WHISTLEBLOWER SUPPORT GUIDE

Group ethics, compliance and duty of care alert procedure (excluding RTE and Enedis)

CONTENTS

INTRODUCTION ..... - 3 -

HOW DO I ISSUE AN ALERT? ..... - 4 -

CAN YOU ISSUE AN ALERT? ..... - 4 -
WHAT FACTS CAN YOU REPORT? ..... - 4 -
EXAMPLES OF CATEGORIES COVERED BY THE ALERT PROCEDURE ..... - 4 -

HOW DO I ISSUE AN ALERT? ..... - 5 -

WHO TO CONTACT ..... - 5 -
WHAT PROTECTION IS THERE? ..... - 6 -

WHAT ACTION IS TAKEN ON YOUR ALERT? ..... - 7 -

HOW IS YOUR ALERT COLLECTED? ..... - 7 -
HOW IS YOUR ALERT ANALYSED? ..... - 7 -
HOW IS YOUR ALERT INVESTIGATED? ..... - 8 -

WHAT ACTION IS TAKEN ON YOUR ALERT? ..... - 9 -

HOW IS YOUR ALERT DATA PROCESSED? ..... - 10 -

WHAT GUARANTEES EXIST FOR THE CONFIDENTIALITY OF YOUR ALERT? ..... - 10 -
HOW IS YOUR DATA STORED AND ARCHIVED? ..... - 12 -
HOW EDF GROUP PROTECTS YOU ....- 12 -

INTRODUCTION

French and European law require companies with at least 50 employees to implement a **procedure for collecting and handling alerts**.

The **new law** protecting whistleblowers provides a framework for **alert procedures** and extends **the status and protection** of whistleblowers.

In order to meet these new requirements, the Group's "**ethics, compliance and duty of care**" alert procedure (excluding RTE and Enedis) is being updated, by means of a **Group instruction memo** and this **whistleblower support guide**. The Ethics and Compliance Officer (ECO) is responsible for supplementing the procedure with an **internal implementation memo** approved by the CODIR (Management Committee) and available to all employees.

The alert procedure is **independent** of any other existing alert system in the company (CSE - Social and Economic Committee, occupational physician, Harassment Referent) that you may wish to choose.

Your choice to issue an alert or to refrain from doing so may not be subject to sanctions or any other retaliatory or discriminatory measures based on this ground.

The purpose of this guide is to present **the framework applicable to the collection and investigation of your alert**. It also reiterates the **protection regime associated with the whistleblower status**.

The **Group Ethics & Compliance Division (GECD)** is designated by the Executive Committee as the division **responsible for** the **EDF Group's** alert collection and handling procedure. Your **local contacts** are identified in your **implementation memo**.

You can contact the DECG with any questions regarding this procedure by logging in to the EDF group's alert page .

HOW DO I ISSUE AN ALERT?

CAN YOU ISSUE AN ALERT?

The EDF Group's procedure for collecting and handling alerts is open:

- To **natural persons** acting in **good faith**
  For example: employee, trainee, temporary worker, job applicant, board member, private customer, employee of a service provider, supplier or customer
- To **legal entities** acting in **good faith whose interests** are or may be affected by the facts covered by the alert
  For example: service provider, customer supplier, contract tenderer, trade union, association or NGO whose purpose is to combat the breaches covered by the alert

YOU WISH TO REMAIN ANONYMOUS

You can submit your alert **anonymously**, provided that the **factual information** is sufficiently **detailed and precise** to enable the facts to be investigated.

WHAT FACTS CAN YOU REPORT?

The EDF Group's alert procedure enables you to report facts that constitute:

- A **violation** or an **attempt to conceal a violation** of the **law** or **regulations**, **in relation to the EDF Group's scope of responsibility;**
- A **violation** or an **attempt to conceal** a violation of an **international agreement** ratified or approved by France, a **unilateral act** of an international organisation taken on the basis of such a commitment, **European Union law** or the **Code of Conduct, in relation to the EDF Group's scope of responsibility**;
- A **threat** or **harm to the public interest, in relation to the EDF Group's scope of responsibility**;
- A **risk** or **serious infringement** of **human rights** and **fundamental freedoms**, the **health** and **safety of individuals** or **the environment, in relation to the EDF Group's scope of responsibility and its business relations.**

EXAMPLES OF CATEGORIES COVERED BY THE ALERT PROCEDURE

CORRUPTION
RIGHTS AND PROTECTION OF INDIVIDUALS
BREACHES OF COMPETITION LAW FRAUD
INTERNATIONAL SANCTIONS - INTERNATIONAL TRADE CONTROLS
HEALTH AND SAFETY OF INDIVIDUALS ENVIRONMENT
MONEY LAUNDERING - FINANCING OF TERRORISM
FINANCIAL CRIMES HARASSMENT - DISCRIMINATION
CONFLICTS OF INTEREST HAZARDS
OTHER

To make it **easy** for you to **choose** the appropriate category, these categories are illustrated by **examples** available on the BKMS whistleblowing platform.

HOW DO I ISSUE AN ALERT?

WHO TO CONTACT

WITHIN THE EDF GROUP

Local contacts	Group Ethics and Compliance Division
• **Ethics and Compliance Officer (ECO)** of my entity • **Line management**, **Human Resources** or **any other function authorised** in my entity's implementation memo	the EDF group's alert page @ SG-DECG@edf.fr EDF SA – Direction Ethique et Conformité Groupe Strictement confidentiel Tour Légende 20, Place de la Défense 92050 Paris la Défense Physical meeting no later than 20 working days after receipt of the request

OUTSIDE THE EDF GROUP

Defender of Rights *(Défenseur des Droits)*	External authority	Judicial authority	Public disclosure
To direct me to the appropriate authority	List of authorities here	Complaint or denunciation to a competent judicial authority	Any public communication or controversy by any means (press, social networks, blog) • If no appropriate action has been taken 3 months (can be extended to 6 months) after my external alert • If my external alert entails a risk of reprisals or prevents effective remediation of the situation • In the event of imminent or obvious danger (in the professional environment) / serious and imminent danger (outside the professional environment)

HOW DO I ISSUE AN ALERT?

WHAT PROTECTION IS THERE?

CONDITIONS TO BENEFIT FROM FRENCH WHISTLEBLOWER STATUS

The admissibility of your report does not automatically entitle you to whistleblower legal status or any other specific protection.

WHO?

Natural person alerting in **good faith** and **without direct financial consideration**

WHAT FACTS[2]?

- **Knowledge of the facts** in the context of **professional activity**[1]
- **No knowledge of the facts** in the context of **professional activity** → **Direct witness** to the facts
- **Violation** or **attempt to conceal** a **violation of the law or regulations**, an **international commitment** ratified by France, **EU law** or the **Code of Conduct**
- **Threat** or **harm** to the **public interest**

HOW?

ALERT

INTERNAL CHANNEL

- Via the **reporting platform** or a **local alert**

EXTERNAL CHANNEL → **PUBLIC DISCLOSURE**

- To the **judicial authority** or **external authorities** listed by decree
- ⚠ Triage of alerts in the event of a large influx
- No appropriate action has been taken 3 months (can be extended to 6 months) after my external alert
- My external reporting entails a risk of reprisals or prevents effective remediation of the situation

IMMINENT OR OBVIOUS DANGER

WHAT PROTECTION IS THERE?

- Exemption from **civil and criminal** liability
- **Professional** protection against **reprisals**
- **Provision** for **legal costs** and **matching CPF contributions**
- **External psychological** and **financial support** measures
- **Reversal of the burden of proof** on condition of **good faith**
- Rights to **personal data**

EXTENSION OF WHISTLEBLOWER PROTECTION TO:

- **Persons who have been subjected to, refused to be subjected to or witnessed** acts of **psychological or sexual harassment**.
- **Facilitators**, **natural persons** or **non-profit private sector legal entities, who help** a whistleblower to **make a report or disclosure**.
- **Natural persons with links to a whistleblower** and who are at risk of reprisals in the context of their professional activities
- **Legal entities controlled** by a **whistleblower** or for which a whistleblower **works**.

[1] Professional activity includes any of the following: former or current members of staff, job applicants; associate shareholders and holders of voting rights at General Meetings; members of the administrative, management or supervisory bodies; external or occasional employees, co-contractors and sub-contractors.

[2] With the exception of **national defence confidentiality**, **medical confidentiality**, the **confidentiality of judicial deliberations**, the **confidentiality of investigations** and **judicial enquiries** and the **professional confidentiality of lawyers**.

WHAT ACTION IS TAKEN ON YOUR ALERT?

HOW IS YOUR ALERT COLLECTED?

You will receive written **acknowledgement** of your alert within **7 days** of receipt.

IF YOU USE THE BKMS REPORTING PLATFORM

If the **BKMS whistleblowing platform** is used, authorised GECD members are informed of the registration of an alert on the outsourced platform via a secure message that does not mention any information contained in the alert. Access to your alert and the data provided therefore takes place **exclusively** on the secure platform, after entering three levels of login and password. You need to create a dialog box to be able to communicate securely with the GECD.

HOW IS YOUR ALERT ANALYSED?

Your alert will be examined for admissibility by the GECD or by the local contact entered (see "Who to contact")**,** in order to determine, before the facts are investigated, whether it falls within the scope of the alert procedure and whether the appropriate protection regime can be identified.

You may be contacted again**, by the GECD, if you created a secure dialog box, or by the local contact entered** (see "Who to contact")**,** to obtain any **additional information** required to finalise the analysis of the admissibility of your alert.

Experts (GECD, Legal Division), HR (Human Resources), ECO, Duty of Care Officer, others) may be called in to analyse the admissibility of the alert, after signing a **confidentiality agreement**.

You will be informed in writing of the result of the analysis within a reasonable period of time, which may not exceed **10 working days** from the date of acknowledgement of receipt of your alert, unless an exception is made due to the specific circumstances of the alert.

- **If your alert is not admissible**, you will be informed of the **reasons** why your alert does not fall within the scope of the alert procedure. Your alert may be forwarded to the appropriate contacts with your consent or, failing that, anonymously. The alert is closed and the personal data **immediately deleted**.

- **If your alert is admissible**, you will be **informed** of its admissibility, the **associated protection regime**[3] and the name of the person appointed to carry out the investigation. This person has the independence, skills and resources required to carry out this mission. The recipient of the alert and the person in charge of the investigation may be the same person, particularly when you refer the matter to the GECD or your ECO.

[3] The protection regime notified when an alert is deemed admissible constitutes an a priori commitment by the company to determine the level of protection to be observed during the investigations. It is subject to change until the investigation is closed. Only the judicial authority is competent to qualify and grant whistleblower status or any other protection linked to the exercise of the right to alert.

WHAT ACTION IS TAKEN ON YOUR ALERT?

ASK THE DEFENDER OF RIGHTS ABOUT YOUR SITUATION

You can also refer the matter to the Defender of Rights for an opinion on your status as a whistleblower within a maximum of 6 months from the date of referral.

HOW IS YOUR ALERT INVESTIGATED?

The **person in charge of the investigation** has access to your alert after signing a **confidentiality agreement**, if he or she is not also the recipient of the alert.

The investigation of the **facts** reported (verification of the facts, interviews with the people concerned, search for evidence, etc.) may be carried out with the support of **business line experts**, entity or subsidiary ECOs, **support divisions** (GECD, HR, Security and Economic Intelligence Division, Legal Department, IT and Telecom Services Division and Audit Division) or, where necessary, **external consultants**. These experts are subject to the **same strict confidentiality obligations** (with the prior signature of a confidentiality agreement).

The **information collected** during the investigation phase is **stored securely** on the platform or on any other secure medium set up by your entity. **Storage on professional or personal computers and telephones is not authorised.**

The person in charge of the investigation has a **maximum of three months from the date of acknowledgement of receipt** or, in the absence of acknowledgement of receipt, from the expiry of the **seven-day period** following the alert, to **provide you with information on the measures planned or taken** to remedy the alert and the **reasons** for these measures.

- **If the facts are not established**, the person in charge of the investigation **will close** the file after informing you of the action taken in response to the alert within the aforementioned period of three months.

- **If the facts reported are established or partially established**, the person in charge of the investigation will draw up a **recommendation for action to be taken in order to put an end to the breach or disturbance that gave rise to your alert** and to prevent its recurrence. The recommendation is sent to the appropriate management level for decision and implementation. Any **corrective action** deemed necessary, as well as any **disciplinary** or **legal proceedings,** are **decided upon and initiated under the responsibility of the management of the respondent,**[4] in conjunction with the Human Resources Division and/or the Legal Division, depending on the nature and seriousness of the facts.

[4] Provided that the scope of the actions to be implemented falls within the scope of the management authority of the respondent.

WHAT ACTION IS TAKEN ON YOUR ALERT?

IF ANONYMITY PREVENTS THE ALERT FROM BEING INVESTIGATED

Anonymity may prevent the investigation from proceeding smoothly or the facts reported from being verified. You may be offered the opportunity to lift your anonymity, on the understanding that the confidentiality of your personal data will be protected in the same way as any other whistleblower. In the event of refusal, the investigation may be suspended until anonymity is lifted at a later date, or closed in the event of persistent refusal, while the investigative difficulties remain. The seriousness of the facts may lead the officer to report them to the judicial authorities.

HOW IS YOUR ALERT DATA PROCESSED?

WHAT GUARANTEES EXIST FOR THE CONFIDENTIALITY OF YOUR ALERT?

In compliance with European legislation on the protection of personal data[1] and the deliberation of the CNIL (French National Commission for Information Technology and Civil Liberties)[2] on the use of personal data in the context of an alert system, **the data recorded in the context of the EDF alert procedure is limited to the following information**:

- **Your identity**: your name and other personal data[3] that you decide to communicate in your alert;
- **Your situation**: employee, external or occasional employee, third party;
- **The personal data** of the **people you mention in your alert** (witnesses, victims, people targeted by the alert, etc.);
- **The category that you feel best corresponds to your alert**;
- **The facts**: date, place, description of the facts, attachments and information collected by the person in charge of the investigation in the context of the investigation**;**
- **Reports on processing operations**;
- **Confidentiality agreements** signed by the person in charge of the investigation assigned to the alert and any experts, limited to those designated.

EDF has taken the appropriate measures to **guarantee the strict confidentiality** of **your personal data**, **that of any person mentioned in the alert** and **the information collected** by all the recipients of the alert:

- The "Sapin 2" law[4] prohibits the disclosure **of information that could identify you** except for:
  - In the event that EDF is required to **report the facts to the judicial authorities**. You will then receive a **reasoned notification** of this communication, **unless** this information risks **compromising legal proceedings**;
  - In the event that it is necessary to **communicate your personal data for the purposes of the investigation**. Your consent will be **requested beforehand** and you will be informed of the name of the recipient;

- Out of respect for the presumption of innocence, **information enabling the identification of the respondents concerned by your alert may not be disclosed**, except to the judicial authority and if the proven nature of your alert is confirmed by investigations;

[1] European Regulation 2016/679 of 27 April 2016 "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data".
[2] Deliberation no. 2017-191 of 22 June 2017 amending Deliberation no. 2005-305 of 8 December 2005 granting a single authorisation for the automated processing of personal data implemented in the context of professional alert systems (AU-004).
[3] Personal data is any information that enables a person to be identified, such as telephone numbers, job titles, social security numbers, etc.
[4] Law no. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life (amended by Law no. 2022-401 of 21 March 2022 aimed at improving the protection of whistleblowers).

HOW IS YOUR ALERT DATA PROCESSED?

- **A confidentiality agreement** is signed by the person in charge of the investigation, and then by any person required to take part in the investigation (experts and support staff) before they can access the alert data.

SECURITY OF THE BKMS REPORTING PLATFORM

- No retention of metadata and no traceability of IP addresses.
- The person in charge of the investigation and any experts **only have access to those alerts for which they are authorised**.
- A **different personal access code** for each user.
- All the data collected and all investigation reports are saved in **the secure alert platform**.
- **Only the GECD has the encryption keys for the secure system**. The GECD authorises those in charge of investigations on a case-by-case basis.
- Exchanges between a whistleblower and the person in charge of the investigation take place within the **secure, encrypted system**.
- To ensure the traceability of the persons accessing the data and operations carried out, each file has a **process log** which traces all the actions carried out by each authorised person.

WHAT RIGHTS AND PROTECTION DO YOU HAVE OVER YOUR PERSONAL DATA?

In compliance with the requirements of the GDPR and the French Data Protection Act, EDF has set up an "ethics, compliance and duty of care" alert procedure involving automated processing of your personal data. All employees and external or occasional staff are informed of the procedure, as are staff representative bodies.

As the author of the alert, like any other respondent or person cited in an alert, you have the **right to information on, access to, rectification of**[5], **deletion of and opposition** to the use of your personal data.

If you invoke your **right to deletion**, the GECD will promptly examine the extent to which the use of your personal data is still necessary to carry out investigations. Data that is no longer required will be deleted.

[5] If it is inaccurate, incomplete, ambiguous or out of date.

HOW IS YOUR ALERT DATA PROCESSED?

If you invoke your **right to oppose**, the GECD will promptly examine whether there are compelling legitimate grounds for carrying out the investigations which override your interests, rights and freedoms, or for establishing, exercising or defending legal claims. You also have the right to lodge a complaint with a supervisory authority.

The request must be made:

- Either to the **Group Ethics and Compliance Division**
  - By logging on to the **BKMS platform** and clicking on the "Submit an alert or request advice/exercise your rights" button
  - By **registered letter** to the following address:

EDF SA – Direction Ethique et Conformité Groupe
Strictement confidentiel
Tour EDF
20, Place de la Défense
92050 Paris la Défense

- Or to the **Data Protection Officer (DPO)** appointed by **EDF SA**
  - **Electronically** to the following address: informatique-et-libertes@edf.fr
  - By **post** to the following address:

Délégué à la Protection des Données (DPO)
EDF – Direction des Systèmes d'Information du Groupe
Mission Informatique et Libertés
Tour PB6, 20 place de la Défense
92050 Paris La Défense CEDEX

- Or to the **Data Protection Officer (DPO)** appointed by your **subsidiary**

You have the right to lodge a complaint with a supervisory authority (including the CNIL).

Under no circumstances may a respondent obtain information concerning the identity of the whistleblower on the basis of his or her rights to personal data.

HOW IS YOUR DATA STORED AND ARCHIVED?

When your alert is declared **inadmissible**, your **personal data** is **destroyed immediately.**

If your alert is declared **admissible** but no **further action** is taken, your personal data will be **destroyed** or **rendered anonymous** once the alert has been **closed**.

When a **disciplinary procedure** or **legal proceedings** are initiated following an alert, the personal data and other elements collected are **kept** until the **end of the proceedings**.

With the exception of cases where no action is taken on your alert, the data relating to your alert may be kept in the form of **intermediate archives**[6] for the purposes of protecting the whistleblower[7] or enabling the establishment of ongoing offences. This retention may not exceed 10 years for crimes, 6 years for misdemeanours and 1 year for other breaches of the law.

Other non-personal data is archived for statistical or reporting purposes**,** for a period not exceeding the statute of limitations for legal proceedings.

HOW EDF GROUP PROTECTS YOU?

The EDF Group ensures optimum protection for whistleblowers (whether or not they are granted whistleblower status by law):

- Confidentiality of the whistleblower's personal data and of the content of the alert (signed confidentiality undertakings, use of secure means of communication and storage, mandatory training of investigators, possibility of making an anonymous alert);

- Protection against possible reprisals by archiving files so as to be able to effectively investigate any reports of reprisals (discrimination or sanction for having issued an alert).

These measures are designed to create a safe and transparent working environment. Please feel free to report any concerns in complete confidence.

[6] Your data is stored with the same level of security as during investigations, but access to it is limited to members of the GECD alert committee (by decision of the Group Director of Ethics and Compliance). Any access to your personal data must be justified in writing.

[7] Members of the GECD who are authorised to do so in a limited manner by their implementation memo may access archived data in order to:

- Check that there have been no retaliatory measures and that the investigation complies with Group procedure;
- Check whether a new alert refers to a previous alert;
- Use the data in the context of an administrative or legal dispute.