Ethics and Compliance Manual

Version 1.0

Contents

Overview of the Shell Ethics and Compliance Manual

Introduction to the Manual

This Shell Ethics and Compliance Manual sets out Shell's commitment to Ethics and Compliance (E&C), and defines requirements for Businesses and Functions to comply with laws on Anti-Bribery and Corruption/Anti-Money Laundering (ABC/AML), Preventing the Facilitation of Tax Evasion, Antitrust, Data Privacy (DP) and Trade Compliance.

This Manual builds on the Shell General Business Principles (SGBP) and the Shell Code of Conduct that set out Shell's commitment to compliance with all applicable laws and regulations of the countries in which Shell operates. The requirements specified in this Manual are in addition to those stated in the Code of Conduct.

Compliance is ultimately the accountability of Business and Function Heads who must ensure that individuals understand their responsibility to comply with the requirements of this Manual. Business and Function Heads must ensure, for their area of responsibility, that applicable laws are identified, associated risks assessed, and the relevant requirements of this Manual are met, including the implementation and monitoring of Ethics and Compliance programme key controls.

Staff must comply with this Manual and seek advice from an Ethics and Compliance Officer if uncertain how to meet the Manual requirements. Failure by Staff to act in accordance with this Manual may result in disciplinary action, up to and including dismissal or contract termination.

Compliance with this Manual is mandatory for all Shell companies and all Shell Operated Ventures (SOV).

Suppliers and contractors who are agents of, or working on behalf of, or in the name of a Shell company (through outsourcing of services, processes or any business activity), are required to act consistently with this Manual when acting on our behalf.

For Non-Shell operated ventures (NOVs), the Business Opportunity Manager (BOM) (for new NOVs) or the Shell Shareholder Representative (SSR) (for existing NOVs) must formally request and seek to influence the adoption and maintain appropriate Ethics and Compliance Standards Acceptable to Shell (SATS), in accordance with the NOV's Ethics and Compliance risk profile.

The Royal Dutch Shell plc Legal Director is the owner of this Manual.

Only the Chief Ethics and Compliance Officer (CECO) has the authority to make exceptions to the mandatory requirements, and requests for exceptions and their approvals or refusals must be retained as a record by the Business or Function.

Terms in blue font are listed in the **Definitions** section. Please note that the URLs and links to other documents are accessible to Shell Staff on the Shell internal network.

Disclaimer

The companies in which Royal Dutch Shell plc directly and indirectly owns investments are separate entities. In this Manual, "Shell", "Group" and "Shell Group" are sometimes used for convenience where references are made to Shell companies in general. Likewise, the words "we", "us" and "our" are also used to refer to Shell companies in general or to those who work for them. These expressions are also used where no useful purpose is served by identifying the particular company or companies.

In the event of conflicts between any translated version and the English language version of this Manual, the English language version shall prevail. The authoritative version of this Manual is available on the Shell Ethics and Compliance website and is classified as unrestricted.

Questions on this Manual must be directed to the relevant Ethics and Compliance Officer or the relevant Group Subject Matter Expert (SME).

General Requirements

1. Carrying out a risk assessment and implementing controls

Antitrust, ABC/AML/Facilitation of Tax Evasion, Data Privacy and Trade Compliance risk exposure must be assessed, jointly with the relevant Ethics and Compliance Officer and supported by the relevant Ethics and Compliance SME. A risk-based set of controls and risk responses must be in place in each Business or Function to mitigate the risks identified, and control effectiveness must be assessed and monitored.

Businesses and Functions must:

- undertake an Integrated Risk Review every two years, or when there is a significant change in business conditions, and agree required actions with the appropriate leadership (assurance committee, leadership team) and relevant Ethics and Compliance SME;
- implement and operate a risk based set of controls and risk responses to address the risks identified;
- monitor both design and operating effectiveness of each control according to the timeframe specified in its control description;
- use the Integrated Risk Review output to support assurance committee briefings; and
- retain the Integrated Risk Review output as a record.

General Requirements

2. Training

Staff must complete appropriate Shell Ethics and Compliance Training.

The Ethics and Compliance training programme uses a risk based approach. The type of Ethics and Compliance training that Staff must take will depend on the level of risk associated with their role: "at risk" or "at higher risk". Businesses and Functions are accountable for Staff training nominations.

Businesses and Functions must:

- identify those roles determined to be "at risk" or "at higher risk" and nominate Staff for training;
- ensure that Staff who have been nominated for Ethics and Compliance training complete the training by the due date; and
- take appropriate action with Staff who have not completed the required Ethics and Compliance training, including consequence management.

Details on courses available and the nomination process can be found on the Group Ethics and Compliance training site.

General Requirements

3. Reporting concerns and responding to incidents

Staff must report any suspicion or allegation of non-compliance with the mandatory requirements in this Shell Ethics and Compliance Manual, the Shell Code of Conduct or the Shell General Business Principles, including non-compliance by a third party where this could affect Shell. Shell will not tolerate any form of retaliation directed against anyone who raises a concern in good faith. Staff must not perform their own investigations into Code of Conduct incidents. Staff must not make external disclosures regarding incidents.

Reports related to the Code of Conduct and the Shell General Business Principles should be made to the Global Helpline, or can be made to Human Resources (HR), Shell Legal, an Ethics and Compliance Officer or directly to the Business Integrity Department. Reports of antitrust concerns should also be made orally to Antitrust Legal Counsel. Staff must follow the Protect Shell policy for misconduct in antitrust matters.

Reports of Data Privacy incidents (and other information security incidents) should be made to the Information Risk Management Incident Management (IRIM) portal or if that is not possible to the Global Helpline, as described in the Data Privacy Incident Handling Process.

Code of conduct investigations must only be performed by the Business Integrity Department (BID) and HR.

Where it is a legal requirement to report a breach, Shell's failure to do so could result in criminal liability for both the individual and Shell.

Businesses and Functions must:

- ensure that line managers maintain a culture in which Staff feel confident to speak up if they know or suspect a violation;
- ensure Staff do not notify the subject of any suspicion or allegation of non-compliance with AML requirements;
- ensure Staff do not perform their own investigations, as this may prejudice an investigation and could itself be a violation of laws;
- ensure Staff follow the Code of Conduct Incident Management Procedure and comply with the RDS Investigation Principles ; and
- route all proposed external disclosures to regulators via the relevant Ethics and Compliance SME or, for DP, the Group Data Privacy SME.

General Requirements

4. Ethics and Compliance due diligence

Ethics and Compliance due diligence is the process to ensure there is an understanding of who Shell is doing business with. When dealing with third parties, the correct level of due diligence must be understood and conducted to make sure Shell's standards of ethical behaviour are maintained.

Ethics and Compliance due diligence does not replace the need for conducting broader, more comprehensive assessments where required or deemed appropriate (e.g., HSSE, financial, legal, operational, and commercial assessments).

The level of Ethics and Compliance due diligence required varies, therefore, it is important to understand the rules which apply in each circumstance and conduct the right Ethics and Compliance due diligence. Some specific circumstances of when Ethics and Compliance due diligence must be conducted are:

- when contracting;
- when engaged in new business development (including acquisition or divestment of an interest or setting up a new joint venture (JV));
- before funding of social investments (SI), donations and sponsorships (refer to **Funding social investment, donations and sponsorships** requirement); and
- to confirm trade associations are appropriate for Staff memberships (refer to **Antitrust and trade associations** requirement).

Businesses and Functions must ensure that:

- Staff who interact with third parties are aware of the relevant red flags and if they are identified, the red flags are reported to an Ethics and Compliance Officer. Red flags can be identified at the commencement of the relationship with the third party or at any point during the life of the relationship;
- all third parties have been screened for Trade Compliance against lists of denied or restricted parties published by relevant government authorities;
- all third parties have had the correct, risk based, screening for ABC, AML and Preventing the Facilitation of Tax evasion;
- the third parties' information and approvals for ABC, AML compliance are obtained prior to contracting;
- Ethics and Compliance due diligence documentation is retained as a record; and
- Ethics and Compliance due diligence steps in the E&C Rule – Ethics and Compliance due diligence are followed.

General Requirements

5. Contract clauses

Contracts with third parties must contain Ethics and Compliance contract clauses relevant to the business activity governed by the contract.

- **ABC/AML requirements:** Standard clauses are incorporated in contracts with third parties. These are found in the Ethics and Compliance website.
- **Antitrust requirements:** Clauses for safeguarding Shell and third party CSI are incorporated in all contracts when third parties have access to Shell CSI (or Shell has access to third party CSI). Antitrust Legal Counsel must be consulted in relation to suitable contract clauses/antitrust completion conditions in all deals, to ensure that all appropriate antitrust merger control clearances are obtained before the deal completes.
- **Data Privacy requirements:** Standard data processing/Data Controller agreements or clauses are incorporated in all contracts with third parties where personal data will be exchanged with, transferred to, or collected by third parties. These are found in the Model Contracts Library, Sales & Licensing Contract Standards, Models and Guidance website and on the Ethics and Compliance website.
- **Trade Compliance requirements:** Standard clauses are incorporated in contracts with third parties. These are found in the Ethics and Compliance website.
- Any exceptions to these contract clauses need to be approved by the relevant Ethics and Compliance SME.

General Requirements

6. Preparing deals

Deals must comply with Antitrust, ABC/AML, DP, and Trade Compliance laws.

Almost all Shell deals will trigger mandatory antitrust approval requirements from many governments around the world. Most antitrust agency approval requirements are "suspensory", meaning the deal cannot be implemented pending receipt of all applicable antitrust approvals.

Antitrust considerations are relevant at every stage of a deal, from preparing the necessary antitrust filings and obtaining the necessary antitrust agency clearances, preparing internal documents, and external statements about the deal, to the sharing of CSI with prospective third parties.

Most countries prohibit gun jumping – meaning the implementation of (or partial implementation of) a deal without first having obtained the necessary merger control antitrust clearance(s).

Shell may be held liable for previous ABC, AML or Antitrust violations relating to assets, licenses and businesses or interests it is acquiring, merging with, joint venturing with, or divesting.

Businesses and Functions must:

- follow the E&C Rule – Ethics and Compliance due diligence before a Shell company enters into a binding commercial contract (e.g., sale and purchase agreement, production sharing contract, JV agreement) and must contact an Ethics and Compliance Officer for advice;
- obtain and follow advice from Antitrust Legal Counsel at the start of a deal and follow it at every stage throughout the deal's progress, including:

  i) the need for antitrust authority approvals;

  ii) internal document creation and internal communications;

  iii) information exchanges;

  iv) the proposed use of clean teams for information exchange purposes;

  v) external communications about (or impacting on) the deal; and

  vi) proposed transition or implementation steps;
- follow the E&C Antitrust Rule – Acquisitions and Divestments and Joint Venture Opportunities;
- execute and record appropriate confidentiality agreements;
- ensure DP risks have been identified at each stage of the deal and appropriate DP agreements executed when sharing or exchanging personal data. Refer to the DP guidance for Acquisitions and Divestments document;

General Requirements

- address residual obligations or license conditions that apply to items being disposed of or re-sold as they generally remain subject to the same Trade Compliance laws and sanctions that applied at the time of their original supply;
- follow the **E&C Trade Compliance Rule - Mergers, acquisitions and divestments**
- formally request and seek to influence the adoption of the **NOV E&C Standards Acceptable to Shell (SATS)**. The Business Opportunity Manager (BOM) must contact the relevant Ethics and Compliance Officer and follow the SATS escalation process if this cannot be achieved before the deal is approved; and
- ensure that Staff comply with the **Protect Shell Policy**.

General Requirements

7. Recruiting

During the early stages of recruiting, it must be determined whether a candidate is a Government Official (GO), former GO, related to a GO, or from a direct competitor to minimise risk and protect Shell's reputation.

Recruiting a GO, former GO, or relative of a GO could be viewed as a favour or advantage, potentially constituting bribery, and/or may create a perceived or actual conflict of interest (COI). Recruiting from direct competitors can create significant antitrust issues as it may facilitate the inappropriate exchange of CSI.

Businesses and Functions must:

- ensure the recruiter informs the hiring manager if a candidate has been confirmed as a GO, former GO, or related to a GO. The hiring manager must seek advice from an Ethics and Compliance Officer;
- instruct any successful applicant who has a COI to make a declaration in the Code of Conduct Register on commencing employment;
- follow the HR onboarding process (embedded in HR Online) applicable to recruitment from a direct competitor; and
- follow the E&C ABC/AML Rule – Conflicts of Interest: Assessing Conflicts of interest for Government Official Candidates.

General Requirements

8. Transfer of individuals to or from third parties (including secondments)

Before arranging any proposed transfer of individuals between Shell and a third party (or where Shell assists in the transfer of individuals between third parties), any potential ethics and compliance risks associated with the proposed transfer must be identified and appropriate controls must be implemented to mitigate any risks identified and comply with applicable laws.

Transfer of individuals to or from third parties (especially third parties who are direct competitors), can potentially give rise to significant antitrust issues as this may facilitate the inappropriate exchange of CSI.

Where the transfer involves a government entity or an individual who is a GO, former GO, or immediate family member or close known associate of a GO, this could be viewed as an inappropriate favour or advantage, and/or may create a perceived or actual COI.

Potential trade control risks can arise where an individual has a connection to a Generally Embargoed Country (GEC) or Highly Restricted Country (HRC). Appropriate controls must be implemented to limit access to Shell's confidential information and intellectual property and individual's personal data.

Businesses and Functions must ensure that:

- all transfers of individuals between Shell and third parties follow the approval process set out in the E&C Rule - Transfer of Individuals between Shell and Third Parties and ensure that all required conditions are met and controls implemented prior to a transfer commencing (unless otherwise provided in the Rules) to mitigate associated compliance risks;
- if the individual is a GO, former GO or immediate family member or close known associate of a GO, or where the third party is a government entity or an organisation which is controlled by a government entity, prior approval must be obtained from the relevant Ethics and Compliance SME;
- if the transfer involves or has a connection to a GEC or HRC, prior approval must be obtained from the relevant Ethics and Compliance SME;
- appropriate Shell IT controls must be implemented prior to a transfer commencing;
- additional Ethics and Compliance training based on the nature of the proposed transfer must be completed within the required timeframe set out in the Rules; and
- before a transfer commences, an agreement between Shell and the third party documenting the terms and conditions relating to the transfer must be entered into and a Non-Disclosure Agreement must be executed (unless otherwise provided in the Rules).

ABC/AML/Tax Evasion

This chapter of the Manual instructs Shell Businesses and Functions how to implement Group requirements relating to compliance with Anti-Bribery and Corruption laws, Anti-Money Laundering laws, and Preventing the Facilitation of Tax Evasion.

Bribery and corruption, money laundering, and facilitation of tax evasion are three different but related Ethics and Compliance subjects. Individually, they are subject to different laws and regulations but share many common risk areas which need to be managed consistently. This chapter describes the requirements to address all these risk areas.

Shell is subject to national and international laws prohibiting bribery and corruption and money laundering. As Royal Dutch Shell plc is a UK company and its securities are traded in the USA and UK, Staff, Shell companies, and Shell-controlled or Shell-operated joint ventures and their associated parties must comply with the US Foreign Corrupt Practices Act and the UK Bribery Act 2010, which have international effect, as well as all applicable anti-bribery and corruption (ABC) and anti-money laundering (AML) legislation in the countries where Shell operates.

Bribery occurs when a payment, gift, favour or advantage is offered, made, sought or accepted to influence a business outcome. Serious penalties, including prison sentences, may be imposed upon those guilty of bribery. Bribery and corruption may involve government officials (GO), companies or private individuals, and may occur directly or indirectly through third parties (including joint ventures or their participants). Shell prohibits all bribes, including facilitation payments.

Money laundering is a term used to describe the process of hiding the criminal origins of money or property which are the proceeds of crime within legitimate business activities. It also describes the use of money of a legitimate origin that supports terrorism. Money laundering could be a consequence of almost any profit-generating crime.

Tax evasion is an illegal practice where a person or entity evades paying their true tax liability, Shell can be subject to criminal liability where it fails to prevent its employees, or others working on its behalf, from facilitating tax evasion by others.

ABC/AML/Tax Evasion

1. ABC/AML requirements for non-Shell operated ventures (NOVs)

The Shell Shareholder Representative (SSR) must formally request and seek to influence the adoption and maintenance of applicable ABC/AML compliance programme Standards Acceptable to Shell (SATS).

For NOVs, the SSR must also take the following minimum steps:

- formally ask the NOV board (or equivalent) to:

i) submit a performance report on the NOV's ABC and AML programme to the NOV board or management committee annually; and

ii) ensure such requests and any responses are minuted and retained as a record; and

- formally record Shell's objection to any proposal to pay per diems to any GO or to pay for gifts and hospitality (G&H) for any immediate family member of any GO and ensure that such objection is retained as a record by the joint venture (JV) or its operator; and
- follow the E&C ABC/AML Rule - ABC/AML Rules for SSRs working with NOVs.

The SSR (or any other Shell Staff working for, or seconded to) of a NOV must immediately notify Shell Legal or an Ethics and Compliance Officer (ECO) if they become aware of a bribe or a request for a bribe being made by or to any employee of the NOV, or of a bribery-related allegation or investigation involving the NOV. The SSR must also attest to an ECO, via the annual attestation process, if they consider that bribes have been paid by or to any employee of the NOV.

Shell Legal must be consulted immediately in cases where NOV board members believe/consider that such notification may render them in breach of their fiduciary duties towards a NOV company.

Also refer to Contract Clauses, Preparing Deals, and Managing competitively sensitive information (CSI) in relation to joint ventures (JVs) requirements.

ABC/AML/Tax Evasion

2. Offering or receiving gifts and hospitality (G&H)

Gifts and Hospitality (G&H) that appear to improperly influence business decisions, create a conflict of interest (COI) or are on the prohibited list must not be offered or accepted. All G&H must be reasonable and proportionate, and when their value exceeds certain levels, they must be entered in the Code of Conduct Register.

Shell discourages Staff from accepting G&H from a business partner. However, Shell recognises that the occasional acceptance or offer of modest G&H may be a legitimate contribution to good business relationships.

Businesses and Functions must ensure Staff:

- do not offer or accept G&H on the prohibited list;
- record in the Code of Conduct Register and obtain line manager approval before offering or receiving G&H:

i) to or from any third party valued at $150 or greater; or

ii) to or from a private individual valued at $150 or greater; or

iii) to or from a GO valued at $20 or greater; or

iv) that could be perceived as influencing or creating an actual, potential or perceived COI, including prizes over $150 in value from external competitions or lotteries if in some way related to your role or to Shell;

- obtain ABC/AML SME support and their EC-2 Manager's approval before offering G&H to a GO worth $500 or greater and enter the G&H in the Code of Conduct Register;
- follow the E&C ABC/AML Rule – Gifts and Hospitality (excluding Formula 1); and
- follow the E&C ABC/AML Rule – Gifts and Hospitality for Formula 1 when giving invitations to Formula 1 events.

ABC/AML/Tax Evasion

3. Avoiding conflicts of interest (COI)

Conflicts of interest (COIs) must be avoided. Where an actual, perceived or potential COI occurs, to enable transparency, the COI must be recorded in the Code of Conduct Register for line management approval.

COIs happen in situations where two or more competing interests conflict and impair an individual's ability to make objective decisions. A COI arises when personal interests interfere with Shell's interests. COIs can be an Ethics and Compliance concern even if they do not result in unethical or illegal acts. Failure to provide transparency about any actual, perceived, or potential COI may expose Shell and Staff to risk. A COI that has been fully disclosed to Shell may be acceptable, assuming appropriate mitigations have been approved by line management and implemented.

Businesses and Functions must ensure that:

- Staff declare any actual, perceived or potential COI in the Code of Conduct Register and update upon a change of circumstances;
- line managers assess each COI entry and determine whether any mitigating action is required;
- line managers escalate any concerns about a COI entry to an ECO for advice;
- line managers acknowledge each COI in a timely manner, and record any mitigating actions in the Code of Conduct Register; and
- Staff follow the E&C ABC/AML Rule – Conflicts of Interest.

4. Facilitation payments

Facilitation payments are bribes and must not be made. A facilitation payment is not permitted by Shell and is illegal under the UK Bribery Act and other applicable legislation.

A facilitation payment is a minor payment to induce a (usually low-ranking) GO to expedite or secure performance of a routine duty which that person is already obliged to perform, and where such payment would exceed what is properly due.

Where a facilitation payment **has been requested:**

- the relevant Ethics and Compliance Officer or Shell Legal must be immediately informed of the request and actions taken; or
- the incident must be immediately reported to the Global Helpline.

Where a facilitation payment **has been made**, it must, in addition to the points above, be accurately recorded in expense reports.

Where a payment **has been made** because of a genuine belief that life, limb or liberty is at risk, this is not a facilitation payment but must be reported and recorded as if it were.

Also refer to Facilitation guidance.

ABC/AML/Tax Evasion

5. Funding social investment, donations and sponsorships

Funding of social investments (SI), donations and sponsorships must never improperly influence a business outcome and must always be contributed to a legitimate organisation and not to any individual.

SI, donations and sponsorships carry certain bribery and corruption risks, particularly in relation to the interaction with third parties. These risks must be identified through required due diligence and mitigated when considering requests from third parties.

Before offering or committing any funds, Businesses and Functions must:

- ensure that the proposed recipient is a legitimate organisation and not an individual;
- ensure red flags are resolved;
- determine if the value of the funds is greater than $500;
- conduct Ethics and Compliance due diligence to identify whether a GO is involved (e.g. a GO has requested the donation or sponsorship; a GO is affiliated with the recipient of the donation or sponsorship). If no GO is involved, the Ethics and Compliance due diligence confirming this must be kept as a record;
- follow the E&C Rule – Ethics and Compliance due diligence:
- for SI funding, work with the SI manager to ensure relevant SI requirements in the Social Performance Handbook are followed; and
- ensure records are kept even if there is no GO or the value is below $500.

Where a GO is involved and the value is greater than $500, Businesses and Functions must ensure:

- ABC/AML Legal Counsel support is obtained;
- approval is received from a manager (level of authority as defined in the Manual of Authorities (MOA)) to release funds;
- ABC/AML clauses are included; and
- all documentation relating to the funding is retained as a record.

In low risk countries, certain categories of GO are exempt from the ABC GO-related requirements.

ABC/AML/Tax Evasion

6. Following the rules on political payments

Political payments or "in-kind contributions" must never be made by or on behalf of Shell companies or by trade associations with Shell funds. Shell companies must not take part in party politics.

Businesses and Functions must:

- follow the E&C Rule – Ethics and Compliance due diligence:

i) to request trade associations to confirm that the trade association is conducted in accordance with antitrust laws; and

ii) to confirm that Shell funds or resources are not used for payments to political parties, political organisations or their representatives either directly or indirectly. If this requirement is not met, the Group Political Payments SME must be contacted before proceeding with the membership.

- contact the Group Political Payments SME if a request for a political payment is made by a trade association, governments, political parties, organisations or their representatives.

Antitrust

This chapter of the Manual instructs Shell Businesses and Functions how to implement Group requirements relating to compliance with antitrust laws.

The purpose of antitrust laws is to promote and safeguard competition and to deter and punish anti-competitive behaviour. Antitrust laws combat illegal practices such as price fixing, market sharing, bid rigging conspiracies, collective boycotts, production limitation agreements and prohibited behaviours that aim to achieve or maintain significant market power. Improper communications with competitors may result in allegations of anti-competitive behaviour, exposing Shell to reputational damage and the risk of severe sanctions and litigation, and its Staff to individual penalties.

A common understanding between competitors on how to behave in the market is usually considered sufficient proof of an illegal agreement, even if the agreement is never acted upon and even if it is not written down. If information is capable of influencing market behaviour, then even a single exchange or one-way sharing of that information (directly or indirectly) between competitors may be illegal. It is therefore critical that Staff understand situations that could give rise to antitrust risk, and that Shell Businesses and Functions take all appropriate steps to mitigate that risk.

Shell does not tolerate anti-competitive practices and behaviours. Shell must always make business decisions about its commercial strategy independently and unilaterally.

Staff must complete appropriate antitrust training and comply with the **Protect Shell Policy**.

Reference to Shell Legal in this chapter means the usual Shell lawyer for the Business or Function, unless the text specifies that advice or approval is to be obtained from Antitrust Legal Counsel or the Group Antitrust SME.

If there are any questions about the Antitrust requirements in this Manual, Antitrust Legal Counsel must be consulted.

Antitrust

1. Communicating with competitors

All communications with competitors must be for legitimate and lawful reasons and any exchange or sharing of competitively sensitive information (CSI) in any form must be limited to the legitimate purpose.

Communications with competitors or exchanges of CSI between competitors may result in illegal arrangements that limit competition, and may influence competitors' market strategies and behaviour. Shell must determine its business strategies and market behaviour independently without sharing CSI inappropriately with competitors.

Antitrust law can also apply to exchanges or flows of CSI between Shell and its joint ventures (JVs), or via JVs to other shareholders or owners who may be Shell's competitors.

There are circumstances where (limited) CSI may legitimately be provided to, or received from, competitors. Where there is no legitimate reason to share CSI, even a single exchange or one-way sharing of CSI may constitute an antitrust violation.

Businesses and Functions must ensure that Staff:

- understand which of their business partners and other industry participants are competitors;
- comply with the E&C Antitrust rule – Communications with Competitors; and
- engaged in deals comply with the Preparing deals requirement.

Also refer to Managing Competitively Sensitive Information (CSI) in relation to joint ventures requirement.

Antitrust

2. Antitrust and trade associations

Membership of or attendance at trade associations or similar industry groups must be registered by Staff in the Code of Conduct Register.

Attendance at trade association meetings involves contact with competitors and creates potential exposure to antitrust risk if CSI is exchanged or shared at these events. Recording memberships of trade associations enables Shell to assess and control the antitrust risks inherent in attendance or in receiving competitor CSI through membership.

Businesses and Functions must ensure:

- Staff register their trade association memberships in the Code of Conduct Register for line manager review in advance of first attendance or receiving information from the trade association;
- Staff register their attendance at a trade association meeting in the Code of Conduct Register even if they are not a member and ensure Staff understand their obligations when communicating with competitors;
- Staff who attend or communicate with trade associations comply with the E&C Antitrust Rule – Communications with Competitors; and
- they support the Shell Ethics and Compliance Office when determining whether a trade association is appropriate for Staff membership.

Antitrust

3. Benchmarking with competitors and competitive intelligence gathering

Benchmarking and competitive intelligence (CI) gathering (or CI sharing) may create antitrust risk, and must be conducted appropriately, subject to adequate safeguards.

Benchmarking and competitive intelligence (CI) gathering (if conducted properly) may enable companies to improve efficiency and become more competitive. However, if benchmarking or CI gathering/CI sharing is done in a way that involves competitors sharing CSI inappropriately (either directly or indirectly), this could result in illegal arrangements which limit competition, and so expose Shell to serious antitrust risk.

Businesses and Functions must ensure:

- Staff who undertake benchmarking or engage in CI activities with competitors, either on a one-to-one basis or with multiple third parties, comply with the E&C Antitrust Rule – Benchmarking and Competitive Intelligence Gathering; and
- Staff comply with the E&C Antitrust Rule – Communication with Competitors.

4. Managing competitively sensitive information (CSI) in relation to joint ventures (JVs)

Adequate measures must be implemented to protect access to (or limit sharing of) CSI in relation to JVs (whether the CSI is proprietary to Shell or to a third party, including information a JV holds in relation to other shareholders or owners).

Antitrust law can apply to all exchanges of CSI:

- between Shell and its non-controlled JVs, especially where those non-controlled JVs are competing JVs (where the non-controlled JV is market-facing and operates in markets in which Shell also operates); and
- between Shell and the other shareholders or co-owners of the JV, whether the JV is controlled by Shell or not, particularly where those other parties are Shell's competitors.

Controls must be in place to ensure Shell and its competitors do not inappropriately exchange CSI via the JV.

While Shell – as shareholder or owner of a JV (whether a NOV or a SOV) – has a legitimate reason to have access to JV information so it can oversee the management of the JV and protect and promote the value of its investment, it is important that controls are in place to ensure that:

- CSI does not flow inappropriately:

i) from Shell to a competing JV

ii) from a competing JV to competing parts of Shell (other than those Staff formally mandated to manage, oversee or support the JV on behalf of Shell);

iii) from Shell to third party co-owners/shareholders of Shell's NOVs or SOVs; or

iv) from third party co-owners/shareholders of Shell's SOVs or NOVs to Shell.

Businesses and Functions must ensure:

- Staff who are involved in or interacting with any non-Shell controlled JV, another third party shareholder or owner of an NOV or SOV comply with the **E&C Antitrust Rules – Managing Competitively Sensitive Information in relation to Joint Ventures**;
- appropriate IT access rights must be implemented to ensure CSI is properly managed and protected; and
- approval from the relevant Business Associate General Counsel and Antitrust Legal Counsel is obtained and recorded for any proposed "double-hatting" together with any required conditions for "recusal". The approval and conditions should be retained as records.

Antitrust

5. Engaging in joint industry advocacy with competitors

When Staff represent industry views jointly with competitors to governments, regulatory bodies or the public, it must be done with appropriate controls and with the advice of Shell Legal.

Joint industry advocacy with Shell's competitors can be a legitimate means to influence new or proposed legislation or regulations affecting Shell. However, as with any interaction with competitors, Shell needs to ensure there is no exchange of CSI that may adversely impact on competition. Adverse impact on competition might include advocating an industry standard that excludes certain players from the market, or results in market players coordinating commercial responses to events.

Only information that is objectively necessary to undertake legitimate joint industry advocacy may be shared. Joint industry advocacy must not be used to agree common commercial positions, behaviours or strategy with competitors.

Businesses and Functions must ensure:

- Staff who undertake joint industry advocacy comply with the E&C Antitrust Rule – Joint Advocacy with Competitors, and obtain and follow advice from Shell Legal on the scope and legitimacy of the joint industry advocacy.

Antitrust

6. Joint procurement and sharing procurement information

Advice from Shell Legal must be obtained before disclosing CSI relating to procurement activities or engaging in joint procurement activities with third parties.

Disclosing CSI to a third party about Shell's current or intended procurement activities may be anti-competitive if the disclosure makes it more likely that those parties would co-ordinate their behaviour in relation to prices or suppliers, e.g., price paid, suppliers used, product pricing.

Procuring goods or services jointly with third parties may be pro-competitive if it reduces costs and increases efficiency but it may be anti-competitive if it reduces the competitive opportunity for suppliers or leads to reduced competition in the relevant markets.

Businesses and Functions must ensure:

- Staff who undertake joint procurement or who share procurement information with third parties comply with the **E&C Antitrust Rules – Joint Procurement and Sharing Procurement Information** and take advice from Shell Legal on the scope and legitimacy of the activity.

Antitrust

7. Antitrust requirements related to Human Resources activities

Staff must obtain advice from Shell Legal before sharing remuneration and benefits information with third parties and must not enter into "no-poaching" arrangements with other employers.

Businesses and Functions must ensure:

- Staff who are involved in recruitment or who share HR remuneration and benefits information (including benchmarking such information) with third parties comply with the E&C Antitrust Rules related to HR activities.

8. Ensuring antitrust compliance in vertical arrangements

Advice from Shell Legal must be taken before including any vertical restrictions on competition in vertical arrangements, including distribution and reseller agreements.

Vertical arrangements are agreements between companies at different levels of the supply chain (e.g., a supplier and reseller/distributor/dealer). Restrictions agreed or imposed in vertical arrangements are called vertical restrictions, and they may harm competition in some circumstances.

Vertical restrictions include but are not limited to:

- Resale Price Maintenance (RPM);
- territorial or customer restraints, export bans or destination restrictions; and
- exclusivity provisions.

RPM (where a supplier attempts to impose a minimum or fixed resale price on its independent resellers or distributors) is illegal in many countries and may expose Shell to significant penalties.

Businesses and Functions must ensure:

- where it is illegal in the country concerned, that Staff involved in vertical arrangements do not engage in RPM; and
- Staff take advice from Shell Legal before entering into any vertical arrangements (including agency, distribution, dealership or reseller agreements) where any vertical restriction is included.

Antitrust

9. Protect Shell Policy

Shell must explicitly and clearly disassociate from all illegal discussions or anti-competitive behaviour. This includes where Shell solicits or discloses competitively sensitive information (CSI), receives unsolicited third party CSI or where Shell was not present when potentially illegal matters were discussed by third parties, but subsequently received CSI following the discussion.

Businesses and Functions must ensure:

- if CSI about a competitor is received in writing, that Staff contact Antitrust Legal Counsel immediately for advice and only share the information as instructed by Antitrust Legal Counsel; and
- if Staff are invited to participate in anti-competitive behaviour in writing, they should contact Antitrust Legal Counsel immediately for advice on how to reject the invitation; and
- if competitor CSI is shared during a meeting (informal or formal, business or social), that Staff immediately ask for the conversation to stop and clearly indicate that Shell cannot participate. If the conversation does not stop, Staff must leave the meeting, ensuring that their withdrawal is noted by others, and contact Antitrust Legal Counsel for advice.

Applications for antitrust immunity or leniency may only be made by Antitrust Legal Counsel and only with the support of the Legal Director and CEO.

Data Privacy

This chapter of the Manual instructs Shell Businesses and Functions how to implement Group requirements relating to compliance with Data Privacy laws.

Shell respects the privacy of individuals and is committed to managing personal data in a professional, lawful and ethical manner. Personal data means any information, whether in a physical document or in electronic form, relating to an identified or identifiable individual; if the information allows someone, somewhere (even outside of Shell) to identify an individual, then the data is personal data.

Examples of personal data include an individual's name, contact information, online identifiers such as IP addresses, cookie strings or mobile device IDs, that can be used to identify an individual, personal preferences or opinions, employment information, financial information, photographs, CCTV images, or location data.

Sensitive personal data are special categories of personal data and are subject to more stringent requirements and IT controls and should only be collected in specific limited circumstances. Examples of sensitive personal data include an individual's racial or ethnic origin, political opinions, membership of political parties or similar organisations, religious or philosophical beliefs, trade union membership, physical or mental health information including any opinion thereof, sexual orientation or sexual life, criminal records or proceedings regarding criminal or unlawful behaviour, or biometric data (such as fingerprints, retinal or facial recognition). In some circumstances, photographs may be considered sensitive personal data when used to identify such information as ethnicity or a health condition.

Shell is subject to a wide range of national and international data privacy laws that protect the personal data and privacy of individuals while maintaining the ability of organisations to use personal data for legitimate business purposes.

Data privacy laws can vary greatly from country to country and, in some countries, are non-existent. Consequently, Shell has adopted Binding Corporate Rules (BCRs) that govern intragroup processing of personal data, including transfers between Shell companies, in a binding and consistent manner worldwide. Personal data processed by Shell in any location is therefore subject to the requirements of the BCRs; the obligations of these are incorporated into the mandatory requirements of this Manual. **These requirements apply even if local data privacy laws are less stringent or where there are no local data privacy laws.** Where local law has stricter requirements then these **must** be met in addition to those in this Manual.

Data Privacy

1. Identifying systems and business operations that process personal data

All instances of processing personal data must be identified, whether in IT systems, applications, mobile applications, cloud computing, websites, campaigns or otherwise.

Where new operations/systems that process personal data are being designed or existing ones updated, Businesses and Functions must ensure that these mandatory requirements are followed and aligned to the principles defined in the Shell Privacy by Design Principles Guidance.

2. Processing personal data for a legitimate business purpose

There must always be a legitimate business purpose to process personal data and it should be carefully considered whether such legitimate business purpose covers all data processing activities.

The legitimate business purpose is the primary purpose for a specific instance of processing personal data. Any secondary purposes for data processing (such as statistical analysis) must be closely aligned to the primary legitimate business purpose.

Legitimate business purposes can be different depending on whether the personal data being processed is that of:

- employees (including their dependents, former employees and job applicants) and other members of Staff; or
- customers, suppliers and other business partners.

2.1. Legitimate business purposes for processing employee personal data and employee sensitive personal data:

There are defined legitimate business purposes for processing employee personal data:

- human resources and personnel management;
  Examples: Preparation, performance or termination of employment contracts or any other contract or relationships; recruitment or outplacement; compensation and benefits; taxes, social security contributions, pensions and similar entitlements; career and talent development, performance evaluations and training; travel and expenses; leave and other absences; security and employees communications.
- organisation and management of the business;
  Examples: Financial management, asset management, work scheduling, time recording, employees surveys, mergers, de mergers, acquisitions and divestitures, implementation of controls, creating and managing employees directories, management reporting, analysis, internal audits and investigations.
- health, safety and security; and
  Examples: Protection of an individual's life, health or vital interests, occupational health and safety, protection of Shell assets and employees, authentication of individual status and access rights.
- legal or regulatory compliance.
  Examples: Compliance with legal or regulatory requirements including investigations, litigation and defence of claims.

Data Privacy

Sensitive personal data of employees may only be processed in specific limited circumstances as detailed in the E&C Data Privacy Rule - Processing Shell Staff Personal Data. Approval of the local DP Legal Adviser (DPLA) or DP Legal Counsel must be sought before processing sensitive personal data of employees.

Where processing of employee personal data or sensitive personal data is not covered by one of the legitimate purposes listed, but it is required or permitted by local law, approval of the local DPLA or a DP Legal Counsel must be sought before such data is processed.

2.2. Legitimate business purposes for processing personal data of customers, suppliers or business partners:

There are defined legitimate business purposes for processing personal data of customers, suppliers or business partners:

- business execution;
  Examples: Researching, developing and improving products or services; concluding and executing agreements; recording and settling services, products and materials to and from a Shell company; managing relationships and marketing e.g. maintaining and promoting contact with existing and prospective customers, account management, customer service, and development, execution and analysis of market surveys and marketing strategies.
- organisation and management of the business;
  Examples: Financial management, asset management, mergers, de-mergers, acquisitions and divestitures, implementation of controls, management reporting, analysis, internal audits and investigations.
- health, safety and security; and
  Examples: Protection of an individual's life or health, occupational safety and health, protection of assets and people, authentication of individual status and access rights.
- legal or regulatory compliance.
  Examples: Compliance with legal or regulatory requirements including investigations, litigation and defence of claims.

Refer to **E&C Data Privacy Rule- Processing Customer Personal Data Rules** for additional information.

Sensitive personal data of customers, suppliers or business partners may only be processed in specific limited circumstances or where required by local law as detailed in the E&C Data Privacy Rule - Processing Customer Personal Data. Approval of the local DPLA or a DP Legal Counsel must be sought before processing sensitive personal data of customers, suppliers or business partners.

Where processing personal data or sensitive personal data of customers, suppliers or business partners is not covered by one of the legitimate purposes listed, but it is required or permitted by local law, prior approval of the local DPLA or a DP Legal Counsel must be sought.

Data Privacy

2.3. Consent to process personal data or sensitive personal data

In addition to a legitimate business purpose, an individual's consent is required in specific instances for processing personal data or sensitive personal data.

There are legal requirements and conditions that must be met for consent to be considered valid. Where a Business or Function intends to rely on consent as the basis for processing personal data, the **E&C Data Privacy Rule- Consent** must be followed.

Shell processes personal data of Staff for legitimate business purposes. However, there are limited circumstances when consent is required, such as if required by local law or if processing personal data is required for the purposes of providing optional programmes and benefits. Advice on local legal requirements must be obtained from your DPLA.

3. Completing a Privacy Impact Assessment (PIA)

The Privacy Impact Assessment (PIA) process must be followed when processing personal data in IT systems.

A PIA is an important tool for documenting accountability, demonstrating compliance with this Manual, legal requirements, and Shell's **Privacy by Design Principles/Guidance**. The Legal and Regulatory Assessment process conducted by Information Risk Management (IRM) determines if a PIA is required. By completing the PIA, Shell will be able to assess the impact of the processing of personal data on the individual, assess the necessity and proportionality of the processing and help manage identified risks by implementing appropriate technical and organisational controls.

Businesses and Functions must:

- initiate the PIA process and, where it has been determined that one is required, complete the PIA, before processing personal data.

The PIA process will assist Businesses and Functions to meet their personal data protection responsibilities by ensuring that:

- processing of personal data is for a legitimate business purpose;
- personal data collected is used only for the intended purpose and is not excessive for this stated purpose;
- data privacy risks to individuals are identified and assessed, with agreed controls implemented;
- privacy notices are developed and communicated;
- consent, where relied on or required, meets legal requirements and conditions;
- mechanisms for responding to individual requests within specified time limits have been implemented;
- any local data privacy laws have been considered and followed where local requirements are stricter than this Manual; and
- personal data that are records are retained and disposed of in accordance with the Group Retention Schedule (as documented in the IT solution records disposal plan), or for personal data that is not a record that the personal data disposal plan is defined in the PIA and implemented for the IT solution.

Data Privacy

4. Ensuring that personal data is accurate and relevant

All personal data processed by Shell must be relevant and limited to that which is strictly necessary to achieve the legitimate business purpose. Personal data must not be collected or kept "just in case" a use for the data can be found in the future.

Personal data must be accurate, and it must be kept up to date. All reasonable steps must be taken to ensure that inaccurate personal data is erased or rectified without delay. All requests from individuals to update their personal data must be promptly addressed.

Businesses and Functions must:

- ensure that the personal data collected is not excessive for the business purpose;
- personal datathat are records are retained and disposed of in accordance with the Group Retention Schedule (as documented in the IT solution records disposal plan), or for personal data that is not a record that the personal data disposal plan is defined in the PIA and implemented for the IT solution; and
- build mechanisms into systems or processes that facilitate timely data updates by individuals, such as self-serve portals.

See Completing a Privacy Impact Assessment (PIA).

Data Privacy

5. Protecting personal data in Shell's custody or control

Personal data must be protected from misuse, accidental, unlawful or unauthorised access, disclosure, corruption, destruction, loss, unavailability or acquisition.

The methods of protecting personal data must include physical measures, for example, restricted access to file rooms; limiting access on a "need-to-know" basis and privacy training for Staff; and technological measures, including adding a password to attachments containing personal data which are sent by email, pseudonymisation or encryption as defined in the Shell IT Control Framework.

Businesses and Functions must:

- ensure processes and systems where personal data is processed are identified and those systems are registered in the Shell IT Asset repository;
- implement required access and loss prevention controls to protect personal data, as identified by the PIA and IRM process and ensure these controls remain operational through the full life of the identified systems or processes;
- implement all available protection capabilities for end-user computing, and ensure that end-user computing is only used for processing personal data where there are no alternative approved applications or tools that can be utilised;
- ensure that Staff who have access to personal data only have access to the information they need to do their job;
- ensure that all third parties engaged by Shell to process personal data have executed the required data privacy agreements;
- assess whether business and IT controls remain adequate when there is a change to a processing operation or system; and
- regularly assess systems and processes to ensure that the personal data has been deleted according to its disposal plan.

Data Privacy

6. Safeguarding personal data transferred to, or processed by, a third party

Personal data must be safeguarded and protected by implementing the required contract clauses to ensure that the third party meets the minimum requirements of Shell's Binding Corporate Rules (BCRs) and local privacy laws.

When Businesses or Functions engage third parties to process personal data, Shell is responsible for ensuring that the personal data is safeguarded and adequately protected. This applies equally to personal data processed by a third party on behalf of Shell or to any personal data transferred to a third party by Shell.

Third parties can be either:

- third party data controllers, who process personal data in an independent manner and determine the purpose and manner of the processing activity for their own needs, e.g., health insurers, car lease companies; or
- third party data processors, who process personal data under instruction from the controlling Shell company, e.g., IT service providers. Shell remains responsible for the processing of personal data by data processors.

A third party, either a data controller or data processors, includes NOVs.

Businesses and Functions must:

- put in place the appropriate Shell template data privacy agreement prior to personal data being processed, transferred to, gathered by or exchanged with a third party. The only exception is where a third party is a government body and the personal data is required for compliance with a legal obligation of the Shell company. The Shell template data privacy agreements can be found on the Shell Ethics and Compliance website; and
- ensure that in the event of international transfers of personal data to a third party, the data privacy agreement contains the appropriate contractual mechanisms. These are attached to the Shell template contracts.

In the case where services and /or products are being procured from a third party, the required agreement should be selected through the category management and contracting process (CMCP) and associated data privacy red threads.

For transfers of personal data not in scope for CMCP, the appropriate template data privacy agreements must be used or an acceptable equivalent as approved by DP Legal Counsel.

See also **Contract Clauses** requirement.

Data Privacy

7. Informing individuals through privacy notices

Every individual whose personal data is processed by Shell must be adequately informed about such processing. There must be a clear explanation in a concise, transparent and easily accessible manner, of what individuals can expect to happen with their personal data.

Being transparent and providing accessible information to individuals about how Shell will use their personal data is a key element of data privacy laws. This information is included in a privacy notice accessible and communicated at the time of collecting personal data.

Businesses and Functions must:

- develop and implement a privacy notice containing the mandatory notice requirements as set out in the **E&C Data Privacy Rule - Privacy Notices** whenever personal data is collected;
- ensure that each privacy notice links to and supplements one of the Global privacy notice templates wherever possible; and
- review the privacy notice against local data privacy legal requirements by contacting the relevant DPLA.

8. Reporting breaches or suspected breaches of personal data

Shell must report breaches of personal data to regulatory authorities within a very short period of time, in line with privacy laws.

Shell can only meet these time limits (for example, the GDPR requirement is 72 hours) if breaches or suspected breaches are reported immediately.

Only the Group Chief Privacy Officer, in consultation with the local country DPLA is permitted to make decisions regarding required notifications to third parties.

A data privacy breach is an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Businesses and Functions must:

- immediately upon becoming aware of a breach or suspected breach, including any breach or suspected breach by a third party, report the breach directly to the Global Helpline;
- ensure that Staff do not communicate the breach to any third party. Only the Group Data Privacy SME (in conjunction with relevant local country DPLA) is permitted to make decisions regarding required notifications to third parties; and
- contact the local DPLA, a DP Focal Point or Ethics and Compliance Officer if advice or guidance is required. Follow all other requirements in **Managing Incidents and Reporting a Concern**.

9. Addressing an individual's request within time limits

Privacy laws grant individuals certain rights in relation to their personal data. Requests from individuals to exercise their rights must be respected and responded to within legislated timelines and in accordance with Shell's defined processes.

Businesses and Functions must:

- ensure that Staff are aware of and follow the processes and timelines for responding to requests as outlined below:

i) Subject Access Requests (SARs)
Individuals have the right to request access to their personal data. Requests for access to personal data must be responded to within legislated timelines. The DP Subject Access Request (SAR) Process explains how such requests are to be dealt with.

ii) Complaints
Individuals have the right to file a complaint where they believe that their personal data processed by Shell is inaccurate, incomplete or not processed in accordance with applicable law or this Manual. Complaints must be responded to within legislated timelines. Any complaints must be forwarded to the relevant Data Privacy Focal Point. The DP Complaints Process contains additional information.

iii) Request to Erase Personal Data
In limited circumstances, individuals have the right to request the deletion of their personal data. Any requests for erasure must immediately be forwarded to the relevant Data Privacy Focal Pointt.

Requests for erasure must be responded to within legislated timelines. The Right to Erasure and Restriction guidelines provides additional information.

iv) Request to restrict processing of personal data
Related to the right of erasure is the right to object to the processing of personal data. If an individual objects to the processing of their personal data, Shell will be required to restrict the processing of the personal data while the request is considered. Requests for restriction must be responded to within legislated timelines. Any requests from individuals to restrict processing of personal data must be forwarded to the relevant Data Privacy Focal Point. The Right to Erasure and Restriction guidelines provides additional information.

v) Request for Data Portability
Individuals can request that they receive a copy of the personal data which the individual has provided to Shell in a structured, commonly-used and machine-readable format and they can request a direct transmission of their personal data from one data controller to another where technically feasible. Any requests for data portability must be forwarded to the relevant DP Focal Point. The Data Portability guidelines contain further information.

Trade Compliance

This chapter of the Manual instructs Shell Businesses and Functions how to implement Group requirements relating to compliance with trade compliance laws.

Trade compliance laws serve many purposes, such as protecting national security, meeting foreign policy objectives and complying with international obligations. They are also designed to keep unauthorised parties from obtaining certain items and, as a result, limit the item's export and import to restricted countries, parties or use.

Depending on: the nature of the item; the country of origin, export and /or destination country; the end-use; and the identity and activities of the customer and any other party to the transaction, trade compliance laws and regulations may restrict or prohibit:

- the export and import of goods, technology, software, and software source code across national boundaries;
- access to and transfer of technology and technical data;
- interactions with embargoed or sanctioned countries, individuals, entities and organisations;
- the export (including re-export and deemed export), import, or release of dual-use and military items; and
- boycotts.

Trade compliance laws also require the proper communication of trade information to government authorities through customs declarations and the payment of any duties and taxes due.

Therefore, it is important for Staff to know:

- **What** is the nature of an item?
- **Where** is it from and where is it going?
- **Who** is it going to? Who else is involved?
- **How** will it get there?
- **What** will it be used for?

Trade Compliance

1. Maintaining a trade compliance programme

A trade compliance programme must be established by all Businesses and Functions to comply with laws and avoid violations which can lead to additional costs, delays, loss of import and export privileges, reputational damage, fines and/or imprisonment of individuals.

Businesses and Functions must:

- dedicate adequate resources to their trade compliance programme, including a Trade Compliance Sponsor and other suitably skilled roles as required;
- ensure procedures and controls are in place to manage trade compliance risks; and
- undertake a trade compliance programme effectiveness review, using the **trade compliance review toolkit**, either annually or earlier when there is a significant change in business conditions, and review the results with the Group Trade Compliance SME and Group Customs SME.

Trade Compliance

2. Working with sanctioned parties, generally embargoed countries (GECs), and highly restricted countries (HRCs)

All activities with or for the benefit of sanctioned parties, GECs and HRCs must be reviewed and supported, and approvals must be received.

Engaging in unlawful activities with sanctioned parties, GECs or HRCs can expose Shell and Staff to significant fines and penalties. While it may be lawful for some Shell companies to engage in certain activities with sanctioned parties, GECs and HRCs, those activities must be compliant with applicable regulations and contract obligations and prohibited Staff or assets must not support those activities.

The list of current GECs and HRCs is available online as it is subject to change.

Businesses and Functions must:

- seek review and support for all activities with or for the benefit of sanctioned parties, GECs and HRCs from:

i) TCM (support);

ii) Trade Compliance Legal Counsel (support); and

iii) EC-2 Manager (approval).

- retain relevant documents as a record; and
- ensure Staff follow the E&C Trade Compliance Rule - Working with sanctioned parties, generally embargoed countries, and highly restricted countries.

Trade Compliance

3. Country entry

Before entering a new country (country entry), support and approvals must be received.

Country entry is entering a country where Shell does not currently have operations. This represents a risk, and the country's status, relevant regulations and any applicable sanctions must be reviewed and assessed.

Businesses and Functions must:

- seek support and/or approval for country entry from:

i) TCM (consult);

ii) Group Trade Compliance SME (support);

iii) Group ABC/AML SME (support)

iv) Government Relations Senior Adviser (support); and

v) the EC-2 Manager (approval).

- retain relevant documents as a record; and
- ensure Staff follow the E&C Trade Compliance Rule – Country Entry.

4. Reviewing for anti-boycott or blocking conditions

All documents and correspondence related to a transaction must be examined to ensure they do not include any boycotts.

Anti-boycott and anti-blocking laws are generally adopted to discourage and, in specified cases, prohibit companies from participating in a boycott.

Businesses and Functions must ensure:

- Staff report requests to actively or passively (for example, by accepting a contract clause) participate in boycotts to a TCM who will seek a review and support from Trade Compliance Legal Counsel to ensure proper handling and reporting, if required, to the relevant government authorities;
- TCMs advise Staff whether reporting to the Global Helpline is required;
- Staff in scope of the regulatory requirements and at risk of being requested to participate in a boycott take the relevant and latest training;
- relevant documents are retained as records; and
- Staff follow the E&C Trade Compliance Rule – Anti-boycotting or blocking statutes.

Trade Compliance

5. Managing exports and imports of items

Items being exported or imported by, or on behalf of, Shell must be classified according to applicable regulations. Items which are identified as controlled items are subject to additional restrictions and requirements. Where additional government authorisation, registration or licensing is required, this must be obtained with the support of Trade Compliance Legal Counsel. Tangible items crossing national borders must be declared according to applicable customs regulations to ensure a rightful customs charge, deferment or exemption.

Many governments define export to include both tangible and intangible forms of exporting; intangible exports take a "non-physical" form, such as electronic transfers or oral communications.

Businesses and Functions must ensure that:

- they have Technical Classification Experts (TCE) responsible for determining the Export Control Classification Number (ECCN) for items;
- items are classified in accordance with the classification guidance;
- any activities involving the manufacture, use, export or import of drug precursors and military items, or provision of items to national governments, military or defence customers, are reported to a TCM;
- they manage the export, import, storage and access to controlled items;
- they obtain authorisations, registrations, or licences required for controlled items, with the support of Trade Compliance Legal Counsel;
- they obtain the approval of a TCM before exporting, importing or releasing controlled items;
- they have classification experts responsible for determining the Harmonised System (HS) code and the correct customs duties;
- they have procedures and controls in place to communicate export/import data to the relevant authorities;
- they retain a list of controlled items licences, exceptions, classifications, and other relevant data as a record;
- Staff follow E&C Trade Compliance Rule – Managing exports and imports of items and
- Staff follow E&C Trade Compliance Rule – Classifying and Handling

Trade Compliance

5.1. Execution of End User Certificates

Manufacturers, suppliers and vendors involved with the supply of controlled items subject to end-use restrictions frequently impose a notification system, or End User Certificate (EUC). This requires the buyer or ultimate consignee to confirm, in writing, their recognition and acceptance of certain conditions before the items are released for delivery. A manufacturer, supplier or vendor may require that Shell signs an EUC to confirm Shell's recognition and acceptance of restrictions on the use, further transfer or disposal of the items. Similarly, Shell may need to obtain similar certifications from a customer or ultimate consignee.

Before executing an EUC, Businesses and Functions must:

- obtain review and approval from a TCM to ensure the conditions imposed by the EUC are reasonable and appropriate. TCMs will seek support as appropriate from Trade Compliance Legal Counsel;
- develop, document, and implement a control plan for proper management of the restricted items;
- retain relevant documents as records; and
- follow the **E&C Trade Compliance Rule – End User Certification**.

Definitions

[ABC/AML, Antitrust, Data Privacy, Trade Compliance] Legal Counsel	A specialist lawyer in Shell Legal who reports to the Group SME for an assigned risk area and undertakes tasks and responsibilities as delegated by that Group SME, including providing advice to all Shell's Businesses and Functions globally.
Anti-Bribery and Corruption (ABC)/Anti-Money Laundering (AML) clauses	Specific clauses to be inserted into a contract that address ABC or AML risk. The clauses can be found at sww.shell.com/ethicsandcompliance/ABC/guidance
Application Owner	Application Owners are individuals who have been explicitly identified and made responsible for IT solutions. In particular they are accountable to approve Business Impact Assessments (BIAs) and IRM Legal and Regulatory Assessments for those IT solutions. IT maintains an inventory of IT solutions and their Application Owners in its portfolio Management tool.
Approved Electronic Record Repository	A repository approved by the Group Records Manager as suitable to store electronic records.
Approved Physical Record Repository	A storage location, physical archive, physical library or other secure container approved by the relevant IM Compliance Manager as suitable for storage of physical records.
Approved Trade Compliance Repository	A repository approved by a Trade Controls Manager as suitable to store export controlled information.
Archived information	Original information which has been placed in an archive system (in electronic form) or a physical archive (on some kind of media). Typically when information is archived the original information will be disposed of in the IT system. Hence Archived information must be treated as if it were the only copy of the information. In particular the Group Retention Schedule will continue to apply to Archived information.
Associated Parties	External parties that in their interactions with Shell may have access to Restricted information in general because a joint venture information sharing risk assessment or third party information sharing risk assessment has determined that they have a legitimate business purpose and lawful right to do so.
At risk/at high risk	The level of exposure, requiring different type of training for the respective target audiences.

Definitions

Audit Logs	Some IT systems have a facility to keep certain information about their usage including events and incidents that occur(red) in log files. Most frequently this will include information about who accessed, modified or deleted information, access rights or other configuration settings in systems.
Backup	A copy of Original information intended for use in case the Original information is damaged or destroyed. Typically backup and restoration of backups is performed by the IT function or its (third party) suppliers. Restoration from backups is expected to usually occur only in exceptional circumstances (i.e. it is not a routine activity to access or use backups).
Binding Corporate Rules (BCR)	Mandatory internal rules adopted by Shell that govern the intragroup processing of personal data, including transfers between Shell companies, in a binding and consistent manner worldwide. These rules enable Shell to meet data processing requirements in different countries, and have been approved by Data Protection regulatory authorities. Regardless of location, Shell companies that process personal data must comply with the Binding Corporate Rules.
Boycott	A refusal to deal commercially or otherwise with a person, firm, or country.
Business Asset	A business asset is anything owned (or leased long-term) which can produce future economic benefit, whether in possession or by right to take possession. The value of a business asset can be expressed in monetary terms and is listed on the company's balance sheet. The term 'asset' is further used in the context of legal assets (e.g. licenses, patents), delivery assets (retail stations, refineries/plants), engineering assets (pipelines, platforms, wells), subsurface assets (fields, reservoirs, plays) and metaphorical assets (people, reputation). Source: Shell Wiki
Business Integrity Department (BID)	Specialist unit within Shell Internal Audit responsible for Code of Conduct incident reporting, including the Shell Global Helpline (which is operated by a third-party supplier), and investigation of Code of Conduct incidents.
Business Opportunity Manager (BOM)	The individual responsible for the overall management of a business opportunity. See the Opportunity Realisation Standards for further detail: https://sww.shell.com/ors
Business partner	Any third party, other than a customer or supplier, that either has or has had a business relationship with a Shell company.

Definitions

Category Management and Contracting Process (CMCP)	Process by which all contracting and procurement is managed. More information on the Category Management and Contracting Process can be found at sww.shell.com/cp/
Clean team	A team (within the deal team) that (subject to LAT advice) exclusively comprises of individuals who may receive CSI from a third party or about the target without violating antitrust law. Such individuals could include third party advisers or recent retirees.
Close known associate (of a government official)	A close known associate of a government official (GO) is someone who has a close business or personal relationship with a GO. This can include: i) an individual known to have joint beneficial ownership of a legal entity or a legal arrangement or any other close business relationship with a GO, ii) an individual who has sole beneficial ownership of a legal entity or a legal arrangement which is known to have been set up for the benefit of a GO.
Code of Conduct	Sets out the rules and guidelines within which every Shell employee must operate every day. Based on the Shell General Business Principles (SGBP), and the company's core values of honesty, integrity and respect for people, it instructs and advises you how to avoid situations that may damage you or Shell. It sets high standards and shows you how to achieve them. The Code applies to every employee, director and officer in every Shell company, as well as contract staff working for a Shell company. Available at http://sww.shell.com/codeofconduct
Code of Conduct Register	Mandatory Group tool for recording actual, perceived or potential COI, G&H and attendance at trade association events. Accessed at sww-codeofconduct.shell.com/.
Collection	Any discrete collection of information – such as a SharePoint site or library; a personal or shared email mailbox; a shared drive. Collections may contain records and non-records. Collections may contain physical and electronic information.
Collection Owner	An individual assigned the responsibility to manage a collection. Where a specific assignment has not been made then any individual who can determine access to the information is a Collection Owner. The Collection Owner for individual storage (e.g., email mailbox, home drive, laptop hard disk, smartphone, tablet, USB stick) is the individual it has been assigned to. The Collection Owner of a SharePoint site is the Functional Site Owner.

Definitions

Communicate/communications (with competitors)	Where competitors interact in any form, either directly or indirectly, whether in person (e.g., formal or informal discussions in meetings, or discussions at social events), or by telephone, email, instant messaging, sharing documents, or through social media.
Competing JVs	Joint ventures in which Shell participates (whether they are characterised as an NOV or SOV), which satisfy the conditions: i) Shell's interest in the JV is not a controlling interest, ii) the JV is on the market in its own right, supplying products or services to customers (and not merely to its own shareholders or owners (or their affiliates), iii) the JV is a direct competitor of Shell.
Competitive intelligence (CI) gathering	Involves monitoring the external environment, including the behaviour of competitors and public domain sources, to take strategic decisions. The CI gathered should generally not include competitively sensitive Information (CSI), but should be limited to gathering information that is in the public domain and drawing internal conclusions from the behaviours observed in the marketplace.
Competitively sensitive information (CSI)	Any information that could affect market behaviour of Shell or its competitors, including but not limited to information concerning sales, prices (e.g., pricing methodology, future prices), discounts, rebates, promotions, contract negotiations, capacity utilisation (e.g., debottlenecking or mothballing intentions), production (e.g., production volumes and production shutdown or output information), customer information, or intentions to sell or not to sell in certain territories or to certain customers.
Competitor	A business that is a direct competitor or potential competitor of Shell, including procurement competitors. Direct competitors are businesses in which Shell does not have a controlling interest that are active in the same market as any member of the Shell Group and compete directly with Shell in the supply of the same products or services in the same geographic market. Potential competitors are businesses in which Shell does not have a controlling interest that could be a direct competitor within a foreseeable time (usually considered within one year). Procurement competitors are businesses that are buying or seeking to buy the same goods or services as Shell, even if the business does not compete with Shell in the sale of products or services.
Conflict of interest (COI)	A situation where two or more competing interests impair an individual's ability to make objective decisions.

Definitions

Consent	The permission granted by an individual to the processing of personal data, which has been clearly expressed, is freely given, is based on complete and correct information and is recorded for evidence. Consent can be given either by a statement or by a clear affirmative action.
Contract staff	Staff providing services under Shell's day-to-day supervision who have no employment contract with Shell but are employed and paid by a third party.
Controlled item	Items identified by a specific Export Control Classification Number (ECCN) or other official government list. Controlled goods, technology, software or services may require government authorisation or a licence before being exported or imported to particular parties or destinations.
Controlling interest	The power to govern the financial and operating policies of an entity to obtain benefits from its activities. Control is presumed to exist when an entity acquires, directly or through subsidiaries, more than half of the voting power of an entity, unless, in exceptional circumstances, it can be demonstrated that such ownership does not constitute control. Further guidance is given in the document "Control for antitrust purposes" sww.shell.com/ethicsandcompliance/areas/trade/antitrust/control_AT.html
Counterparty	Any entity (including both legal entities and other forms of organisation or individuals) with which Shell interacts but which is not part of the Shell Group of companies. This includes entities engaged in trade, including competitors, suppliers and customers; JVs in which Shell does not have a controlling interest (whether Shell is the operator or not); individuals (excluding Staff); business and government agencies; trade associations and similar industry bodies; and external consultants and external advisers who are not contract Staff
Data controller	Any party (a person, public authority, agency or any other body) that, either alone or jointly with others, determines the purposes, conditions and means for processing personal data.
Data processor	Any party (a person, public authority, agency or any other body) that processes personal data on behalf of a data controller and under the instructions of the data controller.
Deal(s)	The preparation, negotiation, and execution of corporate acquisitions, divestments and mergers, the formation of joint ventures, or a change in the structure or ownership of an existing JV. Depending upon local law, this might also extend to the acquisition or divestment of assets.

Definitions

Decision Executive (DE)	Opportunity Realisation Standard (ORS) role, designated by the sponsoring Business, with accountability for the effective management of business opportunities so that maximum value is realised for Shell and its stakeholders; also accountable for delivery of the opportunity, the existence of effective risk management and an opportunity control framework that provides adequate assurance to the Line of Sight.
Decision Review Board (DRB)	Defined in the Opportunity Realisation Standards, members of the DRB assist the DE and BOM in making good quality decisions in relation to the opportunity by providing support and advice based on their expertise.
Deemed export	Releasing or otherwise transferring technology or source code to a foreign person in the United States. The technology or source code is deemed to be exported to the foreign national's most recent country of citizenship or permanent residency.
Distributor(s)	Shell customer who buys Shell product for resale on its own account (i.e., acting independently and at own financial risk) and where both of the following criteria are met: i) where Shell appoints such customer as distributor, reseller or similar on terms that it is purchasing for resale; and ii) Shell customer is allowed to sell product to its customers using a Shell-owned brand or trademark, including but not limited to use on packaging, and where delivery of the product by the customer to its own customer is Shell-branded (e.g., tankers containing product are Shell- branded or co-branded).
Donations	Contributions to an organisation rather than individuals where there is no expectation of anything in return.
Double-hatting	Where individuals are directly involved in the day-to-day management or commercial direction of two potentially conflicting or competing entities e.g., Staff managing a Shell business and being Director or Shell Shareholder Representative (SSR) of a competing JV; Staff being a Director or SSR of two or more Competing JVs; Staff managing a Shell business and being Director of or commercial or strategic adviser to any of Shell's direct competitors.

Definitions

DP Focal Point	DP Focal Points are nominated initial points of contact in the Businesses and Functions for any questions/issues related to data privacy who: i) understand the landscape of processes and IT systems where personal data is processed; ii) provide support for DP incident handling, individual's DP requests and DP complaints processes; iii) assist the Businesses and Functions in identifying the Staff that require data privacy training; iv) embed and promote awareness of the mandatory Manual requirements; and v) identify issues relating to data privacy for their assigned area and assist with the day-to-day data privacy questions.
DP Legal Adviser (DPLA)	DPLAs are designated lawyers in country legal departments with specific data privacy knowledge, responsible for provision of country/region legal advice, approving processing of sensitive personal data where local laws require it contrary to the DP Manual, and advising on individual requests, complaints, and DP incidents, where required.
EC-2	An employee who reports to a person who reports to a member of the Shell Executive Committee.
EC-2 Manager	A manager who is two organisational levels lower than an Executive Committee member
Employee	A person who has an employment relationship with a Shell company.
End user certificate (EUC)	A certificate or statement provided by the exporter of an item to the end-user in fulfilment of export requirements.
End user computing	Any system, tool or application used to collect, manage, store or process personal data, which has not been registered as an IT asset.
Ethics and Compliance due diligence	Ethics and Compliance due diligence is the process to seek third party information and to ensure that there is an understanding of who Shell is doing business with, encompassing red flag identification, screening and mitigation for Trade Compliance, and ABC/AML risks.
Ethics and Compliance Officer	Supports Businesses and Functions in their activities to manage ethics and compliance risks and comply with Shell's Ethics and Compliance requirements; independently monitors and reports the state of compliance in the Group. For purposes of this Manual, this includes Ethics and Compliance Managers (ECMs).

Definitions

Ethics and Compliance Subject Matter Expert (SME)	A general term for a Group SME for a risk area and/or Legal Counsel reporting to them.
Export	A shipment or transmission of items from one country to another. In the USA, this can include a release of technology or software source code to a non-US national. In a customs union such as the European Community, it includes shipment outside the customs territory of the EU. In a very limited number of cases (highly controlled items), an export can include intra-EU movement from one member state to another.
Export Control Classification Number (ECCN)	A system used by some countries to classify items for export. It is generally represented as an alphanumeric designation consisting of five characters – a single-digit number, followed by one letter (A through to E), then followed by a three-digit number.
Export controlled information	Information that contains technical information subject to export or import controls. Export controlled information may be identified by an Export Classification Code or Export Control Classification Number (ECCN) which determines applicable legal requirements. For further information see the Trade Compliance website and the Trade Compliance Manual.
External Party	Any entity (including both legal entities and other forms of organisation or individuals) with which Shell interacts but that is not part of the Shell Group of companies. For the avoidance of doubt, this includes: Entities engaged in trade, including competitors, suppliers and customers; JVs in which Shell does not have a controlling interest (whether Shell is the operator or not); Individuals (other than Staff); Business and Government agencies.
Facilitation payment	A minor payment to induce a (usually low-ranking) government official to expedite or secure performance of a routine duty which that person is already obliged to perform and where such payment would exceed what is properly due. A facilitation payment is not permitted by Shell and is illegal under the UK Bribery Act and other applicable legislation.
File Plan	The set of record types that is applicable to a collection of records and the location where the records are stored (e.g., in SharePoint, an IT solution, a physical record repository).
Generally embargoed country (GEC)	A Shell term for a country subject to a comprehensive embargo. The current list of GECs is available at sww.shell.com/ethicsandcompliance/areas/trade/trade_control/embargoes/gecs.html.

Definitions

Gifts and hospitality (G&H)	Any gifts, travel, accommodation, trips, services, entertainment, prizes from external competitions or lotteries and any other gratuitous item, event, benefit or thing of value received from or offered to any person in connection with Shell business.
Goods	Any physical item, including articles, materials, products, equipment or supplies, excluding technology and software.
Government intermediary (GI)	Any person, company, firm or joint venture that is engaged by Shell and has any direct or indirect dealings with a government official connected with Shell's business, including an intermediary nominated by a government but paid by Shell. These include: processing agents e.g. freight forwarders, customs agents; commercial agents e.g. consultants, business agents; or professional agents e.g. attorneys, accountants, certain contracts e.g. turnkey contracts for the construction of facilities, Chamber of Commerce.
Government official (GO)	Official or employee of any government agency, ministry or department of a government, including any person acting in official capacity for a government, regardless of rank or position; any official or employee of a company wholly or partially controlled by a government (e.g., a state-owned oil company), but excluding employees seconded to such companies; a political party or any official of one; any candidate for political office; any officer or employee of a public international organisation, such as the United Nations or World Bank; and immediate family members (spouse, dependent child, parent or household member) of any of the people listed.
Group [ABC/AML, Antitrust, Data Privacy, Trade Compliance, Customs, Political Payments] Subject Matter Expert (SME)	Accountable for defining Shell's compliance policies for an assigned risk area, including working with Businesses and Functions to identify associated risks and controls to mitigate them. The Group SME supports associated rules and training content, provides advice to all Businesses and Functions, and monitors, communicates, and reports changes in the risk environment. The Group Data Privacy SME also serves as the contact point to the data protection authorities for all data protection issues, including data breach reporting.
Group Screening Service	A Group service that performs integrity screening. For more information go to http://sww.shell.com/ethicsandcompliance/GSS

Definitions

Gun jumping	Gun jumping is when any party to a deal takes steps to implement the deal before all necessary antitrust merger clearances have been obtained. "Taking steps to implement" a deal includes any attempt to exercise management, operational or commercial control or influence over the third party's business or day-to-day commercial decisions.
Harmonised System (HS)	An international nomenclature for the classification of products. It allows participating countries to classify traded goods on a common basis for customs purposes. At the international level, the HS for classifying goods is a six-digit code system.
Highly restricted country (HRC)	A Shell term for a country that is not comprehensively embargoed but is subject to strict controls related to exports or activities with certain persons. The current list of HRCs is available at: sww.shell.com/ethicsandcompliance/areas/trade/trade_control/embargoes/hrcs.html.
Import	A receipt of items shipped or transmitted from another country. In a customs union such as the European Community, this would be a receipt from outside the customs territory of the EU. In a very limited number of cases (highly controlled items) an import can include intra-EU movement from one member state to another.
Information	Information and data under Shell's control, whether proprietary to a Shell company or owned by an external party, in whatever form (including oral communications, physical documents, electronically stored information and data). Also included is information that is processed by suppliers, contractors and other external parties on behalf of Shell companies (for example through business process outsourcing).
Information Management	Information management is defined in the broadest terms in these Standards, meaning any direct or indirect interaction with information, by staff or by automated means (by or on behalf of Shell). This includes: creating, receiving, identifying and classifying information; storing, processing and maintaining information; protecting and securing information; retrieving and using information; the sharing of information directly or indirectly with internal or external parties by whatever means (oral, physical or electronic); and the preservation and disposal of information.

Definitions

Information Management Compliance Manager (IM CM)	Information Management role designated by each Business and Function, who is a subject matter expert serving as the initial point of contact for questions or issues related to information management and records management compliance. Responsible for embedding and promoting awareness of the mandatory requirements of the IM Manual and for identifying and reporting issues relating to IM compliance for their assigned area.
Inside Information	Inside information means information that is precise, not generally available to the public and which would, if generally available, be likely to have a significant effect on the market price of Securities (as defined in the Royal Dutch Shell plc Securities Dealing Code). Information would be likely to have a significant effect on price if and only if it is information of a kind which a reasonable investor would be likely to attach importance in deciding whether to buy, sell or hold the Security (as defined in the Royal Dutch Shell plc Securities Dealing Code). Both positive and negative information can be inside information. See Insider Dealing http://sww.shell.com/ethicsandcompliance/insidersealing/insider_dealings.html
Integrated Risk Review	A biennial (every two years) assessment. The review builds on existing risk inventories and knowledge and identifies ABC/AML, AT, DP, TC and IM risks in the business or function through engagement with business stakeholders and SECO SMEs.
Intellectual property	Includes: patent rights; utility models; trademarks and service marks; domain names; copyright (including copyright of software); design rights; database extraction rights; rights in know-how or other confidential (sometimes called 'trade secret' or 'proprietary') information; and rights under IP-related agreements.
IRM Legal and Regulatory Assessment	The risk assessment http://sww.shell.com/it/irm/legalandregulatory/index.html method used to assess information sharing risks for IT solutions and determine required business, IT and contractual controls. The risk assessment covers requirements regarding personal data (Data Privacy), competitively sensitive information (Antitrust), confidential technical information (Intellectual Property), trade compliance requirements related to export controlled information and hardware/ software, records management, eDiscovery and anti-bribery and corruption.

Definitions

IT Solution	Any combination of IT hardware, software and telecommunications, whether products, applications or services, whether internally or externally provided. This term is used to differentiate from the IT Function or IT activity. Terms such as IT tool, IT service, business application and social media are used for clarity or to aid readability and are all considered IT solutions.
Items	Term used to refer to goods, technology, software or services, collectively.
Joint industry advocacy	Representation, together with other industry participants, of industry views in public, to bodies including governments, regulatory agencies and non-governmental agencies.
Joint Venture Information Sharing Risk Assessment	The risk assessment http://sww.shell.com/it/irm/legalandregulatory/index.html method used to assess information sharing risks related to Sharing Risk Assessment non-Controlled or non-Operated joint ventures and determine required business, IT and contractual controls. In particular, identity management requirements and access and entitlement rules for information and IT solutions are determined.
Label/Labelling	Other means than metadata to describe information – examples for confidentiality are: writing "Confidential" on a letter or an envelope; including "Most Confidential" in the text of an email, or in the header of a document; including the word "Confidential" in the footer of a printed report output by an IT solution.
Legal Privilege	Legal privilege is an important right that allows certain legal advice to be withheld from disclosure under specific circumstances. Information is only legally privileged under specific circumstances. The rules of legal privilege are complex and vary in different legal jurisdictions. Shell Legal must be consulted on any matter related to legal privilege.
Manual of Authorities (MOA)	Documented principal delegated authorities which support Royal Dutch Shell plc and other Shell companies in the maintenance of a risk-based system of internal controls to ensure that transactions are carried out in accordance with management's authorisation. The MOA tool can be found at sww-moa.shell.com/home/.
Metadata	Data (usually in an IT system) added or stored along with information that describes the information. Examples of metadata in SharePoint are the document author; the date a document was last modified; who last changed a document.

Definitions

Military items	Goods, technology, technical data, or services designed specifically for military use.
Non-Record	Information that is not a record.
Non-Shell operated venture (NOV)	A JV that is not a Shell operated venture. An NOV occurs where the JV: is operated by its own management ("self-operated"), or another JV participant or one of its affiliates ("other participant operated"); has more than one operator for different assets/activities within the venture ("multiple operators"); or is managed by a third party contractor ("third party operated").
Per diem	A daily allowance, i.e., a specific amount of money allocated to an individual to spend per day, to cover living and travelling expenses in connection with work.
Personal data	Any information relating to an identified or identifiable individual; if the information allows someone, somewhere (even outside Shell) to identify an individual then the data is personal data. Personal data examples include: a person's name, contact information, on-line identifiers such as IP addresses, cookie strings or mobile device IDs that can be used to identify an individual, personal preferences or opinions, employment information, financial information, CCTV images and photographs, or location data. Pseudonymous or encrypted data is still personal data.
Physical Records	Records that are physical objects such as paper documents, film (e.g., x-rays, microfiche), CDs/DVDs or samples (e.g., soil, water, subsurface).
Political payment	Any payment to a political party or a payment that will directly or indirectly assist in the defeat or election of a political candidate.
Privacy Impact Assessment (PIA)	Series of questions that the process owner in a Business or Function must answer about the business process and/or IT system to identify: key characteristics of processing personal data by the process owner; the potential impact that the business process and/or IT system may have on data privacy compliance and options for mitigation; what IT and business controls must be implemented to ensure compliance with the requirements of the Manual and Rules as well as local data privacy laws (where applicable). See: sww.shell.com/ethicsandcompliance/areas/dataprivacy/pia.html

Definitions

Privacy notice	A statement communicated to the individual at the moment of collection of personal information and informing the individual on the identity of the data controller, the purposes of processing personal data, the rights of the individual in relation to such processing and other details on processing personal data. For specific requirements regarding the content of privacy notices see: sww.shell.com/ethicsandcompliance/areas/dataprivacy/DPrulesregardingnoticerequirement.htm.
Processing (of) personal data	Any action performed with personal data by electronic means or in systematically accessible paper-based filing systems such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, transfer, dissemination, making available, alignment or combination, blocking, erasure or destruction.
Publicly available	Information is considered publicly available when it has been released through appropriate channels, such as press releases, or is generally available through external websites, newspapers or other sources accessible to the general public.
Record	A subset of information created or received as evidence of a business activity, or required for legal, tax, regulatory or accounting purposes, or of importance to the Shell Group's business or corporate memory. Records may exist on paper, as physical items, as images or be stored in an electronically readable or audible format.
Record Type	A classification linked to a record that determines the applicable retention period. Record types are documented in the Group Retention Schedule along with their associated retention periods.
Recorded information	Information that has been physically written down or captured electronically in whatever manner such as words (document; email; instant message), voice (voicemail; recorded meeting) or images (photographs; video). Such information is discoverable for legal purposes. Recorded information may or may not be a record. To avoid ambiguity we state that information must be stored as a record when that is required.
Recusal	The process whereby an individual who is in a decision making or management role (for example a Director of a JV or a member of a Shell Leadership Team – whether at Class of Business or Leadership level) declines to receive CSI and removes himself or herself from the decision making process in relation to competitors.

Definitions

Recycle Bin	A facility provided in some IT systems which allows for 'easy' restoration of Original information that has been deleted in error. In some cases (like the Windows desktop recycle bin) the user is in control of "emptying the recycle bin" (i.e. permanently deleting the information). In other cases (like SharePoint and LiveLink) the period after which recycle bins are emptied is configured at a system level.
Red flag	Term that denotes various indicators and signals, both explicit and implicit, that imply a potential higher ABC, AML, AT, TC, DP or tax evasion risk and may warrant further investigation. Note that red flags are different from risk rating).
Red thread	Red threads are part of the overall process running end-to-end across all chevrons in the Category Management and Contracting Process and represent other functional requirements owned by Subject Matter Experts (SMEs) that impact the Category Management and Contracting Process.
Re-export	The export from one foreign country to another foreign country after initial export.
Relationship Manager	Staff assigned the overall responsibility for managing the relationship between Shell and an external party, such as a supplier, customer, business partner or competitor. Roles such as Contract Holder and Account Manager will often be the Relationship Manager for a particular external party. For Joint Ventures, the Shell Shareholder Representative has this role.
Release	A means of exporting technology or software source code through visual inspection, oral exchanges, electronic exchanges, or application of personal knowledge or technical experience, including the provision of services.
Sanctioned party	A company, individual or organisation subject to sanctions or other restrictions. Sanctioned parties are generally identified on lists published by governmental bodies.
Secondary purpose	Secondary purpose relates to the processing of personal data that is closely aligned to the original processing purpose such as: processing for internal audits or investigations; for the implementation of business controls; for statistical, historical or scientific research; for dispute resolution; for legal or business consulting or insurance purposes.

Definitions

Secondee	An employee (of an "original company") who is temporarily transferred to another company ("host company") to work under the direction and supervision of the host company, but either remains employed by the original company or has the reasonable expectation or right to return to the original company. The categories of secondee used in this Manual are: Secondee-in: A secondment from an external party to a Shell company. Secondees-in may or may not be considered competitors for antitrust purposes. Secondee-out: A secondment from a Shell company to an external party. Competitor Secondee: A secondment from an external party (A) to a Shell joint venture (B) that is also an external party where those companies are considered competitors for antitrust purposes. Individuals who have worked for external parties and are subsequently employed by Shell companies under normal exclusive employment terms and conditions are not considered secondees.
Sensitive personal data	A special category of personal data that reveal: racial or ethnic origin, political opinions, membership of political parties or similar organisations, religious or philosophical beliefs, trade union membership, physical or mental health, including any opinion thereof, disabilities, genetic code or other genetic data, addictions, sexual orientation or sexual life, criminal offences, criminal records, proceedings regarding criminal or unlawful behaviour, or biometric data (e.g., fingerprints, retinal/facial recognition). Local laws may include additional data types as sensitive personal data (social security numbers). In some circumstances, photographs may be considered sensitive personal data when used to identify such information as ethnicity or a health condition.
Shell company	Any company in which Royal Dutch Shell plc holds a controlling interest, either directly or indirectly. A Shell company may be wholly owned or a joint venture (JV).
Shell General Business Principles (SGBP)	Describe the Group's core values, its responsibilities and the principles and behaviours by which it does business. The SGBP can be found at sww.shell.com/ethicsandcompliance/sgbp.
Shell Legal	The usual Shell lawyer for the Business or Function, unless this Manual specifies that advice or approval is to be obtained from the relevant SME within Shell Legal.
Shell Operated Venture (SOV)	A JV where a Shell company has been formally designated as the Operator under the terms of the JV documentation.

Definitions

Shell Shareholder Representative (SSR)	An internal Shell organisational appointment by a Business to govern Shell's investment in a JV on behalf of the ultimate Shell shareholder, Royal Dutch Shell plc.
Social investment (SI)	The contribution of skills and/or resources to a host society to provide lasting benefit to the host society and/or the environment and to Shell. SI activities may range from increasing local capacity building skills to supporting national education, health or conservation programmes. SI may be voluntary or required by a host government under a contract.
Social Media	Social media is broadly defined to refer to 'the many relatively inexpensive and widely accessible electronic tools that enable anyone to publish and access information, collaborate on a common effort, or build relationships.' In this Manual: Internal Social Media means social media that is listed as 'Internal Social Media' in the approved IT tools site https://sww.shell.com/myworkspace/thinksecure/behaviours/social.media.html and is configured so that it is accessible only to individuals who have a (direct or indirect) contractual relationship with Shell that address confidentiality requirements (such as Staff, JVs, suppliers, contractors). Public Social Media means social media that is either accessible to individuals who have no such contractual relationship with Shell (such as members of the general public) or is purchased or accessed under consumer (rather than corporate) terms and conditions. The approved IT tools site https://sww.shell.com/myworkspace/thinksecure/behaviours/social.media.html includes common public social media tools with clarification on acceptable use.
Social Security Number	A government-issued identifier unique t an individual over the course of their life for the purpose of identifying the individual in a national register and/or providing social security, health, tax and other national benefits or liabilities.
Software	A collection of one or more programs or microprograms fixed in any tangible medium of expression.
Source code	Written code that can be compiled into object code.
Sponsorship	A form of advertising to promote the Shell brand in which Shell offers funding to a company, association or other institution in return for a range of promotional opportunities.
Staff	All Shell employees, contract Staff and secondees in every Shell company.

Definitions

Structured IT Solution	An IT solution in which all information that may be stored or processed has been sufficiently classified when the solution was designed such that functionality is built-in that addresses all relevant (legal and regulatory) requirements. When staff use structured IT solutions for their intended purpose and in the manner described in the solution documentation then the IT solution ensures that legal and regulatory requirements are met without the need for further classification or compliance actions by staff. Structured IT solutions may contain unstructured data if it has sufficiently defined content to classify it – for example a Finance system may contain scans of paper invoices or expense receipts.
Technical Classification Experts (TCE)	Technical Classification Experts are a network of resources within the Business or Function providing technical classification support and advice, including responsibility for assigning an ECCN or other export classification for an item. See sww.shell.com/ethicsandcompliance/contacts/sme/contacts.html for a list of TCEs.
Technology	Specific information necessary for the development, production, or use of a product. Technology can take the form of technical data or technical assistance.
Tenant	A person or company who occupies land or property rented from a landlord.
Third party	Any entity (including both legal entities and other forms of organisation or individuals) with which Shell interacts but which is not part of the Shell Group of companies. This includes entities engaged in trade, including competitors, suppliers and customers; JVs in which Shell does not have a controlling interest (whether Shell is the operator or not); individuals (excluding Staff); business and government agencies; trade associations and similar industry bodies; and external consultants and external advisers who are not contract staff.
Third Party Information Sharing Risk Assessment	The risk assessment method used to assess information sharing risks related to external parties which Sharing Risk Assessment are not joint ventures and determine required business, IT and contractual controls. In particular, identity management requirements and access and entitlement rules for information and IT solutions are determined.

Definitions

Trade association	Any organisation (trade association or similar industry body), irrespective of what it is called, that brings competitors together, and where the primary aim of the forum is for competitors to engage in one or more of the following commercial or business-related activities: sharing industry best practices related to commercial activities; advancing industry or joint commercial terms and conditions; market data collection; industry benchmarking activities; or industry joint advocacy. Such bodies may be referred to with names such as "Industry Roundtable" or "Industry Working Group".
Trade compliance laws	Laws and regulations regulating the flow of items across national boundaries, including regulations or sanctions restricting trade and other activities with specific countries, persons or entities. For the purposes of this Manual, trade compliance laws do not include controls or restrictions on the export of data related to the exploration of natural resources, or regulations requiring registration or licensing of hazardous substances subject to controls managed by HSSE.
Trade Compliance Manager (TCM)	The Trade Compliance Manager provides support and oversight of the development, implementation and day-to-day operation of a trade compliance programme that meets the TC requirements in the Manual.
Trade compliance programme effectiveness review	An assessment to identify the specific trade compliance risks associated with a business. Risks must be supported by appropriate metrics. Any risks must also identify the internal controls, processes, and procedures in place to mitigate such risks.
Trade Compliance Sponsor	An EC-1 level manager
Transfer (of personal data)	Disclosure of personal data in any form, electronic or printed, including remote access.
Ultimate consignee	The person or entity identified on shipping documents that has a legal right to claim the goods at the destination. Generally, this party may be the purchaser or end-user.
Unstructured Information/Data	Information or Data that does not have a pre-defined data model or is not organized in a pre-defined manner. Examples include emails, documents, presentations, pictures, audio and video files.

Definitions

Unstructured IT Solution	An IT solution in which some of the information stored or processed must be classified by the users of the system and additional steps must be taken to ensure compliance. Normal use of Email, collaboration and document management tools such as SharePoint fall into this category. Note that it is possible to build structured IT solutions (such as applications) on top of unstructured IT solutions like SharePoint.

Version 1.0 November 2018 | Unrestricted

If there are discrepancies between the translated version and English version, the English version will prevail.