Rabobank Group

Privacy Code for Employee Data

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 for Employee Data indicates how this principle will be implemented in respect of personal data of employees and other individuals working at a Rabobank Entity.

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 requirements apply which require the processing of employee data (e.g. mandatory pre- and in-employment screening and monitoring of employee integrity and insider trading). This Rabobank Group Privacy Code for Employee Data applies to the extent it provides supplemental protection to the processing of personal data of employees and other individuals working at a a Rabobank Entity.

For the rules applicable to the data of customers and other individuals that are processed by Rabobank Group in the context of its business activities, refer to the *Rabobank Group Privacy Code.*

Article 1 – Scope, Applicability and Implementation

Scope	1.1	This Code addresses the Processing of Employee Data in the context of the employment relationship with a Rabobank Entity, by a Rabobank Entity or a Third Party Processor on behalf of a Rabobank Entity. This Code does not address the Processing of Employee Data in the Employee's capacity as a customer of a Rabobank Entity.
Electronic and paper-based Processing	1.2	This Code applies to the Processing of Employee 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 2018.

Applicability of local law and Code	1.3	Employees will keep any rights and remedies they may have under applicable law. For the avoidance of doubt (i) where applicable law provides more protection than this Code, applicable law will apply in addition to this Code and (ii) where this Code provides more protection than applicable law or provides additional safeguards, rights or remedies for Employees, 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 the 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 Intranet and be made available to Employees 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 21.

Article 2 – Purposes for Processing Employee Data

Lawful processing	2.1	Employee Data shall be Processed lawfully. Lawful Processing of Employee Data means that a Rabobank Entity will not Process Employee 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 Employee; b) comply with a legal obligation to which a Rabobank Entity is subject;

c) protect the vital interests of the Employee concerned;

(ii) a Rabobank Entity needs to carry out such Processing to pursue a Rabobank Entity's legitimate interests, and these interests do not prejudice the interests or fundamental rights and freedoms of the Employee concerned; or

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

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

A Rabobank Entity shall not use Employee 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 Purposes

2.2 A Rabobank Entity shall Process Employee Data for one (or more) of the following purposes (**Business Purposes**):

(i) **Human resources and personnel management.** This purpose includes Processing that is necessary for the performance of an employment or other contract with an Employee (or to take necessary steps at the request of an Employee prior to entering into a contract), or for managing the Employment-at-will relationship, e.g. management and administration of recruiting, outplacement, employability, leave and other absences, compensation and benefits (including pensions), payments, tax issues, career and talent development, performance evaluations, training, travel and expenses, and Employee communications.

(ii) **Business process execution and internal management.** This purpose addresses activities such as scheduling work, recording time, managing company assets, provision of central processing facilities for efficiency purposes, conducting internal audits and investigations, implementing business controls, and managing and using Employee directories, Archive and insurance purposes, legal or business consulting, and preparing for or engaging in dispute resolution.

(iii) **Health, safety, security and integrity, including the safeguarding of the security and integrity of the financial sector.** This purpose addresses activities such as those involving 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 pre- and in-employment screening and monitoring of Employees and the use of and participation in a Rabobank Entity's incident registers and financial sector warning systems, occupational safety and health, the protection of a Rabobank Entity and Employee and customer assets, and the authentication of Employee status and access rights.

(iv) **Organizational analysis and development, management reporting and acquisitions and divestitures.** This purpose addresses activities such as conducting Employee surveys, managing mergers, acquisitions and divestitures, and Processing Employee Data for management reporting and analysis.

(v) **Compliance with law.** This purpose addresses the Processing of Employee Data as 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 and the disclosure of Employee Data to government institutions and supervisory authorities, including tax authorities, in relation thereto; or

(vi) **Protecting the vital interests of Employees.** This is where Processing is necessary to protect the vital interests of an Employee.

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

Employee consent

2.3 Employee consent generally cannot be used as a legitimate basis for Processing Employee Data. One of the Business Purposes will have to exist for any Processing of Employee Data. If applicable local law so requires, in addition to having a Business Purpose for the relevant Processing, a Rabobank Entity shall also seek Employee consent for the Processing. If none of the Business Purposes apply, a Rabobank Entity may request Employee consent for Processing Employee Data, but only if the Processing has no foreseeable adverse consequences for the Employee.

A request for Employee consent will require the authorization of the appropriate Privacy Coordinator prior to seeking consent.

Denial or withdrawal of Employee consent

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

Where Processing is undertaken at the Employee's request (e.g. he subscribes to a service or seeks a benefit), he is deemed to have provided consent to the Processing.

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

(i) of the purposes of the Processing for which consent is requested;
(ii) of the possible consequences for the Employee of the Processing; and
(iii) that he is free to refuse and withdraw consent at any time without consequence to his employment relationship.

Limitations on Processing Data of Dependants of Employees

2.5 A Rabobank Entity shall Process Data of Dependants of an Employee if:

(i) the Data were provided with the consent of the Employee or the Dependant;
(ii) Processing of the Data is reasonably necessary for the performance of a contract with the Employee or for managing the Employment-at-will relationship; or
(iii) the Processing is required or permitted by applicable local law.

Consent under GDPR

2.6 A Rabobank Entity shall ensure that any consent for Employee 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, Employee Data will be used only for the Business Purposes for which they were originally collected (**Original Purpose**). Employee 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 Employee Data can be based on a Secondary Purpose, the appropriate Privacy Coordinator will be consulted.

Depending on the sensitivity of the relevant Employee Data and whether use of the Employee Data for the Secondary Purpose has potential negative consequences for the Employee, the secondary use may require additional measures such as:

(i) limiting access to the Employee Data;
(ii) imposing additional confidentiality requirements;

(iii) taking additional security measures;
(iv) informing the Employee about the Secondary Purpose;
(v) providing an opt-out opportunity; or
(vi) obtaining an Employee's consent in accordance with Article 2.3 or Article 4.3 (if applicable).

Article 4 – Purposes for Processing Sensitive Data

Lawful Processing of Sensitive Data

4.1 Sensitive Data will be 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 Employee, but only where it is impossible to obtain the Employee's consent first;
(iv) if the Sensitive Data have manifestly been made public by the Employee;
(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 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 Employee 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 Employees. 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**:

(a) in some countries photos and video images of Employees qualify as racial or ethnic data. A Rabobank Entity may process photos and video images for the protection of one or more Rabobank Entities and their Employees, site access and security reasons, demographic reporting under applicable anti-discrimination laws, communication facilities, verifying and confirming advice provided by a Rabobank Entity (e.g. when Employees participate in video conferencing which is recorded), for inclusion in Employee directories and for compliance with financial regulatory laws, anti-money laundering and financing of terrorism laws;

(b) providing preferential status to persons from particular ethnic or cultural minorities to remove or reduce inequality or to ensure diversity in staffing, provided that use of the relevant Sensitive Data allows an objective determination that an Employee belongs to a minority group and the Employee has not filed a written objection to the relevant Processing.

(ii) **Physical or mental health data** (including any opinion of physical or mental health and data relating to disabilities and absence due to illness or pregnancy):

(a) providing health services to an Employee provided that the relevant health data are processed by or under the supervision of a health professional who is subject to professional confidentiality requirements;

(b) administering pensions, health and welfare benefit plans, maternity, paternity or family leave programmes, or collective agreements (or similar arrangements) that create rights depending on the state of health of the Employee;

(c) reintegrating or providing support for Employees entitled to benefits in connection with illness or work incapacity;

(d) assessing and making decisions on (continued) eligibility for positions, projects or scope of responsibilities;

(e) providing facilities in the workplace to accommodate health problems or disabilities.

(iii) **Criminal data** (including data relating to criminal behavior, criminal records or proceedings regarding criminal or unlawful behavior):

(a) assessing an application by an Employee to make a decision about the Employee or provide a service to the Employee;

(b) protecting the interests of one or more Rabobank Entities, its 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 one or more Rabobank Entities or their Employees and customers, and further for pre- and in-employment screening and monitoring of Employees and the use of and the participation in a Rabobank Entity's incident registers and financial sector warning systems. This also includes mandatory checks against sanction lists pursuant to applicable sanctions legislation.

(iv) **Sexual preference** (including Data relating to partners of Employees):
   (a) administering Employee pensions and benefits programs;
   (b) administering Employee memberships.

(v) **Religious or philosophical beliefs:** insofar as necessary for accommodating religious or philosophical practices, dietary requirements or religious holidays**.**

(vi) **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 Employee, but only where it is impossible to obtain the Employee's consent first;

(iv) to the extent necessary for reasons of substantial public interest;

(v) where the Sensitive Data have manifestly been made public by the Employee; or

(vi) archiving for the purposes of public interest, scientific or historical research purposes or statistical purposes.

Employee consent for Processing Sensitive Data

4.4 Employee consent generally cannot be used as a legitimate basis for Processing Sensitive Data. One of the grounds listed in Article 4.2 or 4.3 must exist for any Processing of Sensitive Data. If applicable local law so requires, in addition to having one of the grounds listed in Article 4.2 or 4.3 for the relevant Processing, a Rabobank Entity shall also seek Employee consent for the Processing. If none of the grounds listed in Article 4.2 or 4.3

applies, a Rabobank Entity may request Employee consent for Processing Sensitive Data, but only if the Processing has no foreseeable adverse consequences for the Employee (e.g. Employee diversity programs or networks, research, product development, selection of candidates in hiring or management development processes). Article 2.3 will apply to the granting, denial or withdrawal of Employee 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, or based on the consent of the Employee, the Processing will require the prior authorization of the appropriate Privacy Coordinator.
Use of Sensitive Data for Secondary Purposes	4.6	Sensitive Data of Employees or Dependants 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 Employee Data to those Employee Data that are reasonably adequate for and relevant to the applicable Business Purpose. A Rabobank Entity shall take reasonable steps to delete Employee 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 time period for which certain categories of Employee 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 Employee Data 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	Employee Data will be accurate, complete and kept up-to-date to the extent reasonably necessary for the applicable Business Purpose.
'Self-service'	5.4	Where a Rabobank Entity requires an Employee to update his own Employee Data, a Rabobank Entity shall remind him at least once a year to do so.

Article 6 – Employee Information Requirements

Information requirements

6.1 Where and insofar the Employee does not already have this information a Rabobank Entity shall provide Employees 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 or Local Data Protection Officer or designated central point of contact;

(iii) the Business Purposes for which their Employee Data are Processed;

(iv) to the extent the GDPR applies to the Processing, the legal basis for the Processing of their Employee 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 Employee Data are disclosed (if any);

(vi) if applicable, the fact that Employee Data will be transferred to a Third Party located in a Non-Adequate Country, including the safeguards in place to protect the Employee Data; and

(vii) to the extent applicable, any other relevant information such as:

(a) the retention period of the Employee Data or the criteria to determine the retention period;

(b) the Employee'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 Employee is required to provide Employee Data;

(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 Employee Data were not collected from the Employee himself, the source from which the Employee Data originate.

Employee Data not obtained from Employees

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

(i) within one month after the Employee Data are recorded in a Rabobank Entity's database;

(ii) at the time that the Employee Data are first used for a mailing, provided that this mailing is done within six months after the

Employee Data are recorded in a Rabobank Entity's database; or

(iii) at the time that the Employee Data are first disclosed to a Third Party, provided that this disclosure is done within six months after the Employee Data are recorded in a Rabobank Entit'sy 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 Employees;
(ii) it results in disproportionate costs;
(iii) the Employee already has this information; or
(iv) disclosure is expressly required by applicable law.

These exceptions will qualify as Overriding Interests.

Article 7 – Employee Rights

Rights of Employees

7.1 Every Employee may request an overview of his Employee 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 the retention period of the relevant Employee Data.

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

In addition, the Employee may:

a) object to the Processing of his Data on the basis of compelling grounds related to his particular situation;
b) object to receiving marketing communications;
c) be informed of the safeguards implemented by a Rabobank Entity to provide an adequate level of protection of Employee Data transferred to a Third Party located in a Non-Adequate Country;
d) restrict the Processing if he contests the accuracy of his Employee Data, or if the Employee objects to the Processing or does not agree to deletion of his Employee Data;
e) restrict the Processing if the Processing is unlawful and the Employee objects to the deletion of his Employee Data; and
f) receive a machine-readable copy of his Employee Data and, where technically possible, to have a Rabobank Entity transmit

his Employee Data to a Third Party directly. This right will only apply where the General Data Protection Regulation applies and the Processing is carried out by automated means and based on consent as set forth in Articles 2.3 or 4.3, or based on a contract.

Where the Employee 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 Employee's interests, the objected Processing will be ceased.

Procedure 7.2 The Employee shall send his request to the contact person, contact point,or appropriate Privacy Coordinator.

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

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

(i) specify the categories of Employee Data to which he is seeking access;
(ii) specify to the extent reasonably possible the data system in which the Employee Data are likely to be stored;
(iii) specify to the extent reasonably possible the circumstances in which a Rabobank Entity obtained the Employee Data;
(iv) pay a fee to compensate a Rabobank Entity for the reasonable costs relating to fulfilling the request of the Employee; and
(v) in the case of a request for rectification, deletion, or restriction, specify the reasons why the Employee Data are incorrect, incomplete or not Processed in accordance with applicable law or this 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 Employee 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) 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 Employee may file a complaint in accordance with Article 16.3 if:

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

An Employee 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 Employee.

Denial of requests

7.5 A Rabobank Entity may deny an Employee request if:
(i) the request does not meet the requirements of Articles 7.1 and 7.2;
(ii) the request manifestly unfounded or is not sufficiently specific (and the Employee was given the opportunity to specify his request);
(iii) the identity of the relevant Employee cannot be established by reasonable means; or
(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 shall generally be deemed to be an unreasonable time interval;
(v) an Overriding Interest exists as set forth in Article 12.

Notification of correction or deletion

7.6 If a Rabobank Entity grants the Employee's request for rectification or erasure of his Employee Data or restriction of the Processing thereof, it shall ensure rectification or erasure of the Personal Data and notify recipients of these Employee 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 Employee Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access. To achieve this, a Rabobank Entity has developed and implemented the Rabobank Group Information Security Policy and other sub-policies.

Employee access

8.2 Employees will be authorized to access Employee 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 Employee Data will meet their confidentiality obligations.

Data Security Breach notification requirement

8.4 In accordance with applicable law, a Rabobank Entity shall notify the Employee 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 Employee 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 the trust in financial market stability. In this case, notification will be delayed or omitted. A Rabobank Entity shall respond promptly to inquiries of Employees 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 – Automated Decision Making and Profiling

Automated decisions

9.1 Automated tools may be used to make decisions about Employees but decisions with a negative outcome for the Employee may not be based solely on the results provided by the automated tool. This restriction will not apply if the:

(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;

(ii) decision is made by a Rabobank Entity for purposes of (a) entering into or performing a contract or (b) managing the Employment-at-will relationship, provided the underlying request leading to a decision by a Rabobank Entity was made by the Employee (e.g. where automated tools are used to filter job applications); or

(iii) Employee has given his explicit consent.

Sensitive Data

9.2 When Processing Sensitive Data, the exceptions of Article 9.1 will not apply, unless the conditions of Article 4 and Article 9.3 are met.

Suitable measures	9.3	In the cases referred to in Articles 9.1(ii) and (iii), a Rabobank Entity shall take suitable measures to safeguard the legitimate interests of the Employee, e.g. by providing the Employee with an opportunity to express his point of view.

Article 10 – Transfer of Employee Data to Third Parties

Transfer to Third Parties	10.1	This Article sets forth requirements concerning the transfer of Employee Data from a Rabobank Entity to a Third Party. Note that a transfer of Employee Data will include situations in which a Rabobank Entity discloses Employee Data to Third Parties (e.g. in the context of corporate due diligence) or where a Rabobank Entity provides remote access to Employee Data to a Third Party.
Third Party Controllers and Third Party Processors	10.2	There will be two categories of Third Parties: (i) **Third Party Processors:** these are Third Parties that Process Employee Data solely on behalf of a Rabobank Entity and at its direction (e.g. Third Parties that Process Employee salaries on behalf of a Rabobank Entity); and (ii) **Third Party Controllers:** these are Third Parties that Process Employee Data and determine the purposes and means of the Processing (e.g. government authorities or service providers that provide services directly to Employees).
Transfer for applicable Business Purposes only	10.3	A Rabobank Entity may transfer Employee Data to a Third Party to the extent necessary to serve the applicable Business Purpose for which the Employee Data are Processed. This will include Secondary Purposes as per Article 3 or purposes for which the Employee has provided consent in accordance with Article 2.
Third Party Controller safeguards	10.4	A Rabobank Entity shall seek to safeguard the data protection interests of Employees when Personal Data are transferred to Third Party Controllers, including by conclusion of a written contract. 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 Employee for legitimate business purposes related to Individual's job responsibilities. All such contracts shall be drafted in consultation with the appropriate Privacy Coordinator.
Third Party Processor contracts	10.5	Third Party Processors may Process Employee 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 Employee 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 Employee Data, keep the Employee Data confidential;

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

(iv) the Third Party Data Processor shall not permit subcontractors and affiliates to Process Employee 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 obligation as set out in the contract with a Rabobank Entity;

(vi) a Rabobank Entity may review the security measures taken by the Third Party Processor and the Third Party Processor shall submit 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 a Rabobank Entity of any actual or suspected security breach involving Employee 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 Employee Data to a Rabobank Entity at the end of the provision of services relating to the processing of Employee Data, unless storing the Employee Data is required by applicable law.

Transfer of Data to a Non-Adequate Country

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

Employee 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 Employee, for managing the Employment-at-will relationship

or to take necessary steps at the request of the Employee prior to entering into a contract or an Employment-at-will relationship, e.g. for processing job applications;

(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 Employee between a Rabobank Entity and a Third Party (e.g. in case of the booking of an airline ticket);

(iv) the Third Party has been certified under a code of conduct or certification program or 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 Employee;

(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 or Local Data Protection Officer.

Employee consent for transfer

10.7 A Rabobank Entity generally shall not seek Employee consent for a transfer of Employee Data to a Third Party located in a Non-Adequate Country. One of the grounds for transfer listed in Article 10.6 must exist. If applicable local law so requires, in addition to having one of the grounds listed in Article 10.6, a Rabobank Entity shall also seek Employee consent for the relevant transfer. In addition to the grounds listed in Article 10.6, a Rabobank Entity may request Employee consent for a transfer to a Third Party located in a Non-Adequate Country, but only if

(i) the transfer has no foreseeable adverse consequences for the Employee; or

(ii) the consent is requested prior to the participation of the Employee in specific projects, assignments or tasks that require the transfer of the Employee Data.

Requesting Employee consent for a transfer requires the prior approval of the appropriate Privacy Coordinator. Prior to requesting Employee consent, the Employee 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 Employee Data will be transferred;
(iv) the categories of Employee Data that will be transferred;
(v) the country to which the Employee Data will be transferred; and
(vi) the fact that the Employee 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

10.8 This Article sets forth additional rules for transfers of Employee 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 10.6, 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

10.9 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 Employees;
(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 Employee; and
(iv) a Rabobank Entity has implemented suitable safeguards to protect the Employee's rights.

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

by the transfer.

GDPO/LDPO approval 10.10 A transfer based on Articles 11.6(viii), (ix) or 10.9 will require the prior approval of the Global Data Protection Officer or Local Data Protection Officer.

Article 11 – Overriding Interests

Overriding Interests 11.1 Some of the obligations of a Rabobank Entity or rights of Employees under this Code may be overridden if, under the specific circumstances at issue, a pressing need exists that outweighs the interest of the Employee (**Overriding Interest**). This rule will be subject to the rights of Employees 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 Employees or other individuals;
  (b) a Rabobank Entity's intellectual property rights, trade secrets or reputation;
  (c) the continuity of one or more Rabobank Entities' 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, breaches of the terms of employment, or non-compliance with the Rabobank Group Code of Conduct or other Rabobank Group policies or procedures 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 11.2 If an Overriding Interest exists, one or more of the following obligations of a Rabobank Entity or rights of the Employee may be set aside:

(i) Article 3.1 (the requirement to Process Employee Data for closely related purposes);
(ii) Article 6.1 (information provided to Employees);
(iii) Article 7.1 (rights of Employees);
(iv) Articles 8.2 and 8.3 (Employee access limitations and

confidentiality requirements); and

(v) Articles 10.4, 10.5 and 10.6 (ii) (contracts with Third Parties).

Sensitive Data 11.3 The requirements of Articles 4.2 and 4.3 (Sensitive Data) may be set aside only for the Overriding Interests listed in Article 11.1 (i) (a), (b), (c) and (e), (ii) and (iii).

Consultation with Global Data Protection Officer 11.4 Setting aside obligations of a Rabobank Entity or rights of Employees based on an Overriding Interest, will require the prior consultation of the Global or Local Data Protection Officer.

Information to Employee 11.5 Upon request of the Employee, a Rabobank Entity shall inform the Employee of the Overriding Interest for which obligations of a Rabobank Entity or rights of the Employee 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 12 – Supervision and Compliance

Global Data Protection Officer 12.1 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 compliance reports, as appropriate, to the Head of Compliance on data protection risks and compliance issues as described in article 15.2;

(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 Employee Data by a government authority;

(v) dealing with conflicts between this Code and applicable law as described in article 19.2 (to the extent that this is not the responsibility of the Local Data Protection Officer);

(vi) approving transfers as described in articles 19.1 and 10.6 (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 or Privacy Coordinator, advising on the execution and periodic review of a Privacy Impact Assessment before a new system or a business

process involving processing Employee 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 16; 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

12.2 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 Employee 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 13);

(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

12.3 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 the Organisational Unit.

The Local Data Protection Officers and 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 13.2);
(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 15);
(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, advising on the execution and periodic review of a Privacy Impact Assessment before a new system or a business process involving processing of Employee 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 16;
(xiii) cooperate with the Global Data Protection Officer, other Privacy Coordinators and Local Data Protection Officers, and, where applicable, the designated compliance officer;
(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; and
(xviii) review and authorize requests for seeking Employee consent.

Privacy Executive

12.4 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 organizational 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 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;
(vi) directing that stored Employee 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; and

(viii) informing the Global Data Protection Officer of any new legal requirement that may interfere with a Rabobank Entity's ability to comply with this Code as required by Article 19.3.

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 19

Default Local Data Protection Officer or Privacy Coordinator	12.5	If at any moment in time there is no Local Data Protection Officer or Privacy Coordinator designated for a function or business, 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	12.6	Where a 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 13 – Policies and Procedures

Policies and procedures	13.1	Rabobank shall develop and implement sub-policies and procedures to comply with this Code.
System information	13.2	A Rabobank Entity shall maintain readily available information regarding the structure and functioning of all systems and processes that Process Employee Data (e.g. inventory of systems and processes, Privacy Impact Assessments).
Privacy Impact Assessment	13.3	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 (includingthe 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 14 – Training

Employee training 14.1 A Rabobank Entity shall provide training on this Code and related confidentiality obligations to Employees who have permanent or regular access to Employee Data.

Article 15 – Monitoring and Auditing Compliance

Audits 15.1 Rabobank Group internal audit shall audit internal control, risk management and governance systems and processes and procedures that involve the Processing of Employee 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 15.1 conducted by an external auditor. Applicable professional standards of independence, integrity and confidentiality will 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 the Privacy Codes will be reported back to the 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 Privacy Report 15.2 The Global Data Protection Officer shall produce a 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 15.3 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 15.4 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 16 – Complaints Procedure

Complaint to Privacy Coordinator

16.1 Employees may file a complaint regarding compliance with this Code or violations of their rights under applicable local law:

(i) in accordance with the applicable complaints procedure; or

(ii) with the appropriate Privacy Coordinator.

The appropriate Privacy Coordinator shall:

(a) notify the Global Data Protection Officer or 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 Employee

16.2 Without prejudice to article 7 of this Code (Employee rights), the appropriate Privacy Coordinator shall inform the Employee without undue delay and in any event within a month of a Rabobank Entity receiving a complaint in writing or electronically either (i) of a Rabobank Entity's position with regard to the complaint and any action a Rabobank Entity has taken or will take in response or (ii) when he will be informed of a 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

16.3 An Employee 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 Employee (e.g. the complaint is rejected);

(ii) the Employee has not received a response as required by Article 16.2;

(iii) the time period provided to the Employee pursuant to Article 16.2 is, in light of the relevant circumstances, unreasonably long and the Employee has objected but has not been provided with a shorter, more reasonable time period in which he will receive a

response; or

(iv) in the events listed in Article 7.4.

The procedure described in Articles 16.1 through 16.2 will apply to complaints filed with the Global Data Protection Officer and, if applicable, the Local Data Protection Officer .

Complaint to Data Protection Authorities 16.4 If an Employee is not satisfied with the replies to his complaint, the Employee has the right to lodge a complaint with the relevant Data Protection Authorities or competent courts in accordance with Article 17.4.

Article 17 – Legal Issues

Applicable law and jurisdiction 17.1 Any Processing by a Rabobank Entity of Employee Data will be governed by applicable local law. Employees 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 17.2 This Code will be governed by and interpreted in accordance with Dutch law. This Code will apply only where it provides supplemental protection for Employee Data. Where applicable local law provides more protection than this Code, local law shall 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 17.3 Data Protection Authorities will coordinate their evaluations of data transfers under the Code. When a Data Protection Authority evaluates data transfers by a Group Company 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 17.4 Any additional safeguards, rights or remedies granted to Employees 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 17.5 Without prejudice to any rights Employees have under applicable law, Employees are encouraged by Rabobank Group to first direct their

option

complaints or claims concerning any supplemental right the Employee 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

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

Available remedies, limitation of damages, burden of proof

17.7 Employees 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. Provided an Employee 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 Employee 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

17.8 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 Employee or
(ii) a lawful investigation or inquiry by a competent government authority.

The Rabobank Entity employing the Employee shall be responsible for handling any communication with the Employee 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, shall bear all costs involved and reimburse Rabobank.

Article 18 – Sanctions for Non-compliance

Non-compliance

18.1 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 19 – Conflicts between the Code and Applicable Local Law

Conflict of law when transferring Data	19.1	Where a legal requirement to transfer Employee 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	19.2	In all other cases, where there is a conflict between applicable local law and this 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	19.3	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 the competent authority	19.4	In the event of a conflict as set forth in this Article 19, the Global Data Protection Officer may seek the advice of the Dutch Data Protection Authority or another competent government authority.

Article 20 – Changes to this Code

20.1 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 Rabobank Entities of any modification this Code without undue delay.

20.2 This Code may be changed by Rabobank without Employee consent even though an amendment may relate to a benefit conferred on Employees.

20.3 Any material change will enter into force with immediate effect after it has been approved in accordance with Article 20.1 and is published on a Rabobank Entity's Intranet.

20.4 Any request, complaint or claim of an Employee involving this Code will be evaluated against the version of this Code that is in force at the time the request, complaint or claim is made.

Article 21 – Transition Periods

General Transition Period	21.1	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 Employee Data shall be undertaken in compliance with the Code. During any transition period, a Rabobank Entity shall strive to comply with the Code.
Transition Period for New Rabobank Entities	21.2	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	21.3	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 Employee Data relating to such Divested Entity.
Transition Period for IT Systems	21.4	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	21.5	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	21.6	Processing of Employee 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 22 – Exception for Local-for-Local Systems

Local-for-Local Systems	22.1	This Code does not apply to the Processing of Employee 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 Employee Data, the relevant Rabobank Entity may

decide whether to apply this Code. Such Processing of Employee Data shall at least be compliant with applicable local laws.

Article 23 – 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/nl/about-rabobank/profile/organisation/index.html

ANNEX 1 Definitions

Archive	ARCHIVE means a collection of Employee 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 controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.
Business Purpose	BUSINESS PURPOSE means a purpose for Processing Employee Data as specified in Article 2 or 3 or for Processing Sensitive Data as specified in Article 4 or 3.
Code	CODE means this Rabobank Group Privacy Code for Employee Data.
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.
Dutch Data Protection Authority	DUTCH DATA PROTECTION AUTHORITY means the Dutch data protection authority (Autoriteit Persoonsgegevens).
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.
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); or (b) a (former) executive or non-executive director of a Rabobank Entity or (former) member of the supervisory board or similar body to a Rabobank Entity.
Employee Data or Data	EMPLOYEE DATA or DATA means any information relating to an identified or identifiable Employee (and his Dependants).
Employment-at-will	EMPLOYMENT-AT-WILL means an employment relationship in which either the employer or employee can terminate the employment relationship at any time for any reason, with or without advance notice.
General Data Protection Regulation or GDPR	GENERAL DATA PROTECTION REGULATION or GDPR means 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 12.1.
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.
Local Data Protection Officer or LDPO	LOCAL DATA PROTECTION OFFICER or LDPO means a data protection officer duly appointed and registered pursuant to applicable data protection law referred to in Article 12.3.
Managing Board	EXECUTIVE BOARD means the board of directors of Rabobank.
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.

Original Purpose	ORIGINAL PURPOSE means the purpose for which Employee 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 11.1 based on which the obligations of a Rabobank Entity or rights of Employees set forth in Article 11.2 and 11.3 may, under specific circumstances, be overridden if this pressing interest outweighs the interest of the Employee.
Privacy Committee	PRIVACY COMMITTEE means the committee referred to in Article 12.2.
Privacy Coordinator	PRIVACY COORDINATOR means a privacy coordinator or relevant compliance officer referred to in Article 12.3.
Privacy Executive	RESPONSIBLE EXECUTIVE means the head of an Organisational Unit.
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 Employee Data and Employees' 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 Employee 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 Employee Data are Processed; • security measures; • data retention periods; • categories of recipients; and • any transfers of Employee 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.

Processing	PROCESSING means any operation that is performed on Employee 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 Employee Data.
Rabobank Group	RABOBANK GROUP means the collective 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 Employee Data is further Processed.
Sensitive Data	SENSITIVE DATA means Employee Data that reveal an Employee'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, r social security numbers issued by the government, or genetic and biometric data for the purpose of uniquely identifying a natural person..
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 Employee Data and determines the purposes and means of the Processing.
Third Party Processor	THIRD PARTY PROCESSOR means a Third Party that Processes Employee Data on behalf of a Rabobank Entity that is not under the direct authority of a Rabobank Entity.


Rabobank

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

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