been approved in accordance with Article 21.1 and is published on a Rabobank Entity's website.

21.4 Any request, complaint or claim of an Individual involving this Code will be evaluated against the version of this Code as it is in force at the time the request, complaint or claim is made.

Article 22 – Transition Periods

General transition period	22.1	Except as indicated below, Rabobank Entities shall comply with this Code as soon as reasonably possible and in any case within two years of the Effective Date. Accordingly, except as otherwise indicated, within two years of the Effective Date, all Processing of Personal Data shall be undertaken in compliance with this Code. During any transition period, A Rabobank Entity shall strive to comply with this Code.
Transition period for new Rabobank Entities	22.2	Any entity that becomes a Rabobank Entity after the Effective Date shall comply with this Code within two years of becoming a Rabobank Entity.
Transition Period for Divested Entities	22.3	A Divested Entity may remain covered by this Code after its divestment for such period as may be required by Rabobank to disentangle the Processing of Personal Data relating to such Divested Entity.
Transition period for IT Systems	22.4	Where implementation of this Code requires updates or changes to information technology systems (including replacement of systems), the transition period will be three years from the Effective Date or from the date an entity becomes a Rabobank Entity, or any longer period as is reasonably necessary to complete the update, change or replacement process.
Transition period for existing agreements	22.5	Where there are existing agreements with Third Parties that are affected by this Code, the provisions of the agreements will prevail until the agreements are renewed in the normal course of business.
Transitional period for Local-for-Local Systems	22.6	Without prejudice to Article 22, Processing of Personal Data that were collected in connection with activities of a Rabobank Entity located in a Non-Adequate Country will be brought into compliance with this Code within five years of the Effective Date.

Article 23 – Exception for local-for-local systems

23.1 This Code does not apply to the Processing of Personal Data collected in connection with activities of a Rabobank Entity located in a Non-Adequate Country, this with the exception of the security and governance requirements of this Code which will remain applicable. In respect of such Processing of Personal Data, the relevant Rabobank Entity may decide whether to apply this Code. Such Processing of Personal Data shall at least be compliant with

applicable local laws.

Article 24 – Contact and company details

Contact details	Rabobank Global Data Protection Officer p/a Rabobank Croeselaan 18, 3521 CB Utrecht, Nederland Postbus 17100, 3500 HG Utrecht, Nederland E-mail: dpo@rabobank.nl
Company structure	https://www.rabobank.com/en/about-rabobank/profile/organisation/index.html

ANNEX 1 Definitions

Archive	ARCHIVE means a collection of Personal Data that are no longer necessary to achieve the purposes for which the Data originally were collected or that are no longer used for general business activities, but are used only for historical, scientific or statistical purposes, dispute resolution, investigations or general archiving purposes. An archive includes any data set that can no longer be accessed by any Employee other than the system administrator.
Article	ARTICLE means an article in this Code.
Binding Corporate Rules	BINDING CORPORATE RULES means a personal data protection policy that is adhered to by a controller or processor established on the territory of an EU member state for transfers or a set of transfers of Personal Data to a controlleror processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.
Business Contact Data	BUSINESS CONTACT DATA means any data typically found on a business card and used by the Individual in his contact with a Rabobank Entity.
Business Partner	BUSINESS PARTNER means any Third Party, other than a Customer or Supplier, that has or had a business relationship or strategic alliance with a Rabobank Entity (e.g. joint marketing partner, joint venture or joint development partner).
Business Purpose	BUSINESS PURPOSE means a purpose for Processing Personal Data as specified in Article 2 or 3 or for Processing Sensitive Data as specified in Article 4 or 3.
Children	CHILDREN mean Individuals under the age of thirteen (13) years.
Code	CODE means this Rabobank Group Privacy Code.
Customer	CUSTOMER means any person, private organization, or government body that purchases may purchase or has purchased a product or service of a Rabobank Entity.
Customer Services	CUSTOMER SERVICES means the services provided by a Rabobank Entity to Customers to support a Rabobank Entity's products and services in use with their employees or customers (e.g. of leased products). These services may include the maintenance, upgrade, replacement, inspection and related support activities aimed at facilitating continued and sustained use of a Rabobank

	Entity's products and services.
Data Security Breach	DATA SECURITY BREACH means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, of, or access to, Personal Data transmitted, stored or otherwise Processed.
Data Protection Authority	DATA PROTECTION AUTHORITY means an EEA data protection authority, duly constituted and competent in accordance to applicable data protection law.
Direct Marketing	DIRECT MARKETING means any marketing message sent by electronic means to an Individual.
Divested Entity	DIVESTED ENTITY means the divestment by a Rabobank Entity of another Rabobank Entity or business by means of: (a) a sale of shares as a result whereof the Rabobank Entity so divested no longer qualifies as a Rabobank Entity and/or (b) a demerger, sale of assets, or any other manner or form.
Dutch Data Protection Authority	DUTCH DATA PROTECTION AUTHORITY means the Dutch data protection authority (Autoriteit Persoonsgegevens).
EEA or European Economic Area	EEA or EUROPEAN ECONOMIC AREA means all Member States of the European Union, plus Norway, Iceland and Liechtenstein.
Effective Date	EFFECTIVE DATE means the date on which this Code becomes effective as set forth in Article 1.6.
Employee	EMPLOYEE means the following persons: (a) an employee, job applicant or former employee of a Rabobank Entity, including temporary workers working under the direct supervision of a Rabobank Entity (e.g. contractors and trainees); and (b) a (former) executive or non-executive director of Rabobank Group or (former) member of the supervisory board or similar body to a Rabobank Entity.
Employee Data	EMPLOYEE DATA means any information relating to an identified or identifiable Employee.
General Data	GENERAL DATA PROTECTION REGULATION or GDPR shall mean

Protection Regulation or GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
Global Data Protection Officer or GDPO	GLOBAL DATA PROTECTION OFFICER or GDPO means the officer as referred to in Article 13.1.
Head of Compliance	HEAD OF COMPLIANCE means the Head of Compliance of Rabobank.
Head of Legal	HEAD OF LEGAL means the Head of Legal of Rabobank.
Individual	INDIVIDUAL means any (employee of or any person working for) Customer, Supplier or Business Partner and any other individual whose Personal Data Rabobank processes in the context of the provision of financial services, including factoring, vendor financing and leasing.
Local Data Protection Officer	LOCAL DATA PROTECTION OFFICER means a data protection officer duly appointed and registered pursuant to applicable data protection law referred to in Article 13.3.
Non-Adequate Country	NON-ADEQUATE COUNTRY means a country that under applicable local law is deemed not to provide an "adequate" level of data protection.
Managing Board	MANAGING BOARD means the board of directors of Rabobank.
Original Purpose	ORIGINAL PURPOSE means the purpose for which Personal Data was originally collected.
Organisational Unit	ORGANISATIONAL UNIT means each business unit and staff function (or grouping thereof) within Rabobank Group.
Overriding Interest	OVERRIDING INTEREST means the pressing interests set forth in Article 12.1 based on which the obligations of a Rabobank Entity or rights of Individuals set forth in Article 12.2 and 12.3 may, under specific circumstances, be overridden if this pressing interest outweighs the interest of the Individual.
Personal Data or Data	PERSONAL DATA or DATA means any information relating to an identified or identifiable Individual.

Privacy Impact Assessment or PIA	PRIVACY IMPACT ASSESSMENT or (PIA means a review procedure to carry out and document an assessment of the impact of an envisaged IT- system or Processing on the protection of Personal Data and Individuals' privacy rights. The PIA will be performed prior to implementation of the envisaged IT-system or Processing and will regard the entire lifecycle management of Personal Data, from collection to Processing to deletion. A PIA contains a description of: • the relevant Rabobank Entities and third parties responsible for the Processing; • the envisaged Processing; • the Business Purpose for which Personal Data are Processed; • security measures; • data retention periods; and • categories of recipients; and • any transfers of Personal Data to Non-Adequate Countries, including suitable transfer mechanisms; and an assessment of: • the necessity and proportionality of the envisaged Processing; • the risks to the privacy rights of Individuals including a description of mitigating (privacy-by-design and privacy-by-default) measures to minimize these risks; and • the context of the Processing.
Privacy Committee	PRIVACY COMMITTEE means the committee referred to in Article 13.2.
Privacy Coordinator	PRIVACY COORDINATOR means a privacy coordinator or the relevant compliance officer referred to in Article 13.3.
Privacy Executive	PRIVACY EXECUTIVE means the head of an Organisational Unit.
Processing	PROCESSING means any operation that is performed on Personal Data, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission or deletion of Personal Data.
Rabobank Group	RABOBANK GROUP means the collective of the Rabobank Entities.
Rabobank Entity	RABOBANK ENTITY means each of Rabobank and any company or legal entity in which Rabobank holds a direct or indirect controlling interest and which is fully consolidated by it in accordance with IFRS.

Rabobank	RABOBANK means Coöperatieve Rabobank U.A. registered at the Chamber of Commerce under number 30.046.259, having its registered seat in Amsterdam, the Netherlands.
Record Keeping Coordinator	RECORD KEEPING COORDINATOR means the coordinator referred to in Article 5.2.
Secondary Purpose	SECONDARY PURPOSE means any purpose other than the Original Purpose for which Personal Data is further Processed.
Sensitive Data	SENSITIVE DATA means Personal Data that reveal an Individual's racial or ethnic origin, political opinions or membership in political parties or similar organizations, religious or philosophical beliefs, membership in a professional or trade organization or union, physical or mental health including any opinion thereof, disabilities, genetic code, addictions, sex life, criminal offenses, criminal records, proceedings with regard to criminal or unlawful behavior, or social security numbers issued by the government, or genetic and biometric data for the purpose of uniquely identifying a natural person..
Supplier	SUPPLIER means any Third Party that provides goods or services to a Rabobank Entity (e.g. an agent, consultant or vendor).
Third Party	THIRD PARTY means any person, private organization or government body outside Rabobank Group.
Third Party Controller	THIRD PARTY CONTROLLER means a Third Party that Processes Personal Data and determines the purposes and means of the Processing.
Third Party Processor	THIRD PARTY PROCESSOR means a Third Party that Processes Personal Data on behalf of a Rabobank Entity that is not under the direct authority of a Rabobank Entity.

Interpretations

INTERPRETATION OF THIS CODE:

(i) unless the context requires otherwise, all references to a particular Article or Annex are references to that Article or Annex in or to this document, as they may be amended from time to time

(ii) headings are included for convenience only and are not to be used in construing any provision of this Code

(iii) if a word or phrase is defined, its other grammatical forms have a corresponding meaning

(iv) the male form shall include the female form

(v) the words "include", "includes" and "including" and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa

(vi) a reference to a document (including, without limitation, a reference to this Code) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by this Code or that other document; and

(vi) a reference to law includes any regulatory requirement, recommendation and best practice issued by relevant national and international supervisory authorities or other bodies.