



Privacy Code for Associate Data

Effective Date: 1st May, 2018

Introduction

JACOBS DOUWE EGBERTS is committed to the protection of its Associates' personal data as espoused in the JACOBS DOUWE EGBERTS Code of Conduct.

This Privacy Code are internal rules adopted by JACOBS DOUWE EGBERTS and its participating Group Companies, to adduce "adequate safeguards for the protection of the privacy and fundamental rights and freedoms of Associates within the meaning of applicable data protection law, especially the data protection laws of member states of European Economic Area ("EEA")

This Privacy Code for Associate Data indicates how this principle shall be implemented. For the rules applicable to Non-Associate Data, refer to the Privacy Code for Consumer, Customer, Supplier and Business Partner Data.

Words in caps have been defined and can be found in **Annex 1** to this Code.

Article 1 – Scope, Applicability and Implementation

- | | | |
|--|-----|--|
| Scope | 1.1 | This Code addresses the Processing of Personal Data of JACOBS DOUWE EGBERTS Associates (Associate Data) by us or a Third Party on our behalf. |
| Electronic and paper-based Processing | 1.2 | This Code applies to the Processing of Associate Data by electronic means and in paper-based filing systems. |
| Applicability of local law and Code | 1.3 | Associates keep any rights and remedies they may have under applicable local law. This Code shall apply only where it provides supplemental |

protection for Associate Data. Where applicable local law¹ provides more protection than this Code, local law shall apply. Where this Code provides more protection than applicable local law or provides additional safeguards, rights or remedies for Associates, this Code shall apply.

Sub-policies and notices	1.4	JACOBS DOUWE EGBERTS may supplement this Code through sub-policies or notices that are consistent with this Code.
Responsibility	1.5	The Responsible Executive shall be accountable for compliance with this Code.
Effective Date and Availability	1.6	This Code shall be effective on 1 May 2011 “ Effective Date ” and shall be posted on JACOBS DOUWE EGBERTS’s Intranet. This Code shall be made available to Associates upon request.
Code supersedes prior policies	1.7	This Code supersedes all JACOBS DOUWE EGBERTS privacy policies and notices that exist on the Effective Date to the extent they address the same issues.
Implementation	1.8	This Code shall be implemented based on the timeframes specified in Article 21.

Article 2 – Purposes for Processing Associate Data

Legitimate Business Purposes	2.1	Associate Data shall be collected, used or otherwise Processed for one (or more) of the following purposes (Business Purposes): <ul style="list-style-type: none">(i) Human resources and personnel management. This purpose includes Processing that is necessary for the performance of an employment or other contract with an Associate (or to take necessary steps at the request of an Associate prior to entering into a contract), or for managing the employment-at-will relationship, e.g., management and administration of recruiting and outplacement, compensation and benefits, payments, tax issues, career and talent development, performance evaluations, training, travel and expenses, and Associate 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 Associate directories(iii) Health, safety and security. This purpose addresses activities such as those involving occupational safety and health, the
-------------------------------------	-----	--

¹ If applicable, the reference to local law also includes federal law.

- (iv) **Organizational analysis and development and management reporting.** This purpose addresses activities such as conducting Associate surveys, managing mergers, acquisitions and divestitures, and Processing Associate Data for management reporting and analysis
- (v) **Compliance with legal obligations.** This purpose addresses the Processing of Associate Data as necessary for compliance with a legal obligation to which JACOBS DOUWE EGBERTS is subject or
- (vi) **Protecting the vital interests of Associates.** This is where Processing is necessary to protect the vital interests of an Associate.

Where there is a question whether a Processing of Associate Data can be based on a purpose listed above, the advice of the appropriate Compliance Officer will be sought before the Processing takes place.

Associate consent

- 2.2 Associate consent generally cannot be used as a legitimate basis for Processing Associate Data. One of the Business Purposes shall exist for any Processing of Associate Data. If applicable local law so requires, in addition to having a Business Purpose for the relevant Processing, JACOBS DOUWE EGBERTS shall also seek Associate consent for the Processing. If none of the Business Purposes applies, JACOBS DOUWE EGBERTS may request Associate consent for Processing Associate Data, but only if the Processing has no foreseeable adverse consequences for the Associate.

A request for Associate consent requires the authorization of the appropriate Compliance Officer prior to seeking consent.

Denial or withdrawal of Associate consent

- 2.3 The Associate may both deny consent and withdraw consent at any time without consequence to his employment relationship. Where Processing is undertaken at the Associate'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 Associate consent, JACOBS DOUWE EGBERTS must inform the Associate:

- (i) of the purposes of the Processing for which consent is requested
- (ii) of the possible consequences for the Associate 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 Dependents of Associates | 2.4 | JACOBS DOUWE EGBERTS may Process Personal Data of Dependents of an Associate if: <ul style="list-style-type: none"> (i) the Personal Data were provided with the consent of the Associate or the Dependent (ii) Processing of the Personal Data is reasonably necessary for the performance of a contract with the Associate or for managing the employment-at-will relationship or (iii) the Processing is required or permitted by applicable local law. |
|---|-----|---|

Article 3 – Use for Other Purposes

- | | | |
|--|-----|---|
| Use of Data for Secondary Purposes | 3.1 | Generally, Associate Data shall be used only for the Business Purposes for which they were originally collected (Original Purpose). Associate Data may be Processed for a legitimate Business Purpose of JACOBS DOUWE EGBERTS different from the Original Purpose (Secondary Purpose) only if the Original Purpose and Secondary Purpose are closely related. The advice of the appropriate Compliance Officer will be sought in the determination of whether the Processing of Associate Personal Data may be based on a Secondary Purpose. Depending on the sensitivity of the relevant Associate Data and whether use of the Data for the Secondary Purpose has potential negative consequences for the Associate, the secondary use may require additional measures such as: <ul style="list-style-type: none"> (i) limiting access to the Data (ii) imposing additional confidentiality requirements (iii) taking additional security measures (iv) informing the Associate about the Secondary Purpose (v) providing an opt-out opportunity or (vi) obtaining Associate consent in accordance with Article 2.2. |
| Generally permitted uses of Data for Secondary Purposes | 3.2 | It is generally permissible to use Associate Data for the following Secondary Purposes provided appropriate additional measures are taken in accordance with Article 3.1: <ul style="list-style-type: none"> (i) transfer of the Data to an Archive (ii) internal audits or investigations (iii) implementation of business controls (iv) statistical, historical or scientific research (v) preparing for or engaging in dispute resolution (vi) legal or business consulting or (vii) insurance purposes. |

Article 4 – Purposes for Processing Special Categories of Data

Specific purposes for Processing Special Categories of Data

- 4.1 This Article sets forth specific rules for processing Special Categories of Data. JACOBS DOUWE EGBERTS shall process Special Categories of Data only to the extent necessary to serve the applicable Business Purpose. The following categories of Special Categories of 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 Associates qualify as racial or ethnic data. JACOBS DOUWE EGBERTS may process photos and video images for the protection of JACOBS DOUWE EGBERTS and Associate assets, site access and security reasons and for inclusion in Associate directories
 - (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 Special Categories of Data allows an objective determination that an Associate belongs to a minority group and the Associate 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 Associate 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 programs, or collective agreements (or similar arrangements) that create rights depending on the state of health of the Associate
 - (c) reintegrating or providing support for Associates 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
 - (f) Genetic or biometric data
 - (iii) **Criminal data** (including data relating to criminal behavior, criminal records or proceedings regarding criminal or unlawful behavior):
 - (a) assessing an application by an Associate to make a decision about the Associate or provide a service to the Associate

- (b) protecting the interests of JACOBS DOUWE EGBERTS with respect to criminal offenses that have been or, given the relevant circumstances are suspected to have been, committed against JACOBS DOUWE EGBERTS or its Staff
- (iv) **Sexual preference** (including data relating to partners of Associates):
 - (a) In so far as is required for the administration of Associate pensions and benefits programs
 - (b) administering Associate memberships
- (v) Religious or philosophical beliefs:
 - (a) In so far as is required for the accommodating religious or philosophical practices, dietary requirements or religious holidays.

General Purposes for Processing of Special Categories of Data

- 4.2 In addition to the specific purposes listed in Article 4.1 above, all categories of Special Categories of Data may be processed for one (or more) of the following:
- (i) as required by or permitted under applicable local law
 - (ii) for the establishment, exercise or defense of a legal claim
 - (iii) to protect a vital interest of an Associate, but only where it is impossible to obtain the Associate’s consent first
 - (iv) to the extent necessary to comply with an obligation of international public law (e.g. treaties) or
 - (v) where the Special Categories of Data have manifestly been made public by the Associate.

Associate consent for Processing Special Categories of Data

- 4.3 Associate consent generally cannot be used as a legitimate basis for Processing Special Categories of Data. One of the grounds listed in Article 4.1 or 4.2 must exist for any Processing of Special Categories of Data. If applicable local law so requires, in addition to having one of the grounds listed in Article 4.1 or 4.2 for the relevant Processing, JACOBS DOUWE EGBERTS shall also seek Associate consent for the Processing. If none of the grounds listed in Article 4.1 or 4.2 applies, JACOBS DOUWE EGBERTS may request Associate consent for Processing Special Categories of Data, but only if the Processing has no foreseeable adverse consequences for the Associate (e.g., Associate diversity programs or networks, research, product development, selection of candidates in hiring or management development processes). Article 2.3 applies to the granting, denial or withdrawal of Associate consent.

Prior Authorization of CPO or BPO

- 4.4 Where Special Categories of 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 Associate, the Processing requires the prior authorization of the Privacy Compliance Officer or the Compliance Officer responsible for the relevant business and geographic area.

Use of Special Categories of Data for Secondary Purposes	4.5	Special Categories of Data of Associates or Dependents may be Processed for Secondary Purposes in accordance with Article 3.
---	-----	--

Article 5 – Quantity and Quality of Data

No Excessive Data	5.1	JACOBS DOUWE EGBERTS shall restrict the Processing of Associate Data to that Data that are reasonably adequate for and relevant to the applicable Business Purpose. JACOBS DOUWE EGBERTS shall take reasonable steps to delete Associate Data that are not required for the applicable Business Purpose.
Storage period	5.2	JACOBS DOUWE EGBERTS generally shall retain Associate Data only for the period required to serve the applicable Business Purpose, to the extent reasonably necessary to comply with an applicable legal requirement or as advisable in light of an applicable statute of limitations. JACOBS DOUWE EGBERTS may specify (e.g., in a sub-policy, notice or records retention schedule) a time period for which certain categories of Associate Data may be kept. Promptly after the applicable storage period has ended, the Responsible Executive shall direct that the Data be: <ul style="list-style-type: none"> (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	Associate Data should be accurate, complete and kept up-to-date to the extent reasonably necessary for the applicable Business Purpose.
‘Self-service’	5.4	Where JACOBS DOUWE EGBERTS requires an Associate to update his own Associate Data, JACOBS DOUWE EGBERTS shall remind him at least once a year to do so.

Article 6 – Associate Information Requirements

Information requirements	6.1	JACOBS DOUWE EGBERTS shall inform Associates through a published privacy policy or notice about: <ul style="list-style-type: none"> (i) the Business Purposes for which their Data are Processed (ii) which Group Company is responsible for the Processing and (iii) other relevant information (e.g., the nature and categories of the Processed Data, the categories of Third Parties to which the Data are disclosed (if any), and how Associates can exercise their rights). (iv) the contact details of the data protection officer,
---------------------------------	-----	--

- (v) where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
- (vi) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.
- (vii) the right to lodge a complaint with a supervisory authority
- (viii) the right to withdraw consent where processing is based on such consent
- (ix) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- (x) (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- (xi) Where the data was not obtained from the Associate, the requirements for provision of information as stated in §6 (i-xi) will apply.

Article 7 – Associate Rights of Access and Rectification

Rights of Associates

7.1 Every Associate has the right to request an overview of his Associate Data Processed by or on behalf of JACOBS DOUWE EGBERTS. Where reasonably possible, the overview shall contain information regarding the source, type, purpose, retention period and categories of recipients of the relevant Associate Data.

If the Associate Data are incorrect, incomplete or not Processed in compliance with applicable law or this Code, the Associate has the right to have his Data rectified, deleted or blocked (as appropriate).

In addition, the Associate has the right to object to the Processing of his Data on the basis of compelling grounds related to his particular situation.

Additionally, the Associate shall have the right to:

- (i) object to the Processing on the basis of compelling grounds related to his particular situation;
 - (ii) be informed of the safeguards implemented by JACOBS DOUWE EGBERTS to provide an adequate level of protection of Personal Data transferred to a Third Party located in a Non-

Adequate Country;

- (iii) 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;
- (iv) restrict the Processing if the Processing is unlawful and the Associate objects to the deletion of his Personal Data;
- (v) receive a structured, machine-readable copy of his Personal Data and, where technically possible, to the transmission of his Personal Data to a Third Party directly. This right will only apply where the Processing is carried out by automated means and is based on consent as set forth in Articles 2.2 or 4.3 or based on a contract.
- (i) The Associate shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Procedure	7.2 Associates should send requests to the Compliance Officer responsible for their business and geographic area. Prior to fulfilling the request of the Associate, JACOBS DOUWE EGBERTS may require the Associate to: <ul style="list-style-type: none">(i) specify the type of Associate Data to which access is being sought(ii) specify, to the extent reasonably possible, the data system in which the Associate Data likely are stored(iii) specify the circumstances in which JACOBS DOUWE EGBERTS obtained the Associate Data(iv) show proof of identity and(v) in the case of a request for rectification, deletion or blockage, specify the reasons why the Associate Data are incorrect, incomplete or not Processed in accordance with applicable law or the Code.
Response period	7.3 Within thirty days of JACOBS DOUWE EGBERTS receiving the request, the Compliance Officer shall inform the Associate in writing either (i) of JACOBS DOUWE EGBERTS' position with regard to the request and any action JACOBS DOUWE EGBERTS has taken or will take in response or (ii) the ultimate date on which the Associate will be informed of JACOBS DOUWE EGBERTS' position (which date shall be no later than 8 weeks thereafter). a
Complaint	7.4 An Associate may file a complaint in accordance with Article 16.3 if: <ul style="list-style-type: none">(i) the response to the request is unsatisfactory to the Associate (e.g. the request is denied)(ii) the Associate has not received a response as required by Article 7.3 or

- (iii) the time period provided to the Associate in accordance with Article 7.3 is, in light of the relevant circumstances, unreasonably long and the Associate has objected but has not been provided with a shorter, more reasonable time period in which the Associate will receive a response.

- Denial of requests**
- 7.5 JACOBS DOUWE EGBERTS may deny an Associate request if:
- (i) the request does not meet the requirements of Articles 7.1 and 7.2
 - (ii) the request is not sufficiently specific
 - (iii) the identity of the relevant Associate 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 shall generally be deemed to be an unreasonable time interval.

Article 8 – Security and Confidentiality Requirements, Privacy by Design

- Data security**
- 8.1 JACOBS DOUWE EGBERTS shall take appropriate commercially reasonable technical, physical and organizational measures to protect Associate Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access.

- Data Breach Notification**
- 8.2 JACOBS DOUWE EGBERTS shall notify the Dutch Data Protection Authority of a Data Security Breach without undue delay unless such breach is unlikely to result in a risk to the rights and freedoms of the Associate. The measures for handling of such data breach shall be as provided in the relevant internal JACOBS DOUWE EGBERTS policies.

Notification to Associates affected by a Data Security Breach shall be made without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of natural persons and all other applicable conditions have been met. The measures for handling of such data breach shall be as provided in the relevant internal JACOBS DOUWE EGBERTS policies.

- Staff access**
- 8.3 Staff members shall be authorized to access Associate Data only to the extent necessary to serve the applicable Business Purpose and to perform their job.

- Confidentiality obligations**
- 8.4 Staff members who access Associate Data must meet their confidentiality obligations.

Article 9 – Automated Decision Making

- Automated decisions**
- 9.1 Automated tools used in processing personal data may be employed as a means to assist in making decisions about Associates. Such decisions may not be based solely on the results provided by the automated tool. This restriction does not apply if:
- (i) the use of automated tools is required or authorized by law
 - (ii) the decision is made by JACOBS DOUWE EGBERTS 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 JACOBS DOUWE EGBERTS was made by the Associate (e.g., where automated tools are used to filter job applications) or
 - (iii) based on the individual's explicit consent.
 - (iv) In the cases of (ii) and (iii) above, JACOBS DOUWE EGBERTS shall implement suitable measures to safeguard the data subject. At a minimum, this must include a right to obtain human intervention for the data subject to be able to express his or her point of view and to contest the decision.
 - (v) In cases of Special Categories of Data: Automated decision-taking based on Special Categories of Data may only take place: with explicit consent; or where the processing is necessary for substantial public interest reasons and on the basis of Union or Member State law – which must include measures to protect the interests of the data subjects.

Article 10 – Transfer of Associate Data to Third Parties

- Transfer to Third Parties**
- 10.1 This Article sets forth requirements concerning the transfer of Associate Data from JACOBS DOUWE EGBERTS to a Third Party. Note that a transfer of Associate Data includes situations in which JACOBS DOUWE EGBERTS discloses Associate Data to Third Parties (e.g., in the context of corporate due diligence) or where JACOBS DOUWE EGBERTS provides remote access to Associate Data to a Third Party.
- Third Party Controllers and Third- Party Processors**
- 10.2 There are two categories of Third Parties:
- (i) **Third Party Processors:** these are Third Parties that Process Associate Data solely on behalf of JACOBS DOUWE EGBERTS and at its direction (e.g., Third Parties that Process Associate salaries on behalf of JACOBS DOUWE EGBERTS)
 - (ii) **Third Party Controllers:** these are Third Parties that Process Associate Data and determine the purposes and means of the Processing (e.g., government authorities or service providers that provide services directly to Associates).
- Transfer for**
- 10.3 JACOBS DOUWE EGBERTS shall transfer Associate Data to a Third Party

applicable Business Purposes only		to the extent necessary to serve the applicable Business Purpose for which the Associate Data are Processed (including Secondary Purposes as per Article 3 or purposes for which the Associate has provided consent in accordance with Article 2.2 and 2.3).
Third Party Controller contracts	10.4	Third Party Controllers (other than government agencies) may Process Associate Data only if they have a written contract with JACOBS DOUWE EGBERTS. In the contract, JACOBS DOUWE EGBERTS shall seek to contractually protect the data protection interests of its Associates. All such contracts shall be drafted in consultation with the appropriate Compliance Officer.
Third Party Processor contracts	10.5	<p>Third Party Processors may Process Associate Data only if they have a written contract with JACOBS DOUWE EGBERTS. The contract with a Third-Party Processor must include the following provisions:</p> <ul style="list-style-type: none"> (i) the Processor shall Process Associate Data only in accordance with JACOBS DOUWE EGBERTS 's instructions and for the purposes authorized by JACOBS DOUWE EGBERTS (ii) the Processor and its Affiliates shall keep the Associate Data confidential (iii) the Processor shall take appropriate technical, physical and organizational security measures to protect the Associate Data (iv) the Third-Party Data Processor shall not permit subcontractors to Process Associate Data without the prior written consent of JACOBS DOUWE EGBERTS (v) JACOBS DOUWE EGBERTS has the right to 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 JACOBS DOUWE EGBERTS or any relevant government authority (vi) the Third-Party Processor shall promptly inform JACOBS DOUWE EGBERTS of any actual or suspected security breach involving Associate Data and (vii) the Third-Party Processor shall take adequate remedial measures as soon as possible and shall promptly provide JACOBS DOUWE EGBERTS with all relevant information and assistance as requested by JACOBS DOUWE EGBERTS regarding the security breach. (viii) Upon the request of JACOBS DOUWE EGBERTS, the Third-Party Processor shall delete or return all Personal Data 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	10.6	<p>This Article sets forth additional rules for the transfer of Associate Data to a Third Party located in a country that is not considered to provide an "adequate" level of protection for Associate Data (Non-Adequate Country).</p> <p>Associate Data may be transferred to a Third Party located in a Non-</p>

Adequate Country only if:

- (i) the transfer is necessary for the performance of a contract with the Associate, for managing the employment-at-will relationship or to take necessary steps at the request of the Associate 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 JACOBS DOUWE EGBERTS 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 Associate between JACOBS DOUWE EGBERTS and a Third Party (e.g. in case of the booking of an airline ticket)
- (iv) the Third Party has been certified under an approved code of conduct (based on the new scheme in Article 40) or an approved certification mechanism (based on the new scheme in Article 42) or any other similar program that is recognized as providing an “adequate” level of data protection
- (v) the Third Party has implemented binding corporate rules or a similar transfer control mechanism which provide adequate safeguards under applicable law
- (vi) the transfer is necessary to protect a vital interest of the Associate
- (vii) the transfer is necessary for the establishment, exercise or defense of a legal claim
- (viii) the transfer is necessary for important reasons of public interest.
- (ix) the transfer is required by any law to which the relevant Group Company is subject.

Items (viii) and (ix) above require the prior approval of the Privacy Compliance Officer.

Associate consent for transfer

10.7 JACOBS DOUWE EGBERTS generally shall not seek Associate consent for a transfer of Associate 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, JACOBS DOUWE EGBERTS shall also seek Associate consent for the relevant transfer. If none of the grounds listed in Article 10.6 exists, JACOBS DOUWE EGBERTS may request Associate 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 Associate or

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

Requesting Associate consent for a transfer requires the prior approval of the appropriate Compliance Officer. Prior to requesting Associate consent, the Associate shall be provided with the following information:

- (i) the purpose of the transfer
- (ii) the identity of the transferring Group Company
- (iii) the identity or categories of Third Parties to which the Data will be transferred
- (iv) the categories of Data that will be transferred
- (v) the country to which the Data will be transferred and
- (vi) the fact that the Data will be transferred to a Non-Adequate Country.

Transfers between Non-Adequate Countries

- 10.8 This Article sets forth additional rules for transfers of Associate Data that were collected in connection with the activities of a Group Company 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 are permitted if they are:
- (i) necessary for compliance with a legal obligation to which the relevant Group Company is subject
 - (ii) necessary to serve the public interest or
 - (iii) necessary to satisfy a Business Purpose.

Article 11 – Overriding Interests

Overriding Interests

- 11.1 Some of the obligations of JACOBS DOUWE EGBERTS or rights of Associates under this Code may be overridden if, due to the specific circumstances at issue, a pressing need exists that outweighs the interest of the Associate (**Overriding Interest**). An Overriding Interest exists if there is a need to:
- (i) protect the legitimate business interests of JACOBS DOUWE EGBERTS including
 - (a) the health, security or safety of Staff
 - (b) JACOBS DOUWE EGBERTS 's intellectual property rights, trade secrets or reputation
 - (c) the continuity of its 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 JACOBS DOUWE EGBERTS Code of Conduct or other JACOBS DOUWE EGBERTS policies or procedures or

- (iii) otherwise protect or defend the rights or freedoms of JACOBS DOUWE EGBERTS, its Staff 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 JACOBS DOUWE EGBERTS or rights of the Associate may be set aside: <ul style="list-style-type: none"> (i) Article 3.1 (the requirement to Process Associate Data for closely related purposes) (ii) Article 6.1 (information provided to Associates) (iii) Article 7.1 (rights of Associates) (iv) Articles 8.2 and 8.3 (Staff access limitations and confidentiality requirements) and (v) Articles 10.4, 10.5 and 10.6 (ii) (contracts with Third Parties).
Special Categories of Data	11.3	The requirements of Articles 4.1 and 4.2 (Special Categories of Data) may be set aside only for the Overriding Interests listed in Article 11.1 (i) (a), (c) and (e), (ii) and (iii).
Consultation with Privacy Compliance Officer	11.4	Setting aside obligations of JACOBS DOUWE EGBERTS or rights of Associates based on an Overriding Interest, requires the prior consultation of the Privacy Compliance Officer.
Information to Associate	11.5	Upon request of the Associate, JACOBS DOUWE EGBERTS shall inform the Associate of the Overriding Interest for which obligations of JACOBS DOUWE EGBERTS or rights of the Associate have been set aside, unless the particular Overriding Interest sets aside the requirements of Articles 6.1 or 7.1, in which case the request shall be denied.

Article 12 – Supervision and compliance

Privacy Compliance Officer	12.1	JACOBS DOUWE EGBERTS shall appoint a Privacy Compliance Officer who is responsible for: <ul style="list-style-type: none"> (i) supervising compliance with this Code (ii) providing periodic reports, as appropriate, to the Privacy Council on data protection risks and compliance issues and (iii) coordinating, in conjunction with the appropriate Compliance Officer, official investigations or inquiries into the Processing of Data by a government authority.
Privacy Council	12.2	JACOBS DOUWE EGBERTS shall establish an advisory Privacy Council. The Privacy Council shall create and maintain a framework for: <ul style="list-style-type: none"> (i) the development, implementation and updating of local Associate data protection policies and procedures (ii) the development of the policies, procedures and system information (as required by Article 13)

- (iii) the development, implementation and updating of the training and awareness programs
- (iv) the monitoring and reporting on compliance with this Code
- (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).

Compliance Officers	12.3	In each country or geographic area where a Group Company is established, one or more Compliance Officers shall be designated who shall be responsible for supervising compliance with this Code in the relevant business and country or geographic area. The Privacy Compliance Officer shall act as the Compliance Officer for JACOBS DOUWE EGBERTS. These Compliance Officers may, in turn, establish a network of Compliance Officers sufficient to direct compliance with this Code within their respective organizations. The Compliance Officers shall: <ul style="list-style-type: none"> (i) regularly advise their respective executive teams and the Privacy Compliance Officer on privacy risks and compliance issues (ii) establish a framework for a privacy compliance program as required by the Privacy Compliance Officer and (iii) cooperate with the Privacy Compliance Officer and the other Compliance Officers.
Default Compliance Officer	12.4	If at any moment in time there is no Compliance Officer designated for a function or business, the Compliance Officer to whom the missing Compliance Officer for the relevant function or business would report, is responsible for supervising compliance with this Code.
Compliance Officer with a statutory position	12.5	Where a Compliance Officer responsible for supervising compliance with this Code (or privacy 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	JACOBS DOUWE EGBERTS shall develop and implement policies and procedures to comply with this Code.
System information	13.2	JACOBS DOUWE EGBERTS shall maintain readily available information regarding the structure and functioning of all systems and processes that Process Associate Data (e.g. inventory of systems and processes, privacy impact assessments).

Article 14 – Training

- Staff training** 14.1 JACOBS DOUWE EGBERTS shall provide training on this Code and related confidentiality obligations to Staff members who have access to Associate Data.

Article 15 – Monitoring and auditing compliance

- Monitoring** 15.1 JACOBS DOUWE EGBERTS management shall monitor compliance with this Code as a part of their regular business processes and procedures.
- Audits** 15.2 The JACOBS DOUWE EGBERTS Audit function shall audit business processes and procedures that involve the Processing of Associate Data for compliance with this Code. The audits shall be carried out in the course of the regular activities of the JACOBS DOUWE EGBERTS Audit function or at the request of the Privacy Compliance Officer. The Privacy Compliance 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 shall be observed when conducting an audit. The Privacy Compliance Officer and the appropriate Compliance Officers shall be informed of the results of the audits. Reported violations of this Code will be reported back to senior management. A copy of the audit results will be provided to the Dutch Data Protection Authority upon request. When required, the Dutch Data Protection Authority may carry out a data protection audit of JACOBS DOUWE EGBERTS. Such audit right will also apply to the Data Protection Authorities with jurisdiction over other Group Company members.
- Annual Report** 15.3 The Privacy Compliance Officer shall produce an annual Associate Data privacy report for the Privacy Council on compliance with this Code and other relevant issues.
- Each Compliance Officer shall provide information relevant to the report to the Privacy Compliance Officer.
- Mitigation** 15.4 JACOBS DOUWE EGBERTS 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 15.

Article 16 – Complaints procedure

- Complaint to Compliance Officer** 16.1 Associates 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 JACOBS DOUWE EGBERTS' Code of Conduct with the Compliance Officer responsible for their business and geographic area.

The Compliance Officer shall:

- (a) notify the Privacy Compliance Officer
- (b) initiate an investigation and
- (c) when necessary, advise the business on the appropriate measures for compliance and monitor, through completion, the steps designed to achieve compliance.

The Compliance Officer may consult with any government authority having jurisdiction over a particular matter about the measures to be taken.

Reply to Associate 16.2 Within thirty days of JACOBS DOUWE EGBERTS receiving a complaint, the Compliance Officer shall inform the Associate in writing either (i) of JACOBS DOUWE EGBERTS position with regard to the complaint and any action JACOBS DOUWE EGBERTS has taken or will take in response or (ii) when he will be informed of JACOBS DOUWE EGBERTS' position (which shall be no later than 16 weeks thereafter). The Compliance Officer shall send a copy of the complaint and his written reply to the Privacy Compliance Officer.

Complaint to Privacy Compliance Officer 16.3 An Associate may file a complaint with the Privacy Compliance Officer if:

- (i) the resolution of the complaint by the Compliance Officer responsible for their business and geographic area is unsatisfactory to the Associate (e.g., the complaint is rejected)
- (ii) the Associate has not received a response as required by Article 16.2
- (iii) the time period provided to the Associate pursuant to Article 16.2 is, in light of the relevant circumstances, unreasonably long and the Associate 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 shall apply to complaints filed with the Privacy Compliance Officer.

Article 17 – Legal issues

Local law and jurisdiction 17.1 Any Processing by JACOBS DOUWE EGBERTS of Associate Data shall be governed by applicable local law. Associates keep their own rights and remedies as available in their local jurisdictions. Local government authorities having jurisdiction over the relevant matters shall maintain their authority.

Law applicable to Code; Code has 17.2 This Code shall be governed by and interpreted in accordance with Dutch law. This Code shall apply only where it provides supplemental protection for Associate Data. Where applicable local law provides more

supplemental character		protection than this Code, local law shall apply. Where this Code provides more protection than applicable local law or provides additional safeguards, rights or remedies for Associates, this Code shall apply. Where the General Data Protection Regulation provides for less protection than this Code, JDE may choose to apply this Code or the General Data Protection Regulation.
Lead Authority for supervision of Code	17.3	Compliance with this Code shall be exclusively supervised by the Dutch Data Protection Authority in The Netherlands, which is also exclusively authorized to advise JACOBS DOUWE EGBERTS on the application of this Code at all times. The Dutch Data Protection Authority shall have investigative powers based on the Dutch Data Protection Act. To the extent the Dutch Data Protection Authority has discretionary powers related to enforcement of the Dutch Data Protection Act, it shall have similar discretionary powers for enforcement of this Code.
Liability and Exclusive jurisdiction under Code	17.4	JACOBS DOUWE EGBERTS shall be responsible for and take the required action to remedy the acts of other Group Company members under this Code. Any complaints or claims of an Associate concerning any supplemental right the Associate may have under this Code shall be directed to JACOBS DOUWE EGBERTS only and shall be brought before the Dutch Data Protection Authority in The Netherlands or the competent court in Amsterdam, The Netherlands. The Dutch Data Protection Authority and courts in Amsterdam, The Netherlands have exclusive jurisdiction over any supplemental rights provided by this Code. Complaints and claims shall be admissible only if the Associate has first followed the complaints procedure set forth in Article 16 of this Code.
Code enforceable against JACOBS DOUWE EGBERTS only	17.5	Any additional safeguards, rights or remedies granted to Associates under this Code are granted by and enforceable in the Netherlands against JACOBS DOUWE EGBERTS only.
Available remedies, limitation of damages, burden of proof re damages	17.6	Associates shall only be entitled to remedies available to data subjects under the Dutch Data Protection Act, the Dutch Civil Code and the Dutch Code on Civil Procedure. However, JACOBS DOUWE EGBERTS shall be liable only for direct damages suffered by an Associate resulting from a violation of this Code. Provided Associates can demonstrate that they have suffered damage and can establish facts which show it is plausible that the damage has occurred because of a violation of the Code, it will be for JACOBS DOUWE EGBERTS to prove that the damages suffered by the relevant Associate due to a violation of the Code are not

attributable to the relevant Group Company.

- Mutual assistance and redress**
- 17.7 All Group Companies shall co-operate and assist each other to the extent reasonably possible to handle:
- (i) a request, complaint or claim made by an Associate or
 - (ii) a lawful investigation or inquiry by a competent government authority.

The Group Company employing the Associate is responsible for handling any communication with the Associate regarding his request, complaint or claim except where circumstances dictate otherwise.

The Group Company that is responsible for the Processing to which the request, complaint or claim relates, shall bear all costs involved and reimburse JACOBS DOUWE EGBERTS.

Article 18 – Sanctions for non-compliance

- Non-compliance**
- 18.1 Non-compliance of Associates with this Code may result in disciplinary action up to and including termination of employment

Article 19 – Conflicts between the Code and applicable local law

- Conflict of law when transferring Data**
- 19.1 Where a legal requirement to transfer Associate Data conflicts with the laws of the Member States of the EEA or the law of Switzerland, the transfer requires the prior approval of the Privacy Compliance Officer. The Privacy Compliance Officer shall seek the advice of the General Counsel. The Privacy Compliance Officer may seek the advice of the Dutch Data Protection Authority or another competent government authority.

- Conflict between Code and law**
- 19.2 In all other cases, where there is a conflict between applicable local law and the Code, the relevant Responsible Executive shall consult with the Privacy Compliance 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 Group Company.

- New conflicting legal requirements**
- 19.3 The relevant Responsible Executive shall promptly inform the Privacy Compliance Officer of any new legal requirement that may interfere with JACOBS DOUWE EGBERTS' ability to comply with this Code.

Article 20 – Changes to the Code

- 20.1 Any changes to this Code require the prior approval of the General Counsel and the Privacy Compliance Officer of JACOBS DOUWE EGBERTS. Group Companies shall be notified of changes to this Code

without undue delay. JACOBS DOUWE EGBERTS shall notify the Dutch Data Protection Authority in case of significant changes to the Code on a yearly basis.

- 20.2 This Code may be changed without Associate consent even though an amendment may relate to a benefit conferred on Associates. Local law including Works Council and other Associates' representation regulations shall apply.
- 20.3 Any amendment shall enter into force after it has been approved and published on JACOBS DOUWE EGBERTS' Intranet.
- 20.4 Any request, complaint or claim of an Associate involving this Code shall be judged against 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, there shall be a two-year transition period for compliance with this Code. Accordingly, except as otherwise indicated, within two years of the Effective Date, all Processing of Associate Data shall be undertaken in compliance with the Code. During any transition period, JACOBS DOUWE EGBERTS shall strive to comply with the Code. |
| Transition Period for New Group Companies | 21.2 | Any entity that becomes a Group Company after the Effective Date shall comply with the Code within two years of becoming a Group Company. |
| Transition Period for IT Systems | 21.3 | Where implementation of this Code requires updates or changes to information technology systems (including replacement of systems), the transition period shall be four years from the Effective Date or from the date an entity becomes a Group Company, or any longer period as is reasonably necessary to complete the update, change or replacement process. |
| Transition Period for Existing Agreements | 21.4 | 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 | 21.5 | Processing of Associate Data that were collected in connection with activities of a Group Company located in a Non-Adequate Country shall be brought into compliance with this Code within five years of the Effective Date. |

Contact details

JACOBS DOUWE EGBERTS
Privacy Compliance Officer
Oosterdoksstraat 80
1011 DK Amsterdam
The Netherlands
Email address: privacy@jdecoffee.com

ANNEX 1 **Definitions**

Archive	ARCHIVE shall mean a collection of Associate 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 Associate other than the system administrator.
Article	ARTICLE shall mean an article in this Code.
Business Purpose	BUSINESS PURPOSE shall mean a purpose for Processing Associate Data as specified in Article 2 or 3 or for Processing Special Categories of Data as specified in Article 4 or 3.
Privacy Compliance Officer	PRIVACY COMPLIANCE OFFICER shall mean the officer as referred to in Article 12.1.
Code	CODE shall mean this Privacy Code for Associate 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.
Dependent	DEPENDANT shall mean the spouse, partner or child belonging to the household of the Associate.
Effective Date	EFFECTIVE DATE shall mean the date on which this Code becomes effective as set forth in Article 1.6.
Associate	ASSOCIATE shall mean an employee, job applicant or former employee of JACOBS DOUWE EGBERTS. This term does not include people working at JACOBS DOUWE EGBERTS as consultants or employees of Third Parties providing services to JACOBS DOUWE EGBERTS.
Associate Data or Data	ASSOCIATE DATA or DATA shall mean any information relating to an identified or identifiable Associate (and his Dependents).
EEA	EEA or EUROPEAN ECONOMIC AREA shall mean all Member States of the European Union, plus Norway, Iceland and Liechtenstein.
EU Data Protection Directive	EU DATA PROTECTION DIRECTIVE shall mean the Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of and the free movement of such data.
General Counsel	GENERAL COUNSEL shall mean the general counsel of JACOBS DOUWE EGBERTS.

Group Company	GROUP COMPANY shall mean JACOBS DOUWE EGBERTS B.V. and any company or legal entity of which JACOBS DOUWE EGBERTS B.V., directly or indirectly owns more than 50% of the issued share capital, has 50% or more of the voting power at general meetings of shareholders, has the power to appoint a majority of the directors, or otherwise directs the activities of such other legal entity; however, any such company or legal entity shall be deemed a Group Company only as long as a liaison and/or relationship exists, and that is covered by the JACOBS DOUWE EGBERTS Code of Conduct.
JACOBS DOUWE EGBERTS	JACOBS DOUWE EGBERTS shall mean JACOBS DOUWE EGBERTS B.V., a Dutch private limited liability company, having its registered seat and its principal place of business in Amsterdam, the Netherlands, and its Group Companies.
Non-Adequate Country	NON-ADEQUATE COUNTRY shall mean a country that under applicable local law (such as Article 25 of the EU Data Protection Directive) is deemed not to provide an "adequate" level of data protection.
Original Purpose	ORIGINAL PURPOSE shall mean the purpose for which Associate Data were originally collected.
Overriding Interest	OVERRIDING INTEREST shall mean the pressing interests set forth in Article 11.1 based on which the obligations of JACOBS DOUWE EGBERTS or rights of Associates set forth in Article 11.2 and 11.3 may, under specific circumstances, be overridden if this pressing interest outweighs the interest of the Associate.
Privacy Council	PRIVACY COUNCIL shall mean the council referred to in Article 12.2
Compliance Officer	COMPLIANCE OFFICER shall mean a Compliance Officer appointed by the Privacy Compliance Officer pursuant to Article 12.3.
Processing	PROCESSING shall mean any operation that is performed on Associate 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 Associate Data.
Responsible Executive	RESPONSIBLE EXECUTIVE shall mean the HR manager with primary budgetary ownership over the relevant processing of Associate Data.
Secondary Purpose	SECONDARY PURPOSE shall mean any purpose other than the Original Purpose for which Associate Data are further Processed.
Special	SPECIAL CATEGORIES OF DATA shall mean Associate Data that reveal an

Categories of Data	Associate'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.
Staff	STAFF shall mean all Associates and other persons who Process Associate Data as part of their respective duties or responsibilities using JACOBS DOUWE EGBERTS information technology systems or working primarily from JACOBS DOUWE EGBERTS 's premises.
Third Party	THIRD PARTY shall mean any person, private organization or government body outside JACOBS DOUWE EGBERTS.
Third Party Controller	THIRD PARTY CONTROLLER shall mean a Third Party that Processes Associate Data and determines the purposes and means of the Processing.
Third Party Processor	THIRD PARTY PROCESSOR shall mean a Third Party that Processes Associate Data on behalf of JACOBS DOUWE EGBERTS that is not under the direct authority of JACOBS DOUWE EGBERTS.