Vopak Privacy Code for Customer, Supplier and Business Partner Data

Introduction

Vopak has committed itself to the protection of personal data it processes of its employees, customers, suppliers and business partners in its Code of Conduct.

This Privacy Code indicates how this principle shall be implemented in respect of personal data of customers, suppliers and business partners and other individuals that are processed by Vopak in the context of its business activities.

For the privacy code applicable to employee data, refer to the *Privacy Code for Employee Data*.

Article 1 – Scope, Applicability and Implementation

Scope	1.1	This Code addresses the Processing of Personal Data of Customers, Suppliers and Business Partners and other Individuals by Vopak or a Third Party Processor on behalf of Vopak. This Code does not address the Processing of Personal Data of Employees of Vopak.
Electronic and paper-based Processing	1.2	This Code applies to the Processing of Personal Data by electronic means and in systematically accessible paper-based filing systems.
Applicability of local law and Code	1.3	Individuals keep any rights and remedies they may have under Applicable Data Controller Law. This Code shall apply only where it provides supplemental protection for Personal Data. Where Applicable Data Controller Law provides more protection than this Code, Applicable Data Controller Law shall apply. Where this Code provides more protection than Applicable Data Controller Law or provides additional safeguards, rights or remedies for Individuals, this Code shall apply.
Sub-policies and notices	1.4	Vopak may supplement this Code through sub-policies or notices that are consistent with this Code.
Accountability	1.5	The Responsible Executives shall be accountable for compliance with this Code.
Effective Date	1.6	This Code has been adopted by the Executive Board of Royal Vopak and shall enter into force as of 01/10/2017 (**Effective Date**) and shall be published on the Vopak's website and Vopak's intranet and shall be made available to Individuals upon request.
Code supersedes prior policies	1.7	This Code supersedes all Vopak's 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 shall be implemented in the Vopak organization based on the timeframes specified in Article 22.

Article 2 – Purposes for Processing Personal Data

Legitimate	2.1	Personal Data shall be collected, used or otherwise Processed by Vopak for

Business Purposes

one (or more) of the following purposes (**Business Purposes**):

(i) **Assessment and acceptance of a Customer, conclusion and execution of agreements with a Customer.** This purpose includes Processing of Personal Data that are necessary in connection with the assessment and acceptance of Customers including confirming and verifying the identity of relevant Individuals and conducting due diligence, screening against publicly available government and/or law enforcement agency sanctions lists. This activity also includes the Processing of Personal Data in connection with the execution of agreements, including the delivery of customer services

(ii) **Development and improvement of products and/or services.** This purpose includes Processing of Personal Data that is necessary for the development and improvement of Vopak's products and/or services, research and development;

(iii) **Conclusion and execution of agreements with Customers, Suppliers and Business Partners.** This purpose addresses the Processing of Personal Data necessary to conclude and execute agreements with Customers, Suppliers and Business Partners, including required screening activities (e.g. for access to Vopak's premises or systems) and to record and financially settle delivered services, products and materials to and from Vopak;

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

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

(vi) **Health, safety and security.** This purpose includes the protection of the interests of Vopak and its Employees and Customers and activities such as those involving safety and health, the protection of Vopak and Employee assets, and the authentication of Customer, Supplier or Business Partner status and access rights;

(vii) **Compliance with law.** This purpose addresses the Processing of Personal Data necessary for the performance of a task carried out to comply with or authorized by law including the disclosure of Personal Data to government institutions or supervisory authorities in relation thereto or

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

Where there is a question whether a Processing of Personal Data can be based on a Business Purpose listed above, it is necessary to seek the advice of the appropriate Privacy Officer before the Processing takes place.

Consent

2.2 If a Business Purpose does not exist or if Applicable Data Controller Law so requires Vopak shall (also) seek consent from the Individual for the Processing.

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

When seeking consent, Vopak must inform the Individual:

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

Denial or withdrawal of consent

2.3 The Individual may both deny consent and withdraw consent at any time. The withdrawal of consent shall not affect the lawfulness of the Processing based on such consent before its withdrawal. Vopak will discontinue such Processing as soon as possible.

Article 3 – Use for Other Purposes

Use of Data for Secondary Purposes

3.1 Generally, Personal Data shall be used only for the Business Purposes for which they were originally collected (**Original Purpose**). Personal Data may be Processed for a legitimate Business Purpose of Vopak different from the Original Purpose (**Secondary Purpose**) only if the Original Purpose and Secondary Purpose are closely related. Depending on the sensitivity of the relevant Personal Data and whether use of the Data for the Secondary Purpose has potential negative consequences for the Individual, the secondary use may require additional measures such as:

(i) limiting access to the Data
(ii) imposing additional confidentiality requirements
(iii) taking additional security measures
(iv) informing the Individual about the Secondary Purpose
(v) providing an opt-out opportunity or
(vi) obtaining an Individual's consent in accordance with Article 2.2 or Article 4.3 (if applicable).

Article 4 – Purposes for Processing Sensitive Data

Specific purposes for Processing Sensitive Data

4.1 This Article sets forth specific rules for Processing Sensitive Data. Vopak shall Process Sensitive Data only to the extent necessary to serve the applicable Business Purpose.

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

(i) **Racial or ethnic data**: in some countries photos and video images of Individuals qualify as racial or ethnic data. Vopak may process photos (e.g. a copy of a passport containing a photo) and video images for the protection of Vopak and Employee assets, site access and security reasons, the identification and the authentication of Customer, Supplier or Business Partner status and access rights and for verifying and confirming advice provided by Vopak (e.g. when Individuals participate in video conferencing which is recorded).
(ii) **Criminal data** (including data relating to criminal behavior, criminal records or proceedings regarding criminal or unlawful behavior) for protecting the interests of Vopak its Employees and Customers with respect to criminal offences that have been or, given the relevant circumstances are suspected to be or have been, committed against Vopak or its Employees.
(iii) **Religion or beliefs:** accommodating specific products or services for a Customer, dietary requirements or religious holidays**.**

General Purposes for Processing of Sensitive Data

4.2 In addition to the specific purposes listed in Article 4.1 above, all categories of Sensitive Data may be Processed for one (or more) of the following purposes:

(i) when necessary for the performance of a task carried out to comply with or authorized by law
(ii) for the establishment, exercise or defence of a legal claim
(iii) to protect a vital interest of an Individual, but only where it is impossible to obtain the Individual's consent first
(iv) to the extent necessary to comply with an obligation of international public law (e.g. treaties) or
(v) where the Sensitive Data have manifestly been made public by the Individual.

Consent, and the denial or withdrawal of consent

4.3 In addition to the specific purposes listed in Article 4.1 and the general purposes listed in Article 4.2, all categories of Sensitive Data may be Processed if the Individual has given his explicit consent to the Processing thereof. If one of the purposes listed in Articles 4.1 and 4.2 apply, Vopak shall in addition seek consent if Applicable Data Controller Law so requires. The information requirements set out in Article 2.2 and Article 2.3 apply to the granting, denial or withdrawal of consent.

Prior Authorization of Privacy Officer

4.4 Where Sensitive Data are Processed based on a requirement of law other than the local law applicable to the Processing, the Processing requires the prior authorization of the appropriate Privacy Officer.

Use of Sensitive Data for Secondary Purposes

4.5 Sensitive Data of Individuals may be Processed for Secondary Purposes in accordance with Article 3.

Article 5 – Quantity and Quality of Data

No Excessive Data

5.1 Vopak shall restrict the Processing of Personal Data to Data that are reasonably adequate for and relevant to the applicable Business Purpose. Vopak shall take reasonable steps to delete Personal Data that are not required for the applicable Business Purpose.

Storage period

5.2 Vopak generally shall retain Personal 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. Vopak may specify (e.g., in a sub-policy, notice or records retention schedule) a time period for which certain categories of Personal Data may be kept.

Promptly after the applicable storage period has ended, the Privacy Officer shall direct that the Data be:

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

Quality of Data

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

Accurate, complete and up-to-date Data

5.4 It is the responsibility of the Individuals to keep his Personal Data accurate, complete and up-to-date. Individuals shall inform Vopak regarding any changes in accordance with Article 7.

Article 6 – Individual Information Requirements

Information requirements

6.1 Vopak shall provide Individuals with the following privacy information:

(i) the Business Purposes for which their Data are Processed
(ii) which Group Company is responsible for the Processing and
(iii) the categories of Third Parties to which the Data are disclosed (if any); if the Third Party is located in a Non-Adequate Country, the Individual will be informed thereof as well, and
(iv) other relevant information (e.g., the nature and categories of the Processed Data, and how Individuals can exercise their rights).

Personal Data not obtained from the Individual

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

(i) at the time that the Personal Data are recorded in a Vopak database or
(ii) at the time that the Personal Data are used for a mailing, provided that this mailing is done within six months after the Personal Data are recorded in a Vopak database.

Exceptions

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

(i) it is impossible or would involve a disproportionate effort to provide the information to Individuals or
(ii) it results in disproportionate costs.

These exceptions to the above requirements qualify as Overriding Interests.

Article 7 – Individual Rights of Access and Rectification

Rights of Individuals

7.1 Every Individual has the right to request an overview of his Personal Data Processed by or on behalf of Vopak. Where reasonably possible, the overview shall contain information regarding the source, type, purpose and categories of recipients of the relevant Personal Data.
If the Personal Data are incorrect, incomplete or not Processed in compliance with Applicable Data Controller Law or this Code, the Individual has the right to have his Data rectified, deleted or blocked (as appropriate).

In addition, the Individual has the right to object to:

(i) the Processing of his Data on the basis of compelling grounds related to his particular situation; and
(ii) receiving marketing communications on the basis of Article 9.5.

Procedure

7.2 The Individual should send his request to the contact person or contact point indicated in the relevant privacy statement or notice. If no contact person or contact point is indicated, the Individual may send his request through the general contact section of the Vopak website.

Prior to fulfilling the request of the Individual, Vopak may require the Individual to:

(i) specify the categories of Personal Data to which he is seeking access
(ii) specify, to the extent reasonably possible, the data system in which the Data are likely to be stored
(iii) specify, to the extent reasonably possible, the circumstances in which Vopak obtained the Personal Data
(iv) provide proof of his identity; and
(v) pay a fee to compensate Vopak for the reasonable costs relating to fulfilling the request of the Individual
(vi) in the case of a request for rectification, deletion, or blockage, specify the reasons why the Personal Data are incorrect,

incomplete or not Processed in accordance with Applicable Data Controller Law or the Code.

Response period 7.3 Within four weeks of Vopak receiving the request, the Vopak contact person, or Privacy Officer shall inform the Individual in writing either (i) of Vopak's position with regard to the request and any action Vopak has taken or will take in response or (ii) the ultimate date on which he will be informed of Vopak's position, which date shall be no later than four weeks thereafter.

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

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

Denial of requests 7.5 Vopak may deny an Individual request if:

(i) the request does not meet the requirements of Articles 7.1 and 7.2
(ii) the request is not sufficiently specific
(iii) the identity of the relevant Individual 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.

Article 8 – Security and Confidentiality Requirements

Data security 8.1 Vopak shall take appropriate commercially reasonable technical, physical and organizational measures to protect Personal Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access.

Staff access 8.2 Staff members shall be authorized to access Personal Data only to the extent necessary to serve the applicable Business Purpose and to perform their job.

Confidentiality obligations 8.3 Staff members who access Personal Data must meet their confidentiality obligations.

Data Security Breach notification requirement 8.4 If Applicable Data Controller Law so requires, Vopak shall notify the Individual of a Data Security Breach within a reasonable period of time following discovery of such breach, unless a law enforcement or supervisory authority determines that notification would impede a criminal investigation or cause damage to national security. In this case, notification shall be delayed as instructed by such authority. Vopak shall respond promptly to inquiries of Individuals relating to such Data Security Breach.

Article 9 – Direct Marketing

Direct marketing 9.1 This Article sets forth requirements concerning the Processing of Personal Data for direct marketing purposes (e.g. contacting the Individual by email, fax, phone, SMS or otherwise, with a view of solicitation for commercial or charitable purposes).

Consent for direct marketing (opt-in) 9.2 If applicable law so requires, Vopak shall only send to Individuals unsolicited commercial communication by fax, email, sms and mms with the prior consent of the Individual ("opt-in"). If applicable law does not require prior consent of the Individual, Vopak shall in any event offer the Individual the opportunity to opt-out of such unsolicited commercial communication.

Exception (opt-out) 9.3 Prior consent of the Individual for sending unsolicited commercial communication by fax, email, sms and mms is not required if:

(i) an Individual has provided his electronic contact details to a Group Company in the context of a sale of a product or service of such Group Company; and

(ii) such contact details are used for direct marketing of such Group Company's own similar products or services

(iii) provided that an Individual clearly and distinctly has been given the opportunity to object free of charge, and in an easy manner, to such use of his electronic contact details when they are collected by the Group Company.

Information to be provided in each communication 9.4 In every direct marketing communication that is made to the Individual, the Individual shall be offered the opportunity to opt-out of further direct marketing communications.

Objection to direct marketing 9.5 If an Individual objects to receiving marketing communications from Vopak, or withdraws his consent to receive such materials, Vopak will take steps to refrain from sending further marketing materials as specifically requested by the individual. Vopak will do so within the time period required by applicable law.

Third Parties and Direct marketing 9.6 No Data shall be provided to, or used on behalf of, Third Parties for purposes of direct marketing of such Third Parties without the prior consent of the Individual.

Personal Data of Children 9.7 Vopak shall not use any Personal Data of Children for direct marketing, without the prior consent of their parent or custodian.

Direct marketing records 9.8 Vopak shall keep a record of Individuals that used their "opt-in" or "opt-out" right and will regularly check the public opt-out registers.

Article 10 – Automated Decision Making

Automated decisions 10.1 Automated tools may be used to make decisions about Individuals but decisions with a negative outcome for the Individual 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 necessary for the performance of a task carried out to comply with or authorized by law.

(ii) the decision is made by Vopak for purposes of (a) entering into or performing a contract or (b) managing the contract, provided the underlying request leading to a decision by Vopak was made by the Individual (e.g., where automated tools are used to filter promotional game submissions) or

(iii) suitable measures are taken to safeguard the legitimate interests of the Individual, e.g., the Individual has been provided with an opportunity to express his point of view.

Article 11 – Transfer of Personal Data to Third Parties

Transfer to 11.1 This Article sets forth requirements concerning the transfer of Personal Data

Third Parties

from Vopak to a Third Party. Note that a transfer of Personal Data includes situations in which Vopak discloses Personal Data to Third Parties (e.g., in the context of corporate due diligence) or where Vopak provides remote access to Personal Data to a Third Party.

Third Party Controllers and Third Party Processors

11.2 There are two categories of Third Parties:

(i) **Third Party Processors:** these are Third Parties that Process Personal Data solely on behalf of Vopak and at its direction (e.g., Third Parties that Process online registrations made by Customers)

(ii) **Third Party Controllers:** these are Third Parties that Process Personal Data and determine the purposes and means of the Processing (e.g. Vopak's Business Partners that provide their own goods or services directly to Customers).

Transfer for applicable Business Purposes only

11.3 Vopak shall transfer Personal Data to a Third Party to the extent necessary to serve the applicable Business Purpose (including Secondary Purposes as per Article 3 or purposes for which the Individual has provided consent in accordance with Article 2).

Third Party Controller safeguards

11.4 Third Party Controllers (other than government agencies) may Process Personal Data only if they have a written contract with Vopak. In the contract, Vopak shall seek to contractually safeguard the data protection interests of its Individuals when Personal Data are transferred to Third Party Controllers. All such contracts shall be drafted in consultation with the appropriate Privacy Officer. Individual Business Contact Data may be transferred to a Third Party Controller without safeguards if it is reasonably expected that such Business Contact Data will be used by the Third Party Controller to contact the Individual for legitimate business purposes related to Individual's job responsibilities.

Third Party Processor contracts

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

(i) the Third Party Processor shall Process Personal Data only in accordance with Vopak's instructions and for the purposes authorized by Vopak

(ii) the Processor shall keep the Personal Data confidential

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

(iv) the Third Party Processor shall not permit subcontractors to Process Personal Data in connection with its obligations to Vopak without the prior written consent of Vopak

(v) Vopak has the right to review the security measures taken by the Third Party Processor and the Third Party Processor shall subject its relevant data processing facilities to audits and inspections by Vopak, a Third Party on behalf of Vopak or any relevant government authority

(vi) the Third Party Processor shall promptly inform Vopak of any actual or suspected security breach involving Personal Data and

(vii) the Third Party Processor shall take adequate remedial measures as soon as possible and shall promptly provide Vopak with all relevant information and assistance as requested by Vopak regarding the security breach.

Transfer of Data to a Non-Adequate Country

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

(i) the transfer is necessary for the performance of a contract with

the Individual, for managing a contract with the Individual or to take necessary steps at the request of the Individual prior to entering into a contract, e.g., for processing orders

(ii) a contract has been concluded between Vopak and the relevant Third Party that (a) such Third Party shall be bound by the terms of this Policy as were it a Group Company; or (b) provides for safeguards at a similar level of protection as that provided by this Code; in which case the contract shall conform to any model contract requirement under applicable local law (if any)

(iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Individual between Vopak and a Third Party (e.g. in case of recalls)

(iv) the Third Party has been certified under a program that is recognized under applicable law as providing an "adequate" level of data protection

(v) the Third Party has implemented Binding Corporate Rules or a similar transfer control mechanism which provides adequate safeguards under applicable law

(vi) the transfer is necessary to protect a vital interest of the Individual

(vii) the transfer is necessary for the establishment, exercise or defense of a legal claim

(viii) the transfer is necessary to satisfy a pressing need to protect the public interests of a democratic society or

(ix) the transfer is necessary for the performance of a task carried out to comply with or authorized by law to which the relevant Group Company is subject.

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

Consent for transfer

11.7 If none of the grounds listed in Article 11.6 exist or if Applicable Data Controller Law so requires Vopak shall (also) seek consent from the Individual for the transfer to a Third Party located in a Non-Adequate Country.
Prior to requesting consent, the Individual 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.

Article 2.3 applies to denial or withdrawal of consent.

Transfers between Non-Adequate Countries

11.8 This Article sets forth additional rules for transfers of Personal Data that were collected in connection with the activities of a 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 11.6, 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 of Vopak.

Article 12 – Overriding Interests

Overriding Interests

12.1 Some of the obligations of Vopak or rights of Individuals under this Code may be overridden if, under the specific circumstances at issue, a pressing need exists that outweighs the interest of the Individual (**Overriding Interest**). An Overriding Interest exists if there is a need to:

(i) protect the legitimate business interests of Vopak including
  (a) the health, security or safety of Employees or Individuals
  (b) Vopak's intellectual property rights, trade secrets or reputation the continuity of Vopak's business operations
  (c) the preservation of confidentiality in a proposed sale, merger or acquisition of a business or
  (d) the involvement of trusted advisors or consultants for business, legal, tax, or insurance purposes
(ii) prevent or investigate (including cooperating with law enforcement) suspected or actual violations of law or
(iii) otherwise protect or defend the rights or freedoms of Vopak, its Employees or other persons.

Exceptions in the event of Overriding Interests

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

(i) Article 3.1 (the requirement to Process Personal Data for closely related purposes)
(ii) Article 6.1 and 6.2 (information provided to Individuals, Personal Data not obtained from the Individuals)
(iii) Article 7.1 (rights of Individuals)
(iv) Articles 8.2 and 8.3 (Staff access limitations and confidentiality requirements) and
(v) Articles 11.4, 11.5 and 11.6 (ii) (contracts with Third Parties).

Sensitive Data

12.3 The requirements of Articles 4.1 and 4.2 (Sensitive Data) may be set aside only for the Overriding Interests listed in Article 12.1 (i) (a), (b), (c) and (e), (ii) and (iii).

Consultation with Chief Privacy Officer

12.4 Setting aside obligations of Vopak or rights of Individuals based on an Overriding Interest requires prior consultation of the Chief Privacy Officer.

Information to Individual

12.5 Upon request of the Individual, Vopak shall inform the Individual of the Overriding Interest for which obligations of Vopak or rights of the Individual 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 13 – Supervision and Compliance

Chief Privacy Officer

13.1 **Royal Vopak** shall appoint a Chief Privacy Officer who is responsible for:

(i) Supervising compliance with this Code;
(ii) Coordinating, communicating and consulting with the Privacy Officers network (appointed in accordance with article 13.3) on central data protection issues;
(iii) Providing annual privacy reports, as appropriate, to the Compliance Committee on data protection risks and compliance issues as described in article 16.2;
(iv) Coordinating, in conjunction with the Privacy Officers network and the Compliance Committee, official investigations or inquiries into the Processing of Personal Data by a government authority;
(v) Dealing with conflicts between this Code and applicable law as described in article 20.2;
(vi) Approving transfers as described in articles 20.1 and 11.6;

(vii) Carrying out a Privacy Impact Assessment (PIA) before a new system or a business process involving Processing of Personal Data is implemented.
(viii) Deciding on complaints as described in article 17; and
(ix) Devising the data management processes, systems and tools to implement the framework for data protection management as established by the Compliance 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 audit systems to monitor, audit and report compliance with this Code and ensure that Vopak's internal audit department can verify and certify such compliance in line with the yearly company assurance process;
(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).

Compliance Committee

13.2 Vopak has a Compliance Committee in place. For the purpose of this Code, the Compliance Committee shall create and maintain a framework for:

(i) the development, implementation and updating of local Individual data protection statements and policies and procedures;
(ii) the maintaining, updating and publishing of this Code and related sub-policies;
(iii) the creating, maintaining and updating of information regarding the structure and functioning of all systems that process Personal Data (as required by Article 14);
(iv) the development, implementation and updating of the relevant data protection training and awareness programs;
(v) the monitoring, auditing and reporting on compliance with this Code to the management board;
(vi) the collecting, investigating and resolving privacy inquiries, concerns and complaints; and
(vii) determining and updating appropriate sanctions for violations of this Code (e.g., disciplinary standards).

Privacy Officers

13.3 Each Division and Group Company shall designate a Privacy Officer. The Chief Privacy Officer shall act as the Privacy Officer for Royal Vopak. These Privacy Officers may, in turn, establish a network of Privacy Officers sufficient to direct compliance with this Code within their respective organizations.

The Privacy Officers shall perform the following tasks:

(i) Implement the data management processes, systems and tools, devised by the Chief Privacy Officer to implement the framework for data protection management established by the Compliance Committee in their respective organizations;
(ii) Support and assess overall data protection management compliance within their respective organizations;
(iii) Regularly advise their Responsible Executive and the Chief Privacy Officer on privacy risks and compliance issues;
(iv) Maintain (or ensure access to) an inventory of the system information about the structure and functioning of all systems that process Personal Data (as required by Article 14.2);
(v) Be available for requests for privacy approvals or advice as described in article 7;

(vi) Provide information relevant to the annual privacy report of the Chief Privacy Officer (as required in Article 16);
(vii) Assist the Chief Privacy Officer in the event of official investigations or inquiries by government authorities;
(viii) Own and authorize all appropriate privacy sub-policies in their respective organizations;
(ix) Direct that stored data be deleted or destroyed, anonymized or transferred as required by article 5.2;
(x) Decide on and notify the Chief Privacy Officer of complaints as described in article 17; and
(xi) Cooperate with the Chief Privacy Officer, other Privacy Officers, and the general business principles compliance officers to:
- Ensure that the instructions, tools and training are in place to enable their respective organizations, to comply with this Code;
- Share and provide guidance on best practices for data protection management within their respective organizations
- Ensure that data protection requirements are taken into account whenever new technology is implemented in their respective organizations;
- Notify the Responsible Executive of the involvement of external service providers with data processing tasks for their respective organizations.

Responsible Executive

13.4 The Responsible Executive is accountable that effective data protection management is implemented in his Division or Group Company, is integrated into business practices, and that adequate resources and budget are available.

Responsible Executives are accountable for:

(i) Ensuring overall data protection management compliance within their respective organizations, also during and following organisational restructuring, outsourcing, mergers and acquisitions and divestitures;
(ii) Implementing the data management processes, systems and tools, devised by the Chief Privacy Officer to implement the framework for data protection management established by the Compliance Committee in their respective organizations;
(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 Vopak to a Third Party (including entering into a written contract with such Third Party and obtaining a sign off of such contract from the legal department);
(v) Ensuring that relevant individuals in their respective organizations follow the prescribed data protection training courses; and
(vi) Directing that stored data be deleted or destroyed, anonymized or transferred as required by article 5.2.

Responsible Executives are responsible for:

(i) Appointing a Privacy Officer for their Division or Group Company ;
(ii) Consulting with the Chief Privacy Officer in all cases where there is a conflict between applicable local law and this Code as described in Article 20.2; and
(iii) Informing the Chief Privacy Officer of any new legal requirement that may interfere with Vopak's ability to comply with this Code as required by Article 20.3.

Default Privacy Officer

13.5 If at any moment in time there is no Privacy Officer designated for a Division or Group Company, the finance manager for the relevant Division or Group Company is responsible for supervising compliance with this Code.

Privacy Officer with a statutory position

13.6 Where a 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 14 – Policies and Procedures

Policies and procedures

14.1 Vopak shall develop and implement sub-policies and procedures to comply with this Code.

System information

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

Article 15 – Training

Staff training

15.1 Vopak shall provide training on this Code and related confidentiality obligations to Staff members who have access to Personal Data.

Article 16 – Monitoring and Auditing Compliance

Audits

16.1 Vopak's Internal Audit shall audit business processes and procedures that involve the Processing of Personal Data for compliance with this Code. The audits shall be carried out in the course of the regular activities of Vopak's Internal Audit or at the request of the Chief Privacy Officer. The Chief Privacy Officer may request to have an audit as specified in this Article 16.1 conducted by an external auditor. Applicable professional standards of independence, integrity and confidentiality shall be observed when conducting an audit. The Chief Privacy Officer and the appropriate Privacy Officers shall be informed of the results of the audits. Reported violations of the Privacy Codes will be reported back to the Responsible Executive.
A copy of the audit results will be provided to a competent EEA Data Protection Authority upon request.

Annual Privacy Report

16.2 The Chief Privacy Officer shall implement appropriate processes to monitor compliance with this Code and produce an annual Personal Data privacy report for the Compliance Committee on compliance with this Code, data protection risks and other relevant issues.

Each Privacy Officer shall provide information relevant to the report to the Chief Privacy Officer.

Mitigation

16.3 Vopak 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.

Article 17 – Complaints Procedure

Complaint

17.1 Individuals may file a complaint regarding compliance with this Code or violations of their rights under Applicable Data Controller Law in accordance with the complaints procedure set forth in the relevant privacy policy or contract. The complaint shall be forwarded to the appropriate Privacy Officer.

The appropriate Privacy Officer shall:

(a) notify the Chief Privacy 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 appropriate Privacy Officer may consult with any governmental authority having jurisdiction over a particular matter about the measures to be taken.

Reply to Individual

17.2 Within four weeks of Vopak receiving a complaint, the appropriate Privacy Officer shall inform the Individual in writing either (i) of Vopak's position with regard to the complaint and any action Vopak has taken or will take in response or (ii) when he will be informed of Vopak's position, which date shall be no later than four weeks thereafter. The appropriate Privacy Officer shall send a copy of the complaint and his written reply to the Chief Privacy Officer.

Complaint to Chief Privacy Officer

17.3 An Individual may file a complaint with the Chief Privacy Officer if:

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

The procedure described in Articles 17.1 through 17.2 shall apply to complaints filed with the Chief Privacy Officer.

Article 18 – Legal Issues

Complaints procedure

18.1 Individuals are encouraged to first follow the complaints procedure set forth in Article 16 of this Code before filing any complaint with the competent data protection authorities or courts.

Local law and jurisdiction

18.2 The rights contained in this Article are in addition to and shall not prejudice any other rights or remedies that an Individual may otherwise have at law.

In case of a violation of this Code, Individuals have the following rights:

Complaints: to file a complaint with the Dutch Data Protection Authority or any other competent EEA Data Protection Authority;

Claims: to file a claim before the competent courts:

- in the EEA country of origin of the data transfer against the Group Company in such country of origin responsible for the relevant data transfer;
- of the EEA country where the Individual resides, against the Group Company being the Data Controller of the relevant Personal Data;
- in the Netherlands, against Royal Vopak.

Breaches by Group Companies located outside the EEA: where an Individual suffers damages as a result of a breach of the Code by a Group Company located outside of the EEA, Royal Vopak accepts, subject to the provisions of Article 17.3 – 17.7, responsibility for the breach, which right shall be exercised against Royal Vopak before the competent courts of the

Netherlands only.

Advice of the Dutch DPA 18.3 Royal Vopak shall abide by the advice of the Dutch DPA issued on the interpretation and application of this Code.

Limitation of damages 18.4 In case an Individual has a claim under Article 17.2, such Individual shall only be entitled to actual direct damages. However, the relevant Group Company or Royal Vopak shall be liable only for actual direct damages (which exclude, without limitation, any indirect, incidental, special, punitive or consequential damages or any lost profits or revenue, lost turnover, cost of capital, downtime cost, and loss of data) suffered by an Individual resulting from a violation of this Code.

Burden of proof in respect of claim for damages 18.5 Regarding the burden of proof in respect of a claim for damages as referred to in Article 17.2, it will be for the Individual to demonstrate that he/she has suffered actual damages and to establish facts which show it is plausible that the damage has occurred because of a violation of the Code. It will subsequently be for Royal Vopak to prove that the damages suffered by the Individual due to a violation of the Code are not attributable to Vopak.

Mutual assistance and redress 18.6 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 Individual or
(ii) a lawful investigation or inquiry by a competent government authority.

The Group Company who receives a request, complaint or claim from an Individual is responsible for handling any communication with the Individual regarding his request, complaint or claim except where circumstances dictate otherwise.

Royal Vopak shall ensure that adequate steps are taken to address violations of this Privacy Code by a Group Company.

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

Law applicable to Code; 18.7 This Code shall be governed by and interpreted in accordance with Dutch law.

Article 19 – Sanctions for Non-compliance

Non-compliance 19.1 Non-compliance of Employees with this Code may result in appropriate measures in accordance with applicable local law up to and including termination of employment.

Article 20 – Conflicts Between the Code and Applicable Local Law

Conflict of law when transferring Data 20.1 Where a legal requirement to transfer Personal Data conflicts with the laws of the Member States of the EEA or the law of Switzerland, the transfer requires the prior approval of the Chief Privacy Officer. The Chief Privacy Officer shall seek the advice of the Head of Legal. The Chief Privacy Officer may seek the advice of the Dutch Data Protection Authority or another competent government authority.

Conflict between Code and law

20.2 In all other cases, where there is a conflict between applicable local law and the Code, the relevant Responsible Executive shall consult with the Chief Privacy 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

20.3 The relevant Responsible Executive shall promptly inform the Chief Privacy Officer of any new legal requirement that may interfere with Vopak's ability to comply with this Code.

Article 21 – Changes to the Code

21.1 Any changes to this Code require the prior approval of the Executive Board. Royal Vopak shall notify Group Companies of the approved changes. Royal Vopak shall notify the Dutch Data Protection Authority in case of material changes to the Code on a yearly basis.

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

21.3 Any change shall enter into force with immediate effect after it has been approved in accordance with this Article 21.1 and is published on the Vopak website.

21.4 Any request, complaint or claim of an Individual involving this Code shall be judged against the version of the Code that is in force at the time the request, complaint or claim is made.

Article 22 – Transition Periods

General transition period

22.1 Except as indicated below, 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 Personal Data shall be undertaken in compliance with the Code. During a transition period, any transfer of Personal Data to a Group Company under this Code as a data transfer mechanism may only take place to the extent the Group Company receiving such Personal Data is (i) compliant with this Code, or (ii) the data transfer meets one of the grounds for data transfer listed in Articles 11.6 – 11.8.

Transition period for new Group Companies

22.2 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 Divested Entities

22.3 A Divested Entity may remain covered by this Code after its divestment for such period as may be required by Vopak to disentangle the Processing of Personal Data relating to such Divested Entity.

Transition period for IT Systems

22.4 Where implementation of this Code requires updates or changes to information technology systems (including replacement of systems), the transition period shall be three 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

22.5 Where there are existing agreements with Third Parties that are affected by this Code, the provisions of the agreements will prevail until the agreements are renewed in the normal course of business.

Transitional period for local-for-local systems	22.6	Processing of Personal 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

Royal Vopak
Chief Privacy Officer
Att. Global Director HR
Westerlaan 10
3016 CK ROTTERDAM

ANNEX 1 Definitions

Applicable Data Controller Law	APPLICABLE DATA CONTROLLER LAW means the provisions of mandatory law of a country containing rules for the protection of individuals with regard to the Processing of Personal Data including security requirements for and the free movement of such Personal Data as applicable to Vopak acting as the Data Controller of Personal Data.
Archive	ARCHIVE shall mean a collection of Personal Data that are no longer necessary to achieve the purposes for which the Data originally were collected or that are no longer used for general business activities, but are used only for historical, scientific or statistical purposes, dispute resolution, investigations or general archiving purposes. An archive includes any data set that can no longer be accessed by any Employee other than the system administrator.
Article	ARTICLE shall mean an article in this Code.
Binding Corporate Rules	BINDING CORPORATE RULES shall mean a privacy policy of a group of undertakings which under applicable local law (such as Article 25 of the EU Data Protection Directive) is considered to provide an adequate level of protection for the transfer of Personal Data within that group of undertakings.
Business Contact Data	BUSINESS CONTACT DATA shall mean any data typically found on a business card and used by the Individual in his contact with Vopak.
Business Partner	BUSINESS PARTNER shall mean any Third Party, other than a Customer or Supplier, that has or had a business relationship or strategic alliance with Vopak (e.g. joint marketing partner, joint venture or joint development partner).
Business Purpose	BUSINESS PURPOSE shall mean a purpose for Processing Personal Data as specified in Article 2 or 3 or for Processing Sensitive Data as specified in Article 4 or 3.
Chief Privacy Officer	CHIEF PRIVACY OFFICER shall mean the officer as referred to in Article 13.1.
Children	CHILDREN shall mean Individuals under the age of thirteen (13) years.
Code	CODE shall mean this Privacy Code for Customer, Supplier and Business Partner Data.
Compliance Committee	COMPLIANCE COMMITTEE shall mean the compliance committee appointed by Royal Vopak.
Customer	CUSTOMER shall mean any Third Party that purchases, may purchase or has purchased a Vopak service.
Data Security Breach	DATA SECURITY BREACH shall mean the unauthorized acquisition, access, use or disclosure of unencrypted Personal Data that compromises the security or privacy of such data to the extent the compromise poses a significant risk of financial, reputational, or other harm to the Individual. A Data Security Breach is deemed not to have occurred where there has been an unintentional acquisition, access or use of unencrypted Personal Data by an employee of Vopak or Third Party Processor or an individual acting under their respective authority, if (i) the acquisition, access, or use of Personal Data was made in good faith and within the course and scope of the employment or professional relationship of such employee or other individual; and (ii) the Personal Data are not further acquired, accessed, used or disclosed by any person.

Divested Entity	DIVESTED ENTITY shall mean the divestment by Vopak of a Group Company or business by means of: (a) a sale of shares as a result whereof the Group Company so divested no longer qualifies as a Group Company and/or (b) a demerger, sale of assets, or any other manner or form.
Division	DIVISION shall mean a department within Royal Vopak for a specific geographical area and for this document Global LNG.
EEA	EEA or EUROPEAN ECONOMIC AREA shall mean all Member States of the European Union, plus Norway, Iceland and Liechtenstein.
EEA Data Protection Authority	EEA DATA PROTECTION AUTHORITY shall mean any of the data protection authorities of an EEA country.
Effective Date	EFFECTIVE DATE shall mean the date on which this Code becomes effective as set forth in Article 1.6.
Employee	EMPLOYEE shall mean the following persons: (a) an employee, job applicant or former employee of Vopak including temporary workers working under the direct supervision of Vopak (e.g. contractors and trainees. This term does not include people working at Vopak as consultants or employees of Third Parties providing services to Vopak; (b) a (former) executive or non-executive director of Vopak or (former) member of the supervisory board or similar body to Vopak.
Employee Data	EMPLOYEE DATA shall mean any information relating to an identified or identifiable Employee.
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.
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 or any successor or replacement thereof.
Executive Board	EXECUTIVE BOARD shall mean the board of directors of Royal Vopak.
Group Company	GROUP COMPANY shall mean Royal Vopak and any company or legal entity of which Royal Vopak, directly or indirectly owns more than 50% of the issued share capital, has more than 50% of the voting power at general meetings of shareholders or has the power to appoint a majority of the directors; however, any such company or legal entity shall be deemed a Group Company only (i) as long as a liaison and/or relationship exists, and (ii) as long as it is covered by the Vopak Code of Conduct.
Head of Legal	HEAD OF LEGAL shall mean the Global Director Legal Affairs & Corporate Secretary of Royal Vopak
Individual	INDIVIDUAL shall mean any (employee of or any person working for) Customer, Supplier or Business Partner and any other individual whose Personal Data Vopak processes in the context of the provision of its services.
Non-Adequate	NON-ADEQUATE COUNTRY shall mean a country that under applicable local

Country	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 Personal Data was originally collected.
Overriding Interest	OVERRIDING INTEREST shall mean the pressing interests set forth in Article 12.1 based on which the obligations of Vopak or rights of Individuals set forth in Article 12.2 and 12.3 may, under specific circumstances, be overridden if this pressing interest outweighs the interest of the Individual.
Personal Data or Data	PERSONAL DATA shall mean any information relating to an identified or identifiable Individual.
Privacy Officer	PRIVACY OFFICER shall mean a privacy officer appointed by the Chief Privacy Officer pursuant to Article 13.3.

Privacy Impact Assessment (PIA)	PRIVACY IMPACT ASSESSMENT (PIA) shall mean a procedure to conduct and document a prior assessment of the impact which a given Processing may have on the protection of Personal Data, where such Processing is likely to result in a high risk for the rights and freedoms of individuals, in particular where new technologies are used.
	A PIA shall contain:
	- a description of:
	  - the Processing;
	  - the Business Purpose for which Personal Data are Processed;
	  - the specific purposes for which Sensitive Data are Processed;
	  - the categories of data recipients;
	  - data retention periods;
	- an assessment of:
	  - the necessity and proportionality of the Processing;
	  - the risks to the rights and freedoms of individuals; and
	  - the measures to mitigate these risks, including safeguards, security measures and other mechanisms (such as privacy-by-design) to ensure the protection of Personal Data.

Processing	PROCESSING shall mean any operation that is performed on Personal Data, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission or deletion of Personal Data.
Royal Vopak	ROYAL VOPAK shall mean Koninklijke Vopak N.V., registered at the Chamber of Commerce in Rotterdam, the Netherlands under number 24295332, having its registered seat in Rotterdam, the Netherlands.
Responsible Executive	RESPONSIBLE EXECUTIVE shall mean the head of a Division or Group Company.
Secondary Purpose	SECONDARY PURPOSE shall mean any purpose other than the Original Purpose for which Personal Data is further Processed.
Sensitive Data	SENSITIVE DATA shall mean Personal Data that reveal an Individual's racial or ethnic origin, political opinions or membership in political parties or similar organizations, religious or philosophical beliefs, membership in a professional or trade organization or union, physical or mental health including any opinion thereof, disabilities, genetic code, addictions, sex life, criminal offenses, criminal records, proceedings with regard to criminal or unlawful behavior, or social security numbers issued by the government.
Staff	STAFF shall mean all Employees and other persons who Process Personal Data as part of their respective duties or responsibilities using Vopak information technology systems or working primarily from Vopak's premises

Supplier	SUPPLIER shall mean any Third Party that provides goods or services to Vopak (e.g. an agent, consultant or vendor).
Vopak	Vopak shall mean Royal Vopak and its Group Companies.
Third Party	THIRD PARTY shall mean any person, private organization or government body outside Vopak.
Third Party Controller	THIRD PARTY CONTROLLER shall mean a Third Party that Processes Personal Data and determines the purposes and means of the Processing.
Third Party Processor	THIRD PARTY PROCESSOR shall mean a Third Party that Processes Personal Data on behalf of Vopak that is not under the direct authority of Vopak.

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 and
(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 or a legal obligation includes any regulatory requirement, recommendation, and best practice issued by relevant national and international supervisory authorities or other bodies.