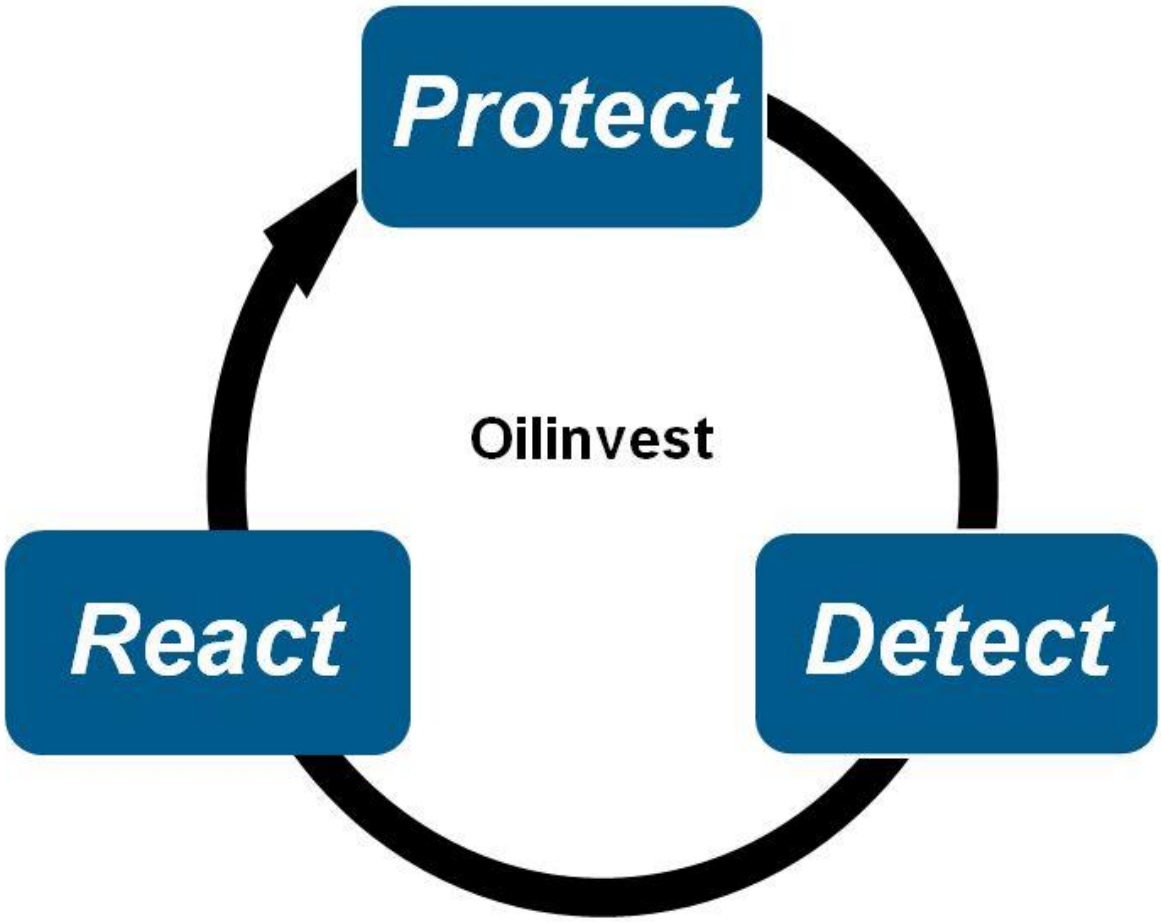
Tamoil (Suisse) SA
Data Protection Policy



PROTECT | DETECT | REACT

Contents

A. Introduction

Tamoil Suisse SA (hereafter "**Tamoil**") and its affiliates is committed to handling Personal Data responsibly and in compliance with the Swiss Federal Act on Data Protectio. This Policy on Data Protection (hereinafter referred to as the "**Policy**") is binding on **Tamoil** and its employees it must be respected by all employees of Tamoil. It is designed to provide a minimum global standard with respect to the protection of Personal Data within Tamoil, and is intended to safeguard the rights and interests of the individuals concerned.

Please familiarize yourself with this Policy.

Definitions: Capitalised terms shall have the meaning given to them in **Annex 1.**

B. Scope of the Policy

This Policy applies to the worldwide Processing of Personal Data by Tamoil.

It covers any **Processing** of **Personal Data** by **Tamoil**, including any **Transfer** and disclosure to other Tamoil companies or third parties (including Oilinvest companies), and shall govern any privacy related aspects within Tamoil.

The Policy applies to any categories of Personal Data Processed within Tamoil, including, but not limited to, Personal Data of employees, customers, suppliers and other business partners. You should be aware that **Personal Data** includes any information relating to an identified or identifiable individual, such as his/her name, contact details (such as address, email, phone), résumé, personnel file, information about the professional and personal life and development, purchase history and preferences, device information (such as unique device identifier, IP address, cookie information, log files, and browsing history), geo location information, and other data, e.g. image data and sounds, i.e. voice records.

C. Principles for Handling Personal Data

Transparency & Information:

- Being open and transparent in the way we use and share Personal Data is an important step to demonstrate good data protection practices.

- All Data Subjects, such as employees or customers, must be informed about the purpose of the data processing latest at the time of data collection. Personal Data may also be processed based on a valid consent declaration of the Data Subject. In general, the Personal Data shall be collected directly from the Data Subjects. The information to be provided to Data Subjects, for instance by means of a privacy notice, shall contain the identity of Tamoil, the contact details of the responsible data protection officer, if any, the purposes of the Processing, and any further information necessary, having regard to the specific circumstances in which the Personal Data is Processed, such as the categories of Personal Data concerned, and the recipients or categories of recipients.

- Tamoil is obligated to inform the data subject of the collection of sensitive personal data or personality profiles; this duty to provide information also applies where the data is collected from third parties.

- There may be limited circumstances where we do not have to comply with the transparency requirement, but you should check with your compliance officer, before you proceed without ensuring transparency (see **Annex 2**).

Purpose Limitation:

- Personal Data shall be processed only as necessary for specified purposes which are lawful and justifiable, and any different or new purposes should have a legitimate basis.

- For instance, Personal Data relating to employees may be processed as necessary for carrying out the employment relationship, performance appraisal, alignment of performance awards and bonuses or as necessary to comply with a legal obligation, and Personal Data relating to customers may be processed as necessary for the performance of the contract to which the customer is party.

- Personal Data shall not be further processed in a way incompatible with the purposes for which it was originally collected.

Data Quality and Proportionality:

- Tamoil shall ensure that Personal Data Processed will be accurate, complete and, to the extent reasonably necessary for the applicable purpose, kept up-to-date. Tamoil shall take reasonable measures to rectify or delete Personal Data, which is inaccurate, incomplete

or outdated, having regard to the purpose for which the data was collected or for which it is further processed.

- Any Processing of Personal Data must be restricted to data that is reasonably adequate and relevant for the applicable purpose, and not excessive in relation to the purposes for which it is collected and/or further Processed.

Data Minimization and Data Avoidance:

- The handling of Personal Data shall be organized in a way to Process as little Personal Data as possible. In particular, it should be assessed whether the applicable purpose can be achieved also by Processing anonymized or, as applicable, pseudonmized information, in which case the Personal Data shall be anonymized or, as applicable, pseudonymized as early as possible with respect to the applicable purpose.

Data Retention:

- Personal Data shall only be kept for as long as is necessary for a specific business purpose and/or to comply with a legal need. If no longer necessary for the respective purposes, Personal Data shall not be Processed any longer, and, unless prescribed otherwise by applicable data retention laws, be securely disposed of.

- The general retention period for files is 10 years. This period depends on the sector, where data is processed. E.g. For HR-departments the recommended retention period is between 2 to 5 years. For tax purpose, the retention periods can be up to 15 years. Therefore, please be aware that applicable statutes or regulations may require that certain Personal Data be retained for a specified length of time, and it may also be prudent to keep certain Personal Data for a specific period, so that Tamoil is able to defend properly any legal claims or manage an on-going business relationship.

- We must follow all internal data retention policies in relation to the applicable retention requirements from both a business and (where applicable) legal perspective, any applicable procedures for ensuring that Personal Data is properly retained and securely destroyed, any applicable process for suspending the destruction of documents in situations relating to pending, threatened, or reasonably likely litigation or governmental investigations, and the responsibilities of those involved in retention activities relating to Personal Data.

Acceptable actions with Personal Data (Need to Know basis):	**Non-acceptable actions with Personal Data:**
• **Filing of succeeding directors with the Chamber of Commerce** • **Provide Competent authorities and financial institutions with KYC-information** • **Absenteeism registration by the HR Department**	• **Providing private contact details of employees to third parties** • **Collecting Sensitive Data according to Annex 1; exceptions apply e.g. to religion when required for church tax purposes**

D. Lawful Grounds for Processing

The Processing of Personal Data must be justified by a legal ground which permits the relevant Processing for the identified purposes, by consent or by an overriding private or public interest or by law. Such legal basis must be determined in accordance with applicable national law. It may, for instance, exist where the Processing is necessary for the performance of a contract to which the Data Subject is party, or where the Processing is necessary for compliance with a legal obligation to which Tamoil is subject.

In particular where no other legal ground is applicable, the Processing may further be based on the Data Subject's prior unambiguous consent, by an overriding private/public interest or by law. Tamoil shall ensure that consent is relied upon as a legal ground for Processing only where it is specific and informed, and provided freely, i.e. without oppressiveness. The Data Subject may withdraw his/her consent with effect for the future use at any time, unless provided otherwise by applicable law.

Please work with your compliance officer in order to determine any applicable legal basis for the envisaged Processing under the laws of your jurisdiction.

E. Processing of Sensitive Data and personality profiles

Since the Processing of Sensitive Data and personality profiles is more intrusive, we should Process Sensitive Data and personality profiles only where absolutely necessary and, except in very limited circumstances, only with the unambiguous consent of the individual affected. Consent from individuals to the use of their Sensitive Data must be explicit, specific, informed, and freely given. Such consent needs to be documented. The Data Subject may withdraw his/her consent with effect for the future at any time, unless provided otherwise by applicable law. The Data Subject must be notified as a minimum of the controller of the data files, the purpose of the processing and the categories of data recipients if a disclosure of data is planned.

The duty for Tamoil to provide information ceases to apply if the Data Subject has already been informed, in case where the data was not collected form Tamoil if the storage or the disclosure of the data is expressly provided for by law or the provision of information is not possible or possible only with disproportionate inconvenience or expensesa.

Please work with your compliance officer to determine whether there is an applicable legal basis for the Processing of Sensitive Data or personality profileunder the laws of your jurisdiction.

F. Privacy Impact Assessments (PIAs)

Where a type of Processing, in particular a type using new technologies, and taking into account the nature, scope, context and purposes of the Processing, is likely to result in a high risk for the rights and liberties of individuals, Tamoil must carry out an assessment of the impact of the envisaged Processing on the individual in form of a PIA. Usually, such an obligation to conduct a PIA may arise where Processing may result in privacy risks to Data Subjects.

It may be necessary, for instance, where (i) Sensitive Data is Processed on a large scale, or (ii) in case of a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based

that produce legal effects concerning the individual or significantly affect the individual in a similar manner.

As a general rule, a PIA should contain a systematic description of the envisaged Processing operations and the purposes of the Processing, including, where applicable, the legitimate interest pursued by Tamoil , an assessment of the necessity and proportionality of the Processing operations in relation to the purposes, an assessment of the risks to the rights and freedoms of Data Subjects affected by the envisaged Processing, the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with the principles of this Policy and applicable law taking into account the rights and legitimate interests of Data Subjects and other persons concerned.

Please contact your compliance officer if you consider a PIA to be necessary, or in cases of doubt whether a PIA should be carried out, and in order to receive any assistance required with respect to carrying out the PIA. You should not proceed with the envisaged Processing until the PIA has been completed and approved. Please note that in certain cases, we may be required to consult with the local data protection authority about the proposed use of the Personal Data.

G. Rights of Data Subjects

Data Subjects have the right to request information as well as a claim to stop data processing, stop disclosure to third parties, correction of data or destruction of data.

Any queries, requests or complaints made by natural and legal persons in connection with their Personal Data shall be answered (normally) within 30 days. The information has to be complete and accurate. In particular, Data Subjects shall have the ability to request information about the Personal Data held about them, including how the data was collected and for what purpose, and about the recipients or categories of recipients to whom the Personal Data is disclosed. Where Personal Data is incomplete, inaccurate or no longer relevant, or where its Processing can no longer be justified, the Data Subject may further request that the Personal Data shall be corrected and/or deleted (or, where this is not feasible, blocked from any further Processing).

H. Technical and Organizational Security Measures

Tamoil shall maintain appropriate technical and organizational security measures to protect Personal Data against accidental or unlawful destruction or alteration, or accidental loss, or unauthorized disclosure or access, and shall impose such security obligations on other parties that maintain or access Personal Data on behalf of the Tamoil companies. Such measures shall ensure a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data. These measures shall be state of the art of technology. Particular attention should be given to the protection of Sensitive Data, which shall be protected by enhanced security measures.

Employees of Tamoil shall have access to Personal Data only to the extent necessary to perform their duties and as required for the respective applicable purpose. All employees having access to Personal Data shall be obliged to handle Personal Data with appropriate confidentiality, and to maintain appropriate security measures, including for the time after the termination of the employment relationship.

I. Use of Service Providers

Where Tamoil engages a service provider to Process Personal Data on its behalf, it must choose a service provider which provides sufficient guarantees in respect of the technical and organizational security measures governing the Processing to be carried out, and must ensure compliance with those measures. This applies irrespective of whether the service provider is part of Tamoil or an external service provider.

Tamoil should always enter into a written contract with any service provider that deals with Personal Data on its behalf. The contract should ensure that the service provider (i) only acts on behalf of Tamoil and in accordance with its instructions and (ii) undertakes to adopt appropriate and equivalent security measures.

Tamoil must not assign the Processing of Personal Data to a third party if the Processing is prohibited by a statutory or contractual duty of confidentiality

Personality profiles and sensitive data cannot be transmitted to third parties without justification.

J. Disclosure to Third Parties

Personal Data shall be kept confidential. Disclosure to third parties in general is possible through agreement by law. It has to be ensured that no legal basis prohibits the disclosure. Personality profiles and sensitive data can't be transmitted to third parties without a justification.

Prior to disclosing Personal Data to third parties, Tamoil companies will take reasonable steps to ensure that (i) the recipient of the information is identified and disclosure is made only to authorized parties, e.g. business partners or vendors, (ii) the disclosure is necessary for specified legitimate business purposes, or otherwise permitted or required by law, (iii) the disclosure is consistent with applicable law and other applicable Tamoil's internal policies or procedures, and (iv) where appropriate or required by law, the third party is contractually committed to complying with obligations corresponding to those imposed on Tamoil companies under this Policy, including with respect to implementing appropriate technical and organizational security measures, limiting further use of any Personal Data, and complying with applicable laws.

K. International Data Transfers

Personal data may not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular due to the absence of legislation that guarantees adequate protection.

In the absence of legislation that guarantees adequate protection, personal data may be disclosed abroad, if an adequate level of data protection can be achieved through a number of mechanisms, such as:

- sufficient safeguards, in particular contractual clauses, ensure an adequate level of protection abroad;

- the data subject has consented in the specific case; or

- the processing is directly connected with the conclusion or the performance of a contract and the personal data is that of a contractual party.

You should liaise with the legal department to ensure that all cross-border Transfers are subject to adequate protection through putting respective mechanisms in place. The Federal Data Protection and Information Commissioner must be informed in some cases.

L. Data Protection Organization

Responsibility and Supervision of Compliance:

- Tamoil is responsible for compliance with the Federal Act on Data Protection and take all necessary measures by appointing a data protection officer or similar function. Oilinvest may audit compliance with this Policy, and Tamol is expected to fully cooperate and to implement any actions necessary to remedy any failure to comply with this Policy or applicable data protection law.

- This Policy must further be respected by all employees of Tamoil. Failure to comply with this Policy could expose Tamoil to regulatory and/or legal action, which could mean the payment of compensation or fines, and could also result in disciplinary actions against you, up to and including termination of employment.

Reporting Data Breaches:

- If you breach this Policy, or become aware of any alleged or actual breach of this Policy, you should immediately inform your supervisor or compliance officer, even if you are not certain whether the breach is serious. You can also report anonymously by email: www.bkms-system.net/oilinvest It is the responsibility of the responsible data protection officer of the relevant Oilinvest Affiliate to determine whether an alleged breach indeed is an actual breach of this Policy and when it should be reported to the authorities.

Training on the Policy:

- We require all employees, who would be processing Tamoil's Personal Data to receive training on the Policy. The training shall cover all relevant data protection and security aspects within Tamoil and specifically inform and raise awareness for the data protection requirements arising from this Policy.

M. Implementation

This Policy is effective from _____ 2018.

N. Maintenance, Questions, Contact

The review and maintenance of this Policy is the responsibility of the Group Compliance Officer. If you have any questions about this Policy, or want more information about our privacy practices, please contact your compliance officer.

Annex 1
Definitions

"**Data Subject**" shall mean an identified or identifiable natural or legal person whose data is processed, by or on behalf of Tamoil, may relate.

"Disclosure" shall mean making personal data accessible, for example by permitting access, transmission or publication

"**EEA**" shall mean all Member States of the European Union, plus Iceland, Liechtenstein and Norway.

"**Oilinvest**" shall mean the Oilinvest group of companies comprising Oilinvest (Netherlands) B.V. and all entities directly or indirectly wholly-owned, majority-owned or controlled by Oilinvest (Netherlands) B.V.

"**Personal Data**" shall mean any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, economic, cultural or social identity.

"**Personality Profile**" shall mean a collection of data that permits an assessment of essential characteristics of the personality of a natural person;

"**Policy**" shall have the meaning as defined in Section A. Introduction.

"**Processing**" shall mean any operation or set of operations which is performed upon Personal Data whether or not by automatic means, such as collection, recording, organization, storage, archeving, adaptation or alteration, retrieval, consultation, use, revison, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking erasure or destruction.

"**Sensitive Data**" shall mean any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, ideological, trade union-related views or activities, and Personal Data concerning health or sex life, social security measures, and may include additional information, as prescribed by applicable national or EU law, such as Social Security or government identification numbers, or data relating to administrative, criminal convictions or offences.

"**Transfer**" shall mean any disclosure of Personal Data, including by transmission, dissemination or otherwise making available to a recipient.

"**Files**" shall mean any other structured set of Personal Data which are accessible according to specific criteria.

Annex 2
Compliance Officers

Compliance Officer	E-mail address
Group Compliance Officer	compliance.group@oilinvest.com
Compliance Officer Oilinvest (Netherlands) B.V.	compliance.oilinvest@oilinvest.com
Compliance Officer Tamoil Italia S.p.A.	compliance.italia@oilinvest.com
Compliance Officer Tamoil (Suisse) S.A.	compliance.switzerland@oilinvest.com
Compliance Officer Tamoil Beheer B.V.	compliance.netherlands@oilinvest.com
Compliance Officer Deutsche Tamoil GmbH	compliance.germany@oilinvest.com
Compliance Officer Tamoil España S.A.	compliance.spain@oilinvest.com
Compliance Officer Tamoil Overseas Limited	compliance.cyprus@oilinvest.com
Compliance Officer Holborn European Marketing Company Limited	compliance.HEMCL@oilinvest.com
Compliance Officer Holborn Europa Raffinerie GmbH	compliance.HER@oilinvest.com