SHELL EMPLOYEE PRIVACY RULES

Contents

Introduction

Shell Companies are committed to the protecting of personal data of (amongst others) their employees, former employees, job applicants. These Employee Privacy Rules ("**the Rules**") describe how this principle is to be implemented.

Capitalized terms used in these Rules are defined in the text of the Rules or in Annex 1.

For practical reasons, male gendering has been used in all cases involving female and male individuals.

Article 1 – Scope and Applicable Law

1.1 Scope

These Rules address the Processing of Employee Data controlled by a Shell Company or the Processing by a Third Party for such Shell Company.

These Rules apply only to the Processing of Employee Data by electronic means, or to Employee Data kept in systematically accessible paper-based filing systems.

These Rules supersede all privacy guidelines, manuals, policies, codes, instructions or notices that exist within the Shell Group Companies on the Effective Date to the extent they address the same issue.

The obligations of Shell Companies in relation to the transfer of Employee Data to Third Parties are especially and exhaustively addressed in Article 11 of these Rules.

1.2 Supplemental protection provided by Rules

The Processing of Data by Shell Companies is governed by applicable local law. Employees keep their own rights and remedies as available in their local jurisdictions. These Rules shall apply only to the extent they contain supplemental safeguards, rights or remedies of Employees with regard to Employee Data over and above those set out in applicable local law. Where

applicable local law provides more protection than these Rules, local law shall apply.

1.3 Conflicting provisions of mandatory local law and related country specific provisions

Where a requirement pursuant to the Employee Privacy Rules to transfer Employee Data conflicts with the applicable local mandatory laws of the Member States of the EEA or the law of Switzerland, the transfer requires the prior approval of the Chief Privacy Officer.

In all other cases, where there is a conflict between applicable local law and the Code, the relevant Shell Company 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 Shell Company.

Any request, complaint or claim of an Employee involving these Rules and handled in accordance with Article 8.5, 14 or 15 of these Rules, will be judged against the provisions of the Rules that are in force at the time the request, complaint or claim is made.

1.4 Law governing the Rules and Lead authority for supervision of the Rules

Without prejudice to Articles 1.2 and 1.3 above, these Rules shall be exclusively governed by Netherlands law. The Dutch Data Protection Authority is the lead authority for the supervision of these Rules.

Article 2 – Purposes for Processing Employee Data

2.1 Legitimate Business Purposes

Shell Companies will only collect, use or otherwise Process Employee Data for one or more of the following Business Purposes:

(i) Human resources and personnel management. This purpose includes, Processing that is necessary for the preparation, performance or termination of an employment contract or any other contract or relationship with an Employee, or for managing an employment-at-will relationship, all in the widest sense. It includes, management and

administration of recruiting and outplacement, calculation, determination and payment of compensation and benefits, calculation and payment of taxes and social security contributions, calculation and payment of pensions of any description, as well as any similar entitlements, career and talent development, performance evaluations, training, travel and expenses, leave and other absence, security and Employee communications, in each case, including litigation and defence of pertinent claims;

(ii) Business Process execution and internal management. This purpose includes, activities such as scheduling work, timerecording, managing company assets, conducting internal audits and investigations, implementing business controls and creating, managing and using Employee directories, in each case, including litigation and defence of pertinent claims;

(iii) Health, safety and security. This purpose includes, activities such as occupational safety and health, the protection of company and Employee assets, and the authentication of Employee status and access rights, in each case, including litigation and defence of pertinent claims;

(iv) Organizational analysis and development and management reporting. This purpose includes, activities such as conducting Employee surveys, managing mergers, demergers, acquisitions and divestments, and Processing Employee Data for management reporting and analysis, in each case, including litigation and defence of pertinent claims;

(v) Compliance with legal obligations. This purpose includes, the Processing of Employee Data as necessary for compliance with a legal obligation to which a Shell Company is subject, in each case, including litigation and defence of pertinent claims.

(vi) Protecting the vital interests of Employees. This purpose permits Processing as necessary to protect the vital interests of an Employee.

2.2 Use of Data for Secondary Purposes

Employee Data may be Processed for a different legitimate Business Purpose (the "Secondary Purpose") than the purpose for which such Employee data was originally collected (the "Original Purpose") only if the Original Purpose and Secondary Purpose are closely related. Depending on the sensitivity of the relevant Employee Data and whether use of the Data for the Secondary Purpose has potential negative consequences for the Employee, the Shell Company Processing the Data for a Secondary Purpose must take additional measures to protect the Employees' interests where necessary.

Shell Companies shall generally be permitted to Process Employee Data for one or more of the following Secondary Purposes:

(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) dispute resolution;
(vi) legal or business consulting; or
(vii) insurance purposes.

Article 3 –Processing Sensitive Data

3.1 Specific purposes for Processing Sensitive Data

Shell Companies shall not Process Sensitive Date unless this is necessary to serve a relevant Business Purpose. The following specific purposes are, for each of the categories of Sensitive Data listed below, considered to be relevant Business Purposes for which such Sensitive Data may be processed:

a) **Racial or ethnic data (including pictures and moving images of an Employee):**
   (i) identifying an Employee for site security as part of a systematic collection of Employee Data intended to detect and deter unlawful activity or to provide for the safety of Employees and visitors of the relevant Shell Company, or of its or their property or that of (unrelated) third parties; or
   (ii) providing preferential status, as permitted by applicable local law and applicable policies, to persons from particular ethnic or cultural minorities to remove or reduce inequality, provided that use of the relevant Sensitive Data allows an objective determination that an Employee belongs to a minority group and further provided that the Employee has not filed a written objection to the relevant Processing; or
   (iii) administering Employee memberships.

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

(i) providing health services to an Employee provided that the relevant data are Processed by or under the supervision of a health professional who is subject to professional confidentiality requirements; or
(ii) administering pensions, health and welfare benefit plans, or plans, collective agreements or other arrangements that create rights depending on the state of health of the Employee; or
(iii) reintegration (including the checking and monitoring fit for work status) or providing support and care for Employees entitled to benefits in connection with illness or (partial or full) work incapacity; or
(iv) emergency and/or (exposure) management programmes on hazardous substances and performing epidemiological studies; or
(v) Assessing and making decisions on (continued) eligibility for positions, projects or scope of responsibilities; or
(vi) Providing facilities in the workplace to accommodate health problems or disabilities; or
(vii) administering Employee memberships.

c) **Criminal data (including data relating to (suspected) criminal behaviour, criminal records or proceedings regarding criminal or unlawful behaviour):**

(i) assessing an application by an Employee to make a decision about Employee or provide a service to Employee; or
(ii) protecting the interests of one or more Shell Companies with respect to criminal offenses that have been committed or are suspected to have been committed.

d) **Sexual preference (including data relating to partners of Employees):**

(i) administering Employee pensions and benefits programs.
(ii) administering Employee memberships

e) **Religious or philosophical beliefs:**

(i) accommodating religious or philosophical practices, dietary requirements; or
(ii) administering religious holidays.

3.2 General Purposes for Processing of Sensitive Data

In addition to the specific purposes listed in Article 3.1 above, all categories of Sensitive Data may be Processed:

(i) as required by or allowed under applicable local law but the latter only after prior approval of the relevant DP Advisor; or
(ii) for the establishment, exercise or defense of a legal claim; or
(iii) to protect a vital interest of an Employee, but only where it is reasonably not possible to obtain the Employee's consent first; or
(iv) to the extent necessary to comply with an obligation other than local data protection law including obligations of international public law, but only after prior approval of the relevant DP Advisor.

3.3 Use of Sensitive Data for Secondary Purposes

Sensitive Data may be Processed for Secondary Purposes in accordance with Article 2.2.

Article 4 – Additional requirements for Processing Data of Dependants

Shell Companies will Process Data of Dependants if:

(i) the Data are provided with the consent of the Employee or the Dependant unless it is not reasonably possible to obtain such consent and Data are Processed to protect a vital interest of Dependant; or
(ii) Processing of the Data is reasonably necessary for the performance of a contract with the Employee or for managing the employment-at-will relationship with the Employee; or
(iii) the Processing is required or allowed by applicable local law but the latter only after prior approval of the relevant DP Advisor;

Article 5 – Employee consent

5.1 General

Employee consent generally cannot be used as a legitimate basis for Processing Employee Data. One of the Business Purposes must exist for any Processing of Employee Data. In addition to the requirement of a Business Purpose, a Shell Company shall seek Employee consent for a Processing if and to the extent applicable local law or the Rules so require. If none of the Business Purposes applies, a Shell Company may request Employee consent for Processing Employee Data, but only if the Processing has no foreseeable adverse consequences for the Employee and after prior approval of the relevant DP Advisor.

5.2 Employee consent for Processing Sensitive Data

Employee consent generally cannot be used as a legitimate basis for Processing Sensitive Data. One of the grounds listed in Article 3 must exist for any Processing of Sensitive Data. In addition to the requirement of the grounds listed in Article 3, a Shell Company shall seek Employee consent for a Processing if and to the extent applicable local law or the Rules so require.
If none of the grounds listed in Article 3 apply, Shell Companies may Process Sensitive Data only after seeking Employee consent and only if the Processing has no foreseeable adverse consequences for the Employee and after prior approval of the Chief Privacy Officer.

5.3 Information to be provided when seeking Employee consent

When seeking Employee consent, the relevant Shell Company will inform the Employee:

(i) of the purpose of the Processing;
(ii) which Shell Company is responsible for the Processing;
(iii) that the Employee is free to refuse or withdraw his consent at any time without consequence to his employment relationship; and
(iv) of other relevant information.

5.4 Employee consent for transfer of Employee data to a Third Party in a Non-Adequate Country

Article 11.6 contains provisions governing the transfer of Employee Data to Third Parties located in a Non-Adequate Country.

If none of the grounds listed in Article 11.6 exists, the relevant Shell Company may transfer the Data to a Third Party located in a Non-Adequate Country only after obtaining the consent of the Employee concerned and only if either:

a) the transfer has no foreseeable adverse consequences for the Employee; or
b) the consent is requested prior to the participation of the Employee in specific projects, assignments or tasks that require the transfer of the Data.

Requesting Employee consent for a transfer as set out in this Article requires the prior approval of the Chief Privacy Officer and the Employee shall be provided with the following information:

(i) the purpose of the transfer;

(ii) the identity of the transferring Shell 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;
(vi) the fact that the Data will be transferred to a Non-Adequate Country; and
(vii) that the Employee is free to refuse or withdraw his consent at any time without consequence to his employment relationship.

5.5 No consent required

If a Processing is undertaken at the Employee's request (e.g., he subscribes to a service or seeks a benefit), he shall be considered to have granted consent to the Processing.

Article 6 – Quantity and Quality of Data

6.1 No Excessive Data and Storage period

Shell Companies shall not Process Employee Data unless this is reasonably necessary for the relevant Business Purpose. Shell Companies shall retain Employee 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 to protect the rights of relevant Shell Companies and/or their Employees. Shell Companies may specify (e.g., in a sub-policy, notice or records retention schedule) a time period for which certain categories of Employee Data should be kept.

6.2 Quality of Data

All Shell Companies shall take reasonable measures to ensure that Employee Data controlled by them are accurate, complete and up-to-date. Such measures may include the establishment of technical facilities that periodically require Employees to check their Data on record.

Employees are responsible for keeping their Data up-to-date where Shell Companies require or enable them to do so.

Article 7 – Information Requirements

Shell Companies shall inform the relevant Employees through a published privacy policy or notice about:

(i) the Business Purposes for which their Data are Processed;
(ii) which Shell Company is responsible for the Processing; and
(iii) other relevant information

The responsible Shell Company does not have to provide this information if and to the extent such information has previously been made available to the Employee concerned, either individually or by means of general notifications.

Article 8 – Employee Rights of Access and Rectification

8.1 Rights of Employees

Every Employee shall have the right to request a Shell Company which he reasonably believes to have Processed Data pertaining to him for an overview of this Data. If in the view of the addressed Shell Company another Shell Company is better placed to deal with the request, it may forward the request to this other Shell Company. Where reasonably possible, the overview shall contain information regarding the source, type, purpose and categories of recipients of the relevant Employee Data.

If the Employee Data are incorrect, incomplete or not Processed in compliance with applicable law or these Rules, the Employee shall have the right to have his Data rectified, deleted or blocked, as the case may be.

In addition, the Employee shall have the right to object to the Processing of his Data on the basis of compelling grounds related to his particular situation.

8.2 Procedure

Any request made pursuant to Article 8.1 shall be made in writing and shall be sent to the Shell Company concerned.
Prior to responding to a request of the Employee as specified in Article 8.1, the responding Shell Company may require the Employee to:

(i) specify the type of Employee Data to which the request relates;
(ii) specify the data system in which the Employee Data likely are stored;
(iii) specify the circumstances in which the Shell Company obtained the Employee Data;
(iv) show proof of his identity and/or,

(v) state the reasons why the Employee Data are incorrect, incomplete or not Processed in accordance with applicable law or the Rules.

8.3 Response period

Within four weeks of receiving a request as specified in Article 8.1 the responding Shell Company shall inform the Employee in writing either:

(i) of the Shell Company's response to the request; or

(ii) if the Shell Company requires more time for a response, when the Employee will be informed of such response (with a maximum of 8 weeks after receipt of the request).

8.4 Denial of requests

The relevant Shell Company may deny a request as referred to in Article 8.1 if and to the extent:

(i) the request does not meet the requirements of Articles 8.1 and 8.2;

(ii) the request is not sufficiently specific;

(iii) the identity of the relevant Employee 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. What constitutes an unreasonable time interval or disproportionate efforts or costs shall in each case be determined by the Shell Company handling the request on the basis of all relevant circumstances of the case. A time interval between requests of 6 months or less shall generally be deemed to be an unreasonable time interval;

(v) the request is not permitted according to applicable law or the data concerned is privileged; or

(vi) the requests will cause disproportionate efforts or costs for the Shell Company concerned.

8.5 Complaint

An Employee may file a complaint in accordance with Article 14.3 if:

(i) the request is denied in accordance with Article 8.3;

(ii) the Employee has not received any response within the timeframe specified in Article 8.3; or

(iii) in a case where the Employee has received a substantive response as provided in Article 8.3 (i), and such response is unsatisfactory to the Employee; or

(iv) in case of a deferral as provided for in Article 8.3 (ii), the Employee has objected to the deferred time for response and has not been provided with a shorter period acceptable to him.

Article 9 – Security and Confidentiality Requirements

9.1 Data security

Shell Companies shall take appropriate, commercially reasonable technical, physical and organizational measures to protect Employee Data from misuse or accidental, unlawful, or unauthorized access, disclosure, alteration, destruction, loss, or acquisition.

9.2 Limitation of Access

Shell Companies shall only grant access to an Employee or Third Party involved in Processing Employee Data to the extent necessary to serve the applicable Business Purpose and to perform their job.

9.3 Confidentiality obligations

Employees who access Employee Data in the course of their work for a Shell Company must comply with their confidentiality obligations.

Article 10 – Automated Decision Making

Shell Companies may use automated tools in making decisions about Employees, but may not base their decisions solely on the results provided by the automated tool. This restriction does not apply, however, if:

(i) the use of automated tools is required or authorized by law; or

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

(iii) measures are taken to safeguard the legitimate interests of the Employee, e.g., the Employee has been provided with an opportunity to express his point of view as part of the decision making process.

Article 11 – Transfer of Employee Data to Third Parties

11.1 Transfer to Third Parties

This Article sets forth requirements concerning the transfer of Employee Data by a Shell Company to a Third Party. In this context, "transfer of Employee Data" includes disclosure by or on behalf of a Shell Company of Employee Data to such Third Party in the context of, for example, corporate due diligence as well as provision by or on behalf of a Shell Company of remote access to Employee Data to a Third Party.

11.2 Third Party Controllers and Third Party Processors

These Rules distinguish two categories of Third Parties:

(i) Third Party Processors: Third Parties that Process Employee Data solely on behalf of the controlling Shell Company concerned and at its direction (e.g., Third Parties that Process Employee salary data on behalf of the Shell Company concerned);

(ii) Third Party Controllers: Third Parties that Process Employee Data and determine the purposes and means of the Processing themselves (e.g., government authorities, or service providers that provide services directly to Employees.

11.3 Transfer for applicable Business Purposes only

Shell Companies shall only transfer Employee Data to a Third Party to the extent necessary to serve the applicable Business Purpose.

11.4 Third Party Controllers

Third Party Controllers may Process Employee Data only if they have a written contract with a Shell Company. Each Shell Group Company shall seek to contractually protect the data protection interests of its Employees if it engages with a Third Party Controller. This obligation shall not apply in respect of government agencies.

11.5 Third Party Processors

Each Shell Company shall ensure that a Third Party Processor engaged by it shall Process Employee Data only after it has entered into a written contract with that Shell Company which as a minimum, includes the following provisions:

(i) the Third Party Processor shall Process Employee Data only in accordance with the Shell Company's instructions and only for the purposes authorized by that Shell Company;
(ii) the Processor shall keep the Employee Data confidential;
(iii) the Processor shall take appropriate technical, physical and organizational security measures to protect the Employee Data;
(iv) the Third Party Data Processor shall not permit subcontractors to Process Personal data in connection with its obligations to the Shell Company concerned without the prior written consent of the Shell Company;
(v) the Shell Company 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 that Shell Company or any relevant government authority;
(vi) the Third Party Processor shall promptly inform the Shell Company concerned of any actual or suspected security breach involving Employee Data; and
(vii) The Third Party Processor shall take adequate remedial measures as soon as possible and shall promptly provide the Shell Company concerned with all the relevant information and assistance as requested by the Shell Company regarding the security breach.

11.6 Transfer of Data to a Third Party located in a Non-Adequate Country

This Article sets forth additional rules for the transfer of Employee Data to a Third Party located in a country that is not considered to provide "adequate" protection for Employee Data ("Non-Adequate Country") in terms of the EU Data Protection Directive.

Without prejudice to Article 5.4 (Employee Consent for transfer of Employee Data), a Shell Company may only transfer Employee Data to a Third Party located in a Non-Adequate Country if:
(i) such transfer is necessary for the performance of a contract or for managing the employment-at-will relationship with an Employee, as the case may be, or to take necessary steps at the request of the Employee prior to entering into a contract or an employment-at-will relationship with the Employee, e.g., for Processing job applications etc.; or
(ii) a contract, conforming to any model contract requirement under applicable local law (if any), has been concluded between the Shell Company transferring the Data and the relevant Third Party that provides for safeguards at a similar level of protection as that provided by these Rules; or

(iii) the Third Party concerned has been certified under the United States Safe Harbor Program or any other similar program that is recognized as providing an "adequate" level of data protection; or

(iv) the Third Party has implemented Binding Corporate Rules which provide adequate safeguards as required by Article 26 (2) of the EU Data Protection Directive; or

(v) the transfer is necessary to protect a vital interest of the Employee; or

(vi) the transfer is necessary for the establishment, exercise or defence of a legal claim; or

(vii) the transfer is necessary to satisfy a pressing need to protect the public interests of a democratic society but only after prior approval of the Chief Privacy Officer; or

(viii) the transfer is required by any law to which the relevant Shell Company is subject but only after prior approval of the Chief Privacy Officer.

11.7 Transfers between Non-Adequate Countries

In addition to the grounds listed in Article 11.6, transfers of Employee Data that have been collected in connection with the activities of a Shell Company located in a Non-Adequate Country to a Third Party that is also located in a Non-Adequate Country are also permitted if they are:

(i) necessary for compliance with a legal obligation to which a transferring Shell Company is subject; or

(ii) necessary to serve the public interest; or

(iii) necessary to satisfy a Business Purpose of a Shell Company.

Article 12 – Overriding Interests

12.1 Overriding Interests

As specified below, the Chief Privacy Officer can authorize to set aside certain obligations of Shell Companies or rights of Employees under these Rules if, under the specific circumstances of the case, a pressing need exists for that Shell Company to Process Data that outweighs the interest of the Employee ("Overriding Interest").

An Overriding Interest exists if there is a need to Process Data:

(i) in order to protect the legitimate business interests of one or more Shell Companies including:
   a) the health, security or safety of Employees;
   b) the intellectual property rights, trade secrets or reputation of one or more Shell Companies;
   c) the continuity of their business operations;

d) the preservation of confidentiality in a proposed sale, merger or acquisition of a business; or
e) the involvement of advisors or consultants for business, legal, tax, or insurance purposes; or

(ii) to prevent or investigate (including cooperating with law enforcement) suspected or actual violations of applicable laws, regulations and permits, breaches of terms of employment, or other contractual terms applicable to the relationship with the Employee, or non-compliance with the Shell Business Principles or Code of Conduct or other applicable policies or procedures; or

(iii) to otherwise protect or defend the rights or freedoms of Shell Companies, its Employees or any other living person.

12.2 Exceptions in the event of Overriding Interests

If an Overriding Interest exists, the Chief Privacy Officer can authorize to set aside any or all of following provisions:

(i) Article 2.2 (the requirement of a close relation between the Secondary and Original Purpose);
(ii) Article 7;
(iii) Article 8.1;
(iv) Articles 9.2 and 9.3; and
(v) Articles 11.4, 11.5 and 11.6 (ii).

If an Overriding Interest as listed in Article 12.1 (i) (a), (c) and (e), (ii) or (iii) exists the Chief Privacy Officer can authorize to set aside the requirements of Article 3 (Sensitive Data).

12.3 Information to Employee

Upon request of the Employee, the Shell Company concerned shall inform the Employee of the nature of the Overriding Interest invoked by the Shell Company unless the nature of the Overriding Interest prevents the Shell Company concerned from doing so.

Article 13 – Supervision and compliance

13.1 Chief Privacy Officer

A Chief Privacy Officer who will be responsible for supervising compliance with these Rules shall be appointed.

13.2 Contact Details

Contact Details of the Chief Privacy Officer are posted on the Data Protection site of the Shell Ethics and Compliance Office. These details may be amended at any time by means of a message on the SWW, by means of an e-mail message to (relevant) Employees or by such other means as Shell International may consider appropriate.

Article 14 – Complaints procedure

14.1 Complaint to a Shell Company

An Employee may file a complaint in accordance with these Rules if he believes that any provision of these Rules or violations of their rights under applicable local law has been violated in respect of his Data. Any such complaint must be made in writing, and must be addressed to the Shell Company that he believes to have breached the Code . A complaint relating to Article 8 may only be filed in accordance with Article 8.5.

14.2 Reply to Employee

Within four weeks of receipt of a complaint, the Shell Company handling it shall inform the Employee in writing either:

(i) of its views on the complaint and any action taken or to be taken in response; or

(ii) when he will be informed of the relevant Shell Company's position (with a maximum of 16 weeks after receipt of the request).

14.3 Complaint to Chief Privacy Officer

An Employee may file a written complaint as described in Article 14.1 with the Chief Privacy Officer if:

(i) the response to his complaint by the Shell Company is unsatisfactory to him; or

(ii) he has not received a response within four weeks as required by Article 14.2; or

(iii) the time period provided to him pursuant to Article 14.2 (ii) is, unreasonably long given the relevant circumstances and he has unsuccessfully objected to it; or

(iv) the conditions as described in Article 8.5 are met.

Article 14.2 shall apply mutatis mutandis to complaints filed with the Chief Privacy Officer.

Article 15 – Remedies

15.1 Local law

Any claims and complaints in relation to Processing by a Shell Company of Employee Data shall be governed by applicable local law.

15.2 Jurisdiction for Employee Data in case of breach of local law

Employees retain the rights and remedies available to them in their local jurisdictions for breaches of local law. Local government authorities having jurisdiction over the relevant matters shall retain their authority.

15.3 Jurisdiction for Employee Data under the Rules

Without prejudice to article 15.4 any complaints or claims of an Employee concerning any supplemental right the Employee may have under these Rules may only be directed to the Shell Company who has allegedly violated these Rules and may only be brought before the Data Protection Authority or the competent court in which that Shell Company is established. In such case the Rules must be interpreted in accordance with Dutch law.
Such complaints and claims shall be admissible only if the Employee has first followed the complaints procedure set forth in Article 14 of these Rules.

15.4 Additional jurisdiction for Employee Data subject to EU law

If Employee Data that is governed by the law of one of the EEA countries is transferred to a Shell Company located in a Non-Adequate Country and this Shell Company violates these Rules, the Employee can choose to bring a complaint or claim either pursuant to Article 15.3 or against the EU Headquarters before the Dutch Data Protection Authority or the competent court in The Hague, the Netherlands. Such complaints and claims shall be admissible only if the Employee has first followed the complaints procedure set forth in Article 14 of these Rules.

The remedies set out in Article 15.3 and 15.4 are mutually exclusive, and an Employee who has opted to pursue either of these remedies cannot switch to the alternative remedy later. Any claims brought against EU Headquarters shall be exclusively brought before the Dutch Data Protection Authority in the Netherlands or the competent district court in The Hague, the Netherlands.

Employees who bring their claim to a Dutch court or governmental authority in accordance with this Article 15.4 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.

15.5 Exclusive remedies

Except as provided otherwise by mandatory local law, the breaching Shell Company or EU Headquarters, as the case may be, shall be liable only for direct damages, resulting from a violation of applicable local law and/or these Rules. Where an Employee can demonstrate that it has suffered damage and establish facts which show it is plausible that the damage has occurred because of a violation of the Rules, it will be for the relevant Shell Company or EU Headquarters, as the case may be**,** to prove that the damages suffered by the Employee due to a violation of the Code are not attributable to the relevant Shell Company.

15.6 Mutual assistance

All Shell Companies shall co-operate and assist each other to the extent reasonably possible in handling:

(i) any request, complaint or claim made by an Employee; or

(ii) any lawful investigation or inquiry by a competent government authority into the handling of Personal Data or the application of these Rules.

The Shell Company employing the Employee is responsible for handling any communication with the Employee regarding a request, complaint or claim except where circumstances dictate otherwise.

15.7 Redress

The Shell Company who has breached (or allegedly breached) these Rules shall bear all costs incurred by any other Shell Company in connection with the handling of a request, complaint or claim resulting from the alleged breach, including but not limited to internal and external lawyer’s fees, court fees, any

fines imposed and/or any damages awarded, and shall, if such amounts have been paid or born by EU Headquarters, reimburse EU Headquarters at its first request for all such costs.

Article 16 – Sanctions for non compliance

Non-compliance with the obligations of these Rules by Employees may result in disciplinary action, and may include termination of employment, as appropriate.

Article 17 – Effective Date, Transition Periods and publication

17.1 Effective Date

These Rules shall enter into force as of 1 April 2011 (Effective Date).

17.2 General Transition Period

There shall be a two-year general transition period after the Effective Date for compliance with these Rules. During this transition period, Shell Companies shall strive to comply with the Rules.

17.3 Individual Transition Period for New Shell Companies

Any entity that becomes a Shell Company after the Effective Date shall comply with the Rules within two years of becoming a Shell Company.

17.4 Transition Period for IT Systems

Where implementation of these Rules require 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 Shell Company, as the case may be, or any longer period as is reasonably necessary to complete the update, change or replacement Process.

17.5 Transition Period for Existing Agreements

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

17.6 Transitional Period for Local-for-Local Systems

Processing of Employee Data that were collected in connection with activities of a Shell Company located in a Non-Adequate Country shall be brought into compliance with these Rules within five years of the Effective Date.

17.7 Changes to the Rules and Publication

Any changes to these Rules require the prior approval of the Chief Privacy Officer**.** The Chief Privacy Officer shall notify the Dutch Data Protection Authority in case of significant changes to the Rules on a yearly basis. These Rules may be changed without Employee consent, even if the amendment relates to a provision which confers rights to, or contains safeguards for the benefit of, Employees. The latest version of these Rules shall be published on the [SWW-Web] and shall upon request be made available to Employees who do not have access to the Shell Wide Web.

ANNEX 1 Definitions

Archive	shall mean a collection of Employee Data that are no longer necessary to achieve the purposes for which the Data were originally 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. ”Archive” includes any data set that can no longer be accessed by any Employee other than the system administrator.
Business Purpose	shall mean a purpose for Processing Employee Data as specified in Article 2 or for Processing Sensitive Data as specified in Article 3 .
Chief Privacy Officer	has the meaning ascribed to that term in Article 13.1.
Dependant	shall mean a spouse, partner or child, who belongs to the household of the Employee.
DP Advisor	shall mean a lawyer of the local legal department who can advise on local legal data privacy matters in relation to the Rules and who will be listed on the Data Privacy site of the Ethics and Compliance website.
DP Focal Point	shall mean a focal point within a Business or Function who can advise on data privacy matters in relation to the Rules and who will be listed on the Data Privacy site of the Ethics and Compliance website.
Effective Date	has the meaning ascribed to that term in Article 17.1.
Employee	shall mean the following persons: • an employee, trainee, job applicant or former employee trainee or job applicant of a Shell Company; • a present or former executive or non-executive director of Shell Companies or a present or former member of the supervisory board or similar body to a Shell Company.

Employee Data or Data	shall mean any information relating to an identified or identifiable Employee or any of his Dependants that is Processed by a Shell Company that is responsible for the Processing or on behalf of such Shell Company.
EEA	shall mean the European Economic Area as that may be defined by EU from time to time.
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 as that may be amended from time to time.
EU Headquarters	shall mean Shell International or such other Shell Company as may subsequently be designated EU Headquarters.
Non-Adequate Country	has the meaning ascribed to that term in Article 11.6.
Original Purpose	has the meaning ascribed to that term in Article 2.2.
Overriding Interest	has the meaning ascribed to that term in Article 12.1.
Process and Processing	shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, blocking, erasure or destruction.
Secondary Purpose	has the meaning ascribed to that term in Article 2.2.
Sensitive Data	shall mean Employee Data that reveal an Employee's racial or ethnic origin, political opinions or membership of 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, as defined in the EU Data Protection Directive.
Shell Company	shall mean Royal Dutch Shell plc. and any company or legal entity of which Royal Dutch Shell, 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, or the right to exercise a controlling influence over how the company is organized and managed.
Shell International	means Shell International B.V. in The Hague.
Third Party	shall mean any person, private organization or government body that is not a Shell Company or an Employee.
Third Party Controller	has the meaning ascribed to that term in Article 11.2.
Third Party Processor	has the meaning ascribed to that term in Article 11.2.

Interpretations

INTERPRETATION OF THESE RULES:

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

(ii) definitions have the meaning as defined in the EU Data Protection Directive

(iii) headings are included for convenience only and are not to be used in construing any provision of these Rules

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

(v) the male form shall include the female form

(vi) 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

(vii) a reference to a document (including, without limitation, a reference to these Rules) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by these Rules or that other document.