Talisman Safe Harbor Statement

Talisman Energy USA Inc. and it affiliates located in the United States of America ("**US**"), including TE Global Services Inc. and Talisman Energy Services Inc. (collectively "**Talisman**") respects and protects personally identifiable information that we collect from our employees, prospective employees, contractors, suppliers and stakeholders. This Statement describes the principles Talisman follows with respect to all transfers of Personal Information (as defined below) and Sensitive Personal Information (as defined below), whether in electronic, paper or verbal format, between countries in the European Economic Area ("**EEA**") and the US.

Safe Harbor

The United States Department of Commerce and the European Commission have agreed on a set of data protection principles and frequently asked questions (the Safe Harbor Principles) to enable US companies to satisfy European Union ("**EU**") law requirements for adequate protection of personal information transferred from the EU to the US. Consistent with our commitment to protect personal privacy, Talisman adheres to the seven Safe Harbor Principles (Notice, Choice, Onward Transfer, Security, Data Integrity, Access and Enforcement) in connection with transfers of personal information into the US. It is Talisman's policy to collect and handle personal information in a fair and lawful manner.

Definitions

Employee - An individual employed by Talisman, a Talisman affiliate, subsidiary or division located in a country of the EEA.

Prospective Employees - Candidates and/or applicants for jobs at Talisman.

Personal Information - Any information or set of information about an identified or identifiable individual including Employees, Prospective Employees, contractors, suppliers and stakeholders, regardless of the medium or format in which the data is stored that could be used by or on behalf of Talisman to identify an individual. Personal Information collected by Talisman related to Employees and Prospective Employees may include:

- Demographic and contact information including name, home or mailing address, telephone number, date of birth, government issued identification number, emergency contacts, and gender;
- Education and employment history;
- Banking or financial information; and
- Other information such as marital status, driver's license information, dependents, beneficiaries and citizenship.

Personal Information collected by Talisman related to landowners, leaseholders, residents, royalty holders and others may include:

- Name and contact information, plus additional information as required (e.g., information required for emergency response procedures);
- Banking information to make payments directly to bank accounts; and
- Leaseholder preferences as appropriate.

Sensitive Personal Information - Personal Information that reveals race, ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or that concerns health or sex life. Sensitive Personal Information collected by Talisman related to Employees and Prospective Employees may include:

- Health information, including medical conditions or disabilities where regulated or required by law or for safety related reasons; and
- Information provided in connection with security background checks, as required.

1. Notice

Talisman clearly identifies the purposes for the collection of Personal Information and Sensitive Personal Information at or before the time of collection.

Talisman processes Personal Information and Sensitive Personal Information in the US at its data center located in Chicago, Illinois which is operated by TE Global Services Inc. as necessary to comply with legislative and regulatory requirements, or as appropriate to perform human resources management, to support health and wellness of Employees and Prospective Employees, to promote safety and manage business and financial aspects of Talisman and its affiliates. Talisman informs individuals about the purposes for which it collects and uses information about them, how to contact Talisman with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means Talisman offers individuals opportunities for limiting the use, disclosure and transmission of this information. Notice will be provided in clear and conspicuous language when individuals are first asked to provide Personal Information and/or Sensitive Personal Information to Talisman or authorize Talisman to collect the information from third parties and before Talisman uses such information for a purpose other than that for which it was originally collected. All persons collecting Personal Information or Sensitive Personal Information from individuals on Talisman's behalf are required to be familiar with the purpose for its use. When new purposes are identified consent will be obtained from the individual prior to use of the information.

2. Choice

Consistent with the Notice provision set forth above, Talisman collects and uses Personal Information and Sensitive Personal Information needed to conduct its business. Talisman requires the affirmative consent of the individual when it collects, uses and discloses Personal Information and Sensitive Personal Information.

Talisman will seek express affirmative consent (either written or verbal), for the collection, use and disclosure of Personal Information and Sensitive Personal Information. By way of example, Talisman will obtain consent before:

(a) disclosing Personal Information/Sensitive Personal Information to a third party (other than disclosure to an agent or contractor processing the data solely on Talisman's behalf, or disclosure required by law); or

(b) using Personal Information/Sensitive Personal Information for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual.

Talisman is not required to seek consent in connection with the transfer of Sensitive Personal Information when the processing is:

- in the vital interests of the individual or another person;
- necessary to establish legal claims and defenses including the investigation of an incident or breach of agreement;
- related to information made publicly available by the individual;
- required to provide medical care or diagnosis as in the event of emergency; or
- required to carry out employment law obligations.

3. Onward Transfer

Before making disclosure to a third party, Talisman will first apply the Notice and Choice principles as described above.

Talisman discloses Personal Information and Sensitive Personal Information externally to third-party contractors or agents that process the data on Talisman's behalf; to satisfy government reporting requirements; to meet other legal obligations; to assert or defend legal claims or interests; or with the consent of the individual. Unless the disclosure is legally required (such as tax reporting or responding to a judicial subpoena), Talisman also ensures that the third party is obligated (by law, contract, or its own Safe Harbor certification) to provide at least the same level of privacy protection as is required by these principles.

Where Talisman contracts with third parties to process Personal Information on its behalf, Talisman's policy is to contractually obligate the third parties to maintain the confidentiality and security of Personal Information they receive; to act upon it only in accordance with the instructions they receive from Talisman and/or the individual; and to handle the information strictly in accordance with these principles.

4. Security

Personal Information and Sensitive Personal Information must be protected by reasonable administrative, technical and physical safeguards appropriate to the sensitivity of the information in order to protect against loss, misuse, theft, unauthorized access, disclosure, alteration, and destruction.

Talisman employs methods of protection of Personal Information and Sensitive Personal Information including:

- physical measures (e.g., locked filing cabinets and desks, restricted access to floors and offices);
- organizational measures (e.g., security clearance, access by authorized individuals only, retention of information for only as long as necessary); and
- technological measures (e.g., passwords, encryption).

All persons who access Personal Information or Sensitive Personal Information held by Talisman are required to keep such information confidential. Talisman's security policies, operating procedures, and technical controls, where applicable, generally adhere to commonly accepted standards for security of networks, infrastructure, applications, and data.

5. Data Integrity

The amount and type of information gathered by Talisman must be limited to what is necessary for the identified purpose(s). In addition Personal Information and Sensitive Personal Information shall be as reliable, accurate, complete and up-to-date as necessary for the purposes for which it is to be used.

Talisman limits its collection of Personal Information and Sensitive Personal Information to that which is relevant for the intended business and legal purposes and will not collect information indiscriminately. Talisman does not use the data in a way that is incompatible with the purposes for which it was collected or subsequently authorized by the individual. To the extent necessary for those purposes, Talisman will foster practices to achieve initial and ongoing accuracy of Personal Information and Sensitive Personal Information to ensure that the information is reliable for its intended use, accurate, complete, and current.

6. Access

Upon reasonable request an individual must be informed of the existence, use and disclosure of his or her Personal Information and/or Sensitive Personal Information and shall be given reasonable access to that information.

Talisman provides individuals an opportunity to access Personal Information about them and to correct, amend or delete that information where it is inaccurate, out-of-date or irrelevant. Talisman will be able to accommodate an individual's reasonable request for access except in certain limited circumstances which include, by way of example, where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy; or where the rights of persons other than the individual would be violated; or disclosure would interfere with law enforcement.

Employees can access and review their own Personal Information and/or Sensitive Personal Information by:

- Reviewing Personal Information contained in on-line self-service applications.
- Contacting their Supervisor or Human Resources Business Partner to arrange to view and/or obtain a copy of the employee file kept in the Human Resources department. The original file must not be removed from the Human Resources department.
- Contacting Occupational Health to arrange to view and/or obtain a copy of the file kept in the Occupational Health department. The original file must not be removed from the Occupational Health department.
- Request access to any remaining Personal Information and/or Sensitive Personal Information not described in items 1-3 by contacting the Talisman Privacy Coordinator at privacycoordinator@talisman-energy.com.

Non-employees can request access to Personal Information or Sensitive Personal Information by contacting the Talisman Privacy Coordinator at privacycoordinator@talisman-energy.com.

To guard against fraudulent requests, Talisman requires sufficient information to confirm the person making the request is authorized to do so. Talisman normally responds to written requests for access to Personal Information and/or Sensitive Personal Information within 45 days or as may be specified in the applicable legislation.

7. Enforcement

Talisman has processes for individual complaints regarding the use of Personal Information and Sensitive Personal Information and verification of compliance with the Safe Harbor principles and assessment of this Statement. Talisman will cooperate with the appropriate regulatory bodies in connection with any complaints.

Talisman will cooperate with European data protection authorities, the U.S. Dept. of Commerce, the U.S. Federal Trade Commission, relevant state or provincial agencies, and law enforcement and judicial authorities in investigating any privacy complaints or suspected violations of privacy laws or Talisman's international Safe Harbor commitments, as well as in rectifying any noncompliant practices. Employees or contractors who violate the terms of these principles may be subject to disciplinary consequences up to and including termination of employment or termination or non-renewal of contract, in addition to any other legal measures that may be taken by Talisman, the affected individuals, and their representatives.

Talisman investigates all complaints concerning compliance with this Statement. A complaint can be made by contacting the Talisman Privacy Coordinator at privacycoordinator@talisman-energy.com.

If a complaint is found to be justified, Talisman will take appropriate measures to resolve the complaint including, if necessary, amending its policies and procedures. Individuals shall be informed of the outcome of the investigation regarding their complaint. In the event of a complaint, and with the consent of the Talisman and the individual making the complaint, mediation of the complaint will be conducted with a view to early and amicable resolution.

For more information or questions about this Statement, please contact the Talisman Privacy Coordinator by email at privacycoordinator@talisman-energy.com, telephone at 403-237-4833 or by mail:

Talisman Privacy Office
Suite 2000, 888 3rd Street S.W.
Calgary, Alberta T2P 5C5
Canada

8. Verification

Talisman will conduct regular reviews of this Statement and related privacy procedures.

Talisman will review this Statement, the privacy principles in this Statement and the embodied standards on an ongoing basis to ensure they remain relevant and current with respect to changing privacy legislation and to verify compliance with these Safe Harbor principles.

9. Accountability

Talisman is responsible for Personal Information and Sensitive Personal Information under its control and has designated its Privacy Coordinator as the person accountable for Talisman's compliance with these principles.

When required, other Talisman individuals may be appointed by senior management to act in the place of the Privacy Coordinator.

The Privacy Coordinator is responsible for privacy matters within Talisman and oversees the maintenance, regular review and interpretation of this Safe Harbor Statement and related policies and procedures.

10. Training

Talisman will train its Employees to take the steps necessary to maintain Safe Harbor principles in this Statement.

Talisman has implemented a communication and education program to ensure that individuals collecting, using or disclosing Personal Information and/or Sensitive Personal Information in the course of their duties on behalf of Talisman are aware of their responsibility to protect the privacy rights of all individuals. Failure of Employees to comply with this Statement or applicable privacy laws may result in disciplinary action, up to and including termination.