# SOMFY GROUP ALERT MECHANISM

SOMFY

BETTER LIVING FOR ALL

CONTENTS

## INTRODUCTION

**In line with its values of integrity and its strategic vision focusing on the well-being of people in their own homes, the SOMFY Group has decided to introduce a general alert mechanism designed to make it possible for anyone to report serious matters so that they can be taken into consideration and handled in accordance with the legal and regulatory provisions in force.**

**Part of the anti-corruption conformity programme deployed within the Group, this alert mechanism also enables the SOMFY Group to satisfy the requirements of law no. 2016-1691 of 9 December 2016 relating to transparency, the fight against corruption and the modernisation of economic life, referred to as the " *Sapin 2 law*" (the "law").**

**The SOMFY Group has thus decided to implement a single mechanism to ensure compliance with the requirements of this law.**

**The mechanism complements the system in force within the Group since 2015 which allows any behaviour in breach of our Ethical Charter to be reported.**

**The aim of the present document is thus to present this mechanism and the conditions for its use.**

**It shall be applied within all entities of the Group, subject to adaptation to the existing mechanisms under local law.**

**A confidentiality policy relating to the personal data processed within the framework of this mechanism is available to the people concerned: it can be found at the following address [Sharepoint / Group Documents site / Ethics & Anti-corruption], as well as in the appendix of the present procedure.**

## TERMINOLOGY

**The words and expressions below have the following meanings. It is specified that words used in the singular include the plural form and vice-versa:**

| | |
|---|---|
| **Person submitting the report / issuing the alert** | **Designates the company employee or external or occasional worker who has issued an alert, unselfishly and in good faith, relating to the fields specified in the present procedure** |
| **Code of conduct** | **Designates the anti-corruption code of conduct adopted by the Group and published on Sharepoint / Group Documents / Ethics & Anti-corruption** |
| **Ethics Committee** | **Designates the Group's Ethics Committee, consisting of the Ethics manager and its permanent members, appointed by the Group in light of their integrity and trained in general ethics. (see appendix)** |
| **Crime or offence** | **Designates the crimes, offences or serious and manifest breaches of an international commitment regularly ratified or approved by the French state, of a unilateral action taken by an international organisation on the basis of such a commitment or of the law or regulations in force or the serious threats or prejudices to the general interest.** |
| **Company** | **Designates any company belonging to the SOMFY Group** |
| **Group** | **Designates the group, consisting of all companies – either French or foreign – controlled by the company SOMFY SA as described in article L.233-3 of the French Commercial Code** |
| **Ethics Manager** | **Designates the Group employee responsible for the deployment and monitoring of the anti-corruption conformity programme, the Group's ethics policy and the alert mechanism.** |
| **Company employee** | **Designates any company employee, and in particular those with a permanent work contract, home-workers, fixed-term contract workers, part-time employees, apprentices and trainees.** |
| **External or occasional worker** | **In particular, this designates interim workers, seconded personnel, service providers' employees, sub-contractors' employees, consultants, etc.** |

## 1. PURPOSE OF THE ALERT

**The mechanism enables company employees and external or occasional workers in the SOMFY Group to exercise their right to issue an alert relating to an action in breach of the provisions of the SOMFY anti-corruption code of conduct and the SOMFY Group Ethics Charter.**

**This alert mechanism also enables company employees and external or occasional workers in the SOMFY Group to report conduct or situations which would constitute:**

- **a crime or offence,**
- **a serious and manifest breach of an international commitment regularly ratified or approved by the French state,**
- **A serious and manifest breach of a unilateral action taken by an international organisation on the basis of a regularly ratified international commitment,**
- **a serious and manifest breach of the law or regulations in force,**
- **a serious threat or prejudice to the general interest.**

**All facts, information or documents covered by national security, medical secrecy or the secrecy of relations between a lawyer and their customer are excluded from the scope of the alert, regardless of the form or media.**

**The only facts, data, information taken into account are those:**

- **in direct relation with the scope of application of the alert mechanism,**
- **divulged as strictly necessary to checking the alleged facts and proportionate to protecting the interests in question,**
- **reported by the person issuing the alert, acting unselfishly and in good faith, in order to divulge facts of a certain gravity of which they are personally aware.**

**Such a fact is reported to the Ethics Committee in accordance with the terms stipulated below.**

**In the absence of due diligence on the part of the Ethics Committee, in particular with a view to checking the admissibility of the report within the deadlines stipulated below, the person issuing the alert can communicate the report to the relevant legal or administrative authority.**

**The person issuing the alert can only make this alert public if it is not handled by the relevant legal or administrative authority within three months of receipt of the report.**

**In the event of serious and imminent danger or in the presence of a risk of irreversible damage, the report can nevertheless be communicated directly to the legal or administrative authority and, where applicable, made public.**

**The members of the Ethics Committee guarantee strict confidentiality of the identity of the person issuing the alert, the people targeted by it and the information collected.**

**Elements which could help identify the person issuing the alert can only be divulged with the consent of the latter, unless required by a judicial authority.**

**Elements which could help identify the person targeted by a report can only be divulged once the validity of the alert has been established, unless required by a judicial authority.**

**Divulging the aforementioned confidential elements outside the scope of possibilities indicated above is punishable by two years of prison and a €30,000 fine.**

**The person issuing the alert may not be omitted from a recruitment procedure or access to a training placement or professional training, sanctioned, made redundant or be subject to any discriminatory measures, either direct or indirect, in particular with regard to remuneration, profit-sharing or share distribution measures, training, reclassification, allocation, qualification, classification, professional promotion, transfer or contract renewal as a result of issuing an alert in accordance with articles 6 to 8 of the law.**

## 2. THE PROCEDURE

**The person issuing the alert may use the alert mechanism in order to:**

- **receive guidance in the event of questions concerning the "right conduct" to adopt in a specific situation,**
- **enter incoming facts in the mechanism's scope of application.**

**The line manager must be able to guide and advise his employees, except if he is the person responsible for the behaviour in question.**

**However, if the person issuing the alert believes that informing his line manager could give rise to difficulties (hypothesis where the line manager is the author of the behaviour in question) or that the alert might not give rise to suitable monitoring, the person can contact the Ethics Manager directly by following the procedure described below.**

### 2.1 The alert procedure and handling the report

**2.1.1) Regardless of the cause of the alert, it can be sent by e-mail or letter mail to the following contact details:**

- **E-mail address: ethics@somfy.com**
- **Postal address: Ethics Manager, SOMFY Group, Case Postale 230, 1215 GENEVE, Switzerland**

**It is therefore addressed confidentially to the Ethics Committee. To this end, e-mails must be classified with the option "Confidential – ethical alert" in the electronic mailbox (see operating mode in the appendix), and the mail must bear the indication "Confidential" on the front of the envelope.**

**This report can be undertaken using the appended form.**

**Any person who cannot easily make use of written communication channels may ask to be contacted by telephone by one of the members of the Ethics Committee to provide help in formalising the alert.**

**The report can be made in French, English or any other official language of the country in which the company operates.**

**It should be noted that any abusive use of the alert mechanism may be punished in accordance with the locally-applicable law. In France, anyone making abusive use of the alert mechanism is subject to the punishments stipulated in article 226-10 of the Penal Code relating to false allegations.**

**For an alert to be taken into account, it must indicate:**

- **the identity, functions and contact details of the person issuing the alert**
- **only the factual elements allowing the alert to be processed,**
- **the identity and, if possible, the professional contact details of the person(s) identified by the alert.**

**You are advised to mention only the information that is useful and strictly necessary to the handling of the alert and to avoid any subjective assessment.**

**In principle, anonymous alerts or reports will not be handled.**

**Exceptionally, anonymous alerts or reports can be submitted in accordance with the present procedure if anonymity is legally authorised by the laws of the country concerned. However, these anonymous alerts can only be handled if the gravity of the facts indicated is confirmed and the factual elements supporting the alert are sufficiently detailed. If this is the case, the handling of this alert is accompanied by specific precautions, such as a prior examination by the Ethics Manager of the opportunity to disseminate the alert within the framework of the mechanism.**

**It is specified that while a report is not anonymous, it is nevertheless confidential. Confidentiality is guaranteed by the technical and organisational measures described in the confidentiality policy appended to this procedure.**

**In the event of an alleged conflict of interests of one of the members of the Ethics Committee, and only in this event, the alerts may be sent to the members of the Ethics Committee not involved in the conflict instead of being sent to all the members of the Ethics Committee via the e-mail address ethics@somfy.com in order to ensure that the alert is handled only by those members of the Ethics Committee not concerned by the conflict of interests. The names and e-mail addresses of the members of the Ethics Committee are listed in the appendix to this procedure.**

**2.1.2) The alert will be handled in strict compliance with the rules applicable to the processing of personal data.**

**2.1.3) The documents and correspondence exchanged or stored electronically will be classified such as to restrict access solely to the members of the Ethics Committee.**

**2.1.4) This processing and any corresponding enquiries are entrusted to the Ethics Committee, the members of which are all bound by heightened confidentiality.**

**2.1.5) Once the alert has been received by the Ethics Committee, the Ethics Manager:**

- **sends acknowledgement of receipt within five (5) days to the author by e-mail or letter, insofar as the person issuing the alert has provided their contact details, thereby facilitating correspondence. It is specified that this acknowledgement does not signify the admissibility of the alert;**

- **informs the person issuing the alert of the fact that their personal data will be processed and of their rights in accordance with the laws and regulations relating to the protection of personal data.**

- **informs the person issuing the alert, within thirty (30) days of receipt of the alert, of the need to complete the alert if any elements are missing and specifies the deadlines for communicating them. If the additional elements requested are not communicated, the alert will be deemed unusable and will therefore not be handled. Nevertheless, the person issuing the alert retains the possibility of issuing a subsequent alert and providing all the elements required;**

- **informs the person issuing the alert of the foreseeable and reasonable time frame required to examine the admissibility of the alert. This time frame shall not exceed sixty (60) days from receipt of the alert.**

**If an alert is deemed admissible, the Ethics Manager announces the foreseeable and reasonable time frame required to examine the dossier (examination deadline).**

**Upon expiry of the examination deadline indicated by the Ethics Committee, the latter notifies the person issuing the alert:**

- **of the next steps in handling the dossier;**
- **where applicable, that a new deadline is necessary with a view to extending the examination of the dossier. It specifies the foreseeable duration of this extension.**

**2.1.6) The conditions of the examination are as follows:**

- **As soon as the alert has been received and its admissibility has been verified, the Ethics Committee informs the person or persons targeted by the alert as well as any other person involved in the alert.**

  **However, if provisional measures are necessary, in particular to prevent the destruction of evidence relating to the alert, this (these) person(s) will be notified after the measures are adopted.**

**Any person targeted by the alert as well as any person involved in the alert will be informed, as far as possible and without prejudice to the rights and freedoms of the person issuing the alert, of:**

- **the name and contact details of the Ethics Manager and of the person responsible for handling the alert,**
- **the facts of which they are accused or in which they are involved,**
- **the fact that their personal data will be processed and of their rights in accordance with the laws and regulations relating to the protection of personal data.**

- **In the strictest confidentiality, the Ethics Committee examines and verifies the facts and behaviours. To this end, it can conduct all interviews it deems useful, in particular with the people targeted. It can also call on the help of local ethics correspondents. In certain cases, the Group's internal audit department can be called on with the prior agreement of the Group's management board. Service providers can also be used to conduct external enquiries if necessary. The Ethics Committee ensures that any person involved in the enquiry is bound by heightened confidentiality.**

**2.1.7) Data retention**

**The data relating to an alert deemed inadmissible within the framework of the mechanism as soon as it is received by the Ethics Committee are destroyed as quickly as possible or immediately archived after anonymisation. When the alert is not followed by disciplinary or legal proceedings, the associated data are destroyed or archived, after anonymisation, within two months of the verification activities being closed.**

**If, however, a disciplinary procedure or legal proceedings are undertaken against the person accused or having issued an abusive alert, the data relating to the alert are archived by the Ethics manager without anonymisation until the procedure is closed.**

**The data archived are retained on two numbered external media and stored in a locked location.**

**2.1.8) The person issuing the alert and the person(s) targeted are informed when the dossier is closed.**

## 2.2 Respect for the rights of the people concerned

**2.2.1) In accordance with the laws and regulations relating to the protection of persona data, the Ethics Manager guarantees any person identified in the professional alert mechanism the right of access to the data concerning them and, if they are inaccurate, incomplete, ambiguous or no longer valid, the right to request the correction or deletion of the data and to oppose, where applicable, or request the limitation of the processing action without prejudice to compliance with the legal obligations of the SOMFY Group.**

**Any person can also define directives relating to the use of these personal data after their death.**

**2.2.2) A person targeted by an alert can in no event obtain any communication from the Ethics Manager concerning the person issuing the alert based on their rights of access.**

**2.2.3) To obtain more detailed information concerning the rights of the users and persons identified, please refer to the confidentiality policy in the appendix.**

### 2.3 Information on the company employees and external or occasional employees

**2.3.1) The implementation of the alert mechanism has been presented to the Works Council for consultation purposes.**

**2.3.2) The company employees and external or occasional workers who may be called on to use the mechanism are informed of the present alert procedure. To this end, the present document is available on the company Intranet (Sharepoint / Group Documents Site / Ethics & Anti-corruption) and is displayed on the company's premises. It is also made available to external or occasional workers by their employer before they begin their mission.**

*****

**03.27.2019**

**Jean Guillaume DESPATURE**

**APPENDIX 1:**

## PRIVACY NOTICE LINKED TO THE WHISTLEBLOWING PROCEDURE

This document explains how Somfy Activités SA (data controller) (hereafter "We" or "Somfy Group") collects, uses and discloses personal data processed in connection with the Whistleblowing Procedure of the Somfy Group. Personal data means any information relating to an identified or identifiable individual. Personal data does not only include information about an individual's private life and family life, but also information regarding an individual's activities, such as his or her working relation and economic or social behavior.

**Identification**

Any personal data provided helps us to better understand the information reported, or to investigate the reported incident. It also allows us to contact the persons involved, should we require further information.

**Lawfulness**

We process personal data:

- to comply with our legal obligations: we are required to implement a whistleblowing procedure to allow everyone to report serious and unlawful conducts mentioned in the Whistleblowing Procedure (provisions of the Act No. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and on the modernization of economic life (also known as the "Sapin II Act")

- to pursue our legitimate interests: The Whistleblowing procedure aims to allow the reporting of the other serious misconduct contrary to the SOMFY Group's Ethics Charter.

**Purposes**

We process personal data for the need of the implementation of Somfy Group's Whistleblowing Procedure. In particular, to conduct investigation, respond and react to any concern that may have been raised, and to prepare a final investigation record.

**Personal data we process**

We may process personal data, including the name, professional role, location and contact information of:

- Any person reporting an incident,
- Any person who is the subject of a reported incident,
- Other persons with information relating to the reported incident, and

- Persons responsible for investigating the reported incident.

We collect or process personal data of such persons especially through:

- The facts contained in the incident report,
- Any answers to follow-up question that we may have, and
- Any evidence gathered in the course of a possible investigation.

As an exception, the alert of a person who wishes to remain anonymous can be processed under the following cumulative conditions:

- if such anonymity is legally permitted by applicable law;
- the seriousness of the facts mentioned is established and the factual elements are sufficiently detailed;
- the management of this alert must be subject to special precautions, such as a preliminary examination by the ethics Manager of the opportunity of its communication within the Whistleblowing Procedure.

**Data sharing**

We handle reported incidents in line with our Whistleblowing Procedure and process personal data solely to address the reported incident. Communication and access to the information processed as part of the investigation related to the alert is only granted strictly on a need to know basis. In particular we may:

(i) confidentially transfer personal data to Ethics Committee members, local ethics correspondents or external expert counsel, if the case maybe, as well as to law enforcement authorities where necessary or required by law.

(ii) After the preliminary investigation, if further actions are to be taken, the data may be confidentially transferred to the personnel who is required to take the appropriate measures (i.e. the Internal Audit Department). In particular, we may transfer the personal data to the employer or his representative or the subject person's direct or indirect hierarchical superior.

In so far as Somfy Group operates globally and recipients aforesaid may be located outside the European Economic Area, the personal data may be transferred out of that area only if the recipient is (i) located in a country offering an adequate level of protection for the data or (ii) subject to an agreement covering European Union requirements for transfers of data outside the European Economic Area.

**Retention period**

We retain personal data processed under the Whistleblowing Procedure no longer than necessary. Unless otherwise required by law, personal data not falling within the scope of the Whistleblowing Procedure will be deleted or archived without undue delay. Personal data relating to a report that does not result in disciplinary or judicial proceedings will be deleted

or archived without undue delay after the decision not to initiate proceedings, and within 2 months after such a decision at the latest.

Where personal data processed under the Whistleblowing Procedure is used in disciplinary or judicial proceedings, we will retain related personal data until the end of such proceedings, unless a longer retention of the personal data is required by law.

In case of archiving, the data are stored on two external and encrypted media, under lock and key.

**Automated decision-making, including profiling**

We do not use automated decision-making processes or profiling.

**Your rights**

As per the laws and regulations, relating to the protection of personal data you may exercise the following rights:

- Right to access: data subjects have the right to obtain confirmation as to whether or not their personal data are being processed and if so, what specific personal data are being processed. Please note that this right should not adversely affect the rights and freedoms of others. To this extend, the access right may be limited considering the person requesting such access and the type of information held. For instance, the person who is the subject of the reported incident may under no circumstances obtain communication of the identity of the person who are reported the incident.
- Right to correct**:** right to obtain the rectification of any inaccurate incomplete, ambiguous or outdated personal data concerning you.
- Right to erasure: In some cases, for instance when the personal data are no longer necessary in relation to the purposes for which they have been collected, the data subject has the right to ask for their erasure.
- Right to restrict the processing: the data subjects have the right to obtain restriction of the processing of their personal data, for instance, during the management of their demand related to the modification of inaccurate personal data. In such case, the personal data will only be processed with your consent or for the exercise or defense of legal claims or for the protection of the rights of another person.
- Right to object**:** data subjects may object on grounds relating to their particular situation, to the processing of their personal data based on Somfy's legitimate interests. In such case, we will no longer process the personal data except if we may demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defense of legal claims.

- Right to define guidelines related to what should happen to the personal data after death: data subjects may define specific or general guidelines for the retention, deletion and communication of their personal data after their death.

To this effect, please contact our Data Protection Officer (dpo@somfy.com).

You may also have the right to lodge a complaint with the data protection authority of your country, or, alternatively, the Commission Nationale de l'Informatique et des Libertés (CNIL), 3 Place de Fontenoy, TSA 80715, 75334 PARIS CEDEX 07, France.

**Security**

The security of personal data of potential users of the Whistleblowing Procedure and of persons concerned by an incident report is important to us. We apply security measures to personal data processed under the Whistleblowing Procedure that are appropriate with regard to the risk of the processing involved.

We keep confidential the personal data of persons involved in the Whistleblowing Procedure and ensure that anyone handling them complies with this privacy notice and is under a strict obligation of secrecy and confidentiality, except otherwise provided by law.

We continuously improve the security of our information systems by implementing a security policy based on the ISO 27001 standard. The information systems security policy defines organizational and technical measures enforced to protect the confidentiality of sensitive information. Especially through:

- a classification of the information with the mention “Confidential – Ethic alert”. This setting enforces digital rights management, meaning that in the event the information is stolen, it cannot be opened without an authorized Microsoft Azure account (see Operating Procedure attached to the Whistleblowing Procedure); In the event a user does not classify the e-mail properly, the DRM will be applied during transport. This means that the e-mail will remain unprotected in the sender’s mailbox, but will be protected in the ethic mailbox.
- a strict access to the ethic mailbox:
    - Only the people in charge of handling the alerts are granted access to the mailbox ;
    - actions made inside the mailbox are logged for one year ;
    - accessing the mailbox require authentication on Office 365, with two-step verification;
    - the password policy is based on NIST 800 63B standard, computing the complexity against modern password attacks mechanisms. Somfy Group also performs periodic robustness trials on all passwords to change weak passwords;
    - Somfy Group’s Information System Division administrators in charge of Office 365 might interact the mailbox to access the data in the case of an opened incident in the Somfy Group ticketing tool;
        - these actions are logged and cannot be erased by such an administrator ;

        - administration authentication leverages the two-step verification process or IP origin filtering.
- the encryption of the emails during transport
    - as soon as an external mail relay delivers the mail to the Office 365 infrastructure
    - always when the mail comes from a Somfy e-mail account
- the encryption of the emails at rest
    - on Office 365 servers
    - in Outlook local mailbox files which are stored on the computers
- To further limit the consequences of a breach, mails are deleted from the mailbox as soon as the alert is processed. They remain recoverable 30 days from the time of their deletion before being permanently deleted.

**How to contact us**

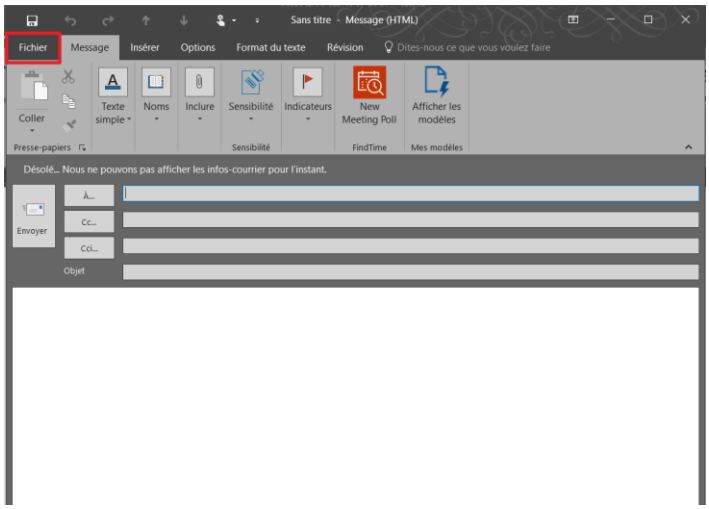
If you have any questions or comments regarding the Whistleblowing Procedure, please email ethics@somfy.com. If you have any question or comments regarding the processing of personal data, please contact dpo@somfy.com.

**APPENDIX 2:**

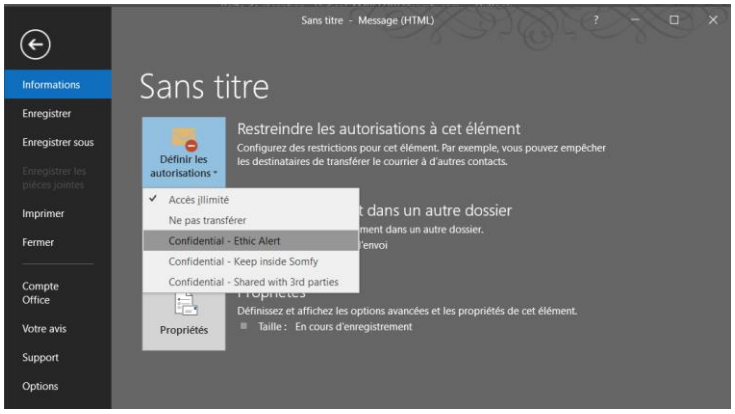
## How to protect the confidentiality of an ethical alert in Outlook?

Ethical alerts are very sensitive and we must prevent the content thereof from being divulged. As we explained in the alert procedure, e-mails are encrypted during transmission and are secured upon receipt. To secure these e-mails at the sender side, you must follow an additional step before sending the e-mail to ethics@somfy.com.

1. Write your e-mail and add the attachments if necessary
2. Click on “File” as shown in the screen shot below (click on the red rectangle):




3. A new menu appears as shown below. Select “Confidential - ethical alert”




4. That’s all! You can send your e-mail. Only people authorised by the ethical alert procedure and yourself can read the e-mail and its attachments.

If you forget to complete this step and you send the e-mail immediately, don’t panic: the e-mail and is attachments will be protected when delivered to the ethics mailbox. It nevertheless remains unprotected in your own mailbox. You can access your “Sent” folder and follow the same steps, then click on Save. Your e-mail is now fully protected.

## APPENDIX 3:

| Ethics Committee | | |
|---|---|---|
| HR | Valérie Dixmier | valerie.dixmier@somfy.com |
| Legal | Delphine Martin | delphine.martin@somfy.com |
| Business | Yann Barou | yann.barou@somfy.com |
| Ethics Officer | Severine Dangel | severine.dangel@dsgsomfy.com |