

# SHELL PRIVACY RULES

## Introduction

The Shell General Business Principles and Code of Conduct express our commitment to conduct our business in accordance with high ethical standards and in accordance with applicable laws and Shell policies, including with respect to the protection of Personal Data. These Privacy Rules explain how Shell will protect the personal data of current, former and future Shell employees, individuals who are engaged or employed by customers, suppliers and business partners, investors as well as any other individuals whose personal data is Processed by Shell in the course of its activities.

These Privacy Rules will enter into force as of 20 May 2019 (“**Effective Date**”). Any questions concerning these Privacy Rules may be directed to the:

Shell Group Chief Privacy Officer Shell International B.V.

P.O. Box 162

2501 AN The Hague

Or via: [privacy-office-SI@shell.com](mailto:privacy-office-SI@shell.com)

Capitalized terms have the meaning set out in **Annex 1** (Definitions). Capitalized terms that are not defined in these Privacy Rules have the meanings given to them in the EU General Data Protection Regulation (Regulation (EU) 2016/679) (“**GDPR**”).

## Article 1. Scope

### 1.1 Scope

These Privacy Rules apply to the Processing of Personal Data by Royal Dutch Shell plc. and its wholly or majority-owned affiliates (each, a “**Shell Group Company**,” and collectively, “**Shell**”).

These Privacy Rules address the global Processing of Personal Data by Shell with respect to (a) Customers, Suppliers, Business Partners, and other individuals in the context of Shell’s activities (“**Individual**” and “**Individual Data**,” respectively) and (b) Employees in the context of their employment relationship with Shell, unless and to the extent such Employee is a customer of Shell (“**Employee**” and “**Employee Data**,” respectively). Such Individuals and Employees will collectively be referred to as “**Persons**”.

Please refer to the following index:

<b>Article 2</b>	Purposes for Processing Personal Data
<b>Article 3</b>	Quantity and Quality of Personal Data
<b>Article 4</b>	Personal Data Requirements
<b>Article 5</b>	Rights of Persons
<b>Article 6</b>	Overriding Interests
<b>Article 7</b>	Security and Confidentiality Requirements

<b>Article 8</b>	Data Transfers to Third Parties or Internal Processors
<b>Article 9</b>	Accountability
<b>Article 10</b>	Complaints and Enforcement of Rights
<b>Article 11</b>	Notification Duties to DPAs
<b>Article 12</b>	Adoption and Modification of these Privacy Rules
ANNEX 1	DEFINITIONS
ANNEX 2	PROCEDURE FOR DATA SUBJECT REQUESTS BY PERSONS
ANNEX 3	PROCEDURES FOR MONITORING AND AUDITING COMPLIANCE

These Privacy Rules provide supplemental rights and remedies to Persons only. Nothing in these Privacy Rules will be construed to take away any rights or remedies that Persons may have under applicable local law.

## 1.2 Electronic and Paper-Based Processing

These Privacy Rules apply to the Processing of Personal Data by electronic means and in systematically accessible paper-based filing systems.

# Article 2. Purposes for Processing Personal Data

## 2.1 Purposes for Processing Personal Data

Shell may Process a Person's Personal Data for one or more of the following business purposes (**Business Purposes**):

- **Business process execution, internal management and management reporting.** This purpose addresses activities such as scheduling work, recording time, managing company and Employee assets (including the IT systems and infrastructure), risk management, conducting (internal) audits and investigations, finance and accounting, implementing business and IT security controls, provision of central processing facilities for efficiency purposes, management reporting and analysis, and managing and using Employee directories; managing mergers, acquisitions and divestitures; Archive and insurance purposes; legal or business consulting; and preventing, preparing for or engaging in dispute resolution;
- **Health, safety, security and integrity, including the safeguarding of the security and integrity of the business sector in which Shell operates.** This purpose includes the protection of the interests of Shell and its Employees and Customers and the sector in which Shell operates, including the screening and monitoring of Persons before and during employment or other engagements, including the screening against publicly available government and/or law enforcement agency sanctions lists and other third-party data sources, the detecting, preventing, investigating and combating (attempted) fraud and other criminal or objectionable conduct directed against Shell, its Employees or Customers, including the use of and participation in Shell's incident registers and sector warning systems, and activities such as those involving health and safety, the protection of Shell and Employee

assets (including IT systems and infrastructure), and the authentication of Customer, Supplier, Business Partner, or Employee status and access rights (such as required screening activities for access to Shell's premises or systems);

- **Compliance with law.** This purpose addresses Processing of Personal Data necessary for the performance of a task carried out to comply with a legal obligation to which Shell is subject, and the disclosure of Personal Data to government institutions and supervisory authorities, including tax and other competent authorities for the sector in which Shell operates, including for the prevention of money laundering, financing of terrorism and other crimes, customer due diligence and the duty of care towards Customers (e.g., credit monitoring); or

- **Protecting the vital interests of Persons. This purpose addresses Processing necessary** to protect the vital interests of a Person such as making arrangements to protect the vital interest of Persons in the event of health, safety and security situations.

#### **Individual Data only:**

- **Assessment and acceptance of a Customer, conclusion and execution of agreements with a Customer.** This purpose includes Processing of Individual Data that is necessary in connection with the assessment and acceptance of Customers, including confirming and verifying the identity and credit status and creditworthiness of relevant Customers (this may involve the use of a credit reference agency or other Third Party), conducting due diligence, and screening against publicly available government and/or law enforcement agency sanctions lists and other third-party data sources, the use of and participation in Shell's incident registers and sector warning systems and/or third party verification services. This purpose also includes Processing of Individual Data in connection with the execution of agreements;

- **Development and improvement of products and/or services.** This purpose includes Processing of Individual Data that is necessary for the development and improvement of Shell products and/or services, research and development. This may include collecting and analyzing customer feedback and analyzing Individuals' use of Shell's products and/or services;

- **Performance of customer services.** This purpose addresses Processing of Individual Data necessary for the performance of services provided by Shell to Customers to support Shell products and services offered to or in use with their Customers (e.g., of energy products). These services may include the maintenance, upgrade, replacement, inspection and related support activities aimed at facilitating continued and sustained use of Shell products and services.

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

- **Relationship management and marketing.** This purpose includes activities such as maintaining and promoting contact with Customers, Suppliers, Business Partners, and Persons (including profiling in so far that the consequences of such profiling do not

disproportionately impact the privacy of Individuals), account management, customer service, recalls, collection of Individual Data through websites, applications and other customer interaction and engagement channels and the development, execution and analysis of market surveys and marketing strategies and campaigns; **Employee Data only:**

- **Human resources and personnel management.** This purpose includes Processing that is necessary for the performance of an employment or other contract with an Employee (or taking necessary steps at the request of an Employee prior to entering into a contract), activities of the human resources department (e.g. management and administration of recruiting, outplacement, employability, leave and other absences), compensation and benefits (including pensions), payments, tax issues, career and talent development, performance evaluations, management of grievances and complaints, training, international mobility (including travel and relocation) and expenses, and Employee communications;
- **Organizational analysis and development, management reporting and acquisition and divestitures.** This purpose addresses various activities, such as conducting Employee surveys, managing mergers, acquisitions and divestitures, and Processing Employee Data for management reporting and analysis;

Where there is a question whether a certain Processing of Personal Data can be based on a Business Purpose listed above, the appropriate DP Lawyer should be consulted before the Processing takes place.

## 2.2 Secondary Purposes for Processing Personal Data

Personal Data may be Processed for a business purpose other than the original Business Purposes (“**Secondary Purpose**”) only if the Secondary Purpose is closely related to (‘compatible’ with) the original Business Purpose. .

For example, to the extent not already covered in Article 2.1, it is generally permissible to Process Personal Data for the following purposes:

- anonymization of Personal Data;
- transfer of Personal Data to an Archive;
- internal or independent external audits or investigations;
- IT systems and infrastructure related Processing such as for life-cycle management, maintenance, support and security (including resilience and incident management);
- statistical, historical or scientific research thereby taking into account applicable requirements where such research results in profiling;
- dispute resolution;
- fraud prevention;
- legal or business consulting; or
- insurance purposes.

If the use of Personal Data for the Secondary Purpose has potential negative consequences for the Person, Shell will take appropriate steps (such as further limiting access and taking additional security measures) to mitigate such consequences as much as reasonably possible. If the consequences cannot be appropriately mitigated, Shell may provide Persons with an optout opportunity or obtain their consent.

## 2.3 Processing Sensitive Data

Shell shall Process Sensitive Data only where permissible under applicable local law and to the extent necessary to serve the applicable Business Purpose. In addition, Sensitive Data may be collected, used or otherwise Processed for one (or more) of the specific and general purposes specified below:

### Specific Purposes for Processing Sensitive Data

- **Racial or ethnic Personal Data:**

- in some countries, photos and video images of Persons qualify as racial or ethnic Personal Data. Shell may process photos (e.g. a copy of a passport containing a photo) and video images for the protection of Shell and Employee assets, including screening and monitoring of Employees before and during employment, for site access and security reasons and for inclusion in Employee directories, for the assessment and acceptance of Individuals, including the identification and authentication of Individuals (including confirming and verifying the identity of relevant Individuals); for status and access rights of Persons; and to verify and confirm advice or record decisions made in the course of business for future reference (e.g., when Persons participate in video conferencing which is recorded);

**Employee Data only:**

- supporting workplace diversity programs to remove or reduce inequality or to ensure diversity in staffing, provided that use of the relevant racial or ethnic Employee Data allows for an objective determination that an Employee belongs to a minority group and the Employee has not filed a written objection against the relevant Processing; and
- for administering Employee affinity groups.

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

**Individual Data only:**

- as necessary for assessing and accepting Individuals and executing agreements with Individuals;
- complying with Shell's duty of care towards Individuals.

**Employee Data only:**

- providing health services to an Employee, provided that the relevant health Employee Data is processed by or under the supervision of a health professional who is subject to professional confidentiality requirements;
- administering pensions, health and welfare benefit plans, maternity, paternity or family leave programs, or collective agreements (or similar arrangements) that create rights depending on the state of health of the Employee;

- accommodating persons with a disability to remove or reduce inequality or to ensure diversity in staffing, provided that use of the relevant Sensitive Data allows for an objective determination that an Employee belongs to the relevant category;
  - reintegrating or providing support for Employees entitled to benefits in connection with illness or work incapacity;
  - emergency and/or (exposure) management programmes on hazardous substances and performing epidemiological studies;
  - for screening and monitoring of Employees before and during employment and for assessing and making decisions on (continued) eligibility for positions, projects or scope of responsibilities;
  - providing facilities in the workplace to accommodate health problems or disabilities;
  - administering Employee memberships.
- **Criminal Personal Data** (including Personal Data relating to criminal behavior, criminal records or proceedings regarding criminal or unlawful behavior):
    - protecting the interests of Shell, its Employees, Customers, and the sector in which Shell operates, with respect to criminal offences that have been or, given the relevant circumstances, are suspected to be or have been, committed against Shell, its Employees, Customers or other companies in the sector in which Shell operates, including the use of and participation in Shell's incident registers and sector warning systems.

**Individual Data only:**

- as necessary for assessing and accepting Individuals, including the identification and authentication of Individuals (including confirming and verifying the identity of relevant Individuals) and executing agreements with Individuals;

**Employee Data only:**

- assessing an application by an Employee, to make a decision about the Employee, or provide a service to the Employee;

- **Religious or philosophical beliefs:**

- accommodating specific religious or philosophical requests or needs of an Individual, such as dietary requirements related to religious or philosophical beliefs or religious holidays.

- **Biometric Personal Data** (e.g., fingerprints):

- for the protection of Shell and Employee assets, access to online services, site access and security reasons.

**Employee Data only:**

- **Sexual life and orientation** (including Employee Data relating to partners of Employees):

- administering Employee pensions and benefits programs;
- administering Employee memberships.

## General Purposes for Processing of Sensitive Data

In addition to the specific purposes listed above, all categories of Sensitive Data may be Processed under one or more of the following general circumstances:

- as required or allowed for the performance of a task carried out to comply with a legal obligation to which Shell is subject (provided, where Sensitive Data is Processed based on a requirement of law other than EEA Data Protection Law, the Processing requires the prior authorization of the appropriate DP Legal Advisor);
- to protect a vital interest of a Person, but only where it is impossible to obtain the Person's consent first;
- for dispute resolution and/or fraud prevention;
- to the extent necessary to comply with an obligation of public international law (e.g., a treaty) (provided there is prior approval by the appropriate DP Legal Advisor); or
- if the Sensitive Data has been posted or otherwise shared at the Person's own initiative within or outside of Shell, such as on the Shell intranet or collaboration platforms and through social media. Such Processing may however only occur in so far as this respects the context and any explicit access conditions under which the Person has shared such Personal Data
- for Secondary Purposes in accordance with Article 2.2.

## 2.4 Consent for Processing of Personal Data

Where required or permitted by applicable law, Shell will or may obtain consent from the Person before Processing Personal Data. When seeking consent, Shell will inform the Person about the purposes of the Processing, and the Shell Group Company that is responsible for the Processing. With regard to EEA Personal Data, Shell will also inform the Person about the right to withdraw consent at any time (and for Employee Data, without consequence to the Employee's employment relationship), and that withdrawal of consent does not affect the lawfulness of the relevant Processing before such withdrawal.

Upon withdrawal of consent, Shell will discontinue Processing as soon as reasonably practical. The withdrawal of consent shall not affect (i) the lawfulness of the Processing based on such consent before its withdrawal and (ii) the lawfulness of Processing for Business Purposes not based on consent, after withdrawal.

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

### **Additional requirements for Employee Data:**

Subject to the exceptions below, Employee consent generally will not be used as the legal basis for Processing Employee Data. One of the Business Purposes should exist for any Processing of Employee Data.

Consent may be requested from Employees only in the following cases:

- If none of the Business Purposes applies, Shell may request Employee consent for Processing Employee Data, but only if the Processing has no foreseeable adverse consequences for the Employee;

- If applicable local law requires that Shell requests the consent of the Employee for the relevant Processing, Shell shall, in addition to ensuring that a Business Purpose exists for the Processing, also seek Employee consent for the Processing; or
- If an individual applies for employment or other work engagement with Shell, Shell may request the individual's consent to Process his or her Employee Data for purposes of evaluating his or her application.

Decisions to seek Employee consent for a Processing require the authorization of the appropriate DP Legal Advisor prior to initiating the consent process.

## 2.5 Dependents

Shell may Process Personal Data of Dependents if:

- such Personal Data was provided with the consent of the Employee or the Dependent, unless it is not reasonably possible to obtain such consent and such Personal Data are Processed to protect a vital interest of Dependent;
- Processing of the Employee Data is reasonably necessary for the performance of a contract with the Employee or the employment-at-will relationship with the Employee; or
- the Processing is required or permitted by applicable local law, provided in the latter case, only after approval of the relevant DP Legal Advisor. .

## 2.6 Direct Marketing

Where required by law, Shell shall send direct marketing communications to a Person only with his or her prior opt-in consent. Shell will offer Persons the opportunity to opt out of future direct marketing communications and to object against further communication.

If a Person objects to receiving marketing communications from a Shell Group Company or withdraws his consent to receive such materials, the Shell Group Company will take steps to refrain from sending further marketing materials as specifically requested by the Person. The Shell Group Company will do so within the time period required by applicable law.

No Personal Data shall be provided to, or used on behalf of, Third Parties for purposes of direct marketing without the prior consent of the Person.

## 2.7 Automated Decisions

Automated tools may be used to make decisions about Persons, but decisions with a potentially significant negative impact for the Person may not be based solely on the results provided by an automated tool. This restriction does not apply if:

- (i) the use of automated tools is necessary for the performance of a task carried out to comply with a legal obligation to which Shell is subject; or
- (ii) the decision is made by Shell for purposes of (a) entering into or performing a contract, including for assessing creditworthiness, eligibility and for fraud prevention purposes or (b) managing a contract, provided, the underlying request leading to a decision by Shell was made by the Person; or
- (iii) the decision is made based on the explicit consent of the Person; or

(iv) the Processing pertains to Personal Data other than EEA Personal Data.

Shell will adopt and implement suitable measures to safeguard the rights and legitimate interests of Persons. Where Personal Data is processed pursuant to items (ii) and (iii) above, Shell shall provide the affected Person with (a) an opportunity to express his or her point of view with regards to the automated decision, or (b) the right to request human intervention from Shell.

The requirements set out in Article 2.4 apply to the requesting, denial or withdrawal of the Person's consent.

## **Article 3. Quantity and Quality of Personal Data**

### **3.1 No Excessive Personal Data and Storage Period**

Shell shall only Process Personal Data in so far as this is reasonably adequate for, relevant and limited to its Business Purpose(s). Shell shall only retain Personal Data for as long as needed for such Business Purposes, including in particular as needed to comply with retention requirements under applicable law. Shell shall take reasonable steps to delete, de-identify or destroy (e.g., by scrambling) Personal Data that is not required for the applicable Business Purpose. Shell maintains data and records retention schedules that define the appropriate retention periods.

When the applicable storage period has ended, the Personal Data will be promptly deleted, destroyed, de-identified or (if appropriate) transferred to an Archive (unless this is prohibited by law or an applicable records retention schedule).

### **3.2 Quality of Personal Data**

Personal Data should be accurate, complete and kept up-to-date to the extent reasonably necessary for the applicable Business Purpose. Shell may involve the relevant Person to update his or her own Personal Data and remind him or her periodically to do so as and when appropriate.

### **3.3 'Privacy by Design'**

Shell shall take commercially reasonable technical and organizational steps to ensure that the requirements of this Article are implemented into the design of new systems and processes used to Process Personal Data.

## **Article 4. Information Requirements**

### **4.1 Information Requirements**

Shell shall inform Persons through a privacy notice of the following:

- the Business Purposes for which their Personal Data is Processed;
- which Shell Group Company is responsible for the Processing as well as its contact details;
- the nature and categories of Personal Data Processed;

With regard to EEA Personal Data, Shell shall inform Persons additionally of the following:

- the contact details of the Data Protection Officer (where applicable);
- the categories of Third Parties to which Personal Data is disclosed (if any), whether any such Third Party is covered by an Adequacy Decision and if not, information on the data

transfer mechanism as referred to in Article 8, as well as the means to get a copy thereof, or access thereto;

- the period for which Personal Data will be stored or (if not possible) the criteria used to determine this period;
- an overview of the rights of Persons under these Privacy Rules and how these can be exercised, including the right to obtain compensation;
- the use of automated decision making referred to in Article 2.7, as well as meaningful information about the logic involved as well as the significance and envisaged consequences thereof for the Person;
- the source of Personal Data (where Personal Data has not been obtained from the Person), including whether Personal Data came from a public source.

## **4.2 Personal Data not Obtained from the Person**

Where EEA Personal Data has not been obtained directly from the Person, Shell shall provide the Person with the information as set out in Article 4.1:

- within a reasonable period after obtaining Personal Data but at the latest within one month, having regard to specific circumstances of the Personal Data Processed;
- if Personal Data is used for communication with a Person, at the latest at the time of the first communication with the Person;
- if a disclosure to another recipient is envisaged, at the latest when Personal Data is first disclosed.

## **4.3 Exceptions**

The requirements of Articles 4.1 and 4.2 may be inapplicable if:

- (i) the Person already has the information as set out in Article 4.1;
- (ii) it would be impossible or would involve a disproportionate effort to provide the information to Persons, in which case Shell will take additional measures to protect the Individual's fundamental rights and freedoms and legitimate interests as appropriate;
- (iii) obtaining Personal Data is expressly laid down in applicable law; or
- (iv) Personal Data must remain confidential subject to an obligation of professional secrecy regulated by applicable local law, including a statutory obligation of secrecy.

# **Article 5. Rights of Persons**

## **5.1 Right of Access**

Every Person has the right to request access to his or her Personal Data Processed by or on behalf of Shell, and further, where reasonably possible, access to the information listed in Article 4.1 or, if applicable, Article 4.2. In addition and where provided for by applicable Data Protection Law, the Person has the right to receive a copy of the Personal Data undergoing Processing, subject to any exemptions provided for by applicable Data Protection Law and in any event without adversely affecting the rights and freedoms of others.

## 5.2 Right to Rectification, Deletion, and Restriction

If Personal Data is incorrect, incomplete, or not Processed in compliance with these Privacy Rules, the Person has the right to have his or her Personal Data rectified, deleted or the Processing thereof restricted (as appropriate). If Personal Data has been made public by Shell, and the Person is entitled to deletion of Personal Data, in addition to deleting the relevant Personal Data, Shell shall take commercially reasonable steps to inform Third Parties that are Processing the relevant Personal Data or linking to the relevant Personal Data, that the Person has requested the deletion of Personal Data by such Third Parties.

## 5.3 Right to Object

The Person has the right to object to:

- (i) the Processing of his or her Personal Data on the basis of compelling grounds related to his or her particular situation, unless Shell can demonstrate a prevailing legitimate interest for the Processing; and
- (ii) receiving marketing communications on the basis of Article 2.6 (including any profiling related thereto).

## 5.4 Restrictions to Rights of Persons

The rights of Persons set out in Articles 5.1 - 5.3 above do not apply in one or more of the following circumstances:

- the Processing is required or allowed for the performance of a task carried out to comply with a legal obligation of Shell;
- the Processing is required by or allowed for a task carried out in the public interest, including in the area of public health and for archiving, scientific or historical research or statistical purposes;
- the Processing is necessary for exercising the right of freedom of expression and information;
- for dispute resolution purposes;
- the exercise of the rights by the Persons adversely affects the rights and freedoms of Shell or others; or
- in case a specific restriction of the rights of Persons applies under applicable Data Protection Law.

## 5.5 Procedure

A Person may exercise rights under this Article 5 by following the procedure outlined in **Annex 2** (Procedure for Data Subject Requests by Persons).

## 5.6 No Requirement to Process Identifying Data

Shell is not obliged to Process additional information in order to be able to identify the Person for the sole purpose of facilitating the rights of the Person under these Privacy Rules.

## Article 6. Overriding Interests

### 6.1 Overriding Interests

The obligations of Shell or rights of Persons as specified in Articles 5.1 – 5.3 may be overridden if, under the specific circumstances at issue, a pressing need exists that outweighs the interest of the Person (“**Overriding Interest**”). An Overriding Interest exists if there is a need to:

- (i) protect the legitimate business interests of Shell, including:
  - the health, security or safety of Employees or Individuals;
  - a) Shell's intellectual property rights, trade secrets or reputation;
  - b) the continuity or security of Shell'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 fraud or violations of law or breaches of the terms of employment, or non-compliance with the Shell Code of Conduct or other Shell policies or procedures; or
- (iii) otherwise protect or defend the rights or freedoms of Shell, its Employees or other persons.

### 6.2 Exceptions in the Event of Overriding Interests

If an Overriding Interest exists, one or more of the following obligations of Shell or rights of the Person may be set aside:

- Article 2.2 (Secondary Purposes for Processing Personal Data);
- Article 3.1 (No Excessive Personal Data);
- Articles 4.1 and 4.2 (Information Requirements);
- Article 5 (Rights of Persons);
- Article 7.2 (Staff Access and Confidentiality); and
- Article 8 (Data Transfers to Third Parties).

### 6.3 Sensitive Data

The requirements of Articles 2.1 and **Annex 2** concerning Sensitive Data may be set aside only for the Overriding Interests listed in Articles 6.1 (i)(a), (b), (c) and (e), 6.1(ii) and 6.1(iii).

### 6.4 Consultation with Chief Privacy Officer

Setting aside obligations of Shell or rights of Persons based on an Overriding Interest requires prior consultation of the Chief Privacy Officer. The Chief Privacy Officer shall document his or her advice.

### 6.5 Information to Persons

Upon request of the Person, Shell shall inform the Person of the Overriding Interest for which obligations of Shell or rights of the Person have been set aside, unless the particular Overriding

Interest sets aside the requirements of Article 4.1 – 4.2 or 5.1 – 5.3, in which case the request shall be denied.

## **Article 7. Security and Confidentiality Requirements**

### **7.1 Data Security**

Shell shall take appropriate commercially reasonable technical, physical and organizational measures to protect Personal Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access. To achieve this, Shell has developed and implemented policies and guidelines with supporting controls relating to the protection of Personal Data under the Shell Code of Conduct and the Shell control framework.

### **7.2 Staff Access and Confidentiality**

Shell shall provide Shell Staff access to Personal Data only to the extent necessary to serve the Processing and to perform their role. Shell shall impose confidentiality obligations on Staff with access to Personal Data.

### **7.3 Data Security Breach Notification Requirement**

Shell shall document any Data Security Breaches, comprising the facts relating to the incident, its effects and the remedial actions taken. Upon request, documentation pertaining to Data Security Breaches involving EEA Personal Data will be made available to the Lead DPA and a DPA competent to audit under Article 2 of **Annex 3**.

Shell Group Companies shall inform Shell International of a Data Security Breach without delay. Where so required by applicable Data Protection Law, or as otherwise directed by the Global Privacy Officer, Shell shall notify Individuals of a Data Security Breach as soon as reasonably possible following its determination that a Data Security Breach is a breach that requires notification under applicable Data Protection Law. Shell may delay or refrain from providing such notifications if otherwise prohibited, such as, if a law enforcement official or a DPA determines that notification would impede a (criminal) investigation or cause damage to national security or the relevant industry sector. In this case, notification shall be delayed as instructed by such law enforcement official or DPA. Shell shall respond promptly to inquiries of affected Persons relating to such Data Security Breach.

## **Article 8. Data Transfers to Third Parties**

### **8.1 Transfers by Shell to Third Party Controllers and Processors**

Each Shell Group Company may transfer Personal Data to third parties or other Shell Group Companies for Processing as needed for the Business Purpose or with the Person's consent.

**Data Transfers to Third Party Controllers.** Shell may transfer Personal Data to a third-party Controller (other than a government agency) only if it has a valid contract in which Shell shall seek to protect the data protection interests of Persons. This provision does not apply in case of incidental transfers of Personal Data to a Third Party Controller, such as, when a reference is

provided for an Employee or where details are shared for purposes of ordering (semi) public services (e.g. making reservations for transport services or hotel bookings).

**Data Transfers to Third Party Processors.** Shell may transfer EEA Personal Data to thirdparty Processors (“**Third Party Processors**” or “**Processors**”) only if it has a valid contract with the Processor (a “**Processor Contract**”). The Processor Contract must in any event include the following provisions:

- (i) the Processor shall Process Personal Data only for the purposes authorized by Shell and in accordance with Shell's documented instructions, including on transfers of EEA Personal Data to any Processor not covered by an Adequacy Decision, unless the Processor is required to do so under mandatory requirements applicable to the Processor and notified to Shell.
- (ii) the Processor shall keep Personal Data confidential and shall impose confidentiality obligations on Staff with access to Personal Data;
- (iii) the Processor shall take appropriate technical, physical and organizational security measures to protect Personal Data and shall promptly inform Shell of a Data Security Breach involving Personal Data;
- (iv) the Third Party Processor shall assist Shell in ensuring compliance with the obligations of article 32 – 36 of the GDPR, taking into account the nature of Processing and the information available to the Processor;
- (v) the Processor shall only permit subcontractors to Process Personal Data in connection with its obligations to Shell (a) with the prior specific or generic consent of Shell and (b) based on a validly entered into written or electronic contract with the subcontractor, which imposes similar privacy protection-related Processing terms as those imposed on the Processor under the Processor Contract and provided that the Processor remains liable to Shell for the performance of the subcontractor in accordance with the terms of the Processor Contract. If Shell provides generic consent for involvement of subcontractors, the Processors shall provide notice to Shell of any changes in its subcontractors and will provide Shell the opportunity to object to such changes based on reasonable grounds;
- (vi) the Processor shall assist Shell in responding to requests from Individuals for exercising their rights under EEA Data Protection Law
- (vii) the Processor shall make available to Shell the information necessary to demonstrate compliance with its obligations under the Processor Contract and further allow for and contribute to audits, including inspections, conducted by Shell or another auditor mandated by Shell; and
- (viii) Upon termination of the Processor Contract, or earlier if directed by Shell, the Processor shall, at the option of Shell, return the Personal Data and copies thereof to Shell or shall securely delete such Personal Data, except to the extent the Processor Contract or applicable law provides otherwise.

Internal Processors may Process EEA Personal Data only if they have a validly entered into written or electronic contract with the Group Company being the Controller of the relevant EEA Personal Data, which contract must in any event include the provisions set out above.

## 8.2 Transfers to Third Parties (Subject To Transfer Restrictions)

Without prejudice to Article 2.4 (Consent for Processing of Personal Data), Personal Data that is subject to a Transfer Restriction may be transferred to a Third Party that is located outside the country in which the Personal Data was collected if:

- (i) The Third Party is covered by an Adequacy Decision;
- (ii) the transfer is necessary for the performance or management of a contract with the Person, or for taking necessary steps at the request of the Person prior to entering into a contract, e.g., for processing orders, for processing job applications;
- (iii) a contract has been concluded between Shell and the relevant Third Party requiring that
  - (a) such Third Party shall be bound by the terms of these Privacy Rules as were it a Shell Group Company; (b) provides for safeguards at a similar level of protection as that provided by these Privacy Rules; or (c) that is recognized under applicable Data Protection Law as providing an “adequate” level of privacy protection (e.g., for the EEA: a model contract approved by the European Commission);
- (iv) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Person between Shell and a Third Party (e.g., booking an airline ticket);
- (v) the Third Party has been certified under a ‘safe harbor’ program that is recognized under applicable Data Protection Law as providing an ‘adequate’ level of privacy protection;
- (vi) the Third Party has implemented Binding Corporate Rules or a similar transfer control mechanism that is recognized under applicable Data Protection Law as providing an ‘adequate’ level of privacy protection;
- (vii) the transfer is necessary to protect a vital interest of the Person;
- (viii) the transfer is necessary for the establishment, exercise or defense of a legal claim;
- (ix) the transfer is necessary to satisfy a pressing need to protect the public interests of a democratic society; or
- (x) the transfer is necessary for the performance of a task carried out to comply with a legal obligation to which the relevant Shell Group Company is subject.

The last two items above require the prior approval of the Chief Privacy Officer.

The requirements set out in Article 2.4 apply to the requesting, denial or withdrawal of the Person’s consent.

## 8.3 Transfers between Non-Adequate Countries

In addition to the grounds listed in Article 8.2, transfers of Personal Data that have been collected in connection with the activities of a Shell Group Company located in a country that does not provide for a Transfer Restriction to a Third Party are permitted if they are:

- (i) necessary for compliance with a legal obligation to which a transferring Shell Group Company is subject;
- (ii) necessary to serve the public interest; or
- (iii) necessary to satisfy a Business Purpose of a Shell Group Company in case of non-EEA Personal Data.

## **Article 9. Accountability**

### **9.1 Role of Shell International**

Royal Dutch Shell plc. has tasked Shell International with the coordination and implementation of these Privacy Rules.

### **9.2 Privacy Governance**

Shell International has appointed a Chief Privacy Officer who also serves as Data Protection Officer under the GDPR. The Chief Privacy Officer is responsible for supervising and directing compliance with these Privacy Rules, annually reporting on global data protection risks and compliance issues to the highest level of management of Shell, and for coordinating investigations and inquiries into the Processing of Personal Data by Data Protection Authorities.

The Chief Privacy Officer heads Shell's Privacy Office. Shell's Privacy Office is embedded and supported by the structure and resources of the Shell Ethics & Compliance Office, including its Ethics & Compliance Officers and Managers. The Privacy Office maintains and leads a global network of DP Managers, Focal Points and Legal Advisors, sufficient to direct compliance with these Privacy Rules within their respective regions and organizations. Where a DP Focal Point holds his or her position pursuant to law, he or she shall carry out his or her job responsibilities to the extent they do not conflict with his or her statutory position.

Where there is a question as to the applicability of these Privacy Rules, Staff shall seek the advice of the Chief Privacy Officer.

### **9.3 Policies and Procedures**

These Privacy Rules supplement all Shell privacy policies, guidelines and notices that exist on the Effective Date. Shell shall develop and implement policies and procedures to comply with these Privacy Rules.

### **9.4 Staff Training**

Shell shall provide training on the obligations and principles laid down in these Privacy Rules and related confidentiality and security obligations to Staff who Process Personal Data.

### **9.5 System Information**

Shell shall maintain readily available information regarding all Processing activities, in accordance with EEA Data Protection Law. A copy of this information will be provided to the Lead DPA or a DPA competent to audit under Article 2 of Annex 3 upon request.

### **9.6 Data Protection Impact Assessment**

Shell shall maintain a procedure to conduct and document a Data Protection Impact Assessment whenever a Processing activity is likely to result in a high risk for the rights and freedoms of Persons, in particular where new technologies are used. Where the Data Protection Impact Assessment shows that, despite mitigating measures taken by Shell, the Processing still presents

a residual high risk for the rights and freedoms of Persons, the Lead DPA will be consulted prior to such Processing taking place.

## **9.7 Monitoring and Audits**

Shell shall monitor and audit compliance with these Privacy Rules in accordance with the procedures set forth in Annex 3 (Procedures for Monitoring and Auditing Compliance).

Shell shall take adequate measures to address violations of these Privacy Rules identified during the monitoring or auditing of compliance pursuant to this Article.

## **9.8 Annual Privacy Report**

The Chief Privacy Officer shall produce a periodic privacy report for the highest level of management of Shell on compliance with these Privacy Rules, privacy protection risks and other relevant issues. Each DP Focal Point shall provide information relevant to the report to the Chief Privacy Officer.

## **9.9 Sanctions for Non-Compliance**

These Privacy Rules are binding on Shell and all Staff must comply with these Privacy Rules as implemented by the relevant policies and guidelines. Non-compliance of Staff with these Privacy Rules may result in disciplinary action in accordance with Shell policies and local law, up to and including termination of employment or contract.

# **Article 10. Complaints and Enforcement of Rights**

## **10.1 Complaints**

Persons may file a written complaint in respect of any claim they have under Article 10.1 with the Privacy Office of the Shell Ethics and Compliance Office. Persons may also file a complaint or claim with the authorities or the courts in accordance with Article 10.3. The Privacy Office shall be responsible for complaint handling. Each complaint will be assigned to an appropriate Staff member (either within the Privacy Office or within the applicable business unit or functional area). This Staff member will:

- promptly acknowledge receipt of the complaint;
- analyze the complaint and, if needed, initiate an investigation;
- If the complaint is well-founded, advise the applicable DP Focal Point so that a remediation plan can be developed and executed; and
- maintain records of all complaints received, responses given, and remedial actions taken by Shell.

Shell will use reasonable efforts to resolve complaints without undue delay, so that a response is given to the Person within one calendar month of the date that the complaint was filed. The response shall be in writing and will be sent via the means that the Person originally used to contact Shell (e.g., via mail or email), or such alternative means as agreed to by the Person. The response will outline the steps that Shell has taken to investigate the complaint and will indicate Shell's decision regarding what steps (if any) it will take as a result of the complaint.

In the event that Shell cannot reasonably complete its investigation and respond within one month, it shall inform the Person within one calendar month that the investigation is ongoing and that a response will be provided within the next two calendar months.

If Shell's response to the complaint is unsatisfactory to the Person (e.g., the request is denied) or Shell does not observe the conditions of the complaints procedure set out in this Article 10.1, the Person can file a complaint with the Chief Privacy Officer or a complaint or claim with the authorities or the courts in accordance with Article 10.3.

## **10.2 Enforcement Rights of Persons**

The rights contained in this Article are in addition to, and shall not prejudice, any other rights or remedies that these Persons may otherwise have under applicable Data Protection Law.

Persons are encouraged to first file a complaint with Shell before filing any complaint or claim with a DPA or court.

If Shell violates these Privacy Rules with respect to its Processing of a Person's Personal Data as a Controller, the affected individual can, as a third-party beneficiary, enforce Articles 2-5, 6.5, 7, 8, 9.7, 10.1-10.4, 11 and 12.1.

## **10.3 Where Complaints or Claims May be Filed**

The Person may, at his or her choice, submit a complaint or a claim under Article 10.2 to:

- (i) The Lead DPA or the courts in the Netherlands, against Shell International;
- (ii) The DPA in the EEA Country where the Person has his or her habitual residence or place of work, against the Shell Group Company that acts as the Data Controller for the relevant Personal Data; or
- (iii) The DPA in the EEA Country where the infringement took place, against the Shell Group Company that acts as the Data Controller for the relevant Personal Data; or
- (iv) The courts in the EEA Country where the Person has his or her habitual residence; or
- (v) The courts in the EEA Country where the Shell Group Company that acts as the Data Controller for the relevant Personal Data is established, against the same Shell Group Company.

The Shell Group Company against which a complaint or claim is brought may not rely on a breach by another Shell Group Company or a Third Party Processor to avoid liability under these Privacy Rules except to the extent any defense of such other Shell Group Company or Third Party Processor would also constitute a defense of the relevant Shell Group Company.

Shell International B.V. shall ensure that adequate steps are taken to address violations of this Code by a Group Company.

The DPAs and courts shall apply their own substantive and procedural laws to the dispute. Any choice made by the Person will not prejudice the substantive or procedural rights he or she may have under applicable law.

## 10.4 Right of Persons to Claim Damages

In case a Person has a claim under Article 10.2, and the relevant Processing is governed by EEA Data Protection Law, such Person shall be entitled to compensation of damages suffered by that Person resulting from a violation of these Privacy Rules to the extent provided by applicable law of the EEA Country. If the relevant Processing is not governed by EEA Data Protection Law, such Person shall be entitled to compensation of actual direct damages (which exclude, without limitation, lost profits or revenue, lost turnover, cost of capital, and downtime cost), suffered by a Person resulting from a violation of these Privacy Rules.

To bring a claim for damages, the Person must demonstrate that he or she has suffered the relevant damages and to establish facts which show it is plausible that the damage has occurred because of a violation of these Privacy Rules. Shell must then prove that the damages suffered by such Person are not attributable to Shell or a Processor or assert other applicable defenses.

## 10.5 Mutual Assistance and Redress

All Shell Group Companies shall co-operate and assist each other to the extent reasonably possible to handle a request, complaint or claim made by a Person and lawful investigations or inquiries by a competent DPA or public authority.

The Shell Group Company that receives a request, complaint or claim from a Person is responsible for promptly notifying the appropriate DP Focal Point thereof and handling any communication with such Person regarding his or her request, complaint or claim as instructed by the appropriate DP Focal Point, except where circumstances dictate otherwise. Noncompliance with the obligations of these Privacy Rules by Employees may result in disciplinary action and may include termination of employment, as appropriate.

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

## 10.6 Advice of the DPAs

Shell shall abide by the advice of the Lead DPA and the DPAs competent to audit Shell pursuant **Annex 3**, issued on the interpretation and application of these Privacy Rules.

## 10.7 Law Applicable to these Privacy Rules

These Privacy Rules shall be governed by and interpreted in accordance with Dutch law.

# Article 11. Conflicts and Notification Duties to DPAs

## 11.1 Conflict Between Privacy Rules and Local Law

Where there is a conflict between applicable local law and these Privacy Rules, including where a legal requirement to transfer Personal Data conflicts with EEA Data Protection Law, the Chief Privacy Officer must be consulted to determine how to comply with these Privacy Rules and resolve the conflict to the extent reasonably practicable given the legal requirements applicable to the relevant Shell Group Company. The Chief Privacy Officer may seek the advice of the Lead DPA or another competent public authority.

## 11.2 Notification of Conflicts and Requests for Disclosure

Subject to the following paragraph, Shell will inform the Lead DPA if Shell becomes aware that the applicable local law of a non-EEA Country is likely to have a substantial adverse effect on the protection of EEA Personal Data offered by these Privacy Rules, including if Shell receives a legally binding request for disclosure of Personal Information from a law enforcement authority or state security body of a non-EEA Country (“**Disclosure Request**”). Notifications of a Disclosure Request shall include information about the data requested, the requesting body, and the legal basis for the disclosure

If notification of a Disclosure Request is prohibited, such as in case of a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, Shell will request the relevant authority to waive this prohibition and will document that it has made this request. If, despite its efforts, Shell does not obtain a waiver, Shell will on an annual basis provide the Lead DPA general information on the number and type of such Disclosure Requests as received during the preceding 12 month period, to the fullest extent permitted by applicable law.

In any event, any transfers by Shell of Personal Data in response to a Disclosure Request will not be massive, disproportionate or indiscriminate in a manner that would go beyond what is necessary in a democratic society.

This Article does not apply to requests received by Shell from other government agencies in the normal course of its activities, which Shell can continue to provide in accordance with applicable law.

## Article 12. Adoption and Modification of these Privacy Rules

### 12.1 Adoption and Publication

These Privacy Rules have been adopted by the Chief Privacy Officer of Royal Dutch Shell plc. and will enter into force as of the Effective Date. These Privacy Rules may be changed without consent by any Persons, even if the amendment relates to a provision which confers rights to, or contains safeguards for the benefit of, Persons. Relevant parts of the applicable Privacy Rules (including a reference list of Shell Group Companies) will be communicated using a Shell public website, by means of an email message to (relevant) Customers, Suppliers, Business Partners, or Employees, or by such other means as Shell International may consider appropriate.

### 12.2 Changes

Any changes to these Privacy Rules require the prior approval of the Chief Privacy Officer of Royal Dutch Shell plc. and shall thereafter be communicated to the Shell Group Companies.

(i) **Effective Time of Changes**

Any change shall enter into force with immediate effect after it is approved in accordance with Article 12.1 and published on the appropriate Shell public website.

(ii) **Governing Version/Prior Versions**

Any request, complaint or claim of a Person involving these Privacy Rules shall be judged against the version of these Privacy Rules as it was in force at the time that the event giving rise to the request, complaint or claim took place.

**(iii) Reporting of Material Changes to Lead DPA**

The Chief Privacy Officer shall promptly inform the Lead DPA of changes to these Privacy Rules that have a material impact on the protection offered by these Privacy Rules and will be responsible for and coordinating Shell's responses to questions from the Lead DPA. Other changes to these Privacy Rules (if any) will be notified by the Chief Privacy Officer to the Lead DPA on a yearly basis.

## **12.3 Transition Periods**

**(i) General Transition Period**

During the transition period, exchanges of Personal Data with a Group Company that is subject to a Transfer Restriction may take place only after such a Group Company has demonstrated to the Chief Privacy Officer that it has adopted and appropriately embedded (i) these Privacy Rules, or (ii) the applicable requirements for the transfer of Personal Data as set out in Articles 8.2 and 8.3.

**(ii) Transition Period for New Shell Group Companies**

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

**(iii) Transition Period for Divested Entities**

Shell may decide that a Divested Entity (or specific parts thereof) will remain covered by these Privacy Rules after its divestment for such period as is required by Shell to separate the Processing of Personal Data relating to such Divested Entity.

**(iv) Transition Period for IT Systems**

Where implementation of these Privacy Rules requires updates or changes to information technology solutions (including replacement of solutions), the transition period shall be four years from the Effective Date or from the date an entity becomes a Shell Group Company. The Chief Privacy Officer may decide to extend this period for as long as is reasonably necessary to complete the update, change or replacement process.

**(v) Transition Period for Existing Agreements**

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

**(vi) Transitional Period for Local-for-Local Processing**

Processing of Personal Data that was collected in connection with activities of a Shell Group Company not covered by an Adequacy Decision shall be brought into compliance with these Privacy Rules within five years of the Effective Date.

<b>Annexes</b>	
Annexes	Details
Annex 1	Definitions
Annex 2	Procedure for Data Subject Requests by Persons
Annex 3	Procedures for Auditing and Monitoring Compliance

## **ANNEX 1 - DEFINITIONS**

**ADEQUACY DECISION** shall mean a decision issued by a competent supervisory authority or government body under Applicable Data Protection Law that a country or region or a category of recipients in such country or region is deemed to provide an "adequate" level of data protection.

**ARCHIVE** shall mean a collection of Personal Data that is no longer necessary to achieve the purposes for which the Personal Data originally was collected or that is no longer used for general business activities, but is used only for historical, scientific or statistical purposes, dispute resolution, investigations or general archiving purposes. An Archive includes any Personal Data set that can no longer be accessed by any Employee other than the system administrator.

**ARTICLE** shall mean an article in these Privacy Rules.

**AUTHORITY** shall have the meaning set forth in Article 11.2.

**BINDING CORPORATE RULES** shall mean a privacy policy of a group of undertakings which, under applicable local law, is considered to provide an adequate level of protection for the transfer of Personal Data within that group of undertakings.

**BUSINESS PARTNER** shall mean any Third Party, other than a Customer or Supplier, that has or has had a business relationship or strategic alliance with Shell (e.g., a joint marketing partner, joint venture, or joint development partner).

**BUSINESS PURPOSE** shall mean a purpose for Processing Personal Data or for Processing Sensitive Data as specified in Article 2.

**CUSTOMER** shall mean any person, private organization, or government body that purchases, may purchase or has purchased a Shell product or service.

**CHIEF PRIVACY OFFICER** shall mean the officer as referred to in Article 9.2.

**DATA CONTROLLER** shall mean the entity or natural person which alone or jointly with others determines the purposes and means of the Processing of Personal Data.

**DATA PROTECTION IMPACT ASSESSMENT (DPIA)** 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 Persons, in particular where new technologies are used. A DPIA shall contain:

- a description of:
  - the scope and context of the Processing;
  - the Business Purposes for which Personal Data is Processed;
  - categories of recipients of Personal Data, including recipients not covered by an Adequacy Decision;
  - Personal Data storage periods;
- an assessment of:
  - the necessity and proportionality of the Processing; ○ the risks to the privacy rights of Person's; 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.

**DATA PROTECTION LAW** shall mean the provisions of mandatory law of a country containing rules for the protection of individuals with regard to the Processing of Personal Data including rules containing requirements relating to security or the free movement of such Personal Data.

**DATA SECURITY BREACH**<sup>1</sup> shall mean the unauthorized acquisition, access, use or disclosure of unencrypted Personal Data that compromises the security or privacy of such information to the extent the compromise poses a high risk of financial, reputational, or other harm to the Person. An Data Security Breach is deemed not to have occurred where there has been an unintentional acquisition, access or use of unencrypted Personal Data by Staff of Shell, a Third Party Processor, or an Employee acting under their respective authority, if:

- the acquisition, access, or use of Personal Data was in good faith and within the course and scope of the employment or professional relationship of such Staff member or other individual; and
- the Personal Data is not further acquired, accessed, used or disclosed by any person.

**DEPENDENT** shall mean the spouse, partner or child belonging to the household of the Employee, or the emergency contact of the Employee.

**DISCLOSURE REQUEST** shall have the meaning set forth in Article 11.2.

**DIVESTED ENTITY** shall mean the divestment by Shell of a Shell Group Company or business by means of:

- a sale of shares that results in the divested Shell Group Company no longer qualifying as a Shell Group Company; and/or
- a demerger, sale of assets, or any other manner or form.

---

<sup>1</sup> See article 33-34 GDPR.

**DP ADVISOR** shall mean a lawyer of the local legal department who can advise on local legal data privacy matters in relation to the Privacy Rules and who will be listed on the Data Privacy site of the Ethics and Compliance website. DP Advisors are designated by the Chief Privacy Officer pursuant to Article 9.2.

**DP FOCAL POINT** shall mean a focal point within a function or business who can advise on data privacy matters in relation to the Privacy Rules and who will be listed on the Data Privacy site of the Ethics and Compliance website. DP Focal Points are appointed by the Chief Privacy Officer pursuant to Article 9.2.

**DPA** shall mean any data protection authority of one of the EEA Countries.

**EEA** or **EUROPEAN ECONOMIC AREA** shall mean all Member States of the European Union, Norway, Iceland and Liechtenstein and, for purposes of these Privacy Rules, Switzerland, and the United Kingdom (post-Brexit). This list may be expanded by Shell to include other countries. **EEA COUNTRIES** shall mean the countries in the EEA.

**EEA DATA PROTECTION LAW** shall mean the provisions of mandatory law of an EEA 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.

**EEA PERSONAL DATA** shall mean Personal Data of which the Processing is subject to EEA Data Protection Law (or was subject to EEA Data Protection Law prior to the transfer of such Personal Data to a Group Company outside of the EEA), every Person will also have the right to request a copy of his or her Personal Data Processed by or on behalf of Shell.

**EEA EMPLOYEE DATA** shall mean Employee Data of which the Processing is subject to Data Protection Law of an EEA country (or was subject to Data Protection Law of an EEA country, prior to the transfer of such Employee Data to a Group Company outside of the EEA).

**EFFECTIVE DATE** shall mean the date on which these Privacy Rules becomes effective as set forth in the Preamble.

**EMPLOYEE** shall mean any natural person in the context of the person's employment or similar relationship with Shell, such as:

- an employee, job applicant or former employee of Shell, including temporary workers working under the direct supervision of Shell (e.g., independent contractors and trainees). This term does not include people working at Shell as consultants or employees of Third Parties providing services to Shell;
- a (former) executive or non-executive director of Shell or (former) member of the supervisory board or similar body to Shell.

**EMPLOYEE DATA** shall mean any information relating to an identified or identifiable natural person (an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online

identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person), insofar as this information relates to an Employee (and his or her Dependents) and is Processed in the context of their (former) employment relationship with Shell. This definition does not cover the Processing of Employee Data in the Employee's capacity as a customer of Shell.

**INDIVIDUAL** shall mean any individual employed by, or any person working for, a Customer, Supplier or Business Partner and any other individual (other than an Employee) whose Personal Data Shell processes in the context of its business activities.

**INDIVIDUAL DATA** shall mean any information relating to an identified or identifiable natural person (an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person), insofar as this information relates to an Individual and is Processed in the context of Shell's business activities.

**INTERNAL PROCESSOR** shall mean any Shell Group Company that Processes Personal Data on behalf of another Shell Group Company that is the Data Controller.

**LEAD DPA** shall mean the DPA of the Netherlands.

**OVERRIDING INTEREST** shall mean the pressing interests set forth in Article 6.1 based on which the obligations of Shell or rights of Persons, under specific circumstances as set forth in Articles 6.2 and 6.3, may be overridden if this pressing interest outweighs the interest of the Person.

**PERSONAL DATA** shall mean any information relating to an identified or identifiable natural person (an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person), insofar as this information relates to an Individual or Employee and is Processed by Shell.

**PERSON** shall mean Employees and Individuals collectively.

**PRIVACY NETWORK** shall mean the council referred to in Article 9.2.

**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.

**PROCESSING PURPOSES** shall mean the Business Purposes and in respect of Sensitive Data, the specific or general purpose for Processing Sensitive Data listed in **Annex 2** (Purposes of Processing) as well as the Secondary Purposes.

**PROCESSOR CONTRACT** shall mean any contract for the Processing of Personal Data entered into by Shell and a Third Party Processor.

**SECONDARY PURPOSE** shall mean any purpose other than the Business Purposes for which Personal Data is further Processed.

**SENSITIVE DATA** shall mean Personal Data that reveals a Person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a Person's sex life or sexual orientation, along with Personal Data relating to criminal convictions and offences or social security numbers issued by the government.

**SHELL** shall mean (collectively) Royal Dutch Shell plc. and any company or legal entity of which Royal Dutch Shell plc., 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 GROUP COMPANY** shall mean Royal Dutch Shell plc. or any company or legal entity of which Royal Dutch Shell plc., directly or indirectly, owns more than 50% of the issued share capital, has 50% or more of the voting power at general meetings of shareholders, has the power to appoint a majority of the directors, or otherwise directs the activities of such other legal entity; however, any such company or legal entity shall be deemed a Shell Group Company only as long as a liaison and/or relationship exists.

**SHELL INTERNATIONAL** shall mean Shell International B.V. in the Hague, Netherlands.

**STAFF** shall mean all current Employees and other persons acting under the direct authority of Shell who Process Personal Data as part of their respective duties or responsibilities towards Shell using Personal Data technology systems or working primarily from Shell's premises.

**SUPPLIER** shall mean any Third Party that provides goods or services to Shell (e.g., an agent, consultant or vendor).

**THIRD PARTY** shall mean any person or entity (e.g., an organization or public authority) outside Shell.

**THIRD PARTY CONTROLLER** shall mean a Third Party that Processes Personal Data and determines the purpose and means of the Processing.

**THIRD PARTY PROCESSOR** shall mean a Third Party that Processes Personal Data on behalf of Shell and at Shell's direction as Data Controller.

**TRANSFER RESTRICTION** shall mean any restrictions and/or requirements under Applicable Data Protection Law in regard of the transfer of Personal Data from the country in which the Personal Data was collected to another country.

## **INTERPRETATION OF THESE PRIVACY RULES:**

- 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;
- headings are included for convenience only and are not to be used in construing any provision of these Privacy Rules;
- if a word or phrase is defined, its other grammatical forms have a corresponding meaning;
- the male form shall include the female form;
- 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;
- a reference to a document (including, without limitation, a reference to these Privacy Rules) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by these Privacy Rules or that other document; and
- a reference to law or a legal obligation includes any regulatory requirement, sectorial guidance, and best practice issued by relevant national and international supervisory authorities or other bodies.

## **ANNEX 2 - PROCEDURE FOR DATA SUBJECT REQUESTS BY PERSONS**

### **1. Procedure**

Persons should send their request to the appropriate DP Focal Point. Persons also may send their request to the office of the Chief Privacy Officer via email to [privacy-office-SI@shell.com](mailto:privacy-office-SI@shell.com).

Prior to fulfilling the request of the Person, Shell may require the Person to:

- specify the categories of Personal Data to which he or she is seeking access;
- specify, to the extent reasonably possible, the system in which the Personal Data is likely to be stored;
- specify the circumstances in which Shell obtained the Personal Data;
- provide proof of his or her identity when Shell has reasonable doubts concerning such identity, or to provide additional information enabling his or her identification;
- pay a fee to compensate Shell for the reasonable costs relating to fulfilling the request, provided Shell can reasonably demonstrate that the request is manifestly unfounded or excessive, e.g., because of its repetitive character; and
- in case of a request for rectification, deletion, or restriction, specify the reasons why the Personal Data is incorrect, incomplete or not Processed in accordance with EEA Data Protection Law or these Privacy Rules.

### **2. Response Period**

Within one calendar month of Shell receiving the request and any information necessary under Section 1 above, Shell shall inform the Person in writing or electronically either (i) of Shell's position with regard to the request and any action Shell has taken or will take in response, or (ii) the ultimate date on which he or she will be informed of Shell's position and the reasons for the delay, which shall be no later than two calendar months after the original one month period.

### **3. Denial of Requests**

Shell may deny a Person's request if:

- the request does not meet the requirements of Articles 5.1 - 5.3 or meets the requirements of Article 5.4;
- the request is not sufficiently specific;
- the identity of the relevant Person cannot be established by reasonable means, including additional information provided by the Person;
- Shell can reasonably demonstrate that the request is manifestly unfounded or excessive, e.g., because of its repetitive character. A time interval between requests of six months or less shall generally be deemed to be an unreasonable time interval;
- the Processing is required or allowed for the performance of a task carried out to comply with a legal obligation of Shell;
- the Processing is required by or allowed for a task carried out in the public interest, including in the area of public health and for archiving, scientific or historical research or statistical purposes;

- the Processing is necessary for exercising the right of freedom of expression and information;
- for dispute resolution purposes;
- in so far as the request violates the rights and freedoms of Shell or others; or
- a specific restriction of the rights of Persons applies under EEA Data Protection Law.

#### **4. Complaints**

A Person may file a complaint in accordance with Article 10.1 and/or file a complaint or claim with the authorities or the courts in accordance with Article 10.2 if:

- the response to the request is unsatisfactory to the Person (e.g., because the request is denied);
- the Person has not received a response as required by Section 2; or
- the time period provided to the Person in accordance with Section 2 is, in light of the relevant circumstances, unreasonably long, and the Person has objected but has not been provided with a shorter, more reasonable time period in which he or she will receive a response.

## ANNEX 3 - PROCEDURES FOR MONITORING AND AUDITING COMPLIANCE

### 1. Internal Audits

Shell International, through its Internal Audit function, shall audit business processes and procedures that involve the Processing of Personal Data for compliance with these Privacy Rules, including methods of ensuring that corrective actions will take place. The audits shall be carried out in the course of the regular activities of Shell 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 Section 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 DP Focal Points shall be informed of the results of the audits. Any violations of these Privacy Rules identified in the audit report will be reported to the relevant DP Focal Point. A copy of the audit results related to compliance with these Privacy Rules will be provided to the Lead DPA and a DPA competent to audit under Section 2 below upon request.

### 2. Audit by the Lead DPA

Subject to Section 3 below, the Lead DPA may request an audit of the facilities used by Shell for the Processing of Personal Data for compliance with these Privacy Rules. In addition, the DPA of the EEA Country at the origin of a transfer of Personal Data to a third country under these Privacy Rules will be authorized to audit such a data transfer for compliance with these Privacy Rules. Shell will facilitate any such audit by taking the following actions:

- (i) **Data sharing:** Shell will attempt to resolve the request using alternative methods of providing information to the DPA, including Shell's internal assurance or audit reports, the assurance or audit reports of an affected supplier, discussion with Shell subject matter experts, and review of security, privacy, and operational controls in place.
- (ii) **Examinations:** If the DPA determines that the information available through these mechanisms is insufficient to address the DPA's stated objectives, Shell will provide the DPA with the opportunity to communicate with Shell's internal or independent external auditor and if required, a direct right to examine Shell's data processing facilities used to process the Personal Data on giving reasonable prior notice and during business hours, with full respect to the confidentiality of the information obtained and to the trade secrets of Shell.

The audits will otherwise be performed in accordance with the relevant DPA's own national procedural laws.

Nothing in these Privacy Rules will be construed to take away any audit rights that a DPA may have under applicable law. These Privacy Rules provides supplemental audit rights to the DPAs only. In the event of any conflict between this Annex and applicable law, the provisions of applicable law will prevail.