# PROCEDURE RELATING TO THE WHISTLEBLOWING SYSTEM AND THE COLLECTION OF REPORTS

Articles 8 and 17 of Law No. 2016-1691 of December 9, 2016 relating to transparency, the fight against corruption and the modernisation of economic life, known as the "Sapin" Law, and Article L.225-102-4 of the French Commercial Code, relating to the duty of vigilance, require the implementation of a whistleblowing system and collection of reports (hereinafter the "**System**").

It is in this context that the LDC Group (hereinafter referred to as "the Group" or "LDC") has set up this System.

This System is open to the Group's corporate officers and employees, as well as to its external and occasional employees (i.e., any natural person who does not hold an LDC employment contract and who, in the course of carrying out an assignment(s), performs missions on behalf of one or more Group subsidiaries). External and casual employees are hereinafter together referred to as "the Employees".

It is specified that when this system is set up within the Group, it guarantees its compliance with:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data (the "General Data Protection Regulation" or "GDPR") which entered into force on May 25, 2018;

- French regulatory requirements and more particularly with Law No. 2018-493 of June 20, 2018 relating to the protection of personal data, as well as to the best practices of the French Data Protection Authority (*Commission nationale de l'informatique et des libertés* (CNIL)).

In this context, this document, which aims to provide clear and complete information, describes in particular the following points:

- The **scope** of the System,

- The **operation** of the System,

- The **guarantees offered to Employees**.

## A - Scope of the System

The system set up within the Group enables all employees to raise an alert, in a disinterested manner and in good faith, regarding any facts of which they are personally aware relating to:

- a crime or an offence;
- a serious and manifest violation of an international commitment duly ratified or approved by France;
- a serious and manifest violation of a unilateral act of an international organisation formulated on the basis of a duly ratified international commitment;
- a serious and manifest violation of the law or regulations;
- a threat or serious harm to the public interest;
- **the existence of conduct or situations contrary to the Group's Anti-Corruption Code of Conduct**, insofar as they are likely to characterise acts of corruption or influence peddling;
- **the existence of anti-competitive practices** contrary to the law, regulations and the Group's commitments;
- **the prevention, existence or occurrence of risks and serious violations of human rights and fundamental freedoms, the health and safety of persons and the environment**, resulting from the activities of the Group and its subsidiaries, as well as the activities of its subcontractors or suppliers.

The alert may not, however, relate to matters covered by national defence secrecy, medical secrecy or the secrecy of relations between a lawyer and his client.

Employees may consult this document on the Group's intranet site or receive it by any means before beginning their assignment within the Group.

The persons who may be the subject of a professional alert or a report are all Employees.

Furthermore, it should be stressed that the normal functioning of an organisation implies that alerts relating to a malfunction, in any field whatsoever, must be escalated to management through the hierarchical channel or through open alert modes such as, in particular, the intervention of staff representative bodies.

Thus, the System supplements but does not replace the Group's usual channels of communication with its Employees, i.e., recourse to the company's hierarchical superior or to the competent staff representative bodies.

It is recalled that the use of the System by Employees is optional.

No penalty may be incurred for non-use of the System.

# B - Operation of the System

## 1. The triggering of the alert or the collection of alerts, and the procedure to be followed

The Employee who issues an alert or report (hereinafter "the Issuer") is required to comply with a specific procedure for issuing a professional alert or report.

In practice, in the event that a breach in the areas referred to in **A** of this document is observed, the Employee is strongly encouraged to discuss it as a matter of priority with his direct supervisor or the supervisor's superior.

Any Employee may also send his report to the LDC Group Ethics Committee (hereinafter the "Recipients") via one of the following specific channels, using the form attached in the appendix to this document and also available on the Group's intranet site:

- A dedicated email address: *alerte.ethique@ldc.fr*
- A dedicated postal address, by letter marked confidential: Comité Ethique du Groupe LDC, ZI Saint Laurent -72300 Sablé-sur-Sarthe

The Issuer is encouraged not to use the System anonymously.

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

- the seriousness of the facts mentioned is established and the factual elements are sufficiently detailed;
- the processing of this alert will be subject to special precautions, such as in particular a prior examination, by its first recipient, of the appropriateness of its dissemination within the framework of the System.

It is specified that the form must imperatively include the Issuer's contact details, except in the case of the aforementioned exception. Indeed, anonymous alerts must remain exceptional.

The Issuer must attach to the form any document or information likely to support the alleged facts.

In order to avoid any risk of abuse of the System and to maintain the confidentiality of the data, it is recalled that this System applies only to the areas referred to in **A** of this document.

Furthermore, it is specified that the Issuer must:

- Act selflessly and in good faith;

- Having personal knowledge of what he alerts or reports. An alert or report based on any rumour is therefore excluded.

Once the professional alert or report has been received, the Recipients inform the Issuer electronically of its receipt and the maximum period of time necessary for the examination of its admissibility, which may not exceed a reasonable period of one month.

After examination by the Recipients, the Issuer will be informed electronically whether or not his alert or report is admissible, i.e. whether or not it falls within the scope of the System.

If the alert or report is admissible, the process described in paragraph 2 "Processing of the professional alert and warning" will be implemented.

## 2. Processing of the professional alert and reporting

**Collection of personal data**

The collection of a professional alert and a report gives rise to automated processing of data subject to the legislation on the protection of personal data.

The System is managed by the LDC Group as data controller.

In the context of a professional alert and a report, only the following categories of data may be recorded:

- The identity, functions and contact details of the Issuer;

- the identity, functions and contact details of the persons who are the subject of the alert or report;

- the identity, functions and contact details of the persons involved in the collection or processing of alerts and reports;

- the reported facts;

- evidence gathered in the course of the verification of reported facts;

- a record of the verification operations;

- the action taken.

The facts collected are strictly limited to the scope of the System as defined in **A** of this document.

The Issuer must only rely on information formulated in an objective manner directly related to the scope of the System and strictly necessary for the verification of the alleged facts.

The Issuer may use the form set out in the Appendix hereto.

**Procedures for verifying the admissibility of the alert and the report**

Once the professional alert or report has been received by the Recipients, the latter first check whether it falls within the scope of the System. If this is not the case, the data relating to the alert or report is (in the same way as if the alert or report is anonymous) immediately destroyed after anonymisation, and the Issuer is informed.

If the Recipients find that the alert or report falls within the scope of the System, it is sent to the Chairman of the Ethics Committee of the LDC Group for processing and investigation as part of an investigation, in particular by gathering all the documents, data and information necessary for this processing.

In the exercise of his investigative functions, the Chairman of the Ethics Committee ensures:

- the confidentiality of all data and information received and used within the framework of its investigative mission, except in cases where the provision of information is required by law;

- an exhaustive analysis of any data, information or documents on the basis of which its action is required;

- the examination of a procedure that is appropriate to the circumstances and always governed by independent action;

- the absence of disciplinary action against the author of a professional alert or a report made in good faith.

The Group guarantees the confidentiality of the information collected in the context of the report and undertakes to process it within a reasonable period of time. When necessary, the Group may outsource all or part of the processing procedures, while strictly observing that the subcontractor complies with all security measures capable of maintaining the confidentiality of data and exchanges.

If the Recipients do not deal with the admissibility of the alert or report received within a period of one month, the Issuer may contact the judicial authority, the administrative authority or the professional bodies, depending on the field of the alert or report.

Failing processing by the abovementioned authorities within a period of three months, the Issuer has the option of making his alert or report public.

By way of exception, in the event of serious and imminent danger or risk of irreversible damage, the Issuer may bring his alert directly to the attention of the relevant judicial authority, administrative authority or professional order alternatively or simultaneously, or make his alert public, without using the System.

# C. Guarantees offered to Employees

## 1. Guarantees offered to the Issuer

**Confidentiality of the identity of the Issuer**

The Group ensures, as part of the processing of the alert or report, that the strictest confidentiality regarding the identity of the Issuer is respected.

Thus, elements of a nature to identify the Issuer may only be disclosed, except to the judicial authority, with the latter's consent.

All persons having knowledge of alerts or reports made by means of the System are required to keep all such information, in particular information relating to the identity of the Issuer, strictly confidential.

**Absence of sanctions**

The Issuer acting in good faith and in a disinterested manner may not be dismissed, sanctioned or discriminated against in any way for having reported facts in compliance with these procedures, even if the facts subsequently prove to be inaccurate or give rise to no action.

Conversely, misuse of the System could, if demonstrated, expose the Issuer to disciplinary sanctions and, where applicable, legal proceedings.

## 2. The guarantees offered to the person concerned by a professional alert or a report

**Information to the person concerned by the alert or report**

The person who is the subject of an alert or report is informed by the Recipients as soon as the data concerning him is recorded, whether or not computerised, in order to enable him, where appropriate, to object, on legitimate grounds, to the processing of such data.

Where precautionary measures are necessary, in particular to prevent the destruction of evidence relating to the alert or alert, the information to that person is provided after the adoption of such measures.

This information will be provided by electronic message and will specify in particular the entity responsible for the System, the alleged facts, the services to which the alert or report may be sent, as well as the procedures for exercising the rights of access and rectification.

**Confidentiality of the person concerned by the alert or report**

The identity of the person concerned by a professional alert or report is treated as strictly confidential.

For example, information that could identify the person concerned by an alert or report may not be disclosed, except to the judicial authority, until the basis for the alert or report has been established.

## 3. Personal data retention period

Data relating to a professional alert or a report considered by the Recipients as not falling within the scope of the System will be destroyed or archived without delay, after anonymisation.

If the professional alert or report is not followed by disciplinary or judicial proceedings after investigation, the data relating to that alert or report will be destroyed or archived, after anonymisation, by the Recipients and those responsible for the investigation referred to above, within two months of the closure of all verification operations. The Issuer, as well as the persons concerned, will be informed of such closure.

Where disciplinary proceedings or legal proceedings are instituted against the person concerned or the Issuer, the data relating to the professional alert or report are kept by the Recipients and the persons responsible for the investigation referred to above until the procedure is completed.

## 4. Respect for rights of access and rectification

The Group guarantees any person identified within the framework of the System the right to access data concerning him and to request, if such data is inaccurate, incomplete, ambiguous or out of date, its correction or deletion.

More specifically, each Group Employee has the right to rectify, complete, update, lock or delete personal data concerning him that is inaccurate, incomplete, ambiguous, outdated, or whose collection, use, communication or retention is prohibited. Each Employee also has a right of access, query and opposition to the processing of his personal data for legitimate reasons. In addition, each Employee may define guidelines for the storage, deletion and disclosure of his personal data after his death.

In order to exercise these rights, the Employee must send his written request either by registered mail, dated and signed, to the registered office of the company LDC SA, and more particularly to the attention of the Referrer for the protection of personal data, or send a message by logging into:

- for Group employees, the following URL: https://www.ldc.fr/rgpd/salaries/

- for consumers, the following URL: www.ldc.fr/rgpd/consommateurs

- for the Group's professional partners or for other entities such as associations, NGOs, etc., the following URL: www.ldc.fr/rgpd/professionnels.

# APPENDIX
# FORM FOR COMMUNICATING A PROFESSIONAL ALERT OR TO COLLECT A REPORT

*All fields are mandatory, unless otherwise stated on the form*

**1. Issuer's contact details (mandatory with some exceptions):**

Surname:

First name:

Function:

Email address:

Telephone [optional]:

**2. Contact details / identification of the person(s) / service(s) / activity(ies) concerned by the alert or report:**

Identification / Designation / Name(s):

First name(s):

Activity(ies) / Function(s):

Email address(es):

Address(es) & Telephone(s) [optional]:

**3. Information on professional alert or report**

*Unless this information is essential for a better understanding of the scope of the alert or warning, please do not provide any sensitive data (sex life, political and religious opinions, health and trade union membership) of any natural person*

Objective description of the facts giving rise to the professional alert or report, showing their presumed nature (facts, date, place, evidence, names of the persons involved in the situation concerned or, if a name is unknown to you, information likely to enable their identification, services and activities involved, etc.):

Reason why you consider that this is a situation falling within the scope of the System:

*The information collected within the framework of this form gives rise to automated data processing managed by LDC SA and whose purpose is the reporting and processing of alerts issued and reports collected within the Group in accordance with Articles 8 and 17 of the Sapin 2 law, and Article L.225-102-4 of the Commercial Code.*

*Furthermore, the Employee declares, as the Issuer, that this communication is made in good faith and disinterestedly, unless there is an involuntary error or omission.*

*He accepts and acknowledges that any abusive report could expose him to disciplinary action or legal proceedings.*

*Finally, the Employee has the right to rectify, complete, update, lock or delete personal data concerning him that is inaccurate, incomplete, ambiguous, outdated, or whose collection, use, communication or retention is prohibited.*

*He also has a right of access, query and opposition to the processing of his personal data for legitimate reasons.*

*In addition, the Employee may define guidelines for the storage, deletion and disclosure of his personal data after his death.*

*In order to exercise these rights, the Employee must send his written request either by registered mail, dated and signed, to the registered office of the company LDC SA, and more particularly to the attention of the Referrer for the protection of personal data, or send a message by logging into:*

- *for Group employees, the following URL: https://www.ldc.fr/rgpd/salaries/*

- *for consumers, the following URL: www.ldc.fr/rgpd/consommateurs*

- *for the Group's professional partners or for other entities such as associations, NGOs, etc., the following URL: www.ldc.fr/rgpd/professionnels*