PROCEDURE FOR COLLECTING AND PROCESSING REPORTS AND ALERTS

This procedure seeks to fulfil the obligations set out in articles 8 and 17 of law N°2016-1691 of 9 December 2016, referred as the 'Sapin II' law. It concerns the Société du Canal de Provence (SCP), as well as its direct and indirect subsidiaries. It is aimed at persons who wish to file a report regarding events of which they have personal knowledge. Using this alert system in good faith, even if the facts later prove to be erroneous or do not give rise to further proceedings, will in no way expose the person filing the report to sanctions or prosecution of any kind. However, inappropriate use of this alert system can expose the person filing the report to possible sanctions or prosecution for libel.

The events reported must, in the reporter's opinion, represent :

- A crime ;
- An offence ;
- A clear and serious violation of :
  - the law or rules in force,
  - an international commitment which is regularly ratified or approved by the French authorities ;
  - a unilateral act on the part of an international organisation and based on an international commitment which is regularly ratified or approved by the French authorities,
- A threat or serious damage to the general interest.

Examples of events (non-exhaustive) : offences relating to corruption, influence-peddling, misappropriation and embezzlement of public funds, illegal interests, or favouritism; actions which may incur major risk or serious harm for the population ; endangering of others, fraud, harm to the environment, etc.

STAGE 1 : FILING THE REPORT

Who in SCP should you send your report to ?

To Mrs. Catherine Leroy, Director of the « legal, audit and quality department », who has been designated as the key point of contact for reports or alerts. Her department is in charge of operations concerning « internal auditing and organisation of internal control ».

For anti-corruption matters, employees may turn to their line manager for advice and guidance, except in cases where their manager may be involved in the events reported.

In all cases, reports must be sent to the point of contact, in line with the relevant procedure.

How do you file your report ?

Reports must respect the confidentiality of the sender, the individuals in question, and the events reported :

- Reports are to be sent via a dedicated, secure platform to the following address : https://alertcys.io/l

All elements of the report must be sent to the point of contact via this address.

It is essential to follow these instructions in order to ensure that the information sent remains confidential.

What information do you need to send ?

You must state your name, position and contact details. You must explain the events reported in as much detail as possible, and, as the case may be, attach any other documents or information which could support your report.

STAGE 2 : PROCESSING THE REPORT

What precautions are taken to ensure the alert remains confidential ?

The point of contact is notified by the platform upon receipt of the report, in full confidentiality and without any intermediary.

Should the point of contact engage other members of the department to lead an audit or investigate into the events reported, he/she takes full responsibility for respecting the confidentiality of the sender, the individuals in questions, and the events reported.

All documents which may identify the author of the report or the individuals involved in the report are subject to a full confidentiality clause.

Any document which identifies the author of the report may not be divulged, except to the judicial authorities, without the prior consent of the author. Any document which identifies the individuals mentioned in the report may not be divulged, except to the judicial authorities, until the merits of the alert have been established.

How will SCP answer you ?

You will immediately receive an acknowledgement of receipt via the platform.
The alert's author will be kept informed of developments throughout the processing period, in full confidentiality. The point of contact may request further information if required.

The point of contact will examine the admissibility of the report and contact its author within a maximum of one month following the date of acknowledgement of receipt :

- If the alert is not admissible, you will be informed via the dedicated platform ;
- If the alert is admissible, the point of contact will inform you of the process and the measures taken via the dedicated platform.

If the report has not been handled by the point of contact after two months, its author may contact - alternatively or simultaneously - the judicial or administrative authority, or advocate.

If the report has not been processed within a period of three months by one of the above organisations, it may be made public.

However, the law dictates that in the case of serious and imminent danger or a risk of irreversible damage, the author of the alert may contact the judicial and administrative authorities directly, and may make his/her report public. This course of action applies to exceptional cases in which, on account of the urgency of the situation, it is clearly impossible to follow the internal procedure.

SCP's General Director is responsible for handling the report. He may decide to take precautionary measures, or appoint experts to deal with it. He may also initiate disciplinary or, as the case may be, legal proceedings. Improvements will be made as and when required.

In order to respect confidentiality, all letters will be sent to you directly from the point of contact via the dedicated platform.

How long are the different documents kept ?

All documents relating to a non-admissible alert are destroyed as soon as acknowledgement of receipt has been sent.

If the alert is not followed by disciplinary or judicial procedure, all relevant documents and analyses will be either destroyed or filed anonymously within a period of two months following the completion of audit operations.

When a disciplinary procedure or legal proceedings are initiated against the accused or the author of a wrongful report, all documents relating to the alert and its analysis are kept until proceedings are complete. They are then either destroyed or filed anonymously within a period of two months following the legal deadline for appeals.

The point of contact is responsible for these operations.

What are the sanctions ?

- **Sanctions against the company or employees**

Breach of confidentiality results in two years' imprisonment and €30,000 in fines.

Obstructing the transfer of a report results in one year of imprisonment and €15,000 in fines.

In the case of libel against the author of an alert, civil fines of up to €30,000 may be imposed.

- **Sanctions against the authors of alerts**

False allegations made by a whistleblower may result in five years' imprisonment and €45,000 in fines.

How is personal data protected ?

Reports are processed automatically thanks to the dedicated secure platform at the following address : https://alertcys.io/ .
This platform complies with AU-004 single authorisation from the CNIL (National Commission for Data Protection), which was last updated on 27 March, 2018. It guarantees the anonymity of alerts. Data is never transferred to countries outside of the European Union.
In compliance with data-protection law no. 78-417 of 6 January, 1978, authors of alerts have a right to access, rectify and oppose personal data which concerns them.

To exercise this right of access, send an e-mail to contact@alertcys.io

Personal data given by the whistleblower to the point of contact via the platform are only to be used by the contact. The platform is responsible for their processing and safekeeping. Without prior consent from the individual, this data may not be transferred to a third party, with the exception of the point of contact and general director and, when applicable, the relevant administrative and judicial authorities.

Documents which identify the individuals mentioned in reports may not be divulged, except to judicial authorities, until the merits of the alert have been established. In accordance with the European regulation UE 2016/679 of 27 April, 2016, relating to the protection of natural persons with regard to the processing and free circulation of personal data, the platform undertakes to take all meaningful technical and organisational

measures to protect the security and confidentiality of personal data, within the framework of the procedure described herein and for any personal data which it receives. In particular, the platform undertakes to ensure that such data is in no way modified, damaged, lost, misused, corrupted, divulged, transferred or communicated to unauthorised persons.

Only the following data categories may be processed :

- name, position and contact details of the author of the alert, the individuals mentioned in the alert, and those in charge of receiving and processing the alert,
- events reported and documents collected during the examination of the events reported,
- reports on auditing operations,
- the consequences of the alert.

Data retention period :

- If the alert is deemed to be outside the scope of the system, all data is deleted or filed anonymously upon receipt.
- If the alert is not followed by disciplinary or judicial procedure, all relevant documents will be destroyed or filed within a period of two months following the completion of audit operations.
- If a disciplinary procedure or legal proceedings are initiated against the accused or the author of a wrongful report, all corresponding datas and documents are kept until proceedings are complete.
- Filed data will be stored in a restricted-access information system for a period not exceeding that of the legal proceedings.